

LAPORAN PENELITIAN

Kluster Research Leader



TERAPAN ALJABAR SEMIPRIMA MENDASAR PADA PENGAMANAN AUTENTIKASI IDENTITAS DIGITAL

Disusun oleh :

Ketua Tim : Dr. Khurul Wardati, M.Si.
(UIN Sunan Kalijaga Yogyakarta)

Anggota :

1. Muhamad Zaki Riyanto, M.Sc.
(UIN Sunan Kalijaga Yogyakarta)

2. Tiara Arifah (NIM 18106010044)
(Mahasiswa Matematika UIN Sunan Kalijaga Yogyakarta)

**DIREKTORAT PENDIDIKAN TINGGI KEAGAMAAN ISLAM
DIREKTORAT JENDERAL PENDIDIKAN ISLAM
KEMENTERIAN AGAMA RI
TAHUN 2021**

يَا أَيُّهَا الَّذِينَ ءَامَنُوا إِن جَاءَكُمْ فَاسِقٌ بِنَبَأٍ فَتَبَيَّنُوا أَن تُصِيبُوا قَوْمًا
بِجَهْلَةٍ فَتُصْبِحُوا عَلَىٰ مَا فَعَلْتُمْ نَادِمِينَ ﴿٦﴾

“Hai orang-orang yang beriman, jika datang kepadamu orang fasik membawa suatu berita, maka periksalah dengan teliti agar kamu tidak menimpakan suatu musibah kepada suatu kaum tanpa mengetahui keadaannya yang menyebabkan kamu menyesal atas perbuatanmu itu.”

(Q.S. Al Hujurat : 6)

Kata Pengantar

Kami tim peneliti bersyukur dengan berucap *Alhamdulillahirabbil 'alamin*, atas terselesaikannya penelitian dan laporannya yang berjudul “**TERAPAN ALJABAR SEMIPRIMA MENDASAR PADA PENGAMANAN AUTENTIKASI IDENTITAS DIGITAL**”. Laporan ini merupakan gambaran menyeluruh mengenai pelaksanaan penelitian beserta hasilnya serta produk penelitian berupa artikel ilmiah.

Hasil penelitian ini semoga dapat bermanfaat baik secara teoritis maupun secara praktis. Secara teoritis, hasil penelitian ini dapat bermanfaat bagi dosen maupun mahasiswa yang menggeluti aljabar abstrak (struktur aljabar) maupun terapan aljabar, khususnya bidang kriptografi. Secara praktis, hasil penelitian ini dapat pula sebagai wacana pengambil kebijakan di bidang sistem informasi.

Penelitian ini merupakan kluster *Research Leader* Nasional LPPM UIN Sunan Kalijaga Yogyakarta tahun 2021. Secara khusus, peneliti mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Rektor dan jajarannya yang telah menetapkan tim peneliti sebagai salah satu penerima dana penelitian tersebut.
2. Pimpinan Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) dan jajarannya yang melayani segala sesuatu kebutuhan pelaksanaan penelitian.
3. Pimpinan Fakultas Sains dan Teknologi dan Kaprodi Matematika.
4. Semua pihak yang telah memberikan bantuan berupa data, masukan, pemikiran, dan tenaga selama penyusunan laporan ini.

Tim Peneliti menyadari bahwa laporan ini masih jauh dari sempurna. Tim Peneliti mengharapkan masukan, saran dan kritik konstruktif demi perbaikan dan penyempurnaan laporan ini.

Wassalamu 'alaikum Warahmatullahi Wabarakatuh

Yogyakarta, 29 Desember 2021
Ketua Tim Peneliti

Dr. Khurul Wardati, M.Si.

DAFTAR GAMBAR

Gambar 1 :	Sistem Kriptografi Simetris	13
Gambar 2 :	Prokotoi pertukaran kunci Diffie-Hellman	15
Gambar 3 :	Protokol autentikasi Diffie-Hellman	15
Gambar 4 :	Skema Protokol Pertukaran Kunci Sphilrain-Ushakov	17
Gambar 5 :	Skema Protokol Pertukaran Kunci Stickel	18
Gambar 6 :	Protokol Autentikasi Lal dan Chaturvedi	20
Gambar 7 :	Protokol Autetentikasi Berdasarkan Masalah Dekomposisi atas Ideal Dasar Semiprima	36
Gambar 8 :	Protokol Autentikasi Identitas Digital atas Ideal Dasar Semiprima untuk Sistem Informasi Akademik	39

DAFTAR ISI

Halaman Judul	i
Halaman Motto	ii
Kata Pengantar	iii
DAFTAR GAMBAR	iv
DAFTAR ISI	v
I. PENDAHULUAN	1
A. LATAR BELAKANG	1
B. RUMUSAN MASALAH	4
C. TUJUAN PENELITIAN	5
D. MANFAAT PENELITIAN	5
II. TINJAUAN PUSTAKA DAN LANDASAN TEORI	7
A. TINJAUAN PUSTAKA	7
B. DASAR TEORI	8
B.1 Aljabar Bebas atas Ring Komutatif Unital	8
B.2 Kriptografi, Protokol Autentikasi dan Masalah Dekomposisi	12
III. METODE DAN TARGET PENELITIAN	21
A. METODE PENELITIAN	21
B. RENCANA PUBLIKASI	22
C. JADWAL PELAKSANAAN PENELITIAN	23
D. PERSONALIA	23
IV. HASIL PENELITIAN DAN PEMBAHASAN	25
A. Sifat-sifat ideal dasar semiprima dalam Aljabar dibangun secara berhingga atas ring komutatif unital	25
B. Aljabar semiprima mendasar dibangun secara berhingga atas ring komutatif unital	28
C. Terapan ideal dasar semiprima dan aljabar semiprima mendasar pada pengamanan autentikasi identitas digital	34
V. PENUTUP	40
A. KESIMPULAN	40
B. SARAN	42
DAFTAR PUSTAKA	43

BIOGRAFI SINGKAT PENELITI	45
RANCANGAN ANGGARAN BELANJA	48
RASIONALISASI PENGGUNAAN ANGGARAN	50
Lampiran-Lampiran	54
Lampiran 1. : SK Penelitian	
Lampiran 2. : Pengumuman Hasil Seleksi Proposal BOPTN 2020	
Lampiran 3 : PPT Seminar Proposal	
Lampiran 4 : Draft naskah hasil alih Bahasa <i>extended abstract</i> dan <i>full paper</i>	
Lampiran 5 : CV Narasumber	
Lampiran 6 : PPT FGD Desiminasi	
Lampiran 7 : Dokumentasi Kegiatan Penelitian	
Lampiran 8 : Surat Pertanggungjawaban (SPJ) Kegiatan Penelitian	

BAB I

PENDAHULUAN

A. LATAR BELAKANG

Salah satu tokoh saintis muslim pada era kejayaan Islam adalah Al-Khawarizmi. Tokoh ini berpengetahuan luas bukan hanya dalam bidang syariat dan sejarah Islam, tetapi juga di dalam bidang falsafah, logika, aritmatika, geometri, musik, ilmu hitung dan kimia. Al-Khawarizmi dikenal sebagai bapak aljabar, karena beliau adalah yang pertama kali mengenalkan aljabar pada era kejayaan Islam.

Penelitian aljabar secara teori sangat lazim berkaitan dengan proses generalisasi (perumuman). Aljabar lintasan dan aljabar lintasan Leavitt baik atas lapangan maupun atas ring komutatif dengan elemen satuan, merupakan aljabar bebas yang pasti memiliki basis (Tomforde, 2011). Ideal sebarang dari aljabar bebas atas lapangan selalu memiliki basis, tetapi tidak untuk ideal dalam aljabar bebas atas ring komutatif dengan elemen satuan. Wardati (2015) telah memperumum definisi ideal dasar dalam aljabar bebas dari aljabar lintasan Leavitt atas ring komutatif dengan elemen satuan oleh Tomforde (2011). Perumuman ideal dasar ini, dapat digunakan dalam menentukan ideal dasar dalam aljabar lintasan atas ring komutatif dengan elemen satuan.

Temuan lain dari Wardati, dkk. (2015) adalah didefinisikannya ideal bebas dalam aljabar bebas, di mana ideal dasar ekuivalen dengan ideal bebas. Beberapa sifat ideal dasar dibuktikan dengan ideal bebas. Salah satunya, sifat-sifat dari ideal dasar prima dari aljabar bebas. Perumuman ideal dasar dan ideal bebas pada aljabar bebas atas ring komutatif dengan elemen satuan terus dilakukan pada aljabar yang dibangun secara berhingga (belum tentu aljabar bebas). Wardati (2018) telah memperumum definisi ideal dasar dan ideal bebas dalam aljabar yang dibangun secara berhingga di mana keduanya tidak selalu ekuivalen. Ideal bebas pasti merupakan ideal dasar tetapi tidak sebaliknya. Namun, sifat-sifat dalam ideal

dasar prima dalam aljabar tak bebas yang dibangun secara berhingga masih tetap berlaku dengan pembuktian tanpa menggunakan ideal bebas.

Keprimaan aljabar (ring) ditentukan oleh keprimaan ideal nolnya. Secara analog, aljabar bebas dikatakan aljabar prima mendasar jika ideal dasar nol merupakan ideal dasar prima. Demikian pula keprimaan mendasar aljabar tak bebas, juga didasarkan pada keprimaan ideal dasar nolnya, yang telah dikaji oleh Wardati, dkk., dalam penelitian klaster riset lider (*research leader*) UIN Sunan Kalijaga Yogyakarta, 2018. Hasil penelitian ini telah dipublikasikan Wardati (2021) yaitu teorema tentang syarat perlu dan cukup dari ideal dasar prima dalam aljabar tak bebas atas ring komutatif. Teorema tersebut berakibat, ditemukannya syarat perlu dan cukup aljabar tak bebas bersifat prima mendasar (*basically prime*).

Sebarang ideal prima merupakan ideal semiprima. Demikian pula, sebarang ideal dasar prima merupakan ideal dasar semiprima tetapi tidak sebaliknya. Artinya, ideal dasar semiprima lebih general daripada ideal dasar prima. Generalisasi ideal dasar semiprima dari ideal dasar prima akan menurunkan syarat perlu dan cukup ideal dasar semiprima dalam aljabar. Hal ini berkonsekuensi didapatkannya syarat perlu dan cukup aljabar tak bebas bersifat semiprima mendasar (*basically semiprime*).

Telah dibuktikan dengan contoh kontra bahwa ideal dasar prima dan ideal prima tidak saling berkaitan (Wardati, 2018). Akibatnya, ideal dasar semiprima dan ideal semi-prima tidak saling berhubungan pula, kecuali ideal nol. Jika ideal nol bersifat semiprima maka pastilah merupakan ideal dasar semiprima. Hal ini, dapat dilihat dari definisi ideal (dasar) semiprima. Perlu dicari contoh kontra suatu ideal nol yang merupakan ideal dasar semiprima akan tetapi tidak semiprima. Jika dapat ditemukan contoh kontranya maka aljabar semiprima mendasar lebih general daripada aljabar semiprima.

Menurut Molina (2008), kesemiprimaan aljabar didefinisikan sebagai aljabar yang *nondegenerate*. Aljabar A bersifat *nondegenerate* jika dan hanya jika $aAa = \{0\}$ berakibat $a = 0$. Kemungkinan besar bahwa sifat *nondegenerate* bukanlah syarat perlu dan cukup kesemiprimaan mendasar suatu aljabar.

Wisbauer (1991) menyatakan bahwa aljabar (ring) A dengan elemen satuan bersifat semiprima jika dan hanya jika irisan semua ideal prima merupakan ideal nol, jika dan hanya jika ideal nol merupakan satu-satunya ideal nilpoten di A . Muncullah konjektur atau hipotesis pertama bahwa irisan ideal-ideal dasar prima yang sama dengan ideal nol merupakan syarat perlu dan cukup suatu aljabar (tak bebas) bersifat semiprima mendasar. Pembuktian bahwa irisan semua ideal prima merupakan syarat perlu aljabar bersifat semiprima, membutuhkan definisi *annihilator* dari aljabar. Annihilator merupakan ideal (Wisbauer, 1991), maka perlu dikaji syarat-syarat agar annihilator merupakan ideal dasar.

Jika ideal nol merupakan satu-satunya ideal nilpoten maka sebarang ideal tak nol bukanlah ideal nilpoten. Ideal nol pasti merupakan ideal dasar dari sebarang aljabar, maka kita punya konjektur kedua bahwa suatu aljabar semiprima mendasar jika dan hanya jika sebarang ideal dasar tak nol bukan merupakan ideal nilpoten.

Aljabar memiliki aplikasi dan manfaat yang sangat berguna di bidang keamanan jaringan komputer, yaitu pada kriptografi. Kriptografi merupakan ilmu yang berkaitan dengan keamanan data yang dikirimkan menggunakan jalur yang tidak terjamin keamanannya seperti internet. Kriptografi tidak hanya menyelesaikan masalah kerahasiaan, tetapi juga pada keutuhan data, autentikasi, tanda tangan, sertifikat data, dan aspek-aspek keamanan informasi yang lainnya (Stinson D.R. dan Paterson M.B., 2019).

Salah satu masalah yang sering dialami pada saat pengiriman data melalui internet adalah terjadinya pemalsuan atau penipuan identitas. Beberapa contoh kasusnya adalah pemalsuan surat digital dan pengiriman pesan menggunakan identitas palsu. Guna mengatasi masalah tersebut, dalam kriptografi dikenal sebuah skema autentikasi. Saat ini, skema autentikasi yang diterapkan luas di internet adalah skema autentikasi Diffie-Hellman. Tingkat keamanan dari skema autentikasi tersebut diletakkan pada kesulitan menyelesaikan masalah logaritma diskrit atas grup komutatif. Masalah logaritma diskrit ini juga menjadi landasan bagi skema pertukaran kunci dan skema kriptografi asimetris.

Berkembangnya komputer kuantum dewasa ini menjadi ancaman sangat nyata pada kriptografi. Peter W. Shor (1997) menyatakan bahwa komputer kuantum dalam skala besar di masa depan mampu menyelesaikan masalah logaritma diskrit secara cepat dan mudah. Oleh karena itu, para ahli kriptografi di seluruh dunia berusaha mengembangkan pengganti dari skema-skema dalam kriptografi, termasuk mengganti skema autentikasi Diffie-Hellman ini. Salah satu hal penting yang menjadi titik lemah skema autentikasi Diffie-Hellman terhadap serangan komputer kuantum adalah penggunaan struktur aljabar komutatif.

Penelitian ini berfokus pada penerapan struktur aljabar non-komutatif sebagai salah satu cara untuk menyangkal serangan komputer kuantum. Masalah matematis pada struktur aljabar non-komutatif yang dapat diterapkan dalam kriptografi adalah masalah konjugasi dan masalah dekomposisi. Masalah konjugasi ditemukan pada grup non-komutatif, sedangkan masalah dekomposisi ditemukan pada struktur aljabar non-komutatif, tidak terbatas pada grup saja (Myasnikov dkk, 2008).

Aljabar semiprima mendasar merupakan salah satu struktur aljabar non-komutatif. Oleh karena itu, pada penelitian ini dikembangkan suatu protokol autentikasi identitas digital yakni pengembangan dari protokol perjanjian kunci yang didasarkan pada masalah dekomposisi atas aljabar semiprima mendasar.

B. RUMUSAN MASALAH PENELITIAN

Jika diidentifikasi dari latar belakang masalah di atas, maka terdapat empat (4) permasalahan dalam penelitian ini. Tiga diantaranya berkaitan dengan teori aljabar dan satu masalah terapan teori aljabar. Keempat masalah dalam penelitian ini dapat dirumuskan sebagai berikut:

- a. Mencari syarat perlu dan cukup ideal dasar semiprima dalam aljabar (tak bebas)
- b. Menelusuri sifat-sifat suatu annihilator yang merupakan ideal dasar dalam aljabar untuk membuktikan bahwa suatu aljabar (tak bebas) semiprima mendasar jika dan hanya jika irisan semua ideal dasar adalah ideal nol

- c. Menganalisis bahwa sebarang ideal dasar tak nol yang bukan ideal nilpoten dalam aljabar (tak bebas) adalah syarat perlu dan cukup aljabar tersebut bersifat semiprima mendasar.
- d. Mengkonstruksi sebuah skema protokol autentikasi identitas digital berdasarkan masalah dekomposisi atas suatu aljabar semiprima mendasar yang dibangun secara berhingga.

C. TUJUAN PENELITIAN

Sebagaimana lazimnya, penelitian ini bertujuan untuk menjawab rumusan masalah yang telah ditetapkan. Tujuan penelitian ini adalah :

1. Menemukan syarat perlu dan cukup ideal dasar semiprima dalam aljabar tak bebas.
2. Menemukan syarat-syarat annihilator merupakan ideal dasar yang digunakan untuk membuktikan bahwa suatu aljabar (tak bebas) semiprima mendasar jika dan hanya jika irisan semua ideal dasar adalah ideal nol.
3. Menganalisis bahwa sebarang ideal dasar tak nol yang bukan ideal nilpoten dalam aljabar (tak bebas) adalah syarat perlu dan cukup aljabar tersebut bersifat semiprima mendasar.
4. Menentukan konstruksi sebuah skema protokol autentikasi identitas digital berdasarkan masalah dekomposisi atas suatu aljabar semiprima mendasar yang dibangun secara berhingga.

D. KONTRIBUSI PENELITIAN

Diharapkan penelitian ini berkontribusi baik secara praktis maupun teori. Secara teori, hasil penelitian ini sangat bermanfaat bagi aljabaris khususnya struktur aljabar dan terapan aljabar dalam bidang kriptografi. Aljabar dalam penelitian ini adalah aljabar dibangun secara berhingga atas ring komutatif unital yang semiprima mendasar.

Secara praktis, hasil penelitian ini dapat pula sebagai wacana pengambil kebijakan di bidang sistem informasi akademik baik di UIN Sunan Kalijaga

Yogyakarta maupun di lingkungan Perguruan Tinggi Keagamaan Islam Negeri (PTKIN). Setiap pengguna (*user*) yang akan masuk (*login*) sistem informasi akademik harus benar-benar merupakan orang yang bersangkutan. Salah satu teknik autentikasi yang umum digunakan saat ini adalah menggunakan kata sandi (*password*) sebagai tantangan (*challenge*) kepada pengguna. Penggunaan protokol autentikasi dianggap lebih aman daripada kata sandi, hal ini dikarenakan pada saat proses autentikasi digunakan parameter publik dan rahasia, serta tantangan dari sistem informasi akademik yang harus direspon oleh pengguna agar dapat masuk ke dalam sistem informasi akademik secara sah.

BAB II

TINJAUAN PUSTAKA DAN LANDASAN TEORI

A. TINJAUAN PUSTAKA

Istilah ideal dasar pertama kali didefinisikan oleh Tomforde (2011) pada aljabar lintasan Leavitt atas ring komutatif dengan elemen satuan,. Ideal dasar ini digunakan untuk mengkarakterisasi sifat sederhana mendasar (*basically simple*) aljabar lintasan Leavitt ini. Karena aljabar lintasan Leavitt merupakan aljabar bebas, Wardati, dkk. (2015) memperumum definisi ideal dasar pada aljabar bebas atas ring komutatif dengan elemen satuan. Berdasarkan ideal dasar ini, dapat dikarakterisasi ideal dasar (semi)prima. Selain itu, Wardati, dkk. (2015) menemukan definisi ideal bebas dalam aljabar bebas, yakni ideal yang memiliki basis subset dari suatu basis aljabarnya. Sifat utamanya, bahwa ideal bebas tersebut ekuivalen dengan ideal dasar. Ideal bebas sangat berperan dalam pembuktian sifat-sifat ideal dasar.

Aljabar bebas dengan basis berhingga dapat diperumum menjadi aljabar yang dibangun secara berhingga (pembangun tidak harus bebas linear). Perumuman aljabar tersebut pastilah bukan ideal bebas dari dirinya sendiri. Sifat ini menunjukkan bahwa ideal bebas belum tentu ideal dasar. Wardati (2018) mengkaji sifat-sifat ideal dasar prima dalam aljabar tak bebas, sehingga diperoleh sifat-sifat ideal dasar prima. Tidak ada perbedaan syarat perlu dan cukup ideal dasar prima dalam aljabar tak bebas, namun berbeda dalam pembuktiannya yang tidak memerlukan ideal bebas.

Penelusuran syarat perlu dan cukup ideal dasar semiprima dalam aljabar tak bebas dapat dianalogkan dengan Wardati (2018). Namun, kesemiprimaan mendasar aljabar tak bebas perlu sintesa dari Wisbauer (1991) dan Bland (2011) yang berkaitan dengan sifat-sifat annihilator dan ideal idempoten, dan Molina (2008) berhubungan dengan sifat *nondegenerate*.

Referensi utama tentang teori dasar aljabar merujuk pada Bland (2011), Grillet (2007), Dummit, dkk. (2004), dan Adkins (1999). Sementara sifat-sifat ideal mengacu pada bukunya Wisbauer (1991) dan Bland (2011).

Protokol autentikasi untuk identitas secara digital yang pertama merupakan hasil pengembangan dari penelitian Diffie dan Hellman (1976) tentang protokol pertukaran kunci. Protokol autentikasi Diffie-Hellman hingga saat masih digunakan pada jaringan komputer dan internet. Adanya kemungkinan serangan pada kriptografi menggunakan komputer kuantum di masa depan dikemukakan oleh Shor (1997). Penelitian Shor tersebut membuat para peneliti dalam bidang kriptografi berusaha untuk mencari algoritma-algoritma kriptografi yang aman dari serangan komputer kuantum, salah satunya adalah protokol autentikasi identitas digital.

Penelitian Sphlrain dan Ushakov (2005) telah mengkaji konstruksi protokol pertukaran kunci menggunakan masalah dekomposisi atas grup non-komutatif. Konstruksi tersebut kemudian dikembangkan oleh Stickel (2005) dengan menambahkan bilangan asli acak serta menggunakan konsep *center* dari grup non-komutatif. Lal dan Chaturvedi (2005) kemudian mengembangkan sebuah protokol autentikasi identitas digital berdasarkan masalah dekomposisi atas grup non-komutatif. Dalam penelitian ini, protokol autentikasi yang telah dikonstruksi oleh Lal dan Chaturvedi (2005) dikembangkan sehingga dapat diterapkan pada ideal dasar semiprima, tingkat kemanannya tetap diletakkan pada masalah dekomposisi.

B. DASAR TEORI

B.1. Aljabar Bebas atas Ring Komutatif Unital

Aljabar atas ring komutatif dengan elemen satuan yang dibangun secara berhingga merupakan perumuman dari aljabar bebas dengan basis berhingga. Fokus utama penelitian ini adalah mengkaji sifat-sifat aljabar semiprima mendasaryang dibangun secara berhingga . Sebelum didefinisikan aljabar, perlu terlebih dahulu diingatkan kembali definisi ring, ring komutatif dan aljabar atas ring komutatif dengan elemen satuan.

Definisi 2.1 (Bland, 2011) *Diberikan suatu himpunan tidak kosong R bersama dengan dua operasi “+” dan “.” pada R . Himpunan R disebut **ring** terhadap operasi “+” dan “.” jika memenuhi tiga kondisi di bawah ini:*

(1) Himpunan R merupakan grup komutatif terhadap operasi “+”. Elemen netral dari R terhadap operasi penjumlahan dinotasikan dengan 0_R .

(2) Untuk setiap $a, b \in R$ berlaku $a \cdot b \in R$

(3) Untuk setiap $a, b, c \in R$ berlaku $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(4) Pada R berlaku sifat distributif kiri dan kanan, yaitu untuk setiap $a, b, c \in R$ berlaku $a \cdot (b + c) = a \cdot b + a \cdot c$ dan $(a + b) \cdot c = a \cdot c + b \cdot c$.

Ring R disebut **ring komutatif** jika operasi perkalian pada R bersifat komutatif, yaitu untuk setiap $a, b \in R$ berlaku $a \cdot b = b \cdot a$. Ring R disebut **ring dengan elemen satuan** jika terdapat $1_R \in R$ sedemikian hingga untuk setiap $a \in R$ berlakua $\cdot 1_R = 1_R \cdot a = a$.

Pengertian ring sangat berperan dalam pendefinisian aljabar atas ring. Aljabar A atas suatu ring R dengan elemen satuan dinotasikan R -aljabar didefinisikan sebagai berikut.

Definisi 2.2 (Grilet, 2007) Himpunan tak kosong A disebut R -aljabar jika A merupakan ring dan terdapat operasi dari $R \times A$ ke A sedemikian sehingga untuk setiap $r, s \in R, a, b \in A$ memenuhi:

- i. $r(a + b) = ra + rb$
- ii. $(r + s)a = ra + sa$
- iii. $(rs)a = r(sa)$
- iv. $r(ab) = (ra)b = a(rb)$
- v. $1_R a = a$ dengan 1_R elemen satuan di R

Aljabar A dikatakan R -aljabar unital jika A memiliki elemen satuan 1_A .

Tampak jelas dari Definisi 2.2, bahwa R -aljabar A adalah ring yang sekaligus merupakan R -modul (kiri). Akibatnya, pengertian subaljabar dan ideal dari R -aljabar A berkaitan dengan R -submodul.

Definisi 2.3 (Grilet, 2007) Diberikan sub-sub himpunan bagian tak kosong S, I dari R -aljabar A . Jika S, I masing-masing R -submodul dari R -modul A maka S, I secara berurutan merupakan R -subaljabar dan ideal dari R -aljabar A jika S

subring dan I ideal dari ring A . Perkalian dua buah ideal $I, J \subset A$ didefinisikan sebagai himpunan semua jumlahan berhingga perkalian elemen di I dengan elemen di J , dinotasikan dengan :

$$IJ = \left\{ \sum_{i=1}^m a_i b_i \mid a_i \in I, b_i \in J, m < \infty \right\}$$

Himpunan bilangan rasional $\mathbb{Q}$ merupakan lapangan, sehingga $\mathbb{Q}$ dapat dipandang sebagai ruang vektor atas dirinya sendiri, maka aljabar $\mathbb{Q}$ memiliki basis. Selain itu, $\mathbb{Q}$ juga dapat dipandang sebagai $\mathbb{Z}$ -modul dan sekaligus $\mathbb{Z}$ -aljabar, namun $\mathbb{Z}$ -aljabar $\mathbb{Q}$ tidak mempunyai basis. Hal inilah yang memotivasi didefinisikannya aljabar bebas atas suatu ring.

Definisi 2.4 (Grillet, 2007) Diberikan R -aljabar unital A . Jika X membangun A , dinotasikan $A = \langle X \rangle$, dan X bebas linear maka X merupakan basis dari A . Himpunan A disebut R -aljabar bebas jika R -aljabar A mempunyai basis.

Jika A merupakan R -aljabar bebas maka A merupakan R -modul bebas, dengan basis-nya tidak tunggal. Berdasarkan Grillet (2007), sebarang dua basis dari R -modul bebas mempunyai kardinalitas yang sama, jika ring R komutatif. Telah diketahui bersama bahwa sebarang aljabar V atas lapangan K merupakan ruang vektor sehingga V pasti K -aljabar bebas. Misalkan S basis dari V maka setiap ideal $J \subseteq V$ selalu berlaku :

$$\text{Untuk setiap elemen tak nol } k \in K, v \in S, \text{ jika } kv \in J \text{ maka } v \in J \quad (1)$$

Hal ini dikarenakan elemen tak nol dalam lapangan K selalu memiliki invers. Selain itu, sebarang ideal dari aljabar atas lapangan senantiasa memiliki basis. Namun, sifat-sifat tersebut tidak selalu berlaku pada ideal dalam aljabar bebas atas ring komutatif dengan elemen satuan.

Contoh 2.5. Diberikan $\mathbb{Z}_{256}$ -aljabar bebas $A = \begin{pmatrix} \mathbb{Z}_{256} & \mathbb{Z}_{256} \\ \mathbb{Z}_{256} & \mathbb{Z}_{256} \end{pmatrix}$ dan suatu ideal L di A ,

$$L = \begin{pmatrix} 16\mathbb{Z}_{256} & 16\mathbb{Z}_{256} \\ 16\mathbb{Z}_{256} & 16\mathbb{Z}_{256} \end{pmatrix} \text{ maka terdapat } 16 \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \in L \text{ tetapi } \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \notin L.$$

Definisi 2.6 (Wardati, dkk., 2015) Diberikan R -aljabar bebas A dan ideal I di A .

1. Ideal I disebut ideal dasar (basic ideal), jika untuk setiap basis $X \subset A$ berlaku : untuk setiap elemen tak nol $r \in R, x \in X$, jika $rx \in I$ maka $x \in I$
2. Ideal I disebut ideal prima jika setiap ideal-ideal $M, N \subset A$, dengan $MN \subset I$ maka berakibat $M \subset I$ atau $N \subset I$
3. Ideal I disebut ideal dasar prima jika I ideal dasar dan setiap ideal-ideal dasar $P, Q \subset A$, jika $PQ \subset I$ maka $P \subset I$ atau $Q \subset I$
4. Ideal I disebut ideal semiprima jika setiap ideal $M \subset A$, dengan $M^2 \subset I$ maka berakibat $M \subset I$
5. Ideal I disebut ideal dasar semiprima jika I ideal dasar dan setiap $P \subset A$ ideal dasar jika $P^2 \subset I$ maka $P \subset I$.
6. Aljabar bebas A dikatakan aljabar prima jika ideal nol merupakan ideal prima, A dikatakan aljabar prima mendasar jika ideal dasar nol merupakan ideal dasar prima.
7. Aljabar bebas A dikatakan aljabar semiprima jika ideal nol merupakan ideal semiprima, A dikatakan aljabar semiprima mendasar jika ideal dasar nol merupakan ideal dasar semiprima.

Jika X basis dari R -aljabar bebas A maka setiap elemen tak nol $k \in R$ dan setiap $x \in X$, berlaku $kx \neq 0$. Berdasarkan Definisi 2.6, poin 1., ideal nol selalu merupakan ideal dasar. Hal ini berakibat bahwa sebarang R -aljabar bebas A mempunyai dua ideal dasar trivial, yaitu ideal nol dan dirinya sendiri sebagaimana telah dikaji dalam Wardati, dkk. (2015).

Kita ketahui bahwa dalam ring tidak berlaku sifat kanselasi terhadap perkalian. Hal ini dikarenakan adanya elemen pembagi nol dalam ring. Berbeda dengan modul atas suatu ring, perkalian antara elemen tak nol dalam ring dengan elemen tak nol dalam modul mungkin menghasilkan nol dalam modul tersebut. Elemen tak nol di ring yang menghasilkan nol di modul karena perkalian dengan suatu elemen tak nol di modul disebut sebagai elemen pengenal. Karena aljabar A atas ring R merupakan ring sekaligus R -modul maka dalam aljabar A terdapat istilah elemen pembagi nol dan elemen pengenal. Himpunan semua elemen

pengenol ini disebut sebagai *annihilator*. Berikut didefinisikan *annihilator* dalam R -aljabar dibangun secara berhingga.

Definisi 2.7 (Bland, 2011) Diberikan R -aljabar A dan subset tak kosong $S \subseteq A$.

1. *Annihilator kiri, kanan dan dua sisi dari S dalam aljabar A secara berurutan dinotasikan sebagai*

$$Ann^l(S) = \{a \in A : as = 0, \forall s \in S\}$$

$$Ann^r(S) = \{a \in A : sa = 0, \forall s \in S\}$$

$$Ann(S) = \{a \in A : as = 0 = sa, \forall s \in S\} = Ann^l(S) \cap Ann^r(S)$$

2. *Annihilator dari S dalam R -modul A dinotasikan sebagai,*

$$Ann_R(S) = \{r \in R : rs = 0, \forall s \in S\}$$

Jika Annihilator dalam R -modul A merupakan ideal nol dalam ring R , yakni $Ann_R(S) = \{0\}$ maka A disebut faithful

Menurut Wisbauer (1991) bahwa annihilator kiri, kanan, dan dua sisi dari S dalam aljabar A secara berurutan merupakan ideal kiri, kanan, dan dua sisi di A . Demikian pula annihilator dari S dalam A sebagai R -modul merupakan ideal dari ring R . Pengertian annihilator ini akan mendukung sifat kesempiprimaan aljabar dibangun secara berhingga yang merupakan focus dari penelitian ini.

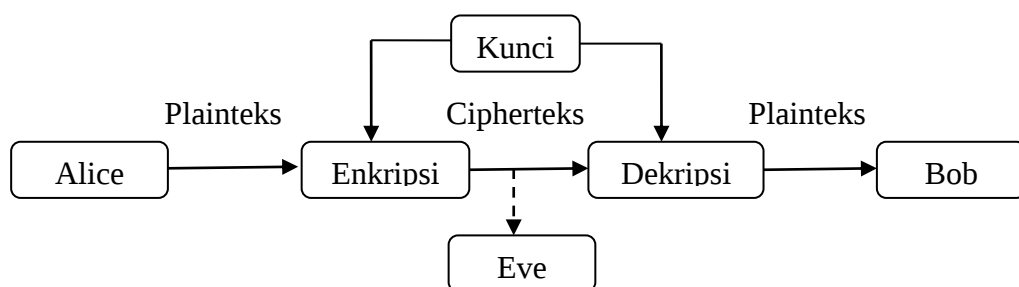
B.2. Kriptografi, Protokol Autentikasi dan Masalah Dekomposisi

Pesatnya perkembangan teknologi informasi saat ini memudahkan setiap orang untuk saling berkomunikasi dengan cepat dan mudah. Melalui telepon genggam dan komputer yang tersambung dengan internet, kita dapat melakukan komunikasi secara langsung dengan mudah ke seluruh penjuru dunia yang tersambung internet. Dibalik kemudahan-kemudahan yang diberikan di internet, terdapat ancaman-ancaman keamanan informasi yang dapat terjadi, hal ini disebabkan karena internet adalah jalur komunikasi umum yang dapat dilewati oleh siapapun. Salah satu ancaman kewanaman informasi tersebut adalah ancaman kerahasiaan.

Salah satu solusi yang digunakan untuk mengatasi masalah tersebut menggunakan ilmu kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-

teknik matematika yang berkaitan dengan aspek-aspek keamanan informasi, seperti kerahasiaan, keabsahan data, integritas data, serta autentikasi. Tetapi tidak seluruh aspek keamanan informasi dapat diselesaikan menggunakan kriptografi. Aspek dalam kriptografi yang biasa dibahas adalah berkaitan dengan keharasiaan data, yaitu menggunakan teknik enkripsi dan dekripsi. Pesan semula (plainteks) dienkripsi menjadi pesan tersandi (cipherteks) menggunakan suatu metode tertentu dan suatu parameter rahasia yang disebut dengan kunci. Algoritma enkripsi yang dikenal luas selama ini adalah DES (Data Encryption Standard), AES (*Advanced Encryption Standard*), RSA (*Rivest-Shamir-Adleman*), ElGamal dan ECC (*Elliptic Curve Cryptography*).

Sistem kriptografi merupakan suatu sistem atau kumpulan aturan-aturan yang digunakan untuk melakukan enkripsi dan dekripsi. Sistem kriptografi simetris adalah sistem kriptografi yang menggunakan kunci enkripsi dan dekripsi yang sama. Sistem ini mengharuskan dua pihak yang berkomunikasi menyepakati suatu kunci rahasia yang sama sebelum keduanya saling berkomunikasi. Keamanan dari sistem ini tergantung pada kunci, membocorkan kunci berarti bahwa orang lain yang berhasil mendapatkan kunci dapat mendekripsi cipherteks (Menezes dkk, 1996). Sistem kriptografi ini sering disebut dengan sistem kriptografi kunci rahasia, seperti dijelaskan pada gambar berikut ini.



Gambar 1. Sistem Kriptografi Simetris

Selain itu juga dikenal protokol pertukaran kunci yang digunakan pada proses enkripsi dan dekripsi, yaitu kedua belah pihak yang melakukan enkripsi-dekripsi dapat menyepakati kunci yang sama. Salah satu protokol pertukaran kunci yang dikenal luas adalah protokol pertukaran kunci Diffie-Hellman yang didasarkan pada masalah logaritma diskrit atas suatu grup siklik.

Aspek autentikasi juga merupakan hal yang penting untuk dilakukan sebelum terjadinya proses komunikasi dilakukan, maupun saat data dikirimkan. Hal tersebut dilakukan agar tidak terjadi penipuan identitas pihak yang saling berkomunikasi. Banyak terjadi kasus pemalsuan identitas dengan tujuan penipuan, seperti pemalsuan identitas pada surat resmi. Perkembangan kriptografi pada aspek autentikasi pada saat ditemukannya skema tanda tangan digital yang diperoleh dari memodifikasi sistem kriptografi kunci publik. Hingga kini, tanda tangan digital yang digunakan secara luas di internet yaitu tanda tangan RSA dan DSA. Tingkat keamanan tanda tangan digital RSA didasarkan pada masalah matematika yaitu memfaktorkan bilangan bulat yang besar, dan lebih prosesnya dilakukan pada ring Z_n , sedangkan tingkat keamanan tanda tangan digital DSA didasarkan pada masalah logaritma diskrit yang didefinisikan atas suatu grup siklik dengan order besar, sama seperti pada protokol pertukaran kunci Diffie-Hellman.

Sistem kriptografi yang menggunakan teknik enkripsi-dekripsi, tanda tangan digital, protokol pertukaran kunci sering memanfaatkan permasalahan matematika yang tidak mudah atau sulit apabila tidak mengetahui parameter-parameter rahasia yang digunakan, seperti masalah faktorisasi bilangan bulat dan masalah logaritma diskrit. Tingkat keamanan dari sistem kriptografi terletak pada tingkat kesulitan penyelesaian masalah tersebut tanpa mengetahui parameter rahasia yang digunakan, artinya semakin sulit penyelesaian masalah matematika yang digunakan mengakibatkan semakin kuat tingkat keamanan pada sistem kriptografi yang digunakan. Berikut ini diberikan skema protokol pertukaran kunci Diffie-Hellman.

Alice atau Bob mempublikasikan suatu grup siklik berhingga G dengan elemen pembangun $g \in G$.	
Alice	Bob
1. Alice memilih secara rahasia $a \in \mathbb{N}$ 2. Alice menghitung g^a 3. Alice mengirim g^a kepada Bob 4. Alice menerima g^b dari Bob 5. Alice menghitung $K_A = (g^b)^a = g^{ba}$	1. Bob memilih secara rahasia $b \in \mathbb{N}$ 2. Bob menghitung g^b 3. Bob mengirim g^b kepada Alice 4. Bob menerima g^a dari Alice 5. Bob menghitung $K_B = (g^a)^b = g^{ab}$
Alice dan Bob berhasil menyepakati kunci rahasia $K = K_A = K_B$.	

Gambar 2. ProkotoL pertukaran kunci Diffie-Hellman.

Berdasarkan protokol pertukaran kunci Diffie-Hellman tersebut, dapat dikembangkan suatu protokol otentikasi yang didasarkan pada masalah logaritma diskrit sebagai berikut. Misalkan Alice sebagai pihak pembukti (prover) dan Bob sebagai pihak verifikator.

Alice mempublikasikan suatu grup siklik berhingga G dengan elemen pembangun $g \in G$.	
Alice	Bob
1. Alice memilih secara rahasia $a \in \mathbb{N}$ 2. Alice menghitung g^a 3. Alice mengirim g^a kepada Bob 4. Alice menerima g^b dari Bob 5. Alice merespon dengan bukti $P = (g^b)^a = g^{ba}$ dan mengirimkannya kepada Bob	1. Bob memilih secara rahasia $b \in \mathbb{N}$ 2. Bob menghitung g^b 3. Bob mengirim tantangan g^b kepada Alice 4. Bob menerima g^a dari Alice 5. Bob memverifikasi apakah $(g^a)^b = P?$

Gambar 3. Protokol autentikasi Diffie-Hellman

Tujuan dari protokol otentikasi adalah sebagai alat untuk melegitimasi Alice sebagai user untuk membuktikan identitasnya kepada Bob sebagai server melalui jalur komunikasi yang tidak aman.

Seiring dengan adanya perkembangan komputer kuantum, terjadi ancaman pada masalah faktorisasi dan masalah logaritma diskrit, walaupun komputer kuantum dalam skala besar tersebut belum dapat diwujudkan. Diyakini bahwa

kedua masalah tersebut dapat diselesaikan dengan mudah menggunakan komputer kuantum dalam skala besar di masa yang akan datang. Akibat dari adanya ancaman tersebut, banyak penelitian dilakukan untuk mencari kandidat skema enkripsi-dekripsi, tanda tangan digital, protokol pertukaran kunci, khususnya protokol autentikasi yang aman dari serangan komputer kuantum.

Salah satu masalah dalam matematika yang diharapkan tetap sulit dipecahkan menggunakan komputer kuantum adalah masalah dekomposisi yang didefinisikan pada struktur aljabar tertentu yang bersifat non-komutatif (Myasnikov dkk, 2008). Salah satu penelitian S. Lal dan Chaturvedi (2005) telah memanfaatkan masalah dekomposisi untuk protokol autentikasi. Keduanya memanfaatkan tingkat kesulitan dalam menyelesaikan masalah dekomposisi atas grup anyaman (*braid group*). Definisi dari masalah dekomposisi diberikan sebagai berikut.

Definisi 2.8 (Myasnikov dkk, 2008) *Diberikan R adalah ring, A dan B adalah himpunan bagian dari R , dan $r, s \in R$. Masalah dekomposisi pada R adalah masalah dalam menentukan $x \in A$ dan $y \in B$ sedemikian hingga $xry = s$.*

Masalah dekomposisi hanya memanfaatkan operasi perkalian pada ring, oleh karena itu masalah dekomposisi juga dapat didefinisikan atas grup maupun semigrup. Masalah dekomposisi telah diteliti dan diterapkan oleh Sphlirain dan Ushakov (2005) untuk konstruksi suatu protokol pertukaran kunci pada sebuah grup non-komutatif yang bernama Grup Thompson. Sphlirain dan Ushakov memberikan skema protokol pertukaran kunci secara umum yang didasarkan pada masalah dekomposisi atas grup non-komutatif sebagai berikut.

Alice atau Bob mempublikasikan suatu grup non-komutatif G , $w \in G$ dan dua subgrup A, B dari G sedemikian hingga $ab = ba$, untuk setiap $a \in A$ dan $b \in B$	
Alice	Bob
1. Alice memilih secara rahasia $a_1 \in A$ dan $b_1 \in B$. 2. Alice menghitung $x = a_1 w b_1$ dan mengirimkan x kepada Bob 3. Alice menerima y , kemudian menghitung $K_1 = a_1 y b_1$	1. Bob memilih secara rahasia $a_2 \in A$ dan $b_2 \in B$. 2. Bob menghitung $y = b_2 w a_2$ dan mengirimkan y kepada Alice 3. Bob menerima x , kemudian menghitung $K_2 = b_2 x a_2$
Alice dan Bob telah menyepakati kunci yang sama $K = K_1 = K_2$	

Gambar 4. Skema Protokol Pertukaran Kunci Sphilrain-Ushakov (2005)

Diketahui $w \in G$ dan subgrup A, B dari G sedemikian hingga $ab = ba$, untuk setiap $a \in A$ dan $b \in B$. Dapat ditunjukkan bahwa perhitungan pada gambar di atas dapat menghasilkan kata sandi yang sama. Diketahui $x = a_1 w b_1$ dan $y = b_2 w a_2$, maka diperoleh

$$K_1 = a_1 b_2 w a_2 b_1 = b_2 a_1 w b_1 a_2 = b_2 x a_2 = K_2.$$

Dengan demikian, terbukti bahwa kedua belah pihak dapat menyepakati kata sandi yang sama berdasarkan parameter-parameter umum yang saling ditukarkan. Pihak ketiga sebagai pihak penyerang dapat mengetahui parameter-parameter umum tersebut, yaitu grup non-komutatif G , $w \in G$, subgrup A dan B .

Stickel (2005) mengembangkan protokol pertukaran kunci menggunakan bilangan asli acak, serta tidak menggunakan dua subgrup yang saling komutatif. Hal ini dilakukan sebagai usaha untuk meningkatkan tingkat keamanan dari protokol pertukaran kata sandi yang dikonstruksi oleh Sphilrain dan Ushakov (2005). Stickel (2005) menggunakan konsep *center* dari grup. Skema protokol pertukaran kunci oleh Stickel (2005) diberikan sebagai berikut.

Alice atau Bob mempublikasikan suatu grup non-komutatif berhingga G , $w \in G$ dan $a, b \in G$ dengan $ab \neq ba$. Misalkan order a adalah N dan order b adalah M .	
Alice	Bob
1. Alice memilih secara acak bilangan asli $n_1 < N$ dan $m_1 < M$. Alice memilih secara rahasia $c_1 \in Z(G)$. 2. Alice menghitung $x = c_1 a^{n_1} w b^{m_1}$ dan mengirimkan x kepada Bob 3. Alice menerima y , kemudian menghitung $K_1 = c_1 a^{n_1} y b^{m_1}$	1. Bob memilih secara acak bilangan asli $n_2 < N$ dan $m_2 < M$. Bob memilih secara rahasia $c_2 \in Z(G)$. 2. Bob menghitung $y = c_2 a^{n_2} w b^{m_2}$ dan mengirimkan y kepada Alice 3. Bob menerima x , kemudian menghitung $K_2 = c_2 a^{n_2} x b^{m_2}$
Alice dan Bob telah menyepakati kunci yang sama $K = K_1 = K_2$	

Gambar 5. Skema Protokol Pertukaran Kunci Stickel (2005)

Diketahui G adalah grup non-komutatif. Diberikan elemen $w \in G$ dan $a, b \in G$ dengan $ab \neq ba$, dengan order a adalah N dan order b adalah M . Diketahui $c_1, c_2 \in Z(G)$, maka untuk setiap $g \in G$ berlaku $c_1 g = g c_1$ dan $c_2 g = g c_2$. Oleh karena itu, dapat diperoleh bahwa

$$\begin{aligned}
 K_1 &= c_1 a^{n_1} y b^{m_1} \\
 &= c_1 a^{n_1} c_2 a^{n_2} w b^{m_2} b^{m_1} \\
 &= c_1 c_2 a^{n_1} a^{n_2} w b^{m_2} b^{m_1} \\
 &= c_2 c_1 a^{n_1 + n_2} w b^{m_2 + m_1} \\
 &= c_2 c_1 a^{n_2 + n_1} w b^{m_1 + m_2} \\
 &= c_2 c_1 a^{n_2} a^{n_1} w b^{m_1} b^{m_2} \\
 &= c_2 a^{n_2} x b^{m_2} \\
 &= K_2.
 \end{aligned}$$

Hasil perhitungan di atas menunjukkan bahwa Alice dan Bob berhasil memperoleh kunci yang sama menggunakan protokol pertukaran kunci Stickel (2005), selanjutnya kata sandi yang telah didapat digunakan dalam proses enkripsi dan dekripsi.

S. Lal dan Chaturvedi (2005) mengkonstruksi suatu protokol autentikasi berdasarkan masalah dekomposisi yang didefinisikan grup non-komutatif, dengan cara memodifikasi protokol pertukaran kunci yang didasarkan pada masalah dekomposisi. S. Lal dan Chaturvedi mengkonstruksi protokol autentikasi atas grup non-komutatif sebagai berikut. Misalkan Alice adalah pihak yang akan membuktikan kebenaran identitasnya, dan Bob adalah pihak verifikatornya. Diberikan A, B, C dan D adalah subgrup-subgrup dari grup G sedemikian hingga A dan C saling komutatif, serta B dan D juga saling komutatif, yaitu apabila memenuhi $ac = ca$, untuk setiap $a \in A$ dan $c \in C$, serta $bd = db$, untuk setiap $b \in B$ dan $d \in D$.

1. Alice memilih dan mempublikasikan grup non-komutatif G , serta subgrup-subgrup A, B, C dan D dari grup G sedemikian hingga A dan C saling komutatif, serta B dan D juga saling komutatif.
2. Alice memilih $a \in A, b \in B$ dan $w \in G$, kemudian menghitung $t = awb$.
3. Alice mengirimkan w dan t kepada Bob.
4. Bob memilih $c \in C$ dan $d \in D$, kemudian menghitung $w' = cwd$.
5. Bob mengirimkan tantangan (*challenge*) w' kepada Alice.
6. Alice menghitung $w'' = aw'b$.
7. Alice mengirimkan respon w'' kepada Bob.
8. Bob melakukan verifikasi, yaitu verifikasi benar apabila $w'' = ctd$.

Diketahui bahwa A dan C saling komutatif, serta B dan D saling komutatif, maka $ac = ca$ dan $bd = db$. Dapat ditunjukkan bahwa:

$$ctd = cawbd = acwdb = aw'b = w''.$$

Dilihat dari operasi yang digunakan, maka protokol autentikasi ini dapat diterapkan pada semigrup, monoid, bahkan juga pada ring, modul dan aljabar. Berikut ini diberikan gambar skema protokol autentikasi berdasarkan masalah dekomposisi atas grup non-komutatif G .

Alice memilih dan mempublikasikan grup non-komutatif G, serta subgrup-subgrup A, B, C dan D dari grup G sedemikian hingga A dan C saling komutatif, serta B dan D juga saling komutatif.	
Alice	Bob
1. Alice memilih $a \in A$, $b \in B$ dan $w \in G$, kemudian menghitung $t = awb$.	
2. Alice mengirimkan w dan t kepada Bob.	
	3. Bob memilih $c \in C$ dan $d \in D$, kemudian menghitung $w' = cwd$.
	4. Bob mengirimkan tantangan (<i>challenge</i>) w' kepada Alice.
5. Alice menghitung $w'' = aw'b$.	
6. Alice mengirimkan respon w'' kepada Bob.	
	7. Bob melakukan verifikasi, yaitu verifikasi benar apabila $w'' = ctd$.

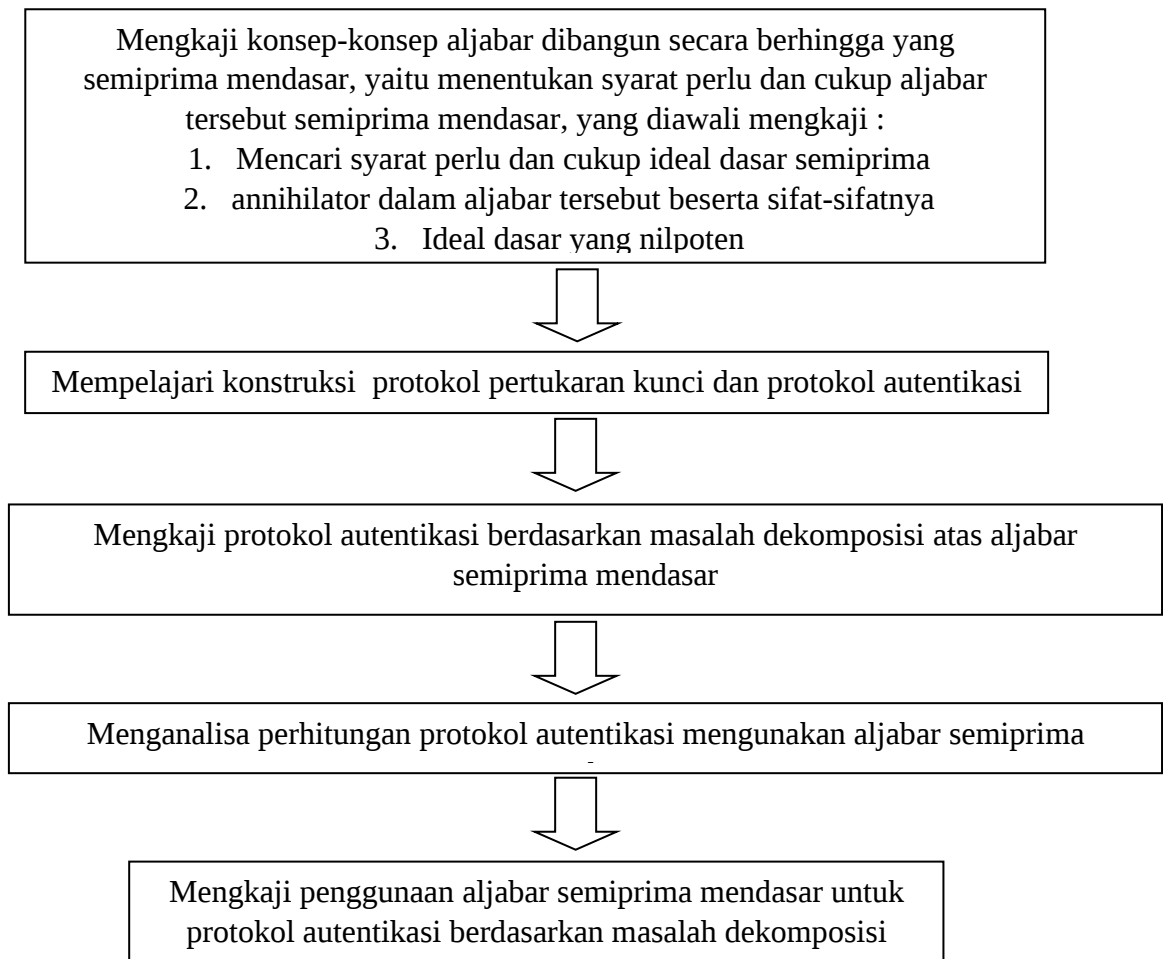
Gambar 6. Protokol Autentikasi Lal dan Chaturvedi (2005)

BAB III METODE DAN TARGET PENELITIAN

A. METODE PENELITIAN

Penelitian ini merupakan penelitian terapan, yakni terapan aljabar pada kriptografi. Pendekatan penelitiannya merupakan penelitian kualitatif dengan metode deduktif-induktif. Deduksi adalah cara berfikir yang diambil dari pernyataan bersifat umum lalu ditarik kesimpulan bersifat khusus. Sebaliknya, induktif merupakan metode berfikir yang bertolak dari hal-hal khusus.

Aljabar dibangun secara berhingga atas ring komutatif dengan elemen satuan yang bersifat semiprima mendasar ini akan diterapkan sebagai struktur yang mendukung proses autentikasi identitas digital menggunakan protokol autentikasi berdasarkan masalah dekomposisi. Alur penelitian secara utuh diberikan dalam bagan alir berikut :



B. RENCANA PUBLIKASI

Penelitian ini ditargetkan menghasilkan dua (2) artikel. Artikel pertama sudah dipresentasikan dalam seminar internasional : *The 2nd International Conference On Natural Sciences, Mathematics, Applications, Research, and Technology*, 2001 (ICON-SMART 2021), 21 – 22 Oktober 2021. Hasil pertama dalam penelitian ini adalah sifat-sifat ideal dasar semiprima dalam aljabar dibangun secara berhingga atas ring komutatif unital dan terapannya dalam skema autentikasi. Artikel dari hasil penelitian awal ini berjudul “*The Application of Semiprime Basic Ideals in Authentication Scheme*”, sudah lolos review pertama untuk publikasi di *proceeding AIP Publishing* terindeks Scopus dan *Web of Science* (WoS).

Hasil penelitian lanjutan yang merupakan inti dari penelitian ini adalah sifat-sifat semiprima mendasar aljabar dibangun secara berhingga dan terapannya dalam kriptografi, khususnya pada skema autentikasi. Sifat-sifat ini memerlukan pembahasan *annihilator* atau pengenol dan juga ideal nilpotent. Hasil penelitian akhir ini, segera disusun artikel yang ditargetkan masuk publikasi di jurnal nasional terakreditasi Sinta 2, Cauchy. Artikel hasil akhir penelitian ini diberi judul “A basically semiprime non-free algebra and its application on securing digital identity authentication”

C. JADWAL PELAKSANAAN

No	Tahap	Bulan					
		VII	VIII	IX	X	XI	XII
1.	Koordinasi awal tim peneliti						
2.	Survey struktur aljabar dan Studi Literatur						
3.	Mengkaji sifat-sifat ideal dasar semiprima, mencari persyaratan annihilator yang merupakan ideal dasar, dan mempelajari ideal dasar yang nilpoten						
4.	Mencari syarat perlu dan cukup ideal dasar semiprima dalam aljabar tak bebas dibangun secara berhingga						
5.	Menganalisis syarat perlu dan cukup aljabar semiprima mendasar yang berkaitan dengan irisan ideal-ideal dasar prima, dan sifat nilpoten ideal dasar						
6.	Penentuan aljabar semiprima mendasar untuk masalah dekomposisi						
7.	Perhitungan protocol autentikasi menggunakan aljabar semiprima mendasar						
8.	Desiminasi Hasil (seminar-seminar)						
9.	Penulisan Draft Artikel						
10.	Penyusunan Laporan.						

D. PERSONALIA

Peneliti terdiri dari 3 orang dengan keahlian tidak semua sama. Ketua peneliti adalah Dr. Khurul Wardati, M.Si. dengan keahlian aljabar teoritis. Salah anggota peneliti (peneliti kedua) dengan keahlian terapan aljabar di bidang

Kriptografi, yakni M. Zaki Riyanto, S.Si., M.Si. Secara detail profil kedua peneliti ini diberikan di Biografi singkat para peneliti. Salah satu anggota peneliti berstatus mahasiswa merupakan mahasiswa bimbingan skripsi ketua tim peneliti, yang tugas akhirnya berbeda dengan tema dari penelitian ini.

Ketua tim peneliti berperan utama dalam memberikan kebaruan secara teori, yakni menemukan syarat perlu dan cukup ideal dalam aljabar dibangun secara berhingga (tidak harus aljabar bebas) atas ring komutatif unital merupakan ideal dasar semiprima. Selain itu, dibahas tentang pengenol atau annihilator dalam aljabar tersebut, juga menentukan syarat perlu dan cukup aljabar dibangun secara berhingga tersebut bersifat semiprima mendasar. Anggota (peneliti kedua) yang ahli kriptografi akan mengaplikasikan contoh-contoh ideal dasar semiprima maupun aljabar semiprima mendasar dalam kriptografi, khususnya dalam skema autentikasi.

Anggota peneliti dari unsur mahasiswa, sangat berperan ketika penelitian awal dimulai. Dia lebih banyak menyiapkan substansi materi, mulai dari menuliskan dan melengkapi dasar teori berdasarkan arahan dari ketua tim peneliti khususnya, juga anggota peneliti kedua. Karena anggota peneliti ini fokus juga di tugas akhirnya, maka agar kegiatan penelitian ini tetap berjalan lancar, kami mengangkat pembantu peneliti non PNS, M. Rouhun Munajih. Kriteria pembantu peneliti adalah yang memiliki kompetensi di bidang matematika meski tidak dari jurusan matematika, juga terampil dalam pengoperasian MS Office dan Latex. Dia membantu beberapa pekerjaan teknis, seperti merapikan artikel sesuai dengan template, menyiapkan slight presentasi baik untuk seminar maupun untuk desiminasi dengan program *Latex (Bimer-Latex)*. Selain itu, pembantu peneliti memberikan bantuan pembuatan laporan keuangan. Peneliti memerlukan pembantu peneliti mulai 23 Agustus 2021, bersamaan dengan sudah tersusunnya artikel untuk publikasi di seminar internasional.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

A. Sifat-sifat ideal dasar semiprima dalam Aljabar dibangun secara berhingga atas ring komutatif unital

Karakterisasi ideal dasar semiprima dianalogkan dengan ideal semiprima dalam Wisbauer (1991), Lam (2001) dan Bland (2011) yang mensyaratkan aljabar unital (dengan elemen satuan). Oleh karenanya, ruang lingkup aljabar dibangun secara berhingga dalam penelitian ini adalah aljabar unital yang hanya dituliskan aljabar (dibangun secara berhingga) saja.

Aljabar dibangun secara berhingga dalam penelitian ini secara umum bukan aljabar bebas. Artinya pembangun dari aljabarnya tidak merupakan basis, lebih karena pembangun tersebut tidak bebas linear. Namun, pembangun berhingga yang dimaksud adalah pembangun minimal, yaitu jika elemen pembangun dikeluarkan salah satu sudah tidak sebagai pembangun aljabar tersebut.

Definisi 4.1.1 (Wardati, 2018) *Diberikan R -aljabar unital A . Himpunan A disebut R -aljabar dibangun secara berhingga jika R -aljabar $A = \langle X \rangle$, dengan X berhingga dan X adalah pembangun minimal berhingga yang belum tentu bebas linear.*

Jika $A = \langle X \rangle$ adalah R -aljabar bebas maka berlaku $rx \neq 0$ untuk setiap elemen tak nol $r \in R$ dan $x \in X$. Konsekuensi dari implikasi ini belum tentu berlaku pada aljabar dibangun secara berhingga. Oleh karenanya, definisi ideal dasar J dalam aljabar bebas, yakni untuk setiap elemen tak nol $r \in R$ dan $x \in X$ berlaku jika $rx \in J$ maka $x \in J$, perlu diperumum dalam aljabar dibangun secara berhingga yang tak bebas.

Definisi 4.1.2 (Wardati 2018). *Diberikan R -aljabar $A = \langle X \rangle$ dibangun secara berhingga. Ideal I di A dikatakan ideal dasar, jika dan hanya jika untuk setiap elemen tak nol $r \in R$, dan setiap $x \in X$, berlaku jika $0 \neq rx \in I$ maka $x \in I$.*

Tampak jelas bahwa Definisi 4.1.2 merupakan generalisasi dari ideal dasar dalam aljabar bebas. Perlu dipertegas bahwa R -aljabar dibangun secara berhingga dalam Definisi 4.1.2 adalah

$$A = \langle X \rangle = \left\{ \sum_{i=1}^m r_i x_i : r_i \in R, x_i \in X, m \in \mathbb{N} \right\} \quad (1)$$

dengan X tidak harus bebas linear. Berikut sifat penting ideal dasar dalam aljabar dibangun secara berhingga.

Lemma 4.1.3 (Wardati, 2018) Jika diberikan $A = \langle X \rangle$ adalah R -aljabar dibangun secara berhingga maka :

- 1) Setiap $x \in X$ berlaku $x \in I$ jika dan hanya jika x merupakan suatu elemen pembangun dari I sebagai R -submodul dari A ;
- 2) Untuk setiap elemen tak nol $r_i \in R$ dan setiap $x_i \in X$, dengan $i = 1, 2, \dots, n$ untuk suatu $n \in \mathbb{N}$, jika $0 \neq \sum_{i=1}^n r_i x_i \in I$ maka $x_i \in I$ untuk setiap i ;
- 3) Ideal dasar $I = \langle X_I \rangle$ dengan $X_I = X \cap I$.

Ideal semiprima dalam Bland (2011) merupakan generalisasi dari ideal prima. Terminologi ideal dasar semiprima dalam aljabar dibangun secara berhingga analog dengan ideal semiprima ini.

Definisi 4.1.4 Diberikan R -aljabar dibangun secara berhingga A . Ideal dasar S di A disebut ideal dasar semiprima jika dan hanya jika, setiap ideal dasar $I \subseteq A$ berlaku jika $I^2 \subseteq S$ maka $I \subseteq S$.

Jika diperhatikan definisi ideal dasar prima maka ideal dasar semiprima lebih umum dari pada ideal dasar prima. Artinya, tidak semua ideal dasar semiprima merupakan ideal dasar prima. Perhatikan contoh berikut ini.

Contoh 4.1.5 Diberikan $\mathbb{Z}$ -aljabar $\mathcal{M} = \left[\begin{pmatrix} \mathbb{Z}_{256} & \mathbb{Z}_{256} \\ \mathbb{Z}_{256} & \mathbb{Z}_{256} \end{pmatrix}, \begin{pmatrix} \mathbb{Z}_6 & \mathbb{Z}_6 \\ 0 & \mathbb{Z}_6 \end{pmatrix} \right]$ dan beberapa idealnya,

- 1) $I = \left[\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \mathbb{Z}_6 \\ 0 & 0 \end{pmatrix} \right]$
- 2) $J = \left[\begin{pmatrix} \mathbb{Z}_{256} & \mathbb{Z}_{256} \\ \mathbb{Z}_{256} & \mathbb{Z}_{256} \end{pmatrix}, \begin{pmatrix} \mathbb{Z}_6 & \mathbb{Z}_6 \\ 0 & 0 \end{pmatrix} \right]$
- 3) $K = \left[\begin{pmatrix} \mathbb{Z}_{256} & \mathbb{Z}_{256} \\ \mathbb{Z}_{256} & \mathbb{Z}_{256} \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right]$
- 4) $L = \left[\begin{pmatrix} 16\mathbb{Z}_{256} & 16\mathbb{Z}_{256} \\ 16\mathbb{Z}_{256} & 16\mathbb{Z}_{256} \end{pmatrix}, \begin{pmatrix} 0 & \mathbb{Z}_6 \\ 0 & 0 \end{pmatrix} \right]$

Berdasarkan Definisi 4.1.4, I ideal dasar semiprima tetapi bukan ideal dasar prima di $\mathcal{M}$ karena $J, M = \left[\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \mathbb{Z}_6 \\ 0 & \mathbb{Z}_6 \end{pmatrix} \right] \not\subseteq I$ dan $JM = I$. Selain itu, ideal I tidak

semiprima di $\mathcal{M}$ karena $L^2 = \{0\} \subset I$ dan $L \not\subset I$. Ideal J adalah semiprima dan sekaligus merupakan ideal dasar semiprima di $\mathcal{M}$, sementara ideal dasar K tidak keduanya. Berdasarkan definisi 4.1.2, L bukan ideal dasar di $\mathcal{M}$ karena terdapat x dalam pembangun standard dengan $x = \left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right] \notin L$ dan $16x \in L$. Otomatis L bukan ideal dasar semiprima tetapi L merupakan ideal semiprima di $\mathcal{M}$.

Meskipun terminology ideal semiprima dan ideal dasar semiprima mirip, namun keduanya tidak saling bergantung. Hal ini ditunjukkan dengan contoh kontra pada Contoh 4.1.5.

Ideal nol $\{0\}$ adalah semiprima jika untuk setiap ideal tak nol I berakibat $I^2 \neq \{0\}$. Jika ideal nol semiprima maka kuadrat semua ideal dasar tak nol pasti tak nol pula, namun tidak sebaliknya. Sebagai contoh kontra, ideal nol di K sebagai $\mathbb{Z}$ -aljabar pada Contoh 4.1.5 merupakan ideal dasar semiprima. Akan tetapi ideal nol ini bukan ideal semiprima di K karena $L^2 = \{0\}$ dan ideal tak nol $L \subset K$.

Akibat 4.1.6 Jika ideal $\{0\}$ semiprima maka $\{0\}$ merupakan ideal dasar semiprima.

Berdasarkan Lemma 3.5 dalam Wardati (2018) bahwa jika diberikan R -aljabar yang dibangun secara hingga $A = \langle X \rangle$ dan $x \in X$ maka ideal yang dibangun oleh x , yakni

$$(x) = \left\{ \sum_i a_i x b_i : a_i, b_i \in A \right\} \quad (2)$$

merupakan ideal dasar. Ideal dasar yang dibangun oleh suatu elemen dalam aljabar sebagai ring dapat digunakan untuk menyelidiki dan membuktikan suatu ideal dasar semiprima.

Teorema 4.1.7 Diberikan R -aljabar yang dibangun secara hingga $A = \langle X \rangle$ dan ideal dasar $S \subset A$, maka ketiga pernyataan di bawah ini ekuivalen :

- 1) Ideal S adalah ideal dasar semiprima
- 2) Untuk setiap $a \in A$ dengan (a) ideal dasar di A , jika $(a)^2 \subseteq S$ maka $a \in S$
- 3) Untuk setiap $a \in A$ dengan (a) ideal dasar di A , jika $aAa \subseteq S$ maka $a \in S$.

Bukti :

1) $\Rightarrow$ 2): Ambil sebarang $a \in A$ dengan (a) ideal dasar di A dan $(a)^2 \subseteq S$. Karena S semiprima maka berdasarkan Definisi 4.1.4, $(a) \subseteq S$. Di sisi lain, $a = 1_A a 1_A \in (a)$ maka $a \in S$.

2) $\Rightarrow$ 3): Ambil sebarang $a \in A$ dengan (a) ideal dasar di A dan $aAa \subseteq S$. Jelas bahwa $axa \in aAa$ untuk setiap $x \in X$, maka

$$axa = (1_A ax)(1_A a 1_A) \in (a)^2$$

Menurut 2), diperoleh $a \in S$.

3) $\Rightarrow$ 1): Ambil sebarang ideal dasar $I \subset A$ sedemikian sehingga $I^2 \subset S$, akan ditunjukkan $I \subset S$. Berdasarkan Lemma 4.3., bahwa $I = \langle X_I \rangle$ dengan $X_I = X \cap I$. Ambil sebarang $v \in X_I \subset I$ dan sebarang $a \in A$ maka berlaku $vav = (va)v \in I^2$. Hal ini berarti bahwa setiap $v \in X_I$, $vAv \subset I^2 \subset S$ berakibat $v \in S$. Ambil sebarang $y \in I$, karena $I = \langle X_I \rangle$ maka $y = \sum_{v \in X_I} r_v v \in S$. Jadi, $I \subset S$.

Definisi aljabar semiprima didasarkan pada karakterisasi ideal nol yang semiprima. Ideal nol merupakan ideal dasar trivial, sehingga karakterisasi ideal dasar nol akan mempengaruhi karakteristik dari aljabar dibangun secara berhingga. Secara analog, jika ideal dasar nol merupakan ideal dasar semiprima dalam aljabar dibangun secara berhingga, maka aljabar ini bersifat semiprima mendasar. Subbab berikut akan membahas sifat-sifat aljabar dibangun secara berhingga yang semiprima mendasar.

B. Aljabar semiprima mendasar dibangun secara berhingga atas ring komutatif unital

Ring semiprima didefinisikan sebagai ring yang ideal nolnya merupakan ideal semiprima (Bland, 2011). Demikian juga secara umum, aljabar semiprima didefinisikan sebagai aljabar yang ideal nolnya merupakan ideal semiprima.

Definisi 4.2.1 R -aljabar yang dibangun secara hingga A dikatakan semiprima mendasar jika ideal nol merupakan ideal dasar semiprima.

Jika diberikan R -aljabar yang dibangun secara hingga $A = \langle X \rangle$ maka berdasarkan kontraposisi poin 3) Teorem 4.1.7, Aljabar A bersifat semiprima

mendasar jika dan hanya jika untuk setiap $a \in A$ dengan (a) ideal dasar di A , jika $a \neq 0$ maka $aAa \neq \{0\}$.

Menurut Abrams, dkk. (2017), suatu aljabar A bersifat semiprima jika dan hanya jika A bersifat *nondegenerate*, yaitu jika $aAa = \{0\}$ maka $a = 0$ untuk setiap $a \in A$. Sifat *nondegenerate* ini ekuivalen dengan pernyataan setiap $a \in A$ jika $a \neq 0$ maka $aAa \neq \{0\}$.

Perhatikan bahwa kontraposisi poin 3) dalam Teorema 4.1.7 tidak ekuivalen dengan sifat *nondegenerate*. Namun, Jika R -aljabar yang dibangun secara hingga $A = \langle X \rangle$ bersifat semiprima, artinya memenuhi sifat *nondegenerate* maka aljabar tersebut bersifat semiprima mendasar karena memenuhi Teorema 4.1.7 poin 3).

Akibat 4.2.2 Jika R -aljabar yang dibangun secara hingga A semiprima atau bersifat *nondegenerate* maka aljabar A semiprima mendasar.

Sifat pada Akibat 4.2.2 tidak berlaku sebaliknya. Hal ini menunjukkan bahwa sifat semiprima mendasar lebih umum dari pada semiprima. Contoh kontra di bawah ini mempertegas perumuman semiprima ke semiprima mendasar aljabar dibangun secara berhingga. Selain itu, contoh ini juga menunjukkan bahwa sifat *nondegenerate* bukan merupakan syarat perlu sifat semiprima mendasar dari aljabar dibangun secara berhingga.

Contoh 4.2.3 Diberikan $\mathcal{M}' = \begin{pmatrix} \mathbb{Z}_{256} & \mathbb{Z}_{256} \\ \mathbb{Z}_{256} & \mathbb{Z}_{256} \end{pmatrix}$ adalah $\mathbb{Z}$ -aljabar dibangun secara berhingga, maka $\mathcal{M}'$ tidak bersifat *nondegenerate* yang berarti $\mathcal{M}'$ tidak semiprima karena,

$$\begin{pmatrix} 16 & 0 \\ 0 & 16 \end{pmatrix} \mathcal{M}' \begin{pmatrix} 16 & 0 \\ 0 & 16 \end{pmatrix} = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

Namun, untuk setiap matriks X di $\mathcal{M}'$ sedemikian sehingga (X) ideal dasar, jika $X\mathcal{M}'X = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$ maka $X = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Artinya, $\mathbb{Z}$ -aljabar $\mathcal{M}'$ merupakan aljabar semiprima mendasar tetapi tidak semiprima.

Sebarang aljabar dibangun secara berhingga yang prima mendasar pastilah semiprima mendasar. Selain itu, irisan semua ideal dasar prima dalam aljabar prima mendasar adalah ideal nol, namun tidak sebaliknya. Perhatikan contoh berikut:

Contoh 4.2.4 Diberikan $\mathbb{Z}$ -aljabar $A^* = \left[\begin{pmatrix} \mathbb{Z}_{256} & \mathbb{Z}_{256} \\ \mathbb{Z}_{256} & \mathbb{Z}_{256} \end{pmatrix}, \begin{pmatrix} \mathbb{Z}_6 & \mathbb{Z}_6 \\ \mathbb{Z}_6 & \mathbb{Z}_6 \end{pmatrix} \right]$. Ideal dasar prima di A^* adalah

$$K = \left[\begin{pmatrix} \mathbb{Z}_{256} & \mathbb{Z}_{256} \\ \mathbb{Z}_{256} & \mathbb{Z}_{256} \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right], K' = \left[\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} \mathbb{Z}_6 & \mathbb{Z}_6 \\ \mathbb{Z}_6 & \mathbb{Z}_6 \end{pmatrix} \right]$$

Perhatikan bahwa $\text{ann}(K) = K'$ dan $\text{ann}(K') = K$. Aljabar A^* bukan aljabar prima mendasar karena $K \cdot \text{ann}(K) = \text{ann}(K') \cdot K' = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$. Namun, aljabar A^* semiprima mendasar dan $K \cap K' = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$.

Contoh 4.2.4 ini memberikan indikasi bahwa ideal nol merupakan ideal dasar semiprima jika dan hanya jika irisan semua ideal dasar prima merupakan ideal nol. Karakterisasi ini memerlukan konsep annihilator. Berkaitan dengan ini, Contoh 4.2.4 juga mengindikasikan sifat bahwa *annihilator* dari ideal dasar juga merupakan ideal dasar.

Lemma 4.2.5 Diberikan R -aljabar yang dibangun secara hingga A dan $I \subseteq A$.

1. Jika $J \subseteq I$ maka $\text{Ann}^l(I) \subseteq \text{Ann}^l(J)$, $\text{Ann}^r(I) \subseteq \text{Ann}^r(J)$ dan $\text{Ann}(I) \subseteq \text{Ann}(J)$
2. Jika I ideal dasar maka secara berurutan $\text{Ann}^l(I)$, $\text{Ann}^r(I)$ dan $\text{Ann}(I)$ adalah ideal kiri dasar, ideal kanan dasar dan ideal dasar.

Bukti :

1. Ambil sebarang $u \in \text{Ann}^l(I)$ maka $u \in A$ dan $ua = 0$ untuk setiap $a \in I$. Karena $J \subseteq I$ maka berlaku $ub = 0$, untuk setiap $b \in J$ dan berarti $u \in \text{Ann}^l(J)$. Jadi, $\text{Ann}^l(I) \subseteq \text{Ann}^l(J)$. Secara analog, jika diambil sebarang $v \in \text{Ann}^r(I)$ maka $v \in A$ dan $av = 0$ untuk setiap $a \in I$. Karena $J \subseteq I$ maka $bv = 0$, untuk setiap $b \in J$ dan berarti $v \in \text{Ann}^r(J)$. Terbukti bahwa $\text{Ann}^r(I) \subseteq \text{Ann}^r(J)$. Terakhir, ambil sebarang $x \in \text{Ann}(I)$ maka $x \in A$ dan $ax = 0 = xa$ untuk setiap $a \in I$. Karena $J \subseteq I$ maka berlaku $xb = 0 = bx$, untuk setiap $b \in J$ dan berarti $x \in \text{Ann}(J)$. Hal ini menunjukkan $\text{Ann}(I) \subseteq \text{Ann}(J)$.
2. Menurut Wisbauer (1991) bahwa secara berurutan $\text{Ann}^l(I)$, $\text{Ann}^r(I)$ dan $\text{Ann}(I)$ merupakan ideal kiri, ideal kanan dan ideal dua sisi dari A . Tanpa mengurangi keumuman bukti, poin 2. ini hanya dibuktikan bahwa

$Ann(I) = \{a \in A: au = 0 = ua, \forall u \in I\}$ adalah ideal dasar dari A , sebagai berikut :

Ambil sebarang elemen tak nol $r \in R, x \in X$ dengan $0 \neq rx \in Ann(I)$. Menurut definisi annihilator, diperoleh bahwa $(rx)u = 0 = u(rx)$, untuk setiap $u \in I$. Akan ditunjukkan $x \in Ann(I)$, yaitu $xu = 0 = ux$.

Andaikan $xu \neq 0$ atau $ux \neq 0$ untuk suatu $u \in I$, maka $xu, ux \in I$. Menurut Lemma 4.1.3, ideal dasar $I = \langle H \rangle, H = X \cap I$, sehingga $0 \neq xu = \sum_{i=1}^k r_i h_i$ untuk suatu $r_i \in R, h_i \in H \subseteq X$. Artinya, terdapat $m, 1 \leq m \leq k$ sedemikian sehingga $r_m h_m \neq 0$ dan $rr_m h_m \neq 0$ untuk suatu $r \in R$. Akibatnya,

$r(xu) = r \sum_{i=1}^k r_i h_i = \sum_{i=1}^k rr_i h_i \neq 0$ untuk suatu $u \in I$, kontradiksi dengan $r(xu) = (rx)u = 0$ untuk setiap $u \in I$. Diperoleh, $xu = 0$ dan secara analog didapat pula $ux = 0$ yang berarti, $x \in Ann(I)$. Jadi, untuk setiap elemen tak nol $r \in R, x \in X$ dengan $0 \neq rx \in Ann(I)$ maka $x \in Ann(I)$. Dengan kata lain, $Ann(I)$ merupakan ideal dasar dari R -aljabar yang dibangun secara hingga A .

Karakterisasi ideal nol merupakan ideal semiprima dapat dipandang dari sifat lain, berkaitan dengan ideal nilpoten. Bland (2010) memberikan syarat perlu dan cukup suatu ring (aljabar) merupakan ring (aljabar) semiprima, yaitu ideal nol merupakan satu-satunya ideal nilpoten. Hal ini ekuivalen dengan setiap ideal tak nol bukan ideal nilpotent.

Jika ideal nol merupakan ideal dasar semiprima maka menurut definisinya berlaku kuadrat setiap ideal dasar tak nol pasti tak nol pula. Hal ini mengindikasikan bahwa setiap ideal dasar tak nol bukan merupakan ideal nilpotent, jika ideal nol merupakan ideal dasar semiprima. Berikut diberikan syarat perlu dan cukup ideal dasar nol merupakan ideal dasar semiprima, sehingga aljabar dibangun secara berhingga merupakan aljabar semiprima mendasar.

Teorema 4.2.6 Diberikan R -aljabar yang dibangun secara hingga $A = \langle X \rangle$, maka pernyataan-pernyataan berikut ekuivalen.

1. Aljabar A semiprima mendasar
2. Irisan dari semua ideal-ideal dasar prima adalah ideal nol
3. Setiap ideal dasar tak nol merupakan ideal idempotent
4. Setiap $x \in X, xAx \neq \{0\}$

Bukti :

(1 $\Rightarrow$ 2) Misalkan $\wp$ adalah keluarga ideal prima dari A . Akan ditunjukkan bahwa irisan dari semua ideal-ideal dasar prima adalah ideal nol, yaitu $\bigcap_{P \in \wp} P = \{0\}$. Artinya, untuk setiap $0 \neq a \in A$ maka $a \notin \bigcap_{P \in \wp} P$. Hal ini berarti bahwa terdapat ideal dasar prima P sehingga $a \notin P$. Karena A ideal dasar trivial maka menurut Lemma 4.2.5, $Ann(A)$ merupakan ideal dasar dari A , sehingga diperoleh bahwa :

$$(Ann(A))^2 = Ann(A).Ann(A) \subseteq Ann(A).A = \{0\}$$

Karena aljabar A aljabar semiprima mendasar, yang berarti $\{0\}$ merupakan ideal dasar semiprima maka $Ann(A) = \{0\}$. Hal ini berkonsekuensi, bahwa untuk setiap $0 \neq a \in A$ maka $aAa \neq \{0\}, AaA \neq \{0\}$, karena :

Andaikan $aAa = \{0\}$ maka $(AaA)^2 = AaAaA \subseteq AaAaA = \{0\}$. Diketahui $\{0\}$ ideal semiprima maka haruslah $AaA = \{0\}$. Aljabar A memuat elemen satuan maka $a = 1_A a 1_A \in AaA$, sehingga diperoleh $a = 0$ yang kontradiksi dengan $a \neq 0$. Jadi, $aAa \neq \{0\}$. Selanjutnya, andaikan $AaA = \{0\}$ maka $Aa \subseteq Ann(A) = \{0\}$ yang berakibat $a \in Ann(A) = \{0\}$. Artinya, $a = 0$ dan kontradiksi dengan $a \neq 0$. Jadi, $AaA \neq \{0\}$.

Dibentuk suatu barisan $\{a_n\}_{n \in \mathbb{N}}$ dengan $0 \neq a_n \in A$ untuk setiap $n \in \mathbb{N}$. Ambil sebarang $0 \neq a \in A$ dan pilih $a = a_1$ maka $a_1 A a_1 \neq \{0\}$ karena $a_1 \neq 0$. Pilih a_2 sehingga $0 \neq a_2 \in a_1 A a_1$ dan $a_2 A a_2 \neq \{0\}$ maka dipilih a_3 sehingga $a_3 \neq 0$ dan $a_3 \in a_2 A a_2$. Demikian seterusnya, diperoleh $a_n \neq 0$ untuk setiap $n \in \mathbb{N}$, sehingga dapat dipilih $0 \neq a_{n+1} \in a_n A a_n$. Jadi, diperoleh barisan elemen-elemen tak nol di A , yakni $S = \{a_n\}_{n \in \mathbb{N}} \subset A$. Selanjutnya dibentuk keluarga ideal-ideal dasar di A yang saling asing dengan S , yakni

$$\mathfrak{I}_S = \{I \subseteq A : I \text{ ideal dasar dengan } I \cap S = \{0\}\}$$

Menurut Lemma Zorn, $\mathfrak{I}_S$ mempunyai elemen maksimal dimisalkan P , maka P ideal dasar dengan $P \cap S = \{0\}$ sehingga jika $a \in S$ maka $a \notin P$. Jadi, diperoleh bahwa setiap $0 \neq a \in A$ terdapat ideal dasar $P \in \mathfrak{I}_S$ sehingga $a \notin P$.

Berikut ditunjukkan bahwa elemen maksimal $P \in \mathfrak{I}_S$ adalah ideal dasar prima:

Ambil sebarang ideal-ideal dasar $L, M \subseteq A$ dengan $L \not\subseteq P$ dan $M \not\subseteq P$ maka diperoleh $P \subset P + L, P \subset P + M$. Karena P ideal dasar maksimal dan saling asing dengan S maka $(P + L) \cap S \neq \emptyset$ dan $(P + M) \cap S \neq \emptyset$. Artinya, terdapat $i, j \in \mathbb{N}$ sehingga $a_i \in P + L, a_j \in P + M$. Jika dipilih $k > \max(i, j)$ maka menurut pembentukan himpunan S , diperoleh

$$a_{k+1} \in a_k A a_k \subseteq (P + L)(P + M) \subseteq P + LM$$

Karena $a_{k+1} \notin P$ maka pastilah $LM \not\subseteq P$. Jadi, untuk setiap ideal-ideal dasar $L, M \subseteq A$, jika $L \not\subseteq P$ dan $M \not\subseteq P$ maka $LM \not\subseteq P$, yang ekuivalan jika $LM \subset P$ maka $L \subset P$ atau $M \subset P$. Dengan kata lain, P merupakan ideal dasar prima. Jadi, terbukti bahwa setiap $0 \neq a \in A$ terdapat ideal dasar prima P sehingga $a \notin P$. Artinya, $\bigcap_{P \in \mathfrak{I}_S} P = \{0\}$, yaitu irisan semua ideal dasar prima di A merupakan ideal nol.

(2 $\Rightarrow$ 3) Andaikan terdapat ideal dasar tak nol I sedemikian sehingga $I^k = \{0\}$ untuk suatu $k \in \mathbb{N}$, artinya I ideal nilpoten. Menurut hipotesis, $I^k = \{0\}$ adalah irisan dari semua ideal prima di A . Hal ini menunjukkan bahwa $I^k = I^{k-1}I \subseteq P$, akibatnya $I \subset P$ untuk setiap ideal dasar prima P , sehingga haruslah $I = \{0\}$ yang kontradiksi dengan $I \neq \{0\}$. Jadi, setiap ideal dasar tak nol bukan merupakan ideal nilpotent.

(3 $\Rightarrow$ 4) Ambil sebarang $x \in X$ dengan X pembangun berhingga dari A , maka menurut persamaan (20), ideal (x) merupakan ideal dasar dan $(x) \neq \{0\}$. Karena setiap ideal tak nol bukan ideal nilpotent maka $(x)^2 \neq \{0\}$.

Andaikan terdapat $x \in X$ sedemikian sehingga $xAx = \{0\}$ maka $xax = 0$ untuk setiap $a \in A$. Ambil sebarang $y \in (x)^2$ maka $y = (pxq)(rxs)$ untuk suatu p, q, r, s di A , sehingga $y = px(qr)xs = p\{xax\}s = p0s = 0$ dengan $a = qr \in A$. Jadi, setiap $y \in (x)^2$ maka $y = 0$. Dengan kata lain, $(x)^2 = \{0\}$ yang kontradiksi dengan $(x)^2 \neq \{0\}$. Terbukti bahwa setiap $x \in X, xAx \neq \{0\}$.

(4 $\Rightarrow$ 1) Ambil sebarang ideal tak nol S di $A = \langle X \rangle$. Berdasarkan Lemma 4.1.3, poin 3), $S = \langle X_S \rangle$ dengan $X_S = X \cap S$. Ambil sebarang $s \in X_S$ maka $s \in X$, dengan $sas \neq 0$ untuk suatu $a \in A$ dari yang diketahui. Selain itu, $s \in S$ sehingga

$$0 \neq sas = (1_A sa)(1_A s 1_A) \in S^2$$

Diperoleh bahwa $S^2 \neq \{0\}$, sehingga, kuadrat dari setiap ideal dasar tak nol di A , juga tak nol. Dengan kata lain, $\{0\}$ merupakan ideal dasar semiprima di A atau aljabar dibangun secara berhingga A merupakan aljabar semiprima mendasar.

Perhatikan $\mathbb{Z}$ -aljabar $\mathcal{M} = \left[\begin{pmatrix} \mathbb{Z}_{256} & \mathbb{Z}_{256} \\ \mathbb{Z}_{256} & \mathbb{Z}_{256} \end{pmatrix}, \begin{pmatrix} \mathbb{Z}_6 & \mathbb{Z}_6 \\ 0 & \mathbb{Z}_6 \end{pmatrix} \right]$ pada Contoh 4.1.5

adalah aljabar dibangun secara berhingga yang tidak semiprima mendasar, karena terdapat elemen pembangun $P = \left[\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right]$ sehingga $PAP = \{0\}$. Hal ini disebabkan, setiap $M = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} p & q \\ 0 & r \end{pmatrix} \right] \in A$, $PMP = \left[\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right]$.

Menurut Akibat 4.2.2, aljabar $\mathcal{M}$ bukanlah aljabar semiprima.

Kajian tentang karakterisasi aljabar dibangun secara berhingga atas ring komutatif unital ini dapat diterapkan dalam kriptografi. Aplikasi kriptografi dalam penelitian ini dikhususkan pada skema autentikasi atau lebih khusus pada pengamanan autentikasi identitas digital, yang akan dibahas pada bagian di bawah ini.

C. Terapan ideal dasar semiprima dan aljabar semiprima mendasar pada pengamanan autentikasi identitas digital

Lal dan Chaturwedi (2005) mengembangkan sebuah protokol autentikasi identitas digital berdasarkan masalah dekomposisi atas ring non-komutatif. Penggunaan ring non-komutatif ini dapat digeneralisasi pada ideal dasar semiprima dari R -aljabar non-komutatif yang dibangun secara hingga atas suatu ring komutatif dengan elemen satuan.

Berdasarkan langkah-langkah protokol autentikasi yang dikembangkan oleh Lal dan Chaturwedi (2005) dalam Gambar 5, protokol autentikasi tersebut dikembangkan sehingga dapat diterapkan pada ideal dasar semiprima sebagai

berikut. Dalam hal ini, Alice adalah pihak pembukti (prover), yang akan melegitimasi identitasnya kepada Bob sebagai pihak verifikator.

1. Alice memilih dan mempublikasikan sebuah ideal dasar semiprima J pada suatu aljabar yang dibangun secara hingga A atas ring komutatif dengan elemen satuan R , dan sebuah elemen $a \in A$.
2. Alice memilih $w \in J$ dan bilangan asli $m, n \in \mathbb{N}$, kemudian Alice menghitung $t = a^m w a^n$.
3. Alice mengirimkan w dan t kepada Bob.
4. Bob memilih secara rahasia bilangan asli $u, v \in \mathbb{N}$, kemudian Bob menghitung $w' = a^u w a^v$.
5. Bob mengirimkan w' sebagai tantangan (challenge) untuk Alice.
6. Alice menghitung $w'' = a^m w' a^n$.
7. Alice mengirimkan w'' sebagai respon kepada Bob.
8. Bob melakukan verifikasi apakah $w'' = a^u t a^v$?

Dapat dilihat bahwa

$$\begin{aligned} a^u t a^v &= a^u a^m w a^n a^v = a^{u+m} w a^{n+v} = a^{m+u} w a^{n+v} \\ &= a^m a^u w a^n a^v = a^m w' a^n = w''. \end{aligned}$$

Berikut ini adalah bagan yang dapat menjelaskan alur protokol yang dilakukan oleh Alice dan Bob, dalam proses protokol autentikasi berdasarkan masalah dekomposisi pada ideal dasar semiprima dari R -aljabar non-komutatif yang dibangun secara hingga atas suatu ring komutatif dengan elemen satuan.

Alice memilih dan mempublikasikan sebuah ideal dasar semiprima J pada suatu aljabar yang dibangun secara hingga A atas ring komutatif dengan elemen satuan R , dan sebuah elemen $a \in A$.		
No	Alice	Bob
1	Alice memilih $w \in J$ dan bilangan asli $m, n \in \mathbb{N}$, kemudian Alice menghitung $t = a^m w a^n$	
2	Alice mengirimkan w dan t kepada Bob	
3		Bob menerima w dan t dari Alice
4		Bob memilih bilangan asli $u, v \in \mathbb{N}$, kemudian Bob menghitung $w' = a^u w a^v$
5		Bob mengirimkan w' sebagai tantangan (<i>challenge</i>) untuk Alice
6	Alice menerima tantangan w' dari Bob	
7	Alice merespon tantangan dengan menghitung $w'' = a^m w' a^n$	
8	Alice mengirimkan w'' sebagai respon kepada Bob	
9		Bob menerima respon w'' dari Alice
10		Bob melakukan verifikasi, yaitu verifikasi benar apabila $w'' = a^u t a^v$

Gambar 7. Protokol Autentikasi Berdasarkan Masalah Dekomposisi atas Ideal Dasar Semiprima

Keamanan dari protokol autentikasi pada Gambar 6 diletakkan pada tingkat kesulitan dalam menyelesaikan masalah dekomposisi pada ideal dasar semiprima

dari R -aljabar. Dapat dilihat bahwa pihak ketiga (pihak penyerang) mengetahui paramter publik dan selalu mendapatkan apapun yang dikirimkan oleh Alice dan Bob. Pihak penyerang mengetahui ideal dasar semiprima J pada suatu aljabar yang dibangun secara hingga A atas ring komutatif dengan elemen satuan R , dan sebuah elemen $a \in A$, juga mengetahui nilai t , w' dan w'' . Untuk dapat menyerang protokol autentikasi ini, dapat dilakukan dengan menyelesaikan masalah dekomposisi, yaitu menentukan nilai a^m dan a^n , atau dengan kata lain, menentukan bilangan asli $m, n \in \mathbb{N}$, serta menentukan bilangan asli $u, v \in \mathbb{N}$. Proses perhitungan di protokol autentikasi tersebut dilakukan di ideal dasar semiprima J , sebab $t = a^m w a^n \in J$, $w' = a^u w a^v \in J$ dan $w'' = a^m w' a^n \in J$.

Contoh 4.2.5. Berikut ini diberikan contoh sederhana dari protokol autentikasi berdasarkan masalah dekomposisi atas ideal dasar semiprima.

1. Alice memilih dan mempublikasikan sebuah ideal dasar semiprima

$$J = \left[\begin{pmatrix} \mathbb{Z}_{256} & \mathbb{Z}_{256} \\ \mathbb{Z}_{256} & \mathbb{Z}_{256} \end{pmatrix}, \begin{pmatrix} \mathbb{Z}_4 & \mathbb{Z}_4 \\ 0 & 0 \end{pmatrix} \right]$$

dari aljabar yang dibangun secara hingga $A = \left[\begin{pmatrix} \mathbb{Z}_{256} & \mathbb{Z}_{256} \\ \mathbb{Z}_{256} & \mathbb{Z}_{256} \end{pmatrix}, \begin{pmatrix} \mathbb{Z}_4 & \mathbb{Z}_4 \\ 0 & \mathbb{Z}_4 \end{pmatrix} \right]$ atas

ring $\mathbb{Z}$, dan sebuah elemen $a = \left(\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \right) \in A$.

2. Alice memilih $w = \left(\begin{pmatrix} 8 & 9 \\ 10 & 11 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 0 & 0 \end{pmatrix} \right) \in J$ dan $m = 14, n = 15$, kemudian

Alice menghitung

$$\begin{aligned} t &= \left(\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \right)^{14} \left(\begin{pmatrix} 8 & 9 \\ 10 & 11 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 0 & 0 \end{pmatrix} \right) \left(\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \right)^{15} \\ &= \left(\begin{pmatrix} 1 & 238 \\ 229 & 230 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 0 & 0 \end{pmatrix} \right) \end{aligned}$$

3. Alice mengirimkan $w = \left(\begin{pmatrix} 8 & 9 \\ 10 & 11 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 0 & 0 \end{pmatrix} \right)$ dan

$$t = \left(\begin{pmatrix} 1 & 238 \\ 229 & 230 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 0 & 0 \end{pmatrix} \right) \text{ kepada Bob.}$$

4. Bob memilih $u = 16, v = 17$, kemudian Bob menghitung $w' = a^u w a^v$ yaitu

$$w' = \left(\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \right)^{16} \left(\begin{pmatrix} 8 & 9 \\ 10 & 11 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 0 & 0 \end{pmatrix} \right) \left(\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \right)^{17}$$

$$= \left(\begin{pmatrix} 49 & 142 \\ 213 & 6 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 0 & 0 \end{pmatrix} \right)$$

5. Bob mengirimkan $w' = \left(\begin{pmatrix} 49 & 142 \\ 213 & 6 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 0 & 0 \end{pmatrix} \right)$ sebagai tantangan untuk Alice.

6. Alice merespon dengan menghitung $w'' = a^m w' a^n$, yaitu

$$w'' = \left(\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \right)^{14} \left(\begin{pmatrix} 49 & 142 \\ 213 & 6 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 0 & 0 \end{pmatrix} \right) \left(\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \right)^{15}$$

$$= \left(\begin{pmatrix} 75 & 186 \\ 23 & 98 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 0 & 0 \end{pmatrix} \right)$$

7. Alice mengirimkan $w'' = \left(\begin{pmatrix} 75 & 186 \\ 23 & 98 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 0 & 0 \end{pmatrix} \right)$ sebagai respon kepada Bob.

8. Bob melakukan verifikasi

$$a^u t a^v = \left(\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \right)^{16} \left(\begin{pmatrix} 1 & 238 \\ 229 & 230 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 0 & 0 \end{pmatrix} \right) \left(\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \right)^{17}$$

$$= \left(\begin{pmatrix} 75 & 186 \\ 23 & 98 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 0 & 0 \end{pmatrix} \right) = w''$$

Dapat dilihat bahwa proses verifikasi benar, sehingga Alice berhasil diautentikasi kebenaran identitasnya oleh Bob.

Protokol autentikasi diterapkan pada awal sebuah komunikasi dilakukan. Sebagai contohnya adalah saat seseorang login ke sebuah website, membuka aplikasi *e-commerce*, *e-banking*, hingga Sistem Informasi Akademik. Beberapa contoh tantangan (*challenge*) yang digunakan adalah dengan mengirimkan kode unik yang dikirimkan ke telepon seluler atau email yang pengirimannya dibatasi oleh waktu tertentu. Akan tetapi sesungguhnya yang terjadi di dalam sistem adalah serangkaian protokol autentikasi yang sedang dijalankan antara pihak pengguna (Alice) dan pihak sistem aplikasi (Bob). Berikut ini adalah penerapan

protokol autentikasi identitas digital pada Sistem Informasi Akademik (SIA). Dalam hal ini, user mendaftarkan identitas dirinya kepada Server SIA dengan memilih parameter publik pertama berupa ideal dasar semiprima, aljabar A atas ring komutatif dengan elemen satuan R , serta elemen $a \in A$ dapat dilakukan oleh server SIA.

Server SIA mengetahui data dari user berupa sebuah ideal dasar semiprima J pada suatu aljabar yang dibangun secara hingga A atas ring komutatif dengan elemen satuan R , dan sebuah elemen $a \in A$.		
No	Pengguna (User)	Server SIA
1	User akan masuk ke dalam website Sistem Informasi Akademik. User memilih $w \in J$ dan bilangan asli $m, n \in \mathbb{N}$, kemudian user menghitung $t = a^m w a^n$	
2	User mengirimkan w dan t kepada Server SIA. (Ini adalah proses pengiriman data pendaftaran kepada server SIA)	
3		Server SIA menerima w dan t dari user
4		Server SIA memilih bilangan asli $u, v \in \mathbb{N}$, kemudian Server SIA menghitung $w' = a^u w a^v$ (Data ini disimpan di Server SIA)
5		Server mengirimkan w' sebagai tantangan (<i>challenge</i>) untuk user
6	User menerima tantangan w' dari Server SIA	
7	User merespon tantangan dengan menghitung $w'' = a^m w' a^n$	
8	User mengirimkan w'' sebagai respon kepada Server SIA	
9		Server SIA menerima respon w'' dari user
10		Server melakukan verifikasi, yaitu benar apabila $w'' = a^u t a^v$. Jika verifikasi benar, maka user diizinkan masuk ke dalam Sistem Informasi Akademik.

Gambar 8. Protokol Autentikasi Identitas Digital atas Ideal Dasar Semiprima untuk Sistem Informasi Akademik

BAB V PENUTUP

A. KESIMPULAN

Definisi ideal dasar pada aljabar dibangun secara berhingga atas ring komutatif unital merupakan generalisasi dari ideal dasar dalam aljabar bebas atas ring tersebut. Ideal dasar yang dibangun oleh suatu elemen (sebagai ring) dapat mengkarakterisasi ideal dasar semiprima, yang merupakan generalisasi ideal dasar prima. Salah satu hasil utama penelitian ini adalah Teorema 4.1.7 yaitu syarat perlu dan cukup suatu ideal merupakan ideal dasar semiprima.

Sebagaimana contoh kotra pada Contoh 4.1.5 bahwa ideal semiprima dan ideal dasar semiprima pada aljabar dibangun secara berhingga atas ring komutatif unital, tidak saling bergantung, meskipun didefinisikan secara analog. Artinya, ideal semiprima belum tentu ideal dasar semiprima karena idealnya belum tentu ideal dasar. Sebaliknya, ideal dasar semiprima belum tentu ideal semiprima. Hal ini dikecualikan pada ideal nol yang selalu selalu merupakan ideal dasar. Jika ideal nol merupakan ideal semiprima maka pastilah ideal dasar semiprima, tetapi tidak berlaku sebaliknya. Konsekuensinya, Jika aljabar dibangun secara berhingga bersifat semiprima maka aljabar tersebut semiprima mendasar, namun tidak sebaliknya.

Hasil utama dari penelitian ini adalah syarat perlu dan cukup aljabar dibangun secara berhingga atas ring komutatif unital bersifat semiprima mendasar. Diberikan R -aljabar yang dibangun secara hingga $A = \langle X \rangle$, maka pernyataan-pernyataan berikut ekuivalen.

1. Aljabar A semiprima mendasar
2. Irisan dari semua ideal-ideal dasar prima adalah ideal nol
3. Setiap ideal dasar tak nol merupakan ideal idempotent
4. Setiap $x \in X, xAx \neq \{0\}$

Sifat *nondegenerate* merupakan syarat perlu dan cukup suatu aljabar bersifat semiprima, namun bukan syarat perlu sifat semiprima mendasar pada aljabar dibangun secara berhingga atas ring komutatif unital. Hal ini ditunjukkan oleh

Contoh 4.2.3. Hal penting lain bahwa aljabar semiprima mendasar belum tentu aljabar prima mendasar sebagaimana Contoh 4.2.4, meskipun ideal nol bukan ideal dasar prima tetapi ideal nolnya merupakan irisan semua ideal dasar prima.

Legitimasi kebenaran identitas pada saat seseorang akan masuk ke dalam sistem informasi apapun sangat memerlukan sebuah metode autentikasi yang aman. Melalui proses autentikasi identitas secara digital, pengguna (*user*) harus memberikan suatu parameter publik yang diberikan kepada sistem, kemudian sistem memberikan suatu tantangan (*challenge*) yang harus direspon oleh pengguna, selanjutnya pengguna mengirimkan hasil responnya kepada sistem. Berdasarkan respon yang diterima, sistem dapat memutuskan apakah pengguna ini diberi legitimasi untuk diperbolehkan masuk ke dalam sistem informasi atau tidak berdasarkan tantangan dan respon yang diberikan. Langkah-langkah autentikasi tersebut dinamakan dengan protokol autentikasi. Protokol tersebut melibatkan parameter publik dan rahasia. Oleh karena itu, dibutuhkan konsep kriptografi kunci publik, tingkat keamanannya diletakkan pada masalah matematika yang sulit diselesaikan apabila tidak mengetahui parameter tertentu yang dirahasiakan. Salah satu masalah dalam matematika yang digunakan pada kriptografi kunci publik adalah masalah dekomposisi atas ring non-komutatif. Salah satu ring non-komutatif yang dapat digunakan adalah ideal dasar semiprima dari suatu aljabar atas ring komutatif dengan elemen satuan.

Protokol autentikasi berdasarkan masalah dekomposisi atas ideal dasar semiprima yang diterapkan pada Sistem Informasi Akademik (SIA), dilakukan melewati tahapan-tahapan sebagai berikut.

1. SIA mengetahui data publik dari pengguna berupa sebuah ideal dasar semiprima J dari aljabar yang dibangun secara hingga A atas ring komutatif dengan elemen satuan R , dan sebuah elemen $a \in A$.
2. Pengguna memilih $w \in J$ dan $m, n \in \mathbb{N}$, kemudian dihitung $t = a^m w a^n$. Pengguna mengirimkan w dan t ke SIA.
3. SIA memilih $u, v \in \mathbb{N}$, kemudian SIA menghitung $w' = a^u w a^v$ dan mengirimkan w' sebagai tantangan kepada pengguna.

4. Pengguna merespon tantangan dengan menghitung $w'' = a^m w' a^n$ dan mengirimkan w'' sebagai respon kepada SIA.
5. SIA melakukan verifikasi, yaitu benar apabila $w'' = a^u t a^v$. Jika verifikasi benar, maka pengguna berhasil masuk ke dalam Sistem Informasi Akademik.

Pihak peretas (*hacker*) dapat menyerang protokol autentikasi tersebut dengan cara mendapatkan parameter publik dan apapun yang dikirimkan oleh pengguna dan SIA. Oleh karena itu, peretas dapat melakukannya dengan menyelesaikan masalah dekomposisi atas ideal dasar semiprima, yaitu menentukan nilai $m, n \in \mathbb{N}$ dan $u, v \in \mathbb{N}$.

B. SARAN

Karakterisasi ideal dasar semiprima dan aljabar semiprima mendasar didasarkan pada sifat ideal dasarnya. Sangat mungkin dikembangkan karakterisasi ideal dasar yang lain, antara lain: ideal dasar minimal, maksimal, dan aljabar semisederhana mendasar beserta sifat-sifatnya. Perlu diteliti juga apakah ada keterkaitan antara ideal dasar maksimal dengan ideal dasar prima, dan lain-lain.

Istilah ideal dasar muncul pertama kali pada aljabar lintasan Leavitt atas ring komutatif unital. oleh karenanya karakterisasi ideal dasar dalam aljabar lintasan dan aljabar lintasan Leavitt juga berpeluang untuk dikembangkan lagi.

Diperlukan kajian lebih lanjut tentang tingkat keamanan protokol autentikasi tersebut dengan cara mengkaji masalah dekomposisi atas ideal dasar semiprima dari aljabar atas ring komutatif dengan elemen satuan. Selain itu, perlu dikaji bagaimana cara implementasi protokol autentikasi pada server Sistem Informasi Akademik.

DAFTAR PUSTAKA

- Abrams, G, Ara, P. and Molina, M. S., 2017. *Leavitt path algebras*, SpringerVerlag, London Ltd.
- Adkins, WA., Weintraub, SH., 1999, 2nd. Ed., *Algebra An Approach via Module Theory*, Springer-Verlag, New York.
- Bland, P. E., 2011, *Ring and Their Modules*, Walter de Gruyter GmbH & Co. KG, berlin New-York.
- Diffie, Whitfield dan Hellman, Martin E. 1976. New Directions in Cryptography. *IEEE Transactions on Information Theory*. 22 (6): 644–654
- Dummit, David S. and Foote, Richard M. 2004. *Abstract Algebra Third Edition*. New Jersey: John Wiley and Sons
- Grillet, PA., 2007, 2nd. Ed., *Abstract Algebra*, Springer Science Business Media, LLC, 233 Spring Street, New York.
- Ko, K. H., Lee, S. J., Cheon, J. H, Han, J. W., Kang, J., and Park, C., 2000, New Public-Key Cryptosystem Using Braid Groups, *Advances in Cryptology – CRYPTO*, Lecture Notes in Computer Science 1880, pp. 166–183, Berlin: SpringerLal, S. dan Chaturvedi. 2005, Authentication Schemes Using Braid Groups. Diunduh dari <http://arxiv.org/abs/cs/0507066>.
- Myasnikov Alexei, Vladimir Shpilrain and Alexander Ushakov. 2008. *Group-based Cryptography*. Basel Switzerland: Birkhauser Verlag.
- Menezes A.J., Oorschoot, Paul C. and Vanstone, Scott A., 1996, *Handbook of Applied Cryptography*, Canada: CRC Press.
- Myasnikov Alexei, Vladimir Shpilrain and Alexander Ushakov, 2008, *Group-based Cryptography*. Basel Switzerland: Birkhauser Verlag.
- Shor, P.W., 1997, *Polynomial-time Algorithms for Prime Factorization and Discrete Logarithm on a Quantum Computer*, *SIAM Journal on Computing*, 26(5), pp. 1484- 1509
- Tomforde, M., 2011, *Leavitt Path Algebras with Coefficient in a Commutative Ring*, *J. Pure Appl. Algebra*, 215, 471 – 484.
- Wardati, K., 2018, *Ideal Dasar Prima dalam Aljabar Atas suatu Ring Komutatif*, *Jurnal Fourier*, Vol. 7 No. 2, 79 - 86.
- Wardati, K., Wijayanti, I.E., Wahyuni, S., 2015, *On Free Ideal in Free Algebra over a Ring*, *J. Indones. Math. Soc.*, 21 (1), pp. 59 – 69.

Wisbauer, R., 1991, Foundations of Module and Ring Theory, A handbook for Study and Research, University of Dusseldorf, Gordon and Breach Publisher.

BIOGRAFI SINGKAT PENELITI

1.	Ketua Peneliti Ketua peneliti berlatar belakang Pendidikan S1, S2, S3 pada Jurusan Matematika FMIPA Universitas Gadjah Mada. Penyelesaian program Doktor (S3) pada tahun 2015. Ketua Peneliti berpangkat Pembina IV/b dengan jabatan akademik Lektor Kepala. Kegiatan ilmiah dalam tujuh (7) tahun terakhir terdiri dari : 1. Partisipasi dalam seminar internasional “The 2nd International Conference on Natural Sciences, Mathematics, Application, Research and Technology (ICON-SMART) 2021, dengan judul artikel : The Application of Semiprime Basic Ideals in Authentication Scheme, dan akan dipublikasikan via proceeding AIP terindeks scopus dan WoS (Web of Science) 2. Publikasi karya ilmiah pada Journal Internasional terindeks scopus Q4, “Journal of Algebra and Applied Mathematics” Vol. 19 (2021), No.2, pp.97-114, dengan judul On basically prime non-free algebras over a commutative unital ring 3. Menulis buku “Terapan Grup Matriks Atas Ring Komutatif pada Protokol Perjanjian Kunci” penerbit Graha Ilmu, tahun 2019 4. Berpartisipasi dalam international conference di Almeria, Spain, 13 - 17 Mei 2019 5. Publikasi karya ilmiah pada Journal Internasional terindeks scopus “JP Journal Algebra, Number Theory and Applications”, Volume 39, Number 5., 2017, pp. 671 – 683, dengan judul On Semisimple Leavitt Path Algebras Over A Commutative Unital Ring. 6. Pembicara Utama pada seminar nasional aljabar dan pengajarannya, di Universitas Sanata Dharma, Yogyakarta, September 2016. 7. Mengikuti <i>research School</i> : CIMPA-TURKEY SCHOOL on Leavitt path algebras and graph C^*-algebras, Jun 29 – jul 12, 2015 di Izmir, Turkey, dengan pembiayaan penuh dari organisasi profesi internasional CIMPA . 8. Invited Speaker pada acara internasional “the SEAMS School” with topic “On Some Aspects of Representaton Theory” di Jurusan Matematika FMIPA Universitas Gadjah Mada, Yogyakarta, Indonesia. Nov 09 – 17, 2015. 9. Publikasi karya ilmiah berjudul On Free Ideals In Free Algebras Over A Commutative Ring, pada journal nasional terakreditasi J. Indones. Math. Soc., 21 (1), pp. 59 – 69. 10. Publikasi karya ilmiah pada Journal Internasional terindeks scopus “JP Journal Algebra, Number Theory and Applications”, Volume 34, Number 2., 2014, pp. 121 – 138, dengan judul On Primeness of Path Algebras over Unital Commutative Ring. 11. Kegiatan Sandwich Program at Malaga University for 2 months (Oct 31 – Dec 31, 2014) dengan pembiayaan dari DIKTIS Kemenag
----	--

2.	Anggota Peneliti Anggota peneliti merupakan dosen Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta, dengan keahlian aljabar dan Kriptografi. Tema penelitian skripsi S1 dan tesis S2 adalah Penerapan Aljabar dalam Kriptografi dan Keamanan Informasi di Jurusan Matematika FMIPA Universitas Gadjah Mada. Kegiatan ilmiah dalam 7 tahun terakhir: 1. Peserta seminar internasional “<i>The 2nd International Conference on Natural Sciences, Mathematics, Application, Research and Technology (ICON-SMART) 2021</i>” 2. Peserta Workshop Penelitian Graf Aljabar "Representasi Graf Pada Grup dan Ring" IndoMS-KPA-UIN Jakarta, 6 Februari 2021 3. Publikasi karya ilmiah pada Jurnal Fourier Vol.9 No.2 Tahun 2020 pp.49-58 dengan judul “Kode Linear untuk Deteksi dan Koreksi Kesalahan Penulisan dalam Huruf Hijaiyah” 4. Menulis buku “Terapan Grup Matriks Atas Ring Komutatif pada Protokol Perjanjian Kunci” penerbit Graha Ilmu, 2019 (Penulis Kedua) 5. Peserta Workshop <i>Current Technological Advances in Cryptography</i>, Badan Siber dan Sandi Negara & Universitas Telkom Bandung, 13 November 2019 6. Peserta Workshop <i>on Maxima: A Computer Algebra System</i> by Prof. Jose Antonio Vallejo di Universitas Negeri Yogyakarta, 2-3 Oktober 2019 7. Peserta SEAMS-UGM-ITB <i>Summer Course on Coding Theory and Cryptography</i> di Universitas Gadjah Mada Yogyakarta, 15-26 Juli 2019 8. Narasumber Seminar Nasional Matematika "Kriptografi Kunci Publik dan Keamanan Jaringan Internet" FST UIN Sunan Kalijaga Yogyakarta, 13 November 2018 9. Peserta Workshop <i>on Cryptography and Coding Theory (Quantum Codes and Post-Quantum Cryptography)</i>, Universitas Gadjah Mada Yogyakarta, 12-16 Maret 2018 10. Publikasi karya ilmiah pada Jurnal Fourier Vol.6 No.1 Tahun 2017 pp.1-8 dengan judul “Protokol Otentikasi Berdasarkan Masalah Konjugasi Pada Grup Unit Atas Ring Endomorfisma $END(Z_p \times Z_p^2)$” 11. Narasumber Kuliah Umum Matematika dengan judul: “Mengenal Kriptografi: Ilmu Pengamanan Pesan Rahasia Berbasis Ilmu Matematika” di UIN Walisongo Semarang, 23 Februari 2017. 12. Peserta <i>IACR-SEAMS School on Cryptography: Foundations and New Directions, Vietnam Institute for Advanced Study in Mathematics (VIASM), Hanoi University of Science and Technology, Hanoi – Vietnam, November 27 – December 4, 2016.</i> 13. Peserta <i>CIMPA-ICTP Research School on Lattices and Applications to Cryptography and Coding Theory</i>, Saigon University, Ho Chi Minh City, Vietnam, August 1-12, 2016. 14. Peserta <i>DAAD Spring School on Combinatorial Stochastic Processes, held</i>
----	---

	<i>at Vietnam Institute for Advanced Study in Mathematics (VIASM), Hanoi University of Science and Technology, Hanoi – Vietnam, March 7-18, 2016.</i> 15. Peserta <i>SEAMS School on Algebras and Their Applications (Quantum Physics, Cryptography and Statistics)</i>, INSPEM Universiti Putra Malaysia (UPM) – Malaysia, November 3-10, 2015. 16. Peserta <i>SEAMS School on Number Theory and Applications in Cryptography and Coding Theory</i>, University of Science, Ho Chi Minh City – Vietnam, August 31 – September 8, 2015. 17. Peserta <i>SEAMS School on Module Theory and Its Applications</i>, Institut Teknologi Bandung – Indonesia, November 10-18, 2014.
3.	Anggota peneliti dari unsur mahasiswa adalah mahasiswa Angkatan 2018/2019 yang duduk di semester 7 di prodi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.

RANCANGAN ANGGARAN BIAYA

NO	Jenis Kegiatan		Vol.	Frek.	Satuan	Harga Satuan (RP)	JUMLAH (RP)
A	PRA KEGIATAN						
	FGD Penyempurnaan Proposal dan penyusunan desain penelitian						
	a.	Honor Narasumber	1	3	JPL	900,000	2,700,000
		Sub Total					2,700,000
B	Penguatan Peneliti dengan Seminar Internasional secara daring 2 hari penuh di ICON-SMART Univ Samratulangi						
	a.	Uang Harian					
		1. Ketua Tim Peneliti	1	2	OH	170,000	340,000
		2. Anggota Peneliti	1	2	OH	170,000	340,000
	b.	Uang Pendaftaran Seminar					
		1. Ketua Tim Peneliti (pemakalah)	1	1	Keg.	200,000	200,000
		2. Anggota Peneliti (partisipan)	1	1	Keg.	50,000	50,000
	c.	Fee Publikasi Proceeding Internasional terindeks scopus dan WoS	1	1	Keg.	2,400,000	2,400,000
		Sub Total					3,330,000
C	FGD : syarat perlu dan cukup ideal dasar semiprima dalam aljabar tak bebas						
	a.	Honor Narasumber	1	3	JPL	900,000	2,700,000
		Sub Total					2,700,000
D	FGD :Konstruksi Protokol Autentikasi						
	a.	Honor Narasumber	1	3	JPL	900,000	2,700,000
		Sub Total					2,700,000
E	FGD : pembuktian bahwa suatu aljabar (tak bebas) semiprima mendasar jika dan hanya jika irisan semua ideal dasar prima adalah ideal nol						
	a.	Honor Narasumber	1	3	JPL	900,000	2,700,000
	b.	Honor Moderator	1	1	OK	700,000	700,000
		Sub Total					3,400,000
F	FGD : Pembuktian bahwa sebarang ideal dasar tak nol yang bukan ideal nilpoten dalam aljabar (tak bebas) adalah syarat perlu dan cukup aljabar tersebut bersifat semiprima mendasar						
	a.	Honor Narasumber	1	3	JPL	900,000	2,700,000
	b.	Honor Moderator	1	1	OK	700,000	700,000
		Sub Total					3,400,000

G	FGD : Penghitungan Kunci						
	a.	Honor Narasumber	1	3	JPL	900,000	2,700,000
		Sub Total					2,700,000
I	Analisis Data Penelitian dan Pembantu Peneliti						
	a.	Honor Penganalisis data	1	1	paket	1,540,000	1,540,000
	b.	Honor Pembantu Peneliti	1	160	OJ	25,000	4,000,000
		Sub Total					5,540,000
J	FGD : Desiminasi Hasil Penelitian						
	a.	Honor Narasumber	2	3	JPL	900,000	5,400,000
		Sub Total					5,400,000
K	Honor Transleter dan Proofrideer						
	a.	Honor Transleter	1	12	halaman	250,000	3,000,000
	b.	Honor Proofreader	1	10	halaman	250,000	2,500,000
		Sub Total					5,500,000
L	Konsumsi Diskusi Tim		4	8	OK	25,000	800,000
		Sub Total					800,000
M	Langganan Zoom 100 (Juli - September)		1	3	bln	150,000	450,000
	Langganan Zoom 100 (Oktober - Des)		1	3	bln	100,000	300,000
		Sub Total					750,000
N	Belanja						
	a.	ATK					
		1. Flashdisk Toshiba 16 GB	2	1	buah	100,000	200,000
		2. Tooner Printer	1	1	buah	250,000	250,000
		3. Kertas A4 dan F4	4	1	rim	40,000	160,000
		5. Meterai	24	1	buah	10,000	240,000
		6. Pen Tablet (2 buah, di Els dan Tokopedia)	1	1	Paket	1,000,000	1,000,000
	b.	Laporan dan Dokumentasi					
		1. Fotocopy	2	100	lembar	200	40,000
		2. Jilid	2	1	eksp	15,000	30,000
	c.	Perjalanan Dinas					
		1. PP Yogyakarta - Ternate Pembantu Peneliti	1	1	Tiket	3,360,000	3,360,000
		2. PCR Pembantu Peneliti (berangkat)	1	1	org	490,000	490,000
		3. Antigen (Ketua Peneliti dan Pembantu Peneliti)	2	1	org	100,000	200,000
		4. Uang Harian Ketua Tim Peneliti	1	2	OH	430,000	860,000
		5. Uang Harian Pembantu Peneliti	1	5	OH	430,000	2,150,000
		6. Penginapan Ketua Peneliti	1	2	OH	600,000	1,200,000

	7. Penginapan Pembantu Peneliti	1	5	OH	180,000	900,000
	Sub Total	11,080,000				
	JUMLAH TOTAL					50,000,000

RASIONALISASI PENGGUNAAN ANGGARAN

Kegiatan penelitian ini, dilakukan berdasarkan SK Rektor No. 127.7 tentang Penetapan Judul dan Personalia Penelitian Riset Lider (*Research Leader*) UIN Sunan Kalijaga Yogyakarta, tertanggal 8 Juli 2021 (Lampiran 1). Kegiatan pertama yang memerlukan pembiayaan adalah FGD untuk penyempurnaan proposal. Kegiatan ini diperlukan karena sebenarnya proposal penelitian ini diajukan untuk pendanaan 2020, yang proposalnya dipresentasikan di awal tahun 2020 sebelum masa pandemi Covid 19. Kegiatan FGD ini dilaksanakan 5 Juli (Sebelum TMT SK Penelitian), karena peneliti sudah mendapatkan pengumuman Hasil Seleksi Proposal BOPTN 2020, tanggal 22 Juni 2021 (Lampiran 2). Kegiatan ini diperlukan untuk mendapatkan masukan dan perbaikan perencanaan penelitian (revisi proposal), sesuai poin 1., surat pengumuman tersebut. Narasumber FGD adalah Ibu Dwi Lestari, S.Si., M.Sc. (Dosen pada Prodi Matematika UNY, sedang S3 di UGM) dengan kualifikasi keahlian Matematika Terapan. Terlampir bukti PPT presentasi seminar proposal. (Lampiran 3)

Kegiatan FGD kedua pada tanggal 9 Agustus 2021, dengan menghadirkan narasumber sama, Dwi Lestari S.Si., M.Sc. berkaitan dengan temuan penelitian pertama. Temuan ini tentang syarat perlu dan cukup ideal dasar semiprima dalam aljabar dibangun secara berhingga atas ring komutatif unital. Selain itu, diberikan contoh-contoh kontra yang menunjukkan bahwa ideal dasar semiprima dengan ideal semiprima tidak saling berhubungan satu sama lain, meski definisinya analog. Juga diberikan contoh kontra bahwa ideal dasar semiprima belum tentu ideal dasar prima. Masukan sangat berharga dari narasumber adalah dari hasil temuan ini, yaitu dari contoh tersebut sudah dapat diaplikasikan ke kriptografi. Nah, di sinilah peran anggota peneliti untuk melanjutkan penelitian, sampai uji cobanya.

Aplikasi ideal dasar semiprima dalam kriptografi ini diawali dengan Konstruksi Protokol Autentikasi. Supaya sejak awal tidak ada permasalahan teknis, maka diperlukan FGD ke tiga dengan narasumber sesuai dengan ahlinya dari sisi IT, yaitu M. Miftakhul Akbar, S.Kom, M.Cs. yang dilaksanakan 23 Agustus 2021. Hasil dari FGD ini, kami peneliti bersepakat untuk menyusun artikel yang dipresentasikan dalam international conference.

Pasca FGD ke-3 ini, kami memerlukan bantuan pembantu (asisten) peneliti. Kriteria pembantu peneliti adalah yang memiliki kompetensi di bidang matematika meski tidak dari jurusan matematika, juga terampil dalam pengoperasian MS Office dan Latex. Pekerjaan awal yang dilakukan pembantu peneliti adalah menyusun *extended abstract* berbahasa Indonesia dan bantuan transleter untuk mengalih Bahasa Inggris. Namun, draft tersebut masih perlu disempurnakan dengan penyesuaian template *extended abstract* pada The 2nd International Conference on Natural Science, Mathematics, Applications, Research and Technology (ICON-SMART) 2021, Universitas Samratulangi Manado, Sulawesi Utara..

Selama bulan September, selain FGD ke-4 berkaitan dengan penghitungan kunci (narsum : M. Miftakhul Akbar, S.Kom, M.Cs), peneliti fokus menulis artikel dari hasil awal ini, dengan naskah berbahasa Indonesia. Naskah ini perlu dialihbahasa Inggris oleh transleter (Muhammad Fakhurrifqi, M.Cs.) dan secara substansi memerlukan proofreader, yaitu narasumber pertama yang sesuai ke ahliannya Matematika Terapan. (draft naskah hasil alih Bahasa *extended abstract* dan *full paper* pada lampiran 4). Penghitungan kunci membutuhkan analisis data menggunakan matlab, sehingga kami memerlukan penganalisis data tersebut.

Sebagian hasil penelitian, yaitu ditemukannya syarat perlu dan cukup ideal dasar semiprima dalam aljabar dibangun secara berhingga beserta terapannya ini, dipresentasikan pada tanggal 21-22 Oktober 2021 di ICON-SMART 2021 oleh ketua tim peneliti. Salah satu anggota tim peneliti tetap berkontribusi pada ICON-SMART sebagai participant. Selama 2 hari ini, kami berdua secara online mengikuti kegiatan tersebut, agar dapat meningkatkan kinerja penelitian.

Alokasi waktu terbanyak dari pembantu peneliti adalah pada bulan oktober, mulai membuat PPT Bimer, pembuatan video presentasi di ICON-SMART (https://drive.google.com/file/d/1TIUtjbuTpq_IJEUWsb7zoZAlZQozjFIE/view?usp=sharing) sampai dengan penyesuaian template artikel. Penyesuaian template draft artikel ke ICON-SMART seperti dua kali kerja. artikel berbahasa Indonesia mengikuti template ICSE (International Conference on Science and Technology, 2021) Fakultas Saintek UIN Sunan Kalijaga Yogyakarta. Ketika proses translate ke Bahasa Inggris, kami mendapat masukan untuk tidak submit ke ICSE karena dikhawatirkan pengakuan PAK nantinya tidak dinilai penuh karena publikasi di rumah sendiri. Oleh karena itu, peneliti pindah Haluan ke ICON_SMART ini, dan sementara submit *full paper* nya terakhir 29 Oktober 2021.

Ketua tim peneliti bersama pembantu peneliti berkesempatan ke Universitas Khairun (Unkhair), Ternate Maluku Utara, 5 – 9 November 2021. Kesempatan ini berawal dari undangan untuk mengikuti konggres FDTI (Forum Dekan Teknik Indonesia) 5 – 7 November 2021 diselenggarakan oleh Fakultas Teknik Unkhair, karena ketua peneliti sekaligus sebagai Dekan Fakultas Sains dan Teknologi. Tanggal 8 – 9 November kami memanfaatkan untuk kuliah tamu sekaligus FGD presentasi hasil penelitian di PMIPA Unkhair, dengan narasumber Ida Kurnia Waliyanti, M.Sc. (Mhs akhir S3 Matematika UGM, bidang Aljabar, CV pada Lampiran 5.). Transport PP, tes PCR berangkat, hotel 2 malam uang harian 3 hari (5 – 7 November) ketua peneliti ditanggung UIN Sunan Kalijaga. Sementara, hotel 2 malam (7 – 9 November), uang harian ketua peneliti 2 hari (8 – 9 November), dan tiket pesawat pp Jogja – Ternate, tes PCR berangkat, penginapan non hotel serta uang harian pembantu peneliti selama 5 hari ditambah tes antigen pulang 2 orang (ketua tim dan pembantu peneliti), ditanggung dari dana penelitian ini. Hal ini, membuktikan bahwa tidak ada double account dalam pertanggungjawaban keuangan ini.

Submit *full paper* yang terakhir 29 Oktober 2021 ini untuk menentukan apakah artikel layak untuk dipublikasikan di proceeding terindeks scopus atau proceeding regular. Selanjutnya, selain membuat PPT dan juga membuat flyer kuliah tamu di awal bulan November untuk acara di PMIPA Unkhair, pembantu

peneliti mengerjakan penyesuaian artikel pada template AIP proceeding, merevisi dari masukan reviewer 1, cek turnitin dan revisi penyesuaian penulisan referensi, membantu revisi dari reviewer 2 sampai tanggal 17 desember, dan submit *final revised* maksimum tanggal 18 Desember.

Kegiatan terakhir FGD adalah desiminasi hasil penelitian secara utuh, pada 7 Desember 2021. (Terlampir PPT Desiminasi, pada Lampiran 6). Kami menghadirkan narasumber dari sisi ahli matematika terapan, Dwi Lestari S.Si., M.Sc., dan sisi IT M. Miftakhul Akbar, S.Kom. M.Cs. secara bersama-sama. (CV narasumber di Lampiran 5)

Hampir semua kegiatan dilaksanakan secara daring, terutama untuk 2 narasumber Dwi Lestari S.Si., M.Sc. dan M. Miftakhul Akbar, S.Kom. M.Cs. Karena seringnya kegiatan pembelajaran dengan daring yang tanpa dokumentasi, maka tidak semua kegiatan daring penelitian kami terdokumentasikan. Hanya beberapa kegiatan daring saja yang terdokumentasikan, selain beberapa kegiatan luring di Ternate. Terlampir dokumentasi kegiatan penelitian (Lampiran 7).

LAMPIRAN – LAMPIRAN

Tahun Anggaran : 2021

No Bukti :

MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Telah terima dari : Kuasa Pengguna Anggaran / Pejabat Pembuat Komitmen/ Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 2.700.000

Terbilang : Dua juta tujuh ratus ribu rupiah

Untuk pembayaran : Honorarium Narasumber a.n. Dwi Lestari M.Sc dalam rangka FGD Penyempurnaan Proposal dan penyusunan desain penelitian dalam Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021 dilaksanakan tanggal 5 Juli 2021 di UIN Sunan Kalijaga Yogyakarta

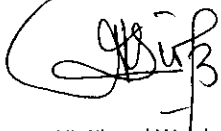
Yogyakarta, 5 Juli 2021

Penerima Uang



Dwi Lestari M.Sc.

Menyetujui,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Daftar Penerimaan Honorarium Narasumber FGD Penyempurnaan Proposal dan penyusunan desain penelitian
Kegiatan Research Leader Strategis UIN Sunan Kalijaga Yogyakarta
Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

No	Nama	Jabatan	Gol	Vol	Satuan	Harga satuan (Rp)	Honorarium (Rp)	15%	6%	5%	Penerimaan (Rp)	Tanda Tangan
1	Dwi Lestari M.Sc.	Narasumber	III	3	JPL	900.000	2.700.000			135.000	2.565.000	1 
Jumlah							2.700.000	-	-	135.000	2.565.000	

Yogyakarta, 5 Juli 2021

Menyetujui,

Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

DAFTAR KEHADIRAN/ABSENSI NARASUMBER

Kegiatan Penelitian berjudul : Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital

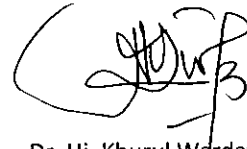
UIN SUNAN KALIJAGA YOGYAKARTA TAHUN ANGGARAN 2021

Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Tanggal: 5 Juli 2021

No	Nama	Waktu	Materi	Tanda Tangan
1.	Dwi Lestari M.Sc.	08.00 - 11.00 WIB	Penyempurnaan Proposal dan penyusunan desain penelitian	

Mengetahui,
Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001



KEMENTERIAN KEUANGAN R.I.
DIREKTORAT JENDERAL PAJAK

CETAKAN KODE
BILLING

NPWP : 68.201.424.6-542.000
NAMA : DRA. HJ KHURUL WARDATI MSI
ALAMAT : DK GANDU, SLEMAN - KAB. SLEMAN

NOP : -
JENIS PAJAK : 411121
JENIS SETORAN : 100
MASA PAJAK : 12-12
TAHUN PAJAK : 2021
NOMOR KETETAPAN : -
JUMLAH SETOR : Rp.135.000
TERBILANG : Seratus Tiga Puluh Lima Ribu Rupiah

URAIAN : FGD Penyempurnaan Proposal dan penyusunan desain penelitian

NPWP PENYETOR : 68.201.424.6-542.000
NAMA PENYETOR : DRA. HJ KHURUL WARDATI MSI

GUNAKAN KODE BILLING DI BAWAH INI UNTUK MELAKUKAN PEMBAYARAN.

ID BILLING : 0259 2172 3806 057
MASA AKTIF : 27/01/2022 14:37:04

PT POS INDONESIA (PERSERO)
Kantor KPC, Yogyakarta Lagondokusuman 55221A

389803107

TANDA TERIMA
Setoran Pajak (MPN Billing)

Tanggal : 30-12-2021 09:12:07
No.Resi : 55221A-10/2021/800889 Petugas : 987446460

Tanggal Buku : 30-12-2021
Kode Cabang Pos : 055000

HTP : 928100585874
NTPN : 74F3567M17G92CB9
STAN : 585874

Waktu Transaksi : 30-12-2021 09:12:09
Kode Billing : 025921723806057
NPWP : 682014246542000
Nama Wajib Pajak: DRA. HJ KHURUL WARDATI MSI
Alamat : DK GANDU, SLEMAN - KAB. SLEMAN
Akun : 411121
Jenis Setoran : 100
Masa Pajak : 12122021
No SK : 0000000000000000
NOP : -
Jumlah Setoran : Rp. 135.000 Mata Uang : IDR
Terbilang : (Seratus tiga puluh lima Ribu Rupiah)

KANTOR POS
POS INDONESIA

Syarat dan ketentuan berlaku
Lacak status : <http://www.posindonesia.co.id>

Tahun Anggaran : 2021

No Bukti :

MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Telah terima dari : Kuasa Pengguna Anggaran / Pejabat Pembuat Komitmen/ Ketua LPPM UIN Sunan Kalijaga Yogyakarta

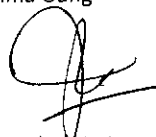
Jumlah Uang : Rp 680.000

Terbilang : Enam ratus delapan puluh ribu rupiah

Untuk pembayaran : Uang harian an. Muhamad Zaki Riyanto, S.Si., M.Sc dkk dalam rangka Seminar Internasional di ICON-SMART Univ Samratulangi tanggal 21-22 Oktober 2021 pada Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

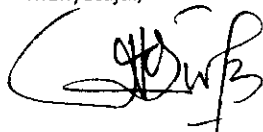
Yogyakarta, 22 Oktober 2021

Penerima Uang



Muhamad Zaki Riyanto, S.Si., M.Sc

Menyetujui,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Daftar Penerimaan Uang Harian
Kegiatan Research Leader Strategis UIN Sunan Kalijaga Yogyakarta
Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

No	Nama	Jabatan	Gol	Vol	Satuan	Harga satuan (Rp)	Uang harian (Rp)	15%	6%	5%	Penerimaan (Rp)	Tanda Tangan
1	Dr. Hj. Khurul Wardati, M. Si	Ketua Tim Peneliti	IV	2	OH	170.000	340.000				340.000	1 
2	Muhamad Zaki Riyanto, S.Si., M.Sc	Anggota Peneliti	III	2	OH	170.000	340.000				340.000	2 
Jumlah							680.000	-	-	-	680.000	

Yogyakarta, 22 Oktober 2021
Menyetujui,
Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

CONFERENCE PAYMENT RECEIPT

Number: CS010

The 2nd International Conference on Natural Sciences,
Mathematics, Applications, Research and Technology (ICON-SMART 2021)

21-22 October 2021

Sam Ratulangi University

Manado, North Sulawesi, Indonesia

Statement Date: 19th October 2021

ICON-SMART 2021 Committee has received the amount of payment: IDR 200,000.00

in words: **Two Hundred Thousand Rupiahs**

from: **Khurul Wardati**

Payment method: Bank Transfer

representing payment of following details:

Description	Participant Name	Amount
Conference Participation Fee as Presenter/Contributed Speaker	Khurul Wardati	IDR 200,000.00
TOTAL:		IDR 200,000.00



CONFERENCE PAYMENT RECEIPT

Number: NCS027

The 2nd International Conference on Natural Sciences,
Mathematics, Applications, Research and Technology (ICON-SMART 2021)

21-22 October 2021

Sam Ratulangi University

Manado, North Sulawesi, Indonesia

Statement Date: 17th October 2021

ICON-SMART 2021 Committee has received the amount of payment: IDR 50,000.00

in words: **Fifty Thousand Rupiahs**

from: **Muhamad Zaki Riyanto**

Payment method: Bank Transfer

representing payment of following details:

Description	Participant Name	Amount
Conference Participation Fee	Muhamad Zaki Riyanto	IDR 50,000.00
TOTAL:		IDR 50,000.00



Tahun Anggaran : 2021

No Bukti :

MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

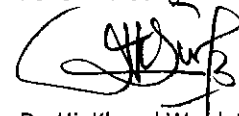
Sudah terima dari : Kuasa Pengguna Anggaran/Pejabat Pembuat Komitmen/Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 2.400.000

Terbilang : Dua juta empat ratus ribu rupiah

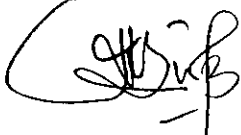
Untuk pembayaran : Biaya Publikasi Proceeding Internasional terindeks scopus dan WoS dalam rangka Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Yogyakarta,
Penerima Uang



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Menyetujui,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001



Transaksi Berhasil

Rekening Tujuan 1252273257
Nama Penerima PANITIA ICON SMART 2
PANITIA
Tanggal Transaksi 09-12-2021
Waktu Transaksi 14:39:11 WIB
Email Penerima
Bank Tujuan BNI
Nama Pengirim KHURUL WARDATI
Nominal 2.400.000
Fee 0
Total 2.400.000
Keterangan Fee AIP Publishing An.
Khurul Wardati

CONFERENCE PAYMENT RECEIPT

Number: CS101

The 2nd International Conference on Natural Sciences,
Mathematics, Applications, Research and Technology (ICON-SMART 2021)

21-22 October 2021

Sam Ratulangi University
Mamado, North Sulawesi, Indonesia

Statement Date: 9th December 2021

ICON-SMART 2021 Committee has received the amount of payment: IDR 2,400,000.00
in words: Two Million and Four Hundred Thousand Rupiahs
from: Khurul Wardati
Payment method: Bank Transfer

representing payment of following details:

Description	Participant Name	Amount
Khurul Wardati	AIP Conference Proceeding	IDR 2,400,000.00
TOTAL:		IDR 2,400,000.00



Ms. Christine Montolalu

Tahun Anggaran : 2021

No Bukti :

MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Telah terima dari : Kuasa Pengguna Anggaran / Pejabat Pembuat Komitmen/ Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 2.700.000

Terbilang : Dua juta tujuh ratus ribu rupiah

Untuk pembayaran : Honorarium Narasumber a.n. Dwi Lestari M.Sc dalam rangka FGD : syarat perlu dan cukup ideal dasar semiprima dalam aljabar tak bebas dalam Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021 dilaksanakan tanggal 9 Agustus 2021 di UIN Sunan Kalijaga Yogyakarta

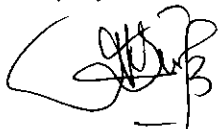
Yogyakarta, 9 Agustus 2021

Penerima Uang



Dwi Lestari M.Sc.

Menyetujui,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

DAFTAR KEHADIRAN/ABSENSI NARASUMBER

Kegiatan Penelitian berjudul : Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital

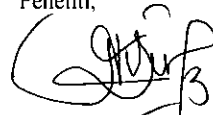
UIN SUNAN KALIJAGA YOGYAKARTA TAHUN ANGGARAN 2021

Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Tanggal: 9 Agustus 2021

No	Nama	Waktu	Materi	Tanda Tangan
1.	Dwi Lestari M.Sc.	08.00 - 11.00 WIB	Syarat perlu dan cukup ideal dasar semiprima dalam aljabar tak bebas	

Mengetahui,
Peneliti,

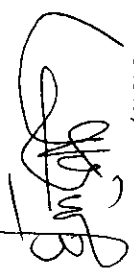


Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Daftar Penerimaan Honorarium Narasumber FGD : syarat perlu dan cukup ideal dasar semiprima dalam aljabar tak bebas
Kegiatan Research Leader Strategis UIN Sunan Kalijaga Yogyakarta
Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

No	Nama	Jabatan	Gol	Vol	Satuan	Harga satuan (Rp)	Honorarium (Rp)	15%	6%	5%	Penerimaan (Rp)	Tanda Tangan
1	Dwi Lestari M.Sc.	Narasumber	III	3	JPL	900.000	2.700.000			135.000	2.565.000	1 
Jumlah							2.700.000	-	-	135.000	2.565.000	

Yogyakarta, 9 Agustus 2021
Menyetujui,
Peneliti,



Dr. Hj. Khurul Wardati, M. SI
NIP. 19660731 200003 2001



KEMENTERIAN KEUANGAN R.I.
DIREKTORAT JENDERAL PAJAK

CETAKAN KODE
BILLING

NPWP : 68.201.424.6-542.000
NAMA : DRA. HJ KHURUL WARDATI MSI
ALAMAT : DK GANDU, SLEMAN - KAB. SLEMAN

NOP : -
JENIS PAJAK : 411121
JENIS SETORAN : 100
MASA PAJAK : 12-12
TAHUN PAJAK : 2021
NOMOR KETETAPAN : -
JUMLAH SETOR : Rp.135.000
TERBILANG : Seratus Tiga Puluh Lima Ribu Rupiah

URAIAN : FGD. : syarat perlu dan cukup ideal dasar semiprima dalam aljabar tak bebas

NPWP PENYETOR : 68.201.424.6-542.000
NAMA PENYETOR : DRA. HJ KHURUL WARDATI MSI

GUNAKAN KODE BILLING DI BAWAH INI UNTUK MELAKUKAN PEMBAYARAN.

ID BILLING : 0259 2172 4844 106
MASA AKTIF : 27/01/2022 14:38:41

PT POS INDONESIA (PERSERO)
Kantor Kpc. Yogyakarta Gondokusuman 55221A
TANDA TERIMA
Setoran Pajak (MPN Billing)

389803108

Tanggal : 30-12-2021 09:12:15
No.Resi : 55221A-10/2021/B00890 Petugas : 987446460

Tanggal Buku : 30-12-2021
Kode Cabang Pos : 055000
NTP : 928135585922
NTPN : 4FCF5588HCTTL22A
STAN : 585922

Waktu Transaksi : 30-12-2021 09:12:17
Kode Billing : 025921724844106
NPWP : 682014246542000
Nama Wajib Pajak : DRA. HJ KHURUL WARDATI MSI
Alamat : DK GANDU, SLEMAN - KAB. SLEMAN
Akun : 411121
Jenis Setoran : 100
Masa Pajak : 12122021
No SK : 0000000000000000
NOP :
Jumlah Setoran : Rp. 135.000 Mata Uang : IDR

Terbilang : (Seratus tiga puluh lima Ribu Rupiah)

KANTOR POS
POS INDONESIA

Syarat dan ketentuan berlaku
Lacak status : <http://www.posindonesia.co.id>

Tahun Anggaran : 2021

No Bukti :

MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Telah terima dari : Kuasa Pengguna Anggaran / Pejabat Pembuat Komitmen/ Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 2.700.000

Terbilang : Dua juta tujuh ratus ribu rupiah

Untuk pembayaran : Honorarium Narasumber a.n. M. Miftakhul Akbar, S.Kom., M.Cs dalam rangka FGD : Konstruksi Protokol Autentikasi dalam Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021 dilaksanakan tanggal 23 Agustus 2021

Yogyakarta, 23 Agustus 2021

Penerima Uang

M. Miftakhul Akbar, S.Kom., M.Cs.

Menyetujui,

Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Daftar Penerimaan Honorarium Narasumber FGD : Konstruksi Protokol Autentikasi
Kegiatan Research Leader Strategis UIN Sunan Kalijaga Yogyakarta
Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

No	Nama	Jabatan	Gol	Vol	Satuan	Harga satuan (Rp)	Honorarium (Rp)	15%	6%	5%	Penerimaan (Rp)	Tanda Tangan
1	M. Miftakhul Akbar, S.Kom., M.Cs.	Narasumber		3	JPL	900.000	2.700.000			135.000	2.565.000	1 
Jumlah							2.700.000	-	-	135.000	2.565.000	

Yogyakarta, 23 Agustus 2021
Menyetujui,
Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

DAFTAR KEHADIRAN/ABSENSI NARASUMBER

Kegiatan Penelitian berjudul : Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital

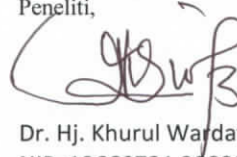
UIN SUNAN KALIJAGA YOGYAKARTA TAHUN ANGGARAN 2021

Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Tanggal: 23 Agustus 2021

No	Nama	Waktu	Materi	Tanda Tangan
1.	M. Miftakhul Akbar, S.Kom., M.Cs.	08.00 - 11.00 WIB	Konstruksi Protokol Autentikasi	

Mengetahui,
Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001



KEMENTERIAN KEUANGAN R.I.
DIREKTORAT JENDERAL PAJAK

CETAKAN KODE
BILLING

NPWP : 68.201.424.6-542.000
NAMA : DRA. HJ KHURUL WARDATI MSI
ALAMAT : DK GANDU, SLEMAN - KAB. SLEMAN

NOP : -
JENIS PAJAK : 411121
JENIS SETORAN : 100
MASA PAJAK : 12-12
TAHUN PAJAK : 2021
NOMOR KETETAPAN : -
JUMLAH SETOR : Rp.135.000
TERBILANG : Seratus Tiga Puluh Lima Ribu Rupiah

URAIAN : FGD :Konstruksi Protokol Autentikasi

NPWP PENYETOR : 68.201.424.6-542.000
NAMA PENYETOR : DRA. HJ KHURUL WARDATI MSI

GUNAKAN KODE BILLING DI BAWAH INI UNTUK MELAKUKAN PEMBAYARAN.

ID BILLING : 0259 2172 5522 057
MASA AKTIF : 27/01/2022 14:39:42

PT POS INDONESIA (PERSERO)
Kantor Kpc. Yogyakarta Gondokusuman 55221A
TANDA TERIMA
Setoran Pajak (MPN Billing)

389803109

Tanggal : 30-12-2021 09:12:23
No.Resi : 55221A-10/2021/800891 Petugas : 987446460

Tanggal Buku : 30-12-2021
Kode Cabang Pos : 055000

NTP : 928173585969
NTPN : 6848A67M17GAM049
STAN : 585969

Waktu Transaksi : 30-12-2021 09:12:25
Kode Billing : 025921725522057
NPWP : 682014246542000
Nama Wajib Pajak: DRA. HJ KHURUL WARDATI MSI
Alamat : DK GANDU, SLEMAN - KAB. SLEMAN
Akun : 411121
Jenis Setoran : 100
Masa Pajak : 12122021
No SK : 0000000000000000
NOP :
Jumlah Setoran : Rp. 135.000 Mata Uang : IDR

Terbilang : (Seratus tiga puluh lima Ribu Rupiah)

Syarat dan ketentuan berlaku

Lacak status : <http://www.posindonesia.co.id>

KANTOR POS
POS INDONESIA

Tahun Anggaran : 2021

No Bukti :

MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Telah terima dari : Kuasa Pengguna Anggaran / Pejabat Pembuat Komitmen/ Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 3.300.000

Terbilang : Tiga juta tiga ratus ribu rupiah

Untuk pembayaran : Honorarium Narasumber dan moderator a.n. Ida Kurnia Waliyanti. M.Sc dkk dalam rangka FGD :
pembuktian bahwa suatu aljabar (tak bebas) semiprima mendasar jika dan hanya jika irisan semua ideal dasar
adalah ideal nol, dalam Kegiatan Penelitian Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul:
"Terapan Aljabar Semiprima Mendasar pada Pengamanan Autentikasi Identitas digital". Berdasarkan SK
Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021 dilaksanakan tanggal 8
November 2021 di JMIPA FKIP Univ Khaerun Ternate.

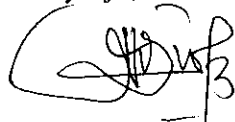
Ternate, 8 November 2021

Penerima Uang



Ida Kurnia Waliyanti. M.Sc

Menyetujui,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2 001

Daftar Penerimaan Honorarium Narasumber dan Moderator
FGD Pembuktian bahwa suatu aljabar (tak bebas) semiprima mendasar jika dan hanya jika irisan semua ideal dasar adalah ideal nol
Kegiatan Penelitian Research Leader UIN Sunan Kalijaga Yogyakarta
Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

No	Nama	Jabatan	Gol	Vol	Satuan	Hari	Harga satuan (Rp)	Honorarium (Rp)	15%	6%	5%	Penerimaan (Rp)	Tanda Tangan
1	Ida Kurnia Walyanti, M.Sc	Narasumber	III	3	JPL	1	900.000	2.700.000			135.000	2.565.000	1 
2	M. Roihan Munajih	Moderator	-	1	OK	1	600.000	600.000			30.000	570.000	2 
Jumlah								3.300.000	-	-	165.000	3.135.000	

Temate, 8 November 2021
Menyetujui,
Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2 001

Daftar Hadir Narasumber, Moderator dan Peserta

FGD : pembuktian bahwa suatu aljabar (tak bebas) semiprima mendasar jika dan hanya jika irisan semua ideal dasar adalah ideal nol

Dalam rangka Kegiatan Penelitian Research Leader UIN Sunan Kalijaga Yogyakarta
Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021
Judul Penelitian : Terapan Aljabar Semiprima Mendasar pada Pengamanan Autentikasi Identitas digital
Hari, Tanggal : Senin, 8 November 2021
Jam : 08.00 - 12.30
Tempat : JMIPA FKIP Univ Khaerun Ternate.

NO	NAMA	JABATAN	PUKUL	TANDA TANGAN
1	Ida Kurnia Waliyanti. M.Sc	Narasumber	09.00 - 12.00	1
2	M. Roihan Munajih	Moderator	08.00 - 12.30	2
3	Dr. Hj. Khurul Wardati, M. Si	Peneliti	08.00 - 12.30	3
7	ABDUL FAZID. TADAPUS	Peserta	08.00 - 12.30	4
8	Dwi Yuliyanti Asmar	Peserta	08.00 - 12.30	5
9	Ismaharini Umaternate	Peserta	08.00 - 12.30	6
10	Hajrah Nabib. Piti	Peserta	08.00 - 12.30	7
11	Deyatna Umasangaji	Peserta	08.00 - 12.30	8
12	Fadimah Ayu	Peserta	08.00 - 12.30	9
13	M. Sorbandrio D	Peserta	08.00 - 12.30	10
14	APRILIA. PANGEMANGEN	Peserta	08.00 - 12.30	11
15	RAFIA SAPSWHA	Peserta	08.00 - 12.30	12
16	AFRIYANTI UMAR	Peserta	08.00 - 12.30	13
17	NURIDA SANGAJI	Peserta	08.00 - 12.30	14
18	Rauda Iestati Jainal	Peserta	08.00 - 12.30	15
19	SARINI. HAMDATI	Peserta	08.00 - 12.30	16
20	SYARIF HIDAYATULLAH L.	Peserta	08.00 - 12.30	17
21	NOFITA KAMARULLAH	Peserta	08.00 - 12.30	18
22	INDRA NANDALIS PIPA	Peserta	08.00 - 12.30	19
23	SUTİYONO	Peserta	08.00 - 12.30	20
24	Syafrin Muhammad	Peserta	08.00 - 12.30	21
25	Widya A. Sarafuddin	Peserta	08.00 - 12.30	22

Ternate, 8 November 2021

Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2 001



KEMENTERIAN KEUANGAN R.I.
DIREKTORAT JENDERAL PAJAK

CETAKAN KODE
BILLING

NPWP : 68.201.424.6-542.000
NAMA : DRA. HJ KHURUL WARDATI MSI
ALAMAT : DK GANDU, SLEMAN - KAB. SLEMAN

NOP : -
JENIS PAJAK : 411121
JENIS SETORAN : 100
MASA PAJAK : 12-12
TAHUN PAJAK : 2021
NOMOR KETETAPAN : -
JUMLAH SETOR : Rp.170.000
TERBILANG : Seratus Tujuh Puluh Ribu Rupiah

URAIAN : FGD : pembuktian bahwa suatu aljabar (tak bebas) semiprima mendasar jika d

NPWP PENYETOR : 68.201.424.6-542.000
NAMA PENYETOR : DRA. HJ KHURUL WARDATI MSI

GUNAKAN KODE BILLING DI BAWAH INI UNTUK MELAKUKAN PEMBAYARAN.

ID BILLING : 0259 2172 6085 111
MASA AKTIF : 27/01/2022 14:40:36

PT POS INDONESIA (PERSERO)
Kantor Kpc. Yogyakarta Gondokusuman 55221A
389803110
TANDA TERIMA
Setoran Pajak (MPN Billing)

Tanggal : 30-12-2021 09:12:37
No.Resi : 55221A-10/2021/800892 Petugas : 987446460

Tanggal Buku : 30-12-2021
Kode Cabang Pos : 055000
Waktu Transaksi : 30-12-2021 09:12:39
Kode Billing : 025921726085111
NPWP : 682014246542000
Nama Wajib Pajak : DRA. HJ KHURUL WARDATI MSI
Alamat : DK GANDU, SLEMAN - KAB. SLEMAN
Akun : 411121
Jenis Setoran : 100
Masa Pajak : 12122021
No SK : 0000000000000000
NOP : -
Jumlah Setoran : Rp. 170.000 Mata Uang : IDR
Terbilang : (Seratus tujuh puluh ribu Rupiah)

NTP : 928224586031
NTPN : 9A5CD0T52820PTVN
STAN : 586031

Syarat dan ketentuan berlaku
Lacak status : <http://www.posindonesia.co.id>

POS INDONESIA

Tahun Anggaran : 2021

No Bukti :

MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Telah terima dari : Kuasa Pengguna Anggaran / Pejabat Pembuat Komitmen/ Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 3.300.000

Terbilang : Tiga juta tiga ratus ribu rupiah

Untuk pembayaran : Honorarium Narasumber dan moderator a.n. Ida Kurnia Waliyanti. M.Sc dkk dalam rangka FGD : Pembuktian bahwa sebarang ideal dasar tak nol yang bukan ideal nilpoten dalam aljabar (tak bebas) adalah syarat perlu dan cukup aljabar tersebut bersifat semiprima mendasar, dalam Kegiatan Penelitian Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima Mendasar pada Pengamanan Autentikasi Identitas digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021 dilaksanakan tanggal 9 November 2021 di JMIPA FKIP Univ Khaerun Ternate.

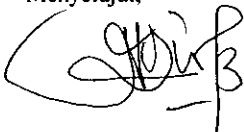
Ternate, 9 November 2021

Penerima Uang



Ida Kurnia Waliyanti. M.Sc

Menyetujui,

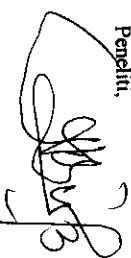


Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2 001

Daftar Penerimaan Honorarium Narasumber dan Moderator
FGD Pembuktian bahwa sebarang ideal tak nol yang bukan ideal nilpoten dalam aljabar (tak bebas) adalah syarat perlu dan cukup aljabar tersebut bersifat semiprima mendasar
Kegiatan Penelitian Research Leader UIN Sunan Kalijaga Yogyakarta
Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

No	Nama	Jabatan	Gol	Vol	Satuan	Hari	Harga satuan (Rp)	Honorarium (Rp)	15%	6%	5%	Penerimaan (Rp)	Tanda Tangan
1	Ida Kurnia Walianti, M.Sc	Narasumber	III	3	JPL	1	900.000	2.700.000			135.000	2.565.000	1 
2	M. Roihan Mumajih	Moderator	-	1	OK	1	600.000	600.000			30.000	570.000	2 
Jumlah												3.135.000	

Ternate, 9 November 2021
Menyetujui,
Peneliti,



Dr. Hj. Khunul Wardah, M. Si
NIP. 19660731 200003 2 001

Daftar Hadir Narasumber, Moderator dan Peserta

FGD : Pembuktian bahwa sebarang ideal dasar tak nol yang bukan ideal nilpoten dalam aljabar (tak bebas) adalah syarat perlu dan cukup aljabar tersebut bersifat semiprima mendasar

Dalam rangka Kegiatan Penelitian Research Leader UIN Sunan Kalijaga Yogyakarta

Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Judul Penelitian : Terapan Aljabar Semiprima Mendasar pada Pengamanan Autentikasi Identitas digital

Hari, Tanggal : Selasa, 9 November 2021

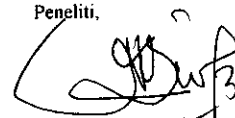
Jam : 08.00 - 12.30

Tempat : JMIPA FKIP Univ Khaerun Ternate.

NO	NAMA	JABATAN	PUKUL	TANDA TANGAN
1	Ida Kumia Waliyanti. M.Sc	Narasumber	09.00 - 12.00	1
2	M. Roihan Munajih	Moderator	08.00 - 12.30	2 ✓
3	Dr. Hj. Khurul Wardati, M. Si	Peneliti	08.00 - 12.30	3
7	FADILA TAMRIM	Peserta	08.00 - 12.30	4
8	NUR AFNI PORA	Peserta	08.00 - 12.30	5
9	NURLAELA M. NUR	Peserta	08.00 - 12.30	6
10	SURILA ARDI	Peserta	08.00 - 12.30	7
11	Nurhasti Muhammad	Peserta	08.00 - 12.30	8
12	RISKA IRWAN	Peserta	08.00 - 12.30	9
13	Dian Sukma Dian Toro	Peserta	08.00 - 12.30	10
14	ATINI AHMAD	Peserta	08.00 - 12.30	11
15	Jumiyati Yamin	Peserta	08.00 - 12.30	12
16	Hariana	Peserta	08.00 - 12.30	13
17	N. Fatahillah Batawi	Peserta	08.00 - 12.30	14
18	DIAR SAPUTRI	Peserta	08.00 - 12.30	15
19	Ayu Safitri Karim	Peserta	08.00 - 12.30	16
20	Sarnawi Kemhay	Peserta	08.00 - 12.30	17
21	Masriyani Labahu	Peserta	08.00 - 12.30	18
22	Fadila Umarangarsi	Peserta	08.00 - 12.30	19
23	SITINUR ALWI	Peserta	08.00 - 12.30	20
24	Sarni Hi. Manuar	Peserta	08.00 - 12.30	21
25	NURJAUHRA. A. DUMATA	Peserta	08.00 - 12.30	22

Ternate, 9 November 2021

Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2 001



KEMENTERIAN KEUANGAN R.I.
DIREKTORAT JENDERAL PAJAK

CETAKAN KODE
BILLING

NPWP : 68.201.424.6-542.000
NAMA : DRA. HJ KHURUL WARDATI MSI
ALAMAT : DK GANDU, SLEMAN - KAB. SLEMAN

NOP : -
JENIS PAJAK : 411121
JENIS SETORAN : 100
MASA PAJAK : 12-12
TAHUN PAJAK : 2021
NOMOR KETETAPAN : -
JUMLAH SETOR : Rp.170.000
TERBILANG : Seratus Tujuh Puluh Ribu Rupiah

URAIAN : FGD : Pembuktian bahwa sebarang ideal dasar tak nol yang bukan ideal nilpot

NPWP PENYETOR : 68.201.424.6-542.000
NAMA PENYETOR : DRA. HJ KHURUL WARDATI MSI

GUNAKAN KODE BILLING DI BAWAH INI UNTUK MELAKUKAN PEMBAYARAN.

ID BILLING : 0259 2172 6794 091
MASA AKTIF : 27/01/2022 14:41:38

PT POS INDONESIA (PERSERO)
Kantor Kpc. Yogyakarta Gondokusuman 55221A
TANDA TERIMA
Setoran Pajak (MPN Billing)

389803111

Tanggal : 30-12-2021 09:12:43
No.Resi : 55221A-10/2021/800893 Petugas : 987446460

Tanggal Buku : 30-12-2021
Kode Cabang Pos : 055000
NTP : 928253586107
NTPN : E044D0T52821FIBB
STAN : 586107

Waktu Transaksi : 30-12-2021 09:12:46
Kode Billing : 025921726794091
NPWP : 682014246542000
Nama Wajib Pajak: DRA. HJ KHURUL WARDATI MSI
Alamat : DK GANDU, SLEMAN - KAB. SLEMAN
Akun : 411121
Jenis Setoran : 100
Masa Pajak : 12122021
No SK : 0000000000000000
NOP :
Jumlah Setoran : Rp. 170.000 Mata Uang : IDR
Terbilang : (Seratus tujuh puluh KANTOR POS POS INDONESIA

Syarat dan ketentuan berlaku
Lacak status : <http://www.posindonesia.co.id>

Tahun Anggaran : 2021

No Bukti :

MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Telah terima dari : Kuasa Pengguna Anggaran / Pejabat Pembuat Komitmen/ Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 2.700.000

Terbilang : Dua juta tujuh ratus ribu rupiah

Untuk pembayaran : Honorarium Narasumber a.n. M. Miftakhul Akbar, S.Kom., M.Cs dalam rangka FGD : Penghitungan Kunci dalam Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021 dilaksanakan tanggal 14 September 2021

Yogyakarta, 14 September 2021

Penyerah Uang

M. Miftakhul Akbar, S.Kom., M.Cs.

Menyetujui,

Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Daftar Penerimaan Honorarium Narasumber FGD : Penghitungan Kunci
Kegiatan Research Leader Strategis UIN Sunan Kalijaga Yogyakarta
Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

No	Nama	Jabatan	Gol	Vol	Satuan	Harga satuan (Rp)	Honorarium (Rp)	15%	6%	5%	Penerimaan (Rp)	Tanda Tangan
1	M. Miftakhul Akbar, S.Kom., M.Cs.	Narasumber		3	JPL	900.000	2.700.000			135.000	2.565.000	1
Jumlah							2.700.000	-	-	135.000	2.565.000	

Yogyakarta, 14 September 2021
Menyetujui,
Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

DAFTAR KEHADIRAN/ABSENSI NARASUMBER

Kegiatan Penelitian berjudul : Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital

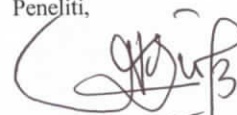
UIN SUNAN KALIJAGA YOGYAKARTA TAHUN ANGGARAN 2021

Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Tanggal: 14 September 2021

No	Nama	Waktu	Materi	Tanda Tangan
1.	M. Miftakhul Akbar, S.Kom., M.Cs.	08.00 - 11.00 WIB	Penghitungan Kunci	

Mengetahui,
Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001



KEMENTERIAN KEUANGAN R.I.
DIREKTORAT JENDERAL PAJAK

CETAKAN KODE
BILLING

NPWP : 68.201.424.6-542.000
NAMA : DRA. HJ KHURUL WARDATI MSI
ALAMAT : DK GANDU, SLEMAN - KAB. SLEMAN

NOP : -
JENIS PAJAK : 411121
JENIS SETORAN : 100
MASA PAJAK : 12-12
TAHUN PAJAK : 2021
NOMOR KETETAPAN : -
JUMLAH SETOR : Rp.135.000
TERBILANG : Seratus Tiga Puluh Lima Ribu Rupiah

URAIAN : FGD : Penghitungan Kunci

NPWP PENYETOR : 68.201.424.6-542.000
NAMA PENYETOR : DRA. HJ KHURUL WARDATI MSI

GUNAKAN KODE BILLING DI BAWAH INI UNTUK MELAKUKAN PEMBAYARAN.

ID BILLING : 0259 2172 7259 120
MASA AKTIF : 27/01/2022 14:42:20

PT POS INDONESIA (PERSERO)
Kantor Kpc, Yogiakartagondokusuman 55221A
TANDA TERIMA
Setoran Pajak (MPN Billing)

389803112

Tanggal : 30-12-2021 09:12:49
No.Resi : 55221A-10/2021/800894 Petugas : 987446460

Tanggal Buku : 30-12-2021
Kode Cabang Pos : 055000
NTP : 928294586163
NTPN : 2FAFF00NIDFLGDFG
STAN : 586163

Waktu Transaksi : 30-12-2021 09:12:52
Kode Billing : 025921727259120
NPWP : 682014246542000
Nama Wajib Pajak : DRA. HJ KHURUL WARDATI MSI
Alamat : DK GANDU, SLEMAN - KAB. SLEMAN
Alan : 411121
Jenis Setoran : 100
Masa Pajak : 12122021
No SK : 0000000000000000
MCP :
Jumlah Setoran : Rp. 135.000 Mata Uang : IDR
Terbilang : (Seratus tiga puluh lima Ribu)

KANTOR POS
POS INDONESIA

Syarat dan ketentuan berlaku
Lacak status : <http://www.posindonesia.co.id>

Tahun Anggaran : 2021

No Bukti :

MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Telah terima dari : Kuasa Pengguna Anggaran / Pejabat Pembuat Komitmen/ Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 1.540.000

Terbilang : *Satu juta lima ratus empat puluh ribu rupiah*

Untuk pembayaran : Honorarium Pengolah Data a.n. M. Miftakhul Akbar, S.Kom., M.Cs dalam rangka Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Yogyakarta, 5 Oktober 2021

Penerima Uang

M. Miftakhul Akbar, S.Kom., M.Cs

Menyetujui,

Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Daftar Penerimaan Honorarium Pengolah Data
Kegiatan Research Leader Strategis UIN Sunan Kalijaga Yogyakarta
Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

No	Nama	Jabatan	Gol	Vol	Satuan	Harga satuan (Rp)	Honorarium (Rp)	15%	6%	5%	Penerimaan (Rp)	Tanda Tangan
1	M. Miftakhul Akbar, S.Kom., M.Cs.	Pengolah data		1	OK	1.540.000	1.540.000			77.000	1.463.000	1
		Jumlah					1.540.000	-	-	77.000	1.463.000	

Yogyakarta, 5 Oktober 2021
Menyetujui,
Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Tahun Anggaran : 2021

No Bukti :

MAK : 2132.BE1.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Telah terima dari : Kuasa Pengguna Anggaran / Pejabat Pembuat Komitmen/ Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 4.000.000

Terbilang : Empat juta rupiah

Untuk pembayaran : Honorarium Pembantu Peneliti a.n. M. Rouhun Munajih dalam rangka Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021 dilaksanakan sejak 23 Agustus sampai dengan 17 Desember 2021

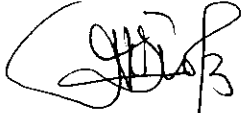
Yogyakarta, 17 Desember 2021

Penerima Uang



M. Rouhun Munajih

Menyetujui,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Daftar Penerimaan Honorarium Pembantu Peneliti
Kegiatan Research Leader Strategis UIN Sunan Kalijaga Yogyakarta
Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

No	Nama	Jabatan	Gol	Vol	Satuan	Harga satuan (Rp)	Honorarium (Rp)	15%	6%	5%	Penerimaan (Rp)	Tanda Tangan
1	M. Rouhun Munajih	Pembantu Peneliti		40	01	100.000	4.000.000			200.000	3.800.000	1
Jumlah							4.000.000	-	-	200.000	3.800.000	

Yogyakarta, 17 Desember 2021
Menyetujui,
Peneliti,



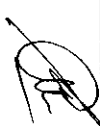
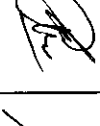
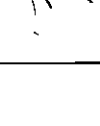
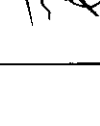
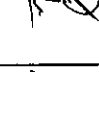
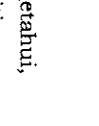
Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

DAFTAR HADIR PEMBANTU PENELITIAN

Dalam rangka Kegiatan Research Leader Strategis UIN Sunan Kalijaga Yogyakarta

Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Judul Penelitian : Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital

NO	NAMA	TANGGAL DAN TANDA TANGAN											
		23-Aug-21	24-Aug-21	25-Aug-21	26-Aug-21	27-Aug-21	4-Oct-21	5-Oct-21	6-Oct-21	7-Oct-21	8-Oct-21		
1	M. Rouhun Munajih												
													
													
													
													
													

Mengetahui,
Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001



KEMENTERIAN KEUANGAN R.I.
DIREKTORAT JENDERAL PAJAK

CETAKAN KODE
BILLING

NPWP : 68.201.424.6-542.000
NAMA : DRA. HJ KHURUL WARDATI MSI
ALAMAT : DK GANDU, SLEMAN - KAB. SLEMAN

NOP : -
JENIS PAJAK : 411121
JENIS SETORAN : 100
MASA PAJAK : 12-12
TAHUN PAJAK : 2021
NOMOR KETETAPAN : -
JUMLAH SETOR : Rp.277.000
TERBILANG : Dua Ratus Tujuh Puluh Tujuh Ribu Rupiah

URAIAN : Analisis Data Penelitian dan Pembantu Peneliti

NPWP PENYETOR : 68.201.424.6-542.000
NAMA PENYETOR : DRA. HJ KHURUL WARDATI MSI

GUNAKAN KODE BILLING DI BAWAH INI UNTUK MELAKUKAN PEMBAYARAN.

ID BILLING : 0259 2172 7695 119
MASA AKTIF : 27/01/2022 14:43:04

PT POS INDONESIA (PERSERO)
Kantor Kpc. Yogyakarta Gondokusuman 55221A
389803113
TANDA TERIMA
Setoran Pajak (MPN Billing)

Tanggal : 30-12-2021 09:12:56
No. Resi : 55221A-10/2021/800895 Petugas : 987446460

Tanggal Buku : 30-12-2021
Kode Cabang Pos : 035000
NTP : 928315586191
NTPN : 28CBF80H0SL5J28F
STAN : 586191

Waktu Transaksi : 30-12-2021 09:12:58
Kode Billing : 025921727695119
NPWP : 682014246542000
Nama Wajib Pajak : DRA. HJ KHURUL WARDATI MSI
Alamat : DK GANDU, SLEMAN - KAB. SLEMAN
Akun : 411121
Jenis Setoran : 100
Masa Pajak : 12122021
No SK : 0000000000000000
NOP :
Jumlah Setoran : Rp. 277.000 Mata Uang : IDR
Terbilang : (Dua ratus tujuh puluh KANTOR POS

Syarat dan ketentuan berlaku
Lacak status : <http://www.posindonesia.co.id>

Tahun Anggaran : 2021

No Bukti :

MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Telah terima dari : Kuasa Pengguna Anggaran / Pejabat Pembuat Komitmen/ Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 5.400.000

Terbilang : Lima juta empat ratus ribu rupiah

Untuk pembayaran : Honorarium Narasumber a.n. Dwi Lestari M.Sc dkk dalam rangka FGD : Desiminasi Hasil Penelitian dalam Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021 dilaksanakan tanggal 7 Desember 2021

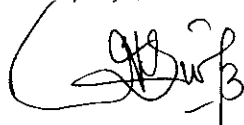
Yogyakarta, 7 Desember 2021

Penerima Uang



Dwi Lestari M.Sc

Menyetujui,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Daftar Penerimaan Honorarium Narasumber FGD : Desiminasi Hasil Penelitian
Kegiatan Research Leader Strategis UIN Sunan Kalijaga Yogyakarta
Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

No	Nama	Jabatan	Gol	Vol	Satuan	Harga satuan (Rp)	Honorarium (Rp)	15%	6%	5%	Penerimaan (Rp)	Tanda Tangan
1	Dwi Lestari M.Sc	Narasumber	III	3	JPL	900.000	2.700.000			135.000	2.565.000	1
2	M. Miftakhul Akbar, S.Kom., M.Cs.	Narasumber		3	JPL	900.000	2.700.000			135.000	2.565.000	2
Jumlah							5.400.000	-	-	270.000	5.130.000	

Yogyakarta, 7 Desember 2021
Menyetujui,
Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

DAFTAR KEHADIRAN/ABSENSI NARASUMBER

Kegiatan Penelitian berjudul : Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital

UIN SUNAN KALIJAGA YOGYAKARTA TAHUN ANGGARAN 2021

Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Tanggal: 7 Desember 2021

No	Nama	Waktu	Materi	Tanda Tangan
1	Dwi Lestari M.Sc	08.00 - 11.00 WIB	Desiminasi Hasil Penelitian	
2	M. Miftakhul Akbar, S.Kom., M.Cs.	08.00 - 11.00 WIB	Desiminasi Hasil Penelitian	

Mengetahui,
Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001



KEMENTERIAN KEUANGAN R.I.
DIREKTORAT JENDERAL PAJAK

CETAKAN KODE
BILLING

NPWP : 68.201.424.6-542.000
NAMA : DRA. HJ KHURUL WARDATI MSI
ALAMAT : DK GANDU, SLEMAN - KAB. SLEMAN

NOP : -
JENIS PAJAK : 411121
JENIS SETORAN : 100
MASA PAJAK : 12-12
TAHUN PAJAK : 2021
NOMOR KETETAPAN : -
JUMLAH SETOR : Rp.270.000
TERBILANG : Dua Ratus Tujuh Puluh Ribu Rupiah

URAIAN : FGD : Desiminasi Hasil Penelitian

NPWP PENYETOR : 68.201.424.6-542.000
NAMA PENYETOR : DRA. HJ KHURUL WARDATI MSI

GUNAKAN KODE BILLING DI BAWAH INI UNTUK MELAKUKAN PEMBAYARAN.

ID BILLING : 0259 2172 8706 053
MASA AKTIF : 27/01/2022 14:44:39

PT POS INDONESIA (PERSERO)
Kantor Kpc. Yogyakarta Gondokusuman 55221A
TANDA TERIMA
Setoran Pajak (PPN Billing)

389803114

Tanggal : 30-12-2021 09:13:06
No. Resi : 55221A-10/2021/800896 Petugas : 987446460

Tanggal Buku : 30-12-2021
Kode Cabang Pos : 055000
NTP : 928351586256
NTPN : 345772101T653T65
STAN : 586256

Waktu Transaksi : 30-12-2021 09:13:08
Kode Billing : 025921728706053
NPWP : 682014246542000
Nama Wajib Pajak : DRA. HJ KHURUL WARDATI MSI
Alamat : DK GANDU, SLEMAN - KAB. SLEMAN
Akun : 411121
Jenis Setoran : 100
Masa Pajak : 12122021
No SK : 0000000000000000
NOP :
Jumlah Setoran : Rp. 270.000 Mata Uang : IDR

Terbilang : (Dua ratus tujuh puluh KANTOR POS POS INDONESIA

Syarat dan ketentuan berlaku
Lacak status : <http://www.posindonesia.co.id>

Tahun Anggaran : 2021

No Bukti :

MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Telah terima dari : Kuasa Pengguna Anggaran / Pejabat Pembuat Komitmen/ Ketua LPPM UIN Sunan Kalijaga Yogyakarta

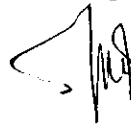
Jumlah Uang : **Rp 3.000.000**

Terbilang : **Tiga juta rupiah**

Untuk pembayaran : Honorarium Transleter a.n. Muhammad Fakhurrirfqi, M.Cs dalam rangka Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

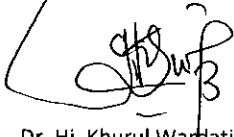
Yogyakarta, 17 Desember 2021

Penerima Uang



Muhammad Fakhurrirfqi, M.Cs

Menyetujui,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Daftar Penerimaan Honorarium Transleter
Kegiatan Research Leader Strategis UIN Sunan Kalijaga Yogyakarta
Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

No	Nama	Jabatan	Gol	Vol	Satuan	Harga satuan (Rp)	Honorarium (Rp)	15%	6%	5%	Penerimaan (Rp)	Tanda Tangan
1	Muhammad Fakhrurriqy, M.Cs	Transleter		12	HLM	250.000	3.000.000			150.000	2.850.000	1 
Jumlah							3.000.000	-	-	150.000	2.850.000	

Yogyakarta, 17 Desember 2021
Menyetujui,
Peneliti,



Dr. Hj. Khuruli Wardati, M. Si
NIP. 19660731 200003 2001

Tahun Anggaran : 2021
No Bukti :
MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Telah terima dari : Kuasa Pengguna Anggaran / Pejabat Pembuat Komitmen/ Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 2.500.000

Terbilang : Dua juta lima ratus ribu rupiah

Untuk pembayaran : Honorarium Proofreader a.n. Dwi Lestari M.Sc dalam rangka Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Yogyakarta, 17 Desember 2021
Penerima Uang



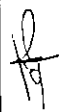
Dwi Lestari M.Sc

Menyetujui,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Daftar Penerimaan Honorarium Proofreader
Kegiatan Research Leader Strategis UIN Sunan Kalijaga Yogyakarta
Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

No	Nama	Jabatan	Gol	Vol	Satuan	Harga satuan (Rp)	Honorarium (Rp)	15%	6%	5%	Penerimaan (Rp)	Tanda Tangan
1	Dwi Lestari M.Sc	Proofreader	III	10	HLM	250.000	2.500.000			125.000	2.375.000	1 
Jumlah							2.500.000	-	-	125.000	2.375.000	

Yogyakarta, 17 Desember 2021
Menyetujui,
Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001



KEMENTERIAN KEUANGAN R.I.
DIREKTORAT JENDERAL PAJAK

CETAKAN KODE
BILLING

NPWP : 68.201.424.6-542.000
NAMA : DRA. HJ KHURUL WARDATI MSI
ALAMAT : DK GANDU, SLEMAN - KAB. SLEMAN

NOP : -
JENIS PAJAK : 411121
JENIS SETORAN : 100
MASA PAJAK : 12-12
TAHUN PAJAK : 2021
NOMOR KETETAPAN : -
JUMLAH SETOR : Rp.275.000
TERBILANG : Dua Ratus Tujuh Puluh Lima Ribu Rupiah

URAIAN : Honor Transleter dan Proofrideer

NPWP PENYETOR : 68.201.424.6-542.000
NAMA PENYETOR : DRA. HJ KHURUL WARDATI MSI

GUNAKAN KODE BILLING DI BAWAH INI UNTUK MELAKUKAN PEMBAYARAN.

ID BILLING : 0259 2172 9299 064
MASA AKTIF : 27/01/2022 14:45:35

PT POS INDONESIA (PERSERO)
Kantor Kpc. Yogyakarta Gondokusuman 55221A
TANDA TERIMA
Setoran Pajak (MPN Billing)

389803115

Tanggal : 30-12-2021 09:13:12
No.Resi : 55221A-10/2021/800897 Petugas : 987446460

Tanggal Buku : 30-12-2021 NTP : 928376586291
Kode Cabang Pos : 055000 NTPN : 879973IDHNP93030
STAN : 586291

Waktu Transaksi : 30-12-2021 09:13:14
Kode Billing : 025921729299064
NPWP : 682014246542000
Nama Wajib Pajak : DRA. HJ KHURUL WARDATI MSI
Alamat : DK GANDU, SLEMAN - KAB. SLEMAN
Akun : 411121
Jenis Setoran : 100
Masa Pajak : 12122021
No SK : 0000000000000000
NOP :
Jumlah Setoran : Rp. 275.000 Mata Uang : IDR

Terbilang : (Dua ratus tujuh puluh lima ribu) **KANTOR POS** POS INDONESIA

Syarat dan ketentuan berlaku
Lacak status : <http://www.posindonesia.co.id>

Tahun Anggaran : 2021

No Bukti :

MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

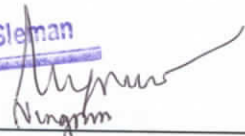
Sudah terima dari : Kuasa Pengguna Anggaran/Pejabat Pembuat Komitmen/Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 800.000

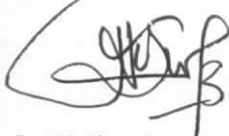
Terbilang : Delapan ratus ribu rupiah

Untuk pembayaran : Konsumsi berupa makan diskusi tim penelitian dalam rangka Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Makan	4	dus	x	8	kali	x	Rp	25.000	=	Rp	800.000
Jumlah										Rp	800.000

Yogyakarta, 17 Desember 2021
Penerima Uang
Catering & Toko Kue
NINGRUM
Manggung CT Depok Sleman


Menyetujui,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Zahri

Catering & Toko Kue

NINGRUM

Alamat:
Manggung RT.03 RW.01 Catur Tunggal Depok Sleman Yogyakarta
No HP: 08995769219

TABLE NO.

Tanggal : 7 Desember 2021

[illegible]

Catering & Toko Kue
NINGRUM
Manggung CT Depok Sleman
Harhat Kami,

Ningmu

Tahun Anggaran : 2021
No Bukti :
MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Sudah terima dari : Kuasa Pengguna Anggaran/Pejabat Pembuat Komitmen/Ketua LPPM UIN Sunan Kalijaga
Yogyakarta

Jumlah Uang : Rp 450.000

Terbilang : Empat ratus lima puluh ribu rupiah

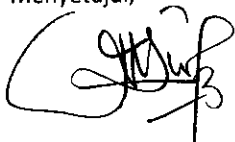
Untuk pembayaran : Langganan Zoom 100 (Juli - September 2021) dalam rangka Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Langganan Zoom 100	1	Keg	x	Rp	450.000	=	Rp	450.000
Jumlah							Rp	450.000

Yogyakarta,
Penerima Uang


M. Roihan Munzir

Menyetujui,



Dr. Hj. Khurul Wafdati, M. Si
NIP. 19660731 200003 2001

INVOICE No. #7841

SEWAZOOMMURAH

Semarang, Jawa Tengah, Indonesia

Instagram : @sewazoommurah

Whatsapp : +6285155088579



NAMA PELANGGAN

Khurul Wardati

085643572794

TANGGAL INVOICE : 2 Juli 2021

KETERANGAN : Penyewaan Zoom

4 Juli 2021

DESKRIPSI	JUMLAH	HARGA SATUAN	HARGA
Sewa Zoom 100 Partisipan Durasi 1 Bulan	2	Rp150,000.00	Rp300,000.00

SEWAZOOMMURAH

Muhammad Abdul Aziz A.

HARGA AWAL Rp300,000.00

DISKON Rp0.00

TOTAL BIAYA Rp300,000.00



CATATAN INVOICE

Invoice ini merupakan bukti pembayaran yang SAH dari SewaZoomMurah
Pengajuan refund HANYA dapat dilakukan H-1 acara

INVOICE No. #7935

SEWAZOOMMURAH

Semarang, Jawa Tengah, Indonesia

Instagram : @sewazoommurah

Whatsapp : +6285155088579



NAMA PELANGGAN

Khurul Wardati

085643572794

TANGGAL INVOICE : 5 Agustus 2021

KETERANGAN : Penyewaan Zoom

Handwritten signature/initials

DESKRIPSI	JUMLAH	HARGA SATUAN	HARGA
Sewa Zoom Meeting 100 Partisipan Durasi 1 Bulan	1	Rp150.000,00	Rp150.000,00

SEWAZOOMMURAH

Muhammad Abdul Aziz A.

HARGA AWAL Rp150.000,00

DISKON Rp0,00

TOTAL BIAYA Rp150.000,00



CATATAN INVOICE

Invoice ini merupakan bukti pembayaran yang SAH dari SewaZoomMurah

Tahun Anggaran : 2021
No Bukti :
MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Sudah terima dari : Kuasa Pengguna Anggaran/Pejabat Pembuat Komitmen/Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 300.000

Terbilang : Tiga ratus ribu rupiah

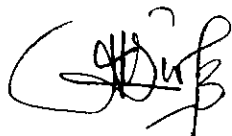
Untuk pembayaran : Langganan Zoom 100 (Oktober - Des 2021) dalam rangka Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Langganan Zoom 100	1	Keg	x	Rp	300.000	=	Rp	300.000
Jumlah							Rp	300.000

Yogyakarta,
Penerima Uang


M. Roihan Munajib

Menyetujui,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Invoice 211211112

JASA SEWA ZOOM

Besalen RT 05 Baturetno Banguntapan Bantul
085725809428



Tanggal
December 1, 2021

Customer
Muhammad Roihan Munajih

Paket	Durasi	Metode Pembayaran	Harga	Total
Zoom A	1 Bulan	Transfer BNI	100.000	100.000
			Total (Rp)	100.000

Terima kasih

Invoice 211211110

JASA SEWA ZOOM

Besalen RT 05 Baturetno Banguntapan Bantul
085725809428



Tanggal
Oktober 4, 2021

Customer
Muhammad Roihan Munajih

Paket	Durasi	Metode Pembayaran	Harga	Total
Zoom A	1 Bulan	Transfer BNI	100.000	100.000
			Total (Rp)	100.000

Terima kasih

Invoice 211211111

JASA SEWA ZOOM

Besalen RT 05 Baturetno Banguntapan Bantul
085725809428



Tanggal
November 2, 2021

Customer
Muhammad Roihan Munajih

Paket	Durasi	Metode Pembayaran	Harga	Total
Zoom A	1 Bulan	Transfer BNI	100.000	100.000
			Total (Rp)	100.000

Terima kasih

Tahun Anggaran : 2021
No Bukti :
MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Sudah terima dari : Kuasa Pengguna Anggaran/Pejabat Pembuat Komitmen/Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 850.000

Terbilang : Delapan ratus lima puluh ribu rupiah

Untuk pembayaran : Pembelian ATK dalam rangka Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

1. Flashdisk Toshiba 16 GB	2 buah x Rp	100.000 = Rp	200.000
2. Tooner Printer	1 buah x Rp	250.000 = Rp	250.000
3. Kertas A4 dan F4	4 rim x Rp	40.000 = Rp	160.000
4. Meterai	24 buah x Rp	10.000 = Rp	240.000
		Rp	850.000

Yogyakarta, 9 Juli 2021
Penerima Uang

Ridwan

Menyetujui,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

PRESTISE

Toko Alat Tulis & Kantor (Melayani Grosir & Eceran)

Jl. Gedongkuning Utara Yogyakarta (087772014188)

Tanggal : 9 Juli 2021

Kepada Yth.

Ibu Khurul W.

No.	Nama Barang	Sebanyak	Harga (Rp.)	Jumlah (Rp.)
1	Flashdisk Toshiba 16 gb	2	100.000	200.000
2	Toner Printer HP	1	250.000	250.000
3	Kertas A4 (RM)	4	40.000	160.000
4	Materai	24	10.000	240.000

Yang Memesan



Terima kasih

()

(Ridwan)

Gross Total Rp.

Diskon %

PPN %

Net Total Rp. 850.000

Barang yang sudah di beli tidak dapat dikembalikan /
ditukar kecuali ada perjanjian terlebih dahulu.

Tahun Anggaran : 2021
No Bukti :
MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Sudah terima dari : Kuasa Pengguna Anggaran/Pejabat Pembuat Komitmen/Ketua LPPM UIN Sunan Kalijaga Yogyakarta

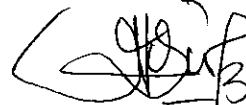
Jumlah Uang : Rp 655.000

Terbilang : Enam ratus lima puluh lima ribu rupiah

Untuk pembayaran : Pembelian Pen tablet dalam rangka Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

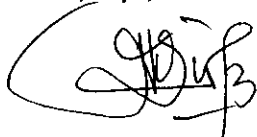
Pen tablet	1	Buah x Rp	655.000 = Rp	655.000
Jumlah			Rp	655.000

Yogyakarta,
Penerima Uang



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Menyetujui,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Tahun Anggaran : 2021
No Bukti :
MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Sudah terima dari : Kuasa Pengguna Anggaran/Pejabat Pembuat Komitmen/Ketua LPPM UIN Sunan Kalijaga Yogyakarta

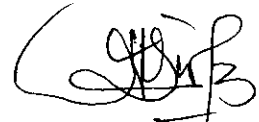
Jumlah Uang : Rp 345.000

Terbilang : *Tiga ratus empat puluh lima ribu rupiah*

Untuk pembayaran : Pembelian Pen tablet dalam rangka Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

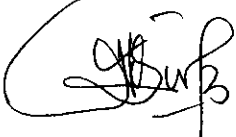
Pen tablet	1	Buah x Rp	348.000	= Rp	348.000
Jumlah				Rp	348.000

Yogyakarta,
Penerima Uang



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Menyetujui,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

tokopedia

Pembayaran

Transfer Manual

Transfer Manual

Ringkasan Pembayaran (1 Invoice)

Total Belanja

- Wisno Grahakom (INV/20210408/MPL/1158725530)

Rp 348.399

Subtotal Belanja

Rp 348.399

Kode Unik (Transfer Manual)

Rp 531

Subtotal Biaya Tambahan

Rp 531

Potensi Cashback Tokopedia

Rp 10.200 (1.020 TokoPoints)

Total Bayar

Rp 348.930

tokopedia

Nomor Invoice : INV/20210408/MPL/1158725530

Diterbitkan atas nama:

Penjual

Wisno Grahakom

Tujuan Pengiriman:

Muhammad Roihan Munajih

[Tokopedia Note: Jl Wonosari km 8,5 Gandubaru
RT07/06 No. 22 Sendangtirta] Berbah Kab. Sleman
55573

D.I. Yogyakarta
6287732652265

Tanggal : 04 Agustus 2021

Nama Produk	Jumlah	Berat	Harga Barang	Subtotal
<u>Pen Tablet Drawing Pad Huion H430P</u>	1	1 kg	Rp 339.999	Rp 339.999
Subtotal Harga Barang				Rp 339.999

Pos Indonesia - Pos Kilat Khusus (Berat: 1 kg) Rp 7.000

Subtotal Ongkos Kirim Rp 7.000

10/10/2010

10/10/2010

ELC
ELECTRONIC LOGIC CONTROLS

10/10/2010

10/10/2010

10/10/2010

10/10/2010

10/10/2010

10/10/2010

10/10/2010

10/10/2010

10/10/2010

10/10/2010

10/10/2010

10/10/2010

10/10/2010

10/10/2010

Tahun Anggaran : 2021
No Bukti :
MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Sudah terima dari : Kuasa Pengguna Anggaran/Pejabat Pembuat Komitmen/Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 70.000

Terbilang : *Tujuh puluh ribu rupiah*

Untuk pembayaran : Fotokopi dan Jilid dalam rangka Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

1. Fotocopy	200	lbr	x	Rp	200	=	Rp	40.000
2. Jilid	2	eks	x	Rp	15.000	=	Rp	30.000
							Rp	70.000

Yogyakarta, 8 Desember 2021
Penerima Uang



Menyetujui,

Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Tahun Anggaran : 2021
No Bukti :
MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

Telah terima dari : Kuasa Pengguna Anggaran / Pejabat Pembuat Komitmen/ Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 3.360.000

Terbilang : Tiga juta tiga ratus enam puluh ribu rupiah

Untuk pembayaran : Transport berupa Tiket Pesawat Udara PP (Pergi-Pulang Yogyakarta (JOG)-Ternate (TTE) pada berangkat tanggal 05 November 2021 dan pulang tanggal 09 November 2021 an. M. Rouhun Munajih (Pembantu Peneliti) dalam rangka Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Yogyakarta, 10 Nopember 2021
Penerima Uang



M. Rouhun Munajih

Menyetujui,

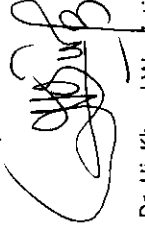


Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Daftar Penerimaan Uang Transport PP (Pergi Pulang) Yogyakarta - Ternate
Kegiatan Research Leader Strategis UIN Sunan Kalijaga Yogyakarta
Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

No	Nama	Jabatan	Gol	Vol	Satuan	Harga satuan (Rp)	Transport (Rp)	15%	6%	5%	Penerimaan (Rp)	Tanda Tangan
1	M. Rouhun Munajih	Pembantu Peneliti		1	OK	3.360.000	3.360.000				3.360.000	1
Jumlah							3.360.000	-	-	-	3.360.000	

Yogyakarta, 22 Oktober 2021
Menyetujui,
Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Bukti Pembayaran

tiket com



Tiket Pesawat

Order ID: 118185427

Detail Pemesan

Nama Lengkap

Mr Muhammad Roihan Munajih

Email

muhammad.roihan.m@mail.ugm.ac.id

Nomor Ponsel

+6287732652265



Detail Pembayaran

Waktu Pembayaran

Rabu, 27 Oktober 2021 - 23:56

Metode Pembayaran

Virtual Account BNI

No.	Produk	Deskripsi	Jumlah	Total
1	Tiket Pesawat	Sriwijaya Air (YIA - TTE) Kode Booking CjEDPE	3	IDR 4.959.000
2	Lainnya	Free Protection	3	IDR 0
			Subtotal	IDR 4.959.000
			Biaya jasa	IDR 11.000
			Diskon	- IDR 45.000

Total Pembayaran

IDR 4.925.000

16-09-2021 / 11

tiket com

PT Global Tiket Network

Jl. Ks. Tubun No.85A, RT.2/RW.7, Slipi, Kec. Palmerah, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta, 11410

Contact Customer Care

+62 804 1500 878 / +62 213 9730 888 +62 858 11500 888

cs@tiket.com

Reservasi Tiket

Bukti Pembayaran

tiket com



Tiket Pesawat

Order ID: 118432666

Detail Pemesan

Nama Lengkap

Mr Muhammad Roihan Munajih

Email

muhammad.roihan.m@mail.ugm.ac.id

Nomor Ponsel

+6287732652265



Detail Pembayaran

Waktu Pembayaran

Sabtu, 6 November 2021 - 12:12

Metode Pembayaran

Virtual Account BNI

No.	Produk	Deskripsi	Jumlah	Total
1	Tiket Pesawat	Batik Air (TTE - YIA) Kode booking: GTX74W	3	IDR 5.154.000
2	Lainnya	Free Protection	3	IDR 0
			Subtotal	IDR 5.154.000
			Biaya jasa	IDR 11.000
Total Pembayaran				IDR 5.165.000

172240146

tiket com

PT Global Tiket Network

Jl. Ks. Tubun No.85A, RT.2/RW.7, Slipi, Kec. Palmerah, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta, 11410

Contact Customer Care

+62 804 1500 878 / +62 213 9730 888 +62 858 11500 888

cs@tiket.com

© 2021 PT Global

PT. LION AIR

Sriwijaya Air
OAG 001 PSES

MOHAMMAD MUHAMMAD



Flight No: 8143 Date: 09 NOV 2018 Time: 06:30

JEDPI

UPG

01

Lion  **air**

Wings  **Air**

Batik  **air**

NAME MUHAMMAD MUHAMMAD DATE 09 NOV
FROM TERNATE H
TO SULTAN HASANUDDIN 34
PNR FJAHKD
GATE
FLIGHT No 6191
SEAT 208
BOARDING TIME 1135
GROUP A

BOARDING GATE CLOSES 10 MINUTES BEFORE DEPARTURE
RUANG TUNGGU TUTUP 10 MENIT SEBELUM JADWAL KEBERANGKATAN

Lion  **air**

Wings  **Air**

Batik  **air**

NAME MUHAMMAD MUHAMMAD DATE 09 NOV
FROM SULTAN HASANUDDIN CLASS Y
TO NEW YOGYAKARTA SEQ 076
PNR GTXZXW
GATE 1
FLIGHT No JT 643
SEAT 36E
BOARDING TIME 1330
GROUP A

BOARDING GATE CLOSES 10 MINUTES BEFORE DEPARTURE
RUANG TUNGGU TUTUP 10 MENIT SEBELUM JADWAL KEBERANGKATAN



**UIN SUNAN KALIJAGA
YOGYAKARTA**

**SURAT TUGAS
NOMOR : B-1973/Un.02/DST/TU.00.1/10/2021**

Dasar	:	1.	Peraturan Direktur Jenderal Perbendaharaan Nomor PER-22/PB/2013 Tentang Ketentuan Lebih Lanjut Pelaksanaan Perjalanan Dinas Dalam Negeri Bagi Pejabat Negara, Pegawai Negeri, dan Pegawai Tidak Tetap.
	:	2.	Surat Edaran No : UIN/02/R.2/KS.02/1426/2013 tentang Mekanisme Penerbitan Surat Perjalanan Dinas (SPD) dan Surat Tugas Perjalanan Dinas.
	:	3.	Surat Keputusan Rektor No : 36 Tahun 2018 tentang Pemberlakuan Sistem Informasi Kearsipan Dinamis (SIKD) atau Tata Persuratan Online dan Penggunaan Sistem Tanda Tangan Elektronik
Memberi Tugas			
Kepada	:	1.	Dr. Dra. Hj. Khurul Wardati, M.Si.
			NIP. 19660731 200003 2 001
			Pembina Tingkat I (IV/B)
			Dekan Fakultas Sains dan Teknologi
	:	2.	Muhammad Rouhun Munajih
			-
			Pembantu Peneliti
Untuk	:	Melaksanakan FGD dan Desiminasi Sebagian Hasil Penelitian pada:	
		Hari	: Jumat s.d Selasa
		Tanggal	: 05 November 2021 s.d 09 November 2021
		Tempat	: FMIPA Universitas Khairun Ternate

Demikian surat tugas ini dibuat untuk dilaksanakan sebagaimana mestinya.



Valid ID: 617915a253eb2p

Sleman, 27 Oktober 2021

Dekan Fakultas Sains dan Teknologi
Khurul Wardati
SIGNED
Sleman

Tembusan :

1. Rektor Universitas Islam Negeri Sunan Kalijaga (sebagai laporan)
2. Kepala Biro Administrasi Umum dan Keuangan
- 3.



UIN SUNAN KALIJAGA
YOGYAKARTA

LAMPIRAN III
PERATURAN DIREKTUR JENDERAL
PERBENDAHARAAN NOMOR PER-22/PB/2013
TENTANG KETENTUAN LEBIH LANJUT
PELAKSANAAN PERJALANAN DINAS DALAM
NEGERI BAGI PEJABAT NEGARA, PEGAWAI NEGERI,
DAN PEGAWAI TIDAK TETAP.

Kementerian Negara/Lembaga:
Kementerian Agama

Lembar Ke :
Kode No : K.I
Nomor : 664/A/2021

Surat Perjalanan Dinas (SPD)

1	Pejabat Pembuat Komitmen	Dekan Fakultas Sains dan Teknologi	
2	Nama/NIP Pegawai yang melaksanakan Perjalanan dinas	Dr. Dra. Hj. Khurul Wardati, M.Si. NIP. 19660731 200003 2 001	
3	a. Pangkat dan Golongan b. Jabatan/Instansi c. Tingkat Biaya Perjalanan Dinas	a. Pembina Tingkat I (IV/B) b. Dekan Fakultas Sains dan Teknologi c. A.I	
4	Maksud Perjalanan Dinas	Melaksanakan FGD dan Desiminasi Sebagian Hasil Penelitian	
5	Alat angkutan yang dipergunakan	Pesawat Udara/Kereta Api/Bus/Taksi/Kendaraan Dinas *)	
6	a. Tempat Berangkat b. Tempat Tujuan	a. Yogyakarta b. Ternate	
7	a. Lamanya Perjalanan Dinas b. Tanggal berangkat c. Tanggal harus kembali/tiba di Tempat baru *)	a. 5 (lima) hari b. 05 November 2021 c. 09 November 2021	
8	Pengikut: Nama	Tanggal Lahir	Keterangan
	1. Muhammad Rouhun Munajih		Pembantu Peneliti
9	Pembebanan Anggaran a. Instansi b. Akun	a. b.	
10	Keterangan lain-lain		

*) Coret yang tidak perlu



Sleman, 27 Oktober 2021
Dekan Fakultas Sains dan Teknologi
Khurul Wardati
SIGNED
Yogyakarta

Valid ID: 617917095176bp



UIN SUNAN KALIJAGA
YOGYAKARTA

LAMPIRAN III
PERATURAN DIREKTUR JENDERAL
PERBENDAHARAAN NOMOR PER-22/PB/2013
TENTANG KETENTUAN LEBIH LANJUT
PELAKSANAAN PERJALANAN DINAS DALAM
NEGERI BAGI PEJABAT NEGERI, PEGAWAI NEGERI,
DAN PEGAWAI TIDAK TETAP.

	I. Berangkat dari : Yogyakarta Ke : Ternate Pada Tanggal : 05 November 2021 Pejabat Pembuat Komitmen Dekan Fakultas Sains dan Teknologi 196607312000032001 Khurul Wardati SIGNED Valid ID: 617917095176bp
II. Tiba di : Ternate Pada Tanggal : 05 November 2021 Kepala : Wakil Dekan II <i>[Signature]</i> Dr. Ade H. Haerullah, S.Pd., M.Si (NIP. 19760120 200312 1 002)	Tiba di : Ternate Pada Tanggal : 09 November 2021 Kepala : Wakil Dekan II <i>[Signature]</i> Dr. Ade H. Haerullah, S.Pd., M.Si (NIP. 19760120 200312 1 002)
III. Tiba di : Pada Tanggal : Kepala : (.....)	Berangkat dari : Ke : Pada Tanggal : Kepala : (.....)
IV. Tiba di : Pada Tanggal : Kepala : (.....)	Berangkat dari : Ke : Pada Tanggal : Kepala : (.....)
V. Tiba di : Yogyakarta Pada Tanggal : 09 November 2021 Pejabat Pembuat Komitmen <i>[Signature]</i> Khurul Wardati	Telaah diperiksa dengan keterangan bahwa perjalanan tersebut atas perintahnya dan semata-mata untuk kepentingan jabatan dalam waktu yang sesingkat-singkatnya Pejabat Pembuat Komitmen <i>[Signature]</i> Khurul Wardati
VI. Catatan Lain-lain	
VII. PERHATIAN PPK yang menerbitkan SPD, pegawai yang melakukan perjalanan dinas, para pejabat yang mengesahkan tanggal berangkat/tiba, serta bendahara pengeluaran bertanggung jawab berdasarkan peraturan-peraturan Keuangan Negara apabila negara menderita rugi akibat kesalahan, kelalaian, dan kealpaannya	

RINCIAN BIAYA PERJALANAN DINAS

Lampiran SPD Nomor
Tanggal

: K.I/664/A/2021
: 5 November 2021

No	Uraian	Biaya	Keterangan
1	Uang harian 5 hari @ Rp430.000,-	Rp 2.150.000	Tgl. 05-09 November 2021
2	Transport Yogyakarta-ternate PP	Rp 3.360.000	Pesawat Udara bukti terlampir
3	Biaya tes Antigen dan PCR	Rp 590.000	Bukti terlampir
4	Biaya penginapan	Rp 900.000	akomodasi 30% daftar terlampir
	Jumlah	Rp 7.000.000	

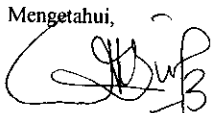
Yogyakarta, 10 November 2021

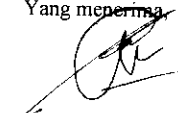
Telah dibayar sejumlah Rp. 7.000.000,-

Telah menerima jumlah uang sebesar Rp. 7.000.000,-

Mengetahui,

Yang menerima,


Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001


M. Rouhun Munajih

RINCIAN BIAYA PERJALANAN DINAS

Lampiran SPD Nomor
Tanggal

: K.I/664/A/2021
: 5 November 2021

No	Uraian	Biaya	Keterangan
1	Uang harian 2 hari @ Rp430.000,-	Rp 860.000	Tgl. 08-09 November 2021
3	Biaya penginapan	Rp 1.200.000	Hotel bukti terlampir
4	Biaya tes Antigen	Rp 100.000	Bukti terlampir
	Jumlah	Rp 2.160.000	

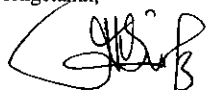
Yogyakarta, 10 November 2021

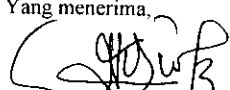
Telah dibayar sejumlah Rp. 2.160.000,-

Telah menerima jumlah uang sebesar Rp. 2.160.000,-

Mengetahui,

Yang menerima,


Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001


Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Tahun Anggaran : 2021
No Bukti :
MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

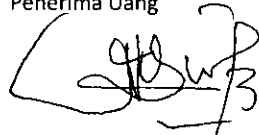
Telah terima dari : Kuasa Pengguna Anggaran / Pejabat Pembuat Komitmen/ Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 690.000

Terbilang : Enam ratus sembilan puluh ribu rupiah

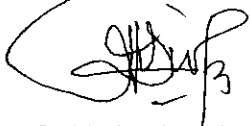
Untuk pembayaran : Biaya tes PCR dan Antigen untuk persyaratan ke Ternate berangkat tanggal 05 November 2021 dan pulang tanggal 09 November 2021 an. Dr. Hj. Khurul Wardati, M. Si dalam rangka Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Yogyakarta, 10 Nopember 2021
Penerima Uang



Dr. Hj. Khurul Wardati, M. Si

Menyetujui,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001



NOTA PEMBAYARAN

No : N-0821K00345



Hai Parahita !
0811 333 21 888

PESAN ONLINE www.labparahita.com
info & promo : @labparahita



SCAN QR CODE

No Lab / Reg : 0821K00345 / A01101555
Nama/Tgl Lahir : Sdr. MUHAMMAD ROUHUN MUNAJIH(L) / 23-05-1997
Tlp. / HP : / 085643380100
Tgl : 03 November 2021
Pengirim : Parahita Jogja Soetomo[120108]
Alamat : GANDU SENDANGTIRTO BERBAH SLEMAN

NO	NAMA PEMERIKSAAN	HARGA	NO	NAMA PEMERIKSAAN	HARGA
1	PCR SARS CoV-2	495,000			

Biaya Pemeriksaan

LUNAS

495,000

NB : - Nota ini harap dibawa saat pengambilan hasil pemeriksaan

- Hasil Pemeriksaan DIAMBIL

- Hasil Selesai

20.00

Tanggal : Jam : Menyusul Tanggal : Jam :

- Pemeriksaan yang tidak dilakukan dalam 14 hari dianggap batal dan uang tidak bisa kembali

Rcpt : ANGGITA LIONI PUTRI

Jogjakarta, 03 November 2021 06:24:15

Printed by : ANGGITA LIONI PUTRI

*** Anda Sehat Kami Bangga ***



LABORATORIUM KLINIK AGUNG AMANAH

Jln. Cempaka No. 722 RT 015 / RW 005 Kel Maliaro, Kec. Ternate Tengah

Kota Ternate, Provinsi Maluku Utara

HP. 0813-5608-5210

Nomor : 162761

Telah Terima dari

Uang Sejumlah

Untuk Pembayaran

: MUHAMMAD ROUHUN MUNAJIH

: Seratus Ribu Rupiah

: Biaya Pemeriksaan Rapid Test Antigen Covid-19 di Laboratorium Klinik Agung Amanah
Ternate Pada Tanggal 08 November 2021

Terbilang : Rp.# 100.000 #

Ternate, 08 November 2021

Yang Menerima

(Kartini M. Ali)



LABORATORIUM KLINIK AGUNG AMANAH

Jln. Cempaka No. 722 RT 015 / RW 005 Kel Maliaro, Kec. Ternate Tengah
Kota Ternate, Provinsi Maluku Utara
HP. 0813-5608-5210

Nomor : 162759
Telah Terima dari
Uang Sejumlah
Untuk Pembayaran

: DRA. HJ. KHURUL WARDATI, M.SI
: Seratus Ribu Rupiah
: Biaya Pemeriksaan Rapid Test Antigen Covid-19 di Laboratorium Klinik Agung Amanah
Ternate Pada Tanggal 08 November 2021

Terbilang : Rp.# 100.000 #

Ternate, 08 November 2021
Yang Menerima


(Kartini M. Ali)

Tahun Anggaran : 2021
No Bukti :
MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

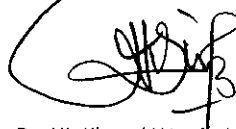
Telah terima dari : Kuasa Pengguna Anggaran / Pejabat Pembuat Komitmen/ Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 3.010.000

Terbilang : Tiga juta sepuluh ribu rupiah

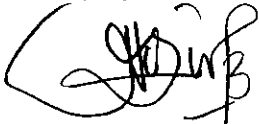
Untuk pembayaran : Uang harian Ketua Tim Peneliti dan Pembantu peneliti dalam perjalanan dinas ke Ternate berangkat tanggal 05 November 2021 dan pulang tanggal 09 November 2021 an. Dr. Hj. Khurul Wardati, M. Si dkk dalam rangka Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Yogyakarta, 10 Nopember 2021
Penerima Uang



Dr. Hj. Khurul Wardati, M. Si

Menyetujui,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Daftar Penerimaan Uang Harian ke Ternate
Kegiatan Research Leader Strategis UIN Sunan Kalijaga Yogyakarta
Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

No	Nama	Jabatan	Gol	Vol	Satuan	Harga satuan (Rp)	Uang harian (Rp)	15%	6%	5%	Penerimaan (Rp)	Tanda Tangan
1	Dr. Hj. Khurul Wardati, M. Si	Ketua Tim Peneliti	IV	2	OH	430.000	860.000				860.000	
2	M. Rouhun Munajih	Pembantu Peneliti		5	OH	430.000	2.150.000				2.150.000	
	Jumlah						3.010.000	-	-	-	3.010.000	

Yogyakarta, 22 Oktober 2021
Menyetujui,
Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Tahun Anggaran : 2021
No Bukti :
MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

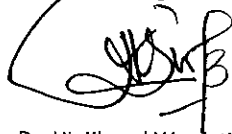
Telah terima dari : Kuasa Pengguna Anggaran / Pejabat Pembuat Komitmen/ Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : Rp 1.200.000

Terbilang : Satu juta dua ratus ribu rupiah

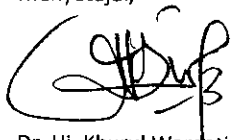
Untuk pembayaran : Biaya Penginapan Ketua Tim Peneliti dalam perjalanan dinas ke Ternate berangkat tanggal 05 November 2021 dan pulang tanggal 09 November 2021 an. Dr. Hj. Khurul Wardati, M. Si dalam rangka Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Yogyakarta, 10 Nopember 2021
Penerima Uang



Dr. Hj. Khurul Wardati, M. Si

Menyetujui,

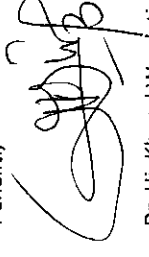


Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Daftar Penerimaan Biaya Akomodasi di Ternate
Kegiatan Research Leader Strategis UIN Sunan Kalijaga Yogyakarta
Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

No	Nama	Jabatan	Gol	Vol	Satuan	Harga satuan (Rp)	Akomodasi (Rp)	15%	6%	5%	Penerimaan (Rp)	Tanda Tangan
1	Dr. Hj. Khurul Wardati, M. Si	Ketua Tim Peneliti	IV	2	OH	600.000	1.200.000				1.200.000	
	Jumlah						1.200.000	-	-	-	1.200.000	

Yogyakarta, 22 Oktober 2021
Menyetujui,
Peneliti,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Guest Invoice

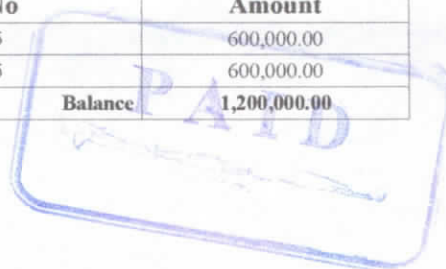
Sahid Belaternate Hotel
Jl. Jati Raya No. 500, Ternate Selatan,
Jati - Kota Ternate, Maluku Utara
t : +62 921 3121800
f : +62 921 3125000
info@sahidbelaternate.com

., UNKHAIR

Guest Name : MR. , KHURUL WARDATI

Room No : 2405
Adult : 2
Arrival : 05/11/21
Departure : 09/11/21
Room Rate :
Bill No : 27052 / 3

Date	Description/Voucher	Qty	RmNo	Amount
07/11/21	ROOM CHARGE	1	2405	600,000.00
08/11/21	ROOM CHARGE	1	2405	600,000.00
Balance				1,200,000.00



05/11 } Dibayar dan fakultas FST
06/11

I agree to remain personally liable for the payment of the account if the corporation or other third party billed fails to pay part or all of these charges.
My signature is authorization for Sahid Bela Ternate Hotel to use credit card imprinted for the payment of these charges.

Printed by : 12
Date : 09/11/2021 07:39

Guest Signature _____

Jalan Jati Raya No. 500, Ternate Selatan, Jati - Kota Ternate, Maluku Utara
t : +62 921 3121800 f : +62 921 3125000 e : info@sahidbelaternate.com

Please check that you have not left any valuables in the in-room personal safe.
Thank You for choosing to stay with Us and we wish you pleasant onward journey

Tahun Anggaran : 2021
No Bukti :
MAK : 2132.BEI.003.004.QA.521219

KWITANSI / BUKTI PEMBAYARAN

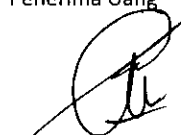
Telah terima dari : Kuasa Pengguna Anggaran / Pejabat Pembuat Komitmen/ Ketua LPPM UIN Sunan Kalijaga Yogyakarta

Jumlah Uang : **Rp 900.000**

Terbilang : **Sembilan ratus ribu rupiah**

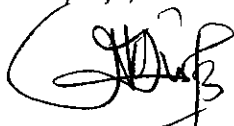
Untuk pembayaran : Biaya Penginapan Pembantu Peneliti dalam perjalanan dinas ke Ternate berangkat tanggal 05 November 2021 dan pulang tanggal 09 November 2021 an. M. Rouhun Munajih dalam rangka Kegiatan Research Leader UIN Sunan Kalijaga Yogyakarta dengan judul: "Terapan Aljabar Semiprima mendasar pada Pengamanan Autentifikasi Identitas Digital". Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

Yogyakarta, 10 Nopember 2021
Penerima Uang



M. Rouhun Munajih

Menyetujui,



Dr. Hj. Khurul Wardati, M. Si
NIP. 19660731 200003 2001

Daftar Penerimaan Biaya Akomodasi di Ternate
Kegiatan Research Leader Strategis UIN Sunan Kalijaga Yogyakarta
Berdasarkan SK Rektor UIN Sunan Kalijaga Yogyakarta No. 127.7 Tahun 2021 Tanggal 8 Juli 2021

No	Nama	Jabatan	Gol	Vol	Satuan	Harga satuan (Rp)	Jumlah (Rp)	15%	6%	5%	Akomodasi 30% (Rp)	Tanda Tangan
1	M. Rouhun Munajjih	Pembantu Peneliti		5	OH	600.000	3.000.000				900.000	1
	Jumlah						3.000.000	-	-	-	900.000	

Yogyakarta, 22 Oktober 2021
Menyetujui,
Peneliti,



Dr. Hj. Khurul Waridati, M. Si
NIP. 19660731 200003 2001



KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PAJAK

NPWP : 53.060.482.6-542.000

MUHAMMAD ROIHAN MUNAJIH

NIK: 3404082305970001

WONOSARI KM 8.5 NO. 022 RT. 007 RW. 008

SENDANGTIRTO BERBAH

KAB. SLEMAN DAERAH ISTIMEWA YOGYAKARTA



KPP PRATAMA SLEMAN

Terdaftar : 29 Oktober 2021

PROVINSI DAERAH ISTIMEWA YOGYAKARTA
KABUPATEN SLEMAN

NIK : 3404082305970001

Nama : MUHAMMAD ROIHAN MUNAJIH
Tempat/Tgl Lahir : YOGYAKARTA, 23-05-1987
Jenis Kelamin : LAKI-LAKI Gol. Darah : O
Alamat : GANDU
RT/RW : 007/008
Kel/Desa : SENDANGTIRTO
Kecamatan : BERBAH
Agama : ISLAM
Status Perkawinan: BELUM KAWIN
Pekerjaan : PELAJAR/MAHASISWA
Kewarganegaraan: WNI
Berlaku Hingga : SEUMUR HIDUP



SLEMAN
08-10-2020

[Signature]

PROVINSI JAWA TENGAH
KABUPATEN SUKOHARJO

NIK 3311030308920002

Nama	M. MIFTAHUL AKBAR
Tempat/Tgl. Lahir	SUKOHARJO, 03-08-1989
Jenis Kelamin	LAKI-LAKI Gol. Darah O
Alamat	DK. CEMETUK
RT/RW	001/003
Kelurahan	LOROG
Kecamatan	TAWANGSARI
Agama	ISLAM
Status Perkawinan	BELUM KAWIN
Pendidikan	PELAJARAN MAHASISWA
Kewarganegaraan	WNI
Berkas Hingga	BELAKUR HIDUP



SI KONSER
04-08-2010

Handwritten signature or mark.

NPWP : 83.357.165.6-532.000

M. MIFTAHUL AKBAR

NIK : 3311030308920002

JALAN PATTIMURA NO. 56 RT. 03 RW. 01
LOROG TAWANGSARI
KAB. SUKOHARJO JAWA TENGAH

KOP PRATAMA

PROVINSI DAERAH ISTIMEWA YOGYAKARTA
KABUPATEN SLEMAN

NIK : 3404082305970003

Nama : MUHAMMAD ROUHUN MUNAJIH
Tempat/Tgl Lahir : YOGYAKARTA, 23-05-1997
Jenis Kelamin : LAKI-LAKI Gol. Darah : A
Alamat : GANDU
RT/RW : 007/008
Kel. Desa : SENDANGTIRTO
Kecamatan : BERBAH
Agama : ISLAM
Status Perkawinan : BELUM KAWIN
Pekerjaan : PELAJAR/MAHASISWA
Kewarganegaraan : WNI
Berlaku Hingga : SEUMUR HIDUP



SLEMAN
05-07-2018

npw.p.

KPP PRATAMA SLEMAN

42.071.474.3-542.000

MUHAMMAD ROUHUN MUNAJIH



WENGBARIKMEJ, NO. 22 RT. 007 RW. 008
SENDANGTIRTO BERBAH
KAB. SLEMAN DAERAH ISTIMEWA YOGYAKARTA
KAB. SLEMAN





NPWP : 45.608.478.9-541.000

MUHAMMAD FAKHRURRIFIQI

KARANGKAJEN MG III/911 RT 043 RW 011
BRONTOKUSUMAN MERGANGSAN YOGYAKARTA

TERDAFTAR : 25-04-2012

PROVINSI DAERAH ISTIMEWA YOGYAKARTA
KOTA YOGYAKARTA

NIK : 3471121611860001

Nama	MUHAMMAD FAKHRURRIFIQI S KOM M Cs
Tempat/Tgl Lahir	YOGYAKARTA 16-11-1986
Jenis kelamin	LAKI LAKI Gol Darah B
Alamat	KARANGKAJEN MG III 911 YK
RT/RW	043/011
Kel. Desa	BRONTOKUSUMAN
Kecamatan	MERGANGSAN
Agama	ISLAM
Status Perkawinan	KAWIN
Pekerjaan	DOSEN
Kewarganegaraan	WNI
Berlaku Hingga	SEUMUR HIDUP



KOTA YOGYAKARTA
21-12-2015

PROVINSI MALUKU UTARA
KOTA TERNATE

NIK : 8271025102810007

Nama : IDA KURNIA WALIYANTI
Tempat/Tgl Lahir : MAGETAN 11-02-1981
Jenis Kelamin : PEREMPUAN Gol Darah : O
Alamat : JL. AKE OTI
RT/RW : 008-003
Kel/Desa : UBO-UBO
Kecamatan : TERNATE SELATAN
Agama : ISLAM
Status Perkawinan : KAWIN
Pekerjaan : PEGAWAI NEGERI SIPIL (PNS)
Kewarganegaraan : WNI
Berlaku Hingga : 11-02-2017



KOTA TERNATE
21-07-2012

[Signature]

NPWP : 79.123.846.2-942.000
Nama : IDA KURNIA WALIYANTI
Alamat : JL. KAMPUS GAMBESI
D/A UNIV. KHAIRUN TERNATE
KEL. GAMBESI
KEC. TERNATE SELATAN
KOTA TERNATE

PROVINSI DAERAH ISTIMEWA YOGYAKARTA
KOTA YOGYAKARTA

NIK : 3471125305850001

Nama : DWI LESTARI, M.SC
Tempat/Tgl Lahir : KLATEN, 13-05-1985
Jenis Kelamin : PEREMPUAN Gol Darah : B
Alamat : KARANGKAJEN MG.INDO 1 YK
RT/RW : 043 / 031
Kel/Desa : BRONTOKUSUMAN
Kecamatan : MERGANDHAN
Agama : ISLAM
Status Perkawinan : KAWIN
Pekerjaan : DOSEN
Kewarganegaraan : WNI
Berlaku Hingga : 13-05-2017



KOTA YOGYAKARTA
11-03-2013

[Signature]



KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

DIREKTORAT JENDERAL PAJAK

NPWP : 36.425.692.5-525.000

DWI LESTARI

BANJAR

KRAGI

KLATEN

TERDA