SKRIPSI

SISTEM KRIPTOGRAFI SIMETRIS MINI-AES ATAS LAPANGAN HINGGA GF(2^4)

SITI SOBARIAH NOER HASANAH

14610010

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2020

SISTEM KRIPTOGRAFI SIMETRIS MINI-AES ATAS LAPANGAN HINGGA GF(2^4)

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

diajukan oleh

SITI SOBARIAH NOER HASANAH

14610010

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2020

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi/Tugas akhir
Lamp : -

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama	: Siti Sobariah Noer Hasanah
NIM	: 14610010
Judul Skripsi	: Sistem Kriptografi Simetris Mini-AES atas Lapangan Hingga GF(2^4)

sudah dapat diajukan kembali kepada Program Studi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam bidang matematika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqasyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 29 Januari 2020
Pembimbing

Muhamad Zaki Riyanto, S.Si., M.Sc.
NIP. 19840113 201503 1 001

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-755/Un.02/DST/PP.00.9/03/2020

Tugas Akhir dengan judul : SISTEM KRIPTOGRAFI SIMETRIS MINI-AES ATAS LAPANGAN HINGGA GF(2^4)

yang dipersiapkan dan disusun oleh:

Nama	: SITI SOBARIAH NOER HASANAH
Nomor Induk Mahasiswa	: 14610010
Telah diujikan pada	: Kamis, 20 Februari 2020
Nilai ujian Tugas Akhir	: A/B

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Muhamad Zaki Riyanto, S.Si., M.Sc.
NIP. 19840113 201503 1 001

Penguji I

Dr. Muhammad Wakhid Musthofa, S.Si., M.Si.
NIP. 19800402 200501 1 003

Penguji II

Malahayati, S.Si., M.Sc
NIP. 19840412 201101 2 010

Yogyakarta, 20 Februari 2020
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

Dr. Murtono, M.Si.
NIP. 19691212 200003 1 001

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama : Siti Sobariah Noer Hasanah

NIM : 14610010

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Dengan ini menyatakan bahwa isi skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi dan sesungguhnya skripsi ini merupakan hasil pekerjaan penulis sendiri sepanjang pengetahuan penulis, bukan duplikasi atau saduran dari karya orang lain kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 29 Januari 2020

Yang Menyatakan

Siti Sobariah Noer Hasanah

HALAMAN PERSEMBAHAN

Karya sederhana ini penulis persembahkan

untuk orang tua dan keluarga tercinta

yang senantiasa mendoakan, memberi

dukungan dan motivasi

serta almamater UIN Sunan Kalijaga Yogyakarta
khususnya program studi Matematika.

MOTTO

"Jika kamu berbuat baik (berarti) kamu berbuat baik bagi dirimu sendiri dan jika kamu berbuat jahat maka kejahatan itu bagi dirimu sendiri"

(QS. Al-Isra : 7)

PRAKATA

Puji syukur Alhamdulillah kehadirat Allah SWT yang telah melimpahkan rahmat, taufiq, dan hidayahnya, sehingga penulis dapat menyelesaikan Tugas Akhir ini.

Skripsi ini merupakan tugas akhir dari kegiatan-kegiatan perkuliahan yang beberapa tahun penulis jalani. Tugas akhir ini dibuat berdasarkan syarat untuk memperoleh gelar sarjana.

Pada kesempatan ini penulis mengucapkan terima kasih sebesar-besarnya kepada :

1. Bapak Dr. Murtono, M.Si. selaku dekan fakultas Sains dan Teknologi.
2. Ibu Malahayati, M.Sc. sebagai Dosen pembimbing akademik yang selalu memotivasi supaya lulus cepat. Walaupun pada akhirnya lulus dengan waktu yang tidak cepat.
3. Bapak Muhamad Zaki Riyanto, S.Si., M.Sc. selaku dosen pembimbing skripsi yang telah sabar dan sudah meluangkan waktunya untuk membimbing saya sehingga dapat terbentuklah karya tulis ini.
4. Dosen-dosen matematika yang lain yang telah memberikan ilmunya dalam perkuliahan : pak Wakhid, Bu Pipit, Bu Khurul, Pak Farhan, Pak Saif, Pak Abrori, pak Sugi, dan dosen-dosen dari prodi lain serta staf-staf di fakultas.
5. Kedua orangtuaku tercinta bapak Uju dan mamah Titin sebagai penyemangat saat kuliah selama beberapa tahun ini, dan selalu memberika doa dan restunya sampai saat ini saya dapat memperoleh gelar sarjana.

6. Aa dan Teteh ku : Teh Ade, Teh Nyai, A Ali, A Irman, A Asep, Teh Aini. Yang telah memberikan suport baik berupa moril ataupun materi selama saya sekolah di Djogja. Dan buat adeku Iyus sebagai motivasi aku supaya cepet lulus, walaupun pada akhirnya gak cepat.
7. Temen-temen diprodi Matematika, khususnya buat temen-temen E-Math yang sudah saling memotivasi satu sama lain supaya kita bisa lulus bareng, tapi diriku malah lulus belakangan.
8. Teman-teman yang lain diluar matematika UIN.
9. Dan beberapa pihak lain yang tidak dapat penulis sebut satu persatu.

Penulis masih menyadari bahwa skripsi ini masih jauh dari kata sempurna, maka saran dan kritik yang konstuktif dari semua pihak sangat diharapkan demi penyempurnaan selanjutnya.

Akhirnya hanya kepada Allah SWT kita kembalikan semua urusan dan semoga skripsi ini dapat bermanfaat bagi semua pihak, khususnya bagi penulis dan bagi para pembaca pada umumnya. Semoga Allah meridhoi, Amin.

Sleman, 28 Januari 2018

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG

$\mathcal{K}$	: Hmpunan semua kunci
$\mathcal{P}$	: Himpunan semua plainteks atau pesan asli
$\mathcal{C}$	: Himpunan semua cipherteks atau pesan sandi
$\mathbb{Z}_p[x]$	: himpunan semua polinomial atas $\mathbb{Z}_p$
GF(p)	: Lapangan Galois berorde p
Gf(p^n)	: Lapangan Galois berorde p^n
$m(x)$	: irreducible polynomial
$f(x) \in$GF(2^n)	: $f(x)$ anggota GF(2^n)
$f(x) + g(x)$ mod $m(x)$	: penjumlahan $f(x)$ dan $g(x)$ modulo $m(x)$
$f(x)g(x)$ mod $m(x)$	: perkalian $f(x)$ dan $g(x)$ modulo $m(x)$
$\sum_{i=1}^{n} a_i$	: penjumlahan $a_1 + a_2 + \cdots + a_n$

INTISARI

Sistem Kriptografi Simetris Mini-AES atas Lapangan Hingga GF(2^4)

Oleh

SITI SOBARIAH NOER HASANAH

14610010

Advanced Encryption Standard (AES) merupakan sistem kriptografi simetris yang saat ini digunakan sebagai standar enkripsi di dunia, khususnya di internet. AES digunakan untuk menggantikan DES dan *Triple* DES yang sudah dianggap tidak aman untuk keamanan jaringan.AES memiliki panjang kunci 128 bit, 192 bit dan 256 bit. AES memiliki varian yang lebih kecil yaitu Mini-AES yang memiliki ukuran kunci yang lebih kecil daripada kunci yang digunakan di AES.

Mini-AES merupakan suatu sistem kriptografi simetris jenis block-cipher dengan panjang kunci 16 bit. Proses enkripsi menggunakan metode substitusi dan permutasi serta perulangan pada matriks 2×2 dengan setiap entrinya terdiri dari 4 bit. Setiap proses substitusi-permutasi digunakan kunci yang berbeda-beda. Kunci-kunci tersebut diperoleh melalui proses penjadwalan kunci yang diperoleh dari kunci awal.

Algoritma yang digunakan Mini-AES untuk proses enkripsi yaitu *NibbleSub, ShiftRow, MixColumn, AddRoundKey*, dan algoritma untuk proses Dekripsi menggunakan invers dari masing-masing algoritmma enkripsi Mini-AES. Seluruh proses enkripsi dan dekripsi mengguankan struktur aljabar berupa lapangan hingga $Z_2[x]$ modulo polinomial $m(x) = x^4 + x + 1$.

Kata kunci : ring polinomial, lapangan hingga, kriptografi, block-cipher, AES, Min-AES, nibblesub, shiftrow, mixcolumn, addroundkey

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Semakin berkembangnya zaman semakin berkembang pula penggunaan internet di dunia, yang menyebabkan keamanan internet semakin berkurang. Sehingga lembaga standar Amerika Serikat NIST (*National Institute of Standards and Technology*) menggantikan DES (*Data Encryption Standard*) dengan AES (*Advanced Encryption Standard*).

DES terbukti menjadi algoritma enkripsi yang aman di dunia selama puluhan tahun. Meski demikian, pada tahun 1990 panjang kunci DES dianggap terlalu pendek dan pada tahun 1998, 70 ribu PC diinternet dapat membobol satu kunci DES dalam tempo 96 hari, maka dari itu dibuat mesin khusus untuk memecahkan algoritma DES. Mesin tersebut dapat memecahkan 25% kunci DES dalam waktu 2,3 hari dan dapat memecahkan seluruh kunci dalam waktu rata-rata 4,5 hari. Karena alasan tersebut, pada tahun 90-an algoritma penyandian DES disinyalir tidak aman lagi untuk digunakan, yang menyebabkan NIST mengadakan sayembara untuk mencari keamanan baru yang dapat menggantikan DES, dengan sebuah penyandian yang disebut AES pada tanggal 12 September 1997. Dengan spesifikasi: harus memiliki panjang blok 128 bit dan mampu mendukung kunci dengan panjang 128 bit, 192 bit, dan 256 bit.

Sebelum terbentuknya AES secara resmi, NIST menggunakan penyandian *Triple* DES sebagai pengganti DES sementara. *Triple* DES adalah salah satu sistem enkripsi berlapis tiga dari sistem yang sebelumnya sudah ada yaitu DES.

Triple lebih aman dari DES, karena mengalami enkripsi sebnyak tiga kali sedangkan DES hanya mengalami enkripsi tunggal atau sekali proses pengenkripsian. Namun, dengan meningkatkan komputasi, serangan brutal telah mungkin terjadi. Tanpa memerlukan perancangan *block cipher* yang baru, *triple* DES menyediakan metode sederhana dengan menambah ukuran kunci DES untuk mencegah serangan tersebut.

Setelah beberapa seleksi, dan sayembarapun dimenangkan oleh Joan Daemen dan Vincent Rijment dengan mengembangkan sistem peyandian Rijndael. AES diumumkan oleh NIST sebagai standar pemrosesan informasi Federal (FIPS) pada dokumen FIPS-PUB 197 pada 26 November 2001.

Semua rangkaian algoritma enkripsi dan dekripsi menggunakan mode bit, dengan memroses seluruh data dan informasi dengan rangkaian bit yaitu menggunakan sistem bilangan biner 0 dan 1. Plainteks di enkripsi menjadi cipherteks, begitu juga sebaliknya dalam bentuk rangkaian bit. Namun, untuk mempelajari Algoritma AES yang mempunyai panjang blok 128 sedikit rumit dan harus memiliki pemahaman betul. Untuk itu akan dikaji bentuk mini dari AES dengan panjang blok 16 bit dan panjang kunci berukuran 16 bit yang disebut Mini-AES.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka perumusan masalah yang akan dikaji dalam karya penelitian ini adalah:

1. Bagaimana langkah algoritma enkripsi AES, dengan menggunakan versi mininya yaitu Mini-AES atas lapangan hingga GF(2^4).
2. Bagaimana penerapan algoritma Mini-AES dalam keamanan pesan rahasia serta uji coba perhitungannya secara manual dan menggunakan Maple 18.

1.3. Tujuan Penulisan

Berdasarkan permasalahan yang diajukan, maka tujuan penelitian ini adalah:

1. Mengkaji materi mengenai langkah-langkah algoritma pada keamanan jaringan Internet saat ini dengan Mini-AES.
2. Untuk mengetahui cara menenkripsi dan mendekripsi pesan dengan mini-AES menggunakan Maple 18.

1.4. Manfaat Penulisan

Karya tulis ini diharapkan dapat memberi manfaat, diantaranya:

1. Bagi penulis

   Hasil penelitian ini menjadi tambahan pengetahuan tentang sistem keamanan jaringan di internet saat ini, dan menambah pemahaman tentang beberapa algoritma pengenkripsian AES dengan ukuran yang lebih kecil yaitu Mini-AES.

2. Bagi prodi matematika

   Hasil dari penelitian ini dapat dijadikan sebagai alat belajar mengenai keamana jaringan yang dipakai internet saat ini dengan praktis dan lebih mudah dimengerti.

1.5. Tinjauan Pustaka

Reverensi utama yang digunakan dalam penelitian ini adalah jurnal yang berjudul ”*Mini Advanced Encryption Standard (Mini-AES): A testbed for Cryptanalysis Students*”(*Chung-Wei Phan, Raphael*,2002). Dimana pada jurnal ini dijelaskan menganai bentuk mini dari AES yaitu mini-AES, dari algoritma

enkripsi serta juga pembuatan kunci-kunci ronde pada mini-AES. Terinpirasi dari jurnal tersebut, penulisan ini akan manjelaskan mengenai mini-AES dengan struktur-struktur yang digunakan pada kriptografi modern.

Terdapat juga hasil penelitian yang terdapat pada buku carlos Cid, dkk(2006), dengan judul "*Algebraic Aspects of the Advanced Encryption Standard*", buku tersebut memaparkan tentang aspek-aspek yang digunakan pada kriptografi AES, seperti struktur aljabar yang digunakan, dan juga algoritma enkripsi mapun dekripsi AES.

Selanjutnya reverensi yang digunakan sebagai tinjauan pustaka adalah buku yang berjudul "Kriptografi untuk keamanan jaringan", karya dari Rifki Sadikin(2012). dimana buku tersebut berisi tentang kriptografi-kriptografi modern, serta penjelasan mengenai algoritma-algoritmanya dan juga penulisan program dalam bahasa java.

1.6. Metode Penulisan

Metode penelitian yang digunakan dalam penulisan skripsi ini adalah dengan studi literatur, yaitu dengan membahas dan menjabarkan konsep-konsep yang sudah ada dalam bentuk literatur. Baik dalam bentuk buku-buku referensi, maupun bahan-bahan berbentuk jurnal yang diperoleh dari perpustakaan maupun dari internet.

1.7. Sistematika Penulisan

Secara garis besar gambaran menyuluruh mengenai sistem kriptografi simetris mini-AES atas lapangan hingga GF(2^4):

Bab I: Pendahuluan, berisi latar belakang masalah, rumusan masalah, tujuan penulisan manfaat penulisan, tinjauan pustaka, metode penulisan serta sistematika

penulisan.

Bab II: Landasan teori, berisi tentang teori-teori yang menunjang pembahasan dalam penulisan tugas akhir ini, teori yang terdapat dalam tulisan ini adalah kriptografi, struktur aljabar untuk kriptografi kunci simetris, block-cipher, matriks dan advanced encryption standard (AES).

Bab III: Pembahasan, berisi tentang penjelasan mengenai sistem kriptografi simetris mini-AES atas lapangan hingga GF(2^4).

Bab IV: Penutup: berisi kesimpulan dari pembahasan serta saran untuk penelitian berkutnya.

BAB IV

PENUTUP

4.1. Kesimpulan

Berdasarkan pada pembahasan mengenai pengenkripsian Mini-AES pada keamanan pesan dapat diambil kesimpulan sebagai berikut:

1. Proses enkripsi pesan menggunakan Mini-AES ini dilakukan dengan 2 ronde. Semua proses enkripsi menggunakan metode subtitusi dan permutasi serta perulangan pada matriks 2×2 dengan setiap entrinya terdiri dari 4 bit. Algoritma-agoritma pada enkripsi Min-AES sama dengan algoritma pada enkripsi AES yaitu:

   a. *NibbleSub* yaitu subtitusi menggunakan tabel *nibblesub* disebut dengan S-Box *NibbleSub* yang sudah diketahhui.

   b. *ShiftRow* yaitu menggeser komponen pada setiap baris matriks.

   c. *MixColumn* yaitu mencampur matriks hasil dari transformasi *shiftrow* denga matriks $\begin{bmatrix} 3 & 2 \\ 2 & 3 \end{bmatrix}$ yang sudah ditetapkan.

   d. *AddRoundKey* yaitu penjumlahan dengan kunci ronde yang telah di bentuk dari kunci Asli atau kunci induk.

   Setiap transformasi Algoritma-Algoritma tersebut berada di GF(2^4) dengan *irreducible polynomial* $m(x) = x^4 + x + 1$.

Algoritma-algoritma pada dekripsi pada Mini-AES yaitu menggunakan invers dari setiap algoritma enkripsi Mini-AES, berupa *InvNibbleSub, InvShiftRow,*

InvMixColum, dan khusus pada algoritma *AddRoundKey* tidak perlu menggunakan invers karena menggunakan kunci yang sama yg dipakai pada algoritma enkripsi.

Setiap ronde memerlukan kunci, dan pada enkripsi pesan menggunakan Mini-AES dilakukan dengan 2 ronde maka memerlukan 3 kunci ronde yang didapat dari kunci induk, dimana kunci induk merupakan k_0, 2 kunci ronde lainnya yaitu k_1 dan k_2.

2. Maple 18 digunakan untuk uji coba perhitungan enkripsi dan dekripsi mini-AES. Perintah yang digunakan berupa : *LinearAlgebra[Generic]*, $GF(p, k, a)$, *Matrix([[*$a11, a12$*],[*$a21, a22$*]])*, *Map(*$F : -Converin, A$*)*, *Matrixinvers[*F*](*A*)*, *MatrixMatrixMultiply[*F*](*A, B*)*.

4.2. Saran

AES merupakan hal yang sangat penting dalam menjaga keamanan jaringan yang dipakai saat ini. Oleh karena itu dibuat karya tulis ini yang membahas tentang Mini-AES yang merupakan bentuk kecil dari AES, supaya lebih mudah untuk di pahami.

Penulissan tentang Mini-AES ini tidak membahas mengenai adanya kemungkinan serangan dari pihak ketiga untuk. Diharapkan ada penelitian lebih lanjut yang membahas terkait adanya pihak ketiga dalam Mini-AES.

DAFTAR PUSTAKA

Carles Cid, dkk. 2006, *Algebraic Aspects of the Advanced Ecryption Standard*, USA.

Chung-Wei Phan, Raphael. 2002, *Mini Advanced Encryption Standard (Mini-AES): A testbed for Cryptanalysis Students*, Jurnal dari https://www.researchgate.net.

Federal Information proccesing Standard Publication 197. 2001, *Announcing the Advanced Encryption Standard (AES)*, jurnal dari https://www.cisco.com.

Inayah, Nunung. 2018, *Autentikasi Identitas Digital Menggunakan Grup Matriks Polinomial Atas lapangan Hingga*. Skripsi. Yogyakarta: UIN Sunan Kalijaga.

Malik, dkk. 2007, *An Introduction to Abstract Algebra*, USA.

NIST. 2000, *AES Development effort*, Jurnal dari http://csrc.nist.gov/encryption/aes/index2.html.

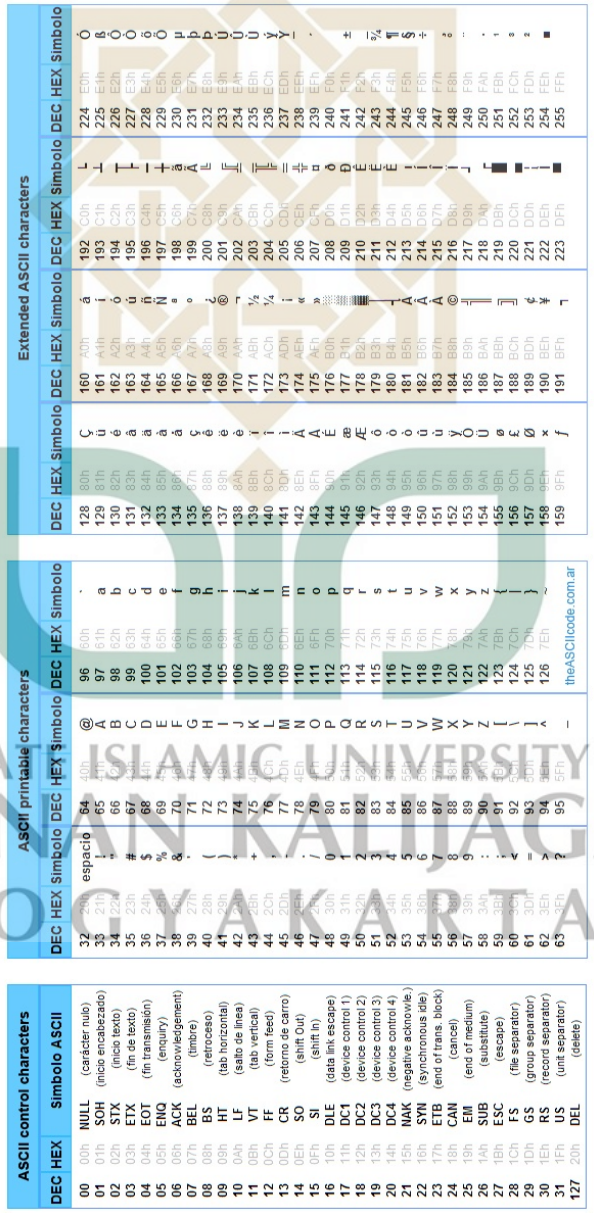
NIST. 2002, *AES Homepage*, Jurnal dari http://www.nist.gov/aes.

Sadikin, RAfiki. 2012, Kriftografi untuk Keamanan Jaringan. Yogyakarta : Penerbit Andi.

Tabel ASCII dari https://fdokumen.com/document/ascii-5584ae07498ff.html.

LAMPIRAN A

TABEL KODE ASCII



CURRICULUM VITAE

A. Biodata Diri

Nama Lengkap : Siti Sobariah Noer Hasanah
Jenis Kelamin : Perempuan
Tempat, Tanggal Lahir : Tasikmalaya, 30 Mei 1996
Alamat Asal : Sukarindik 1 06/01, Bungursari, Kota Tasikmalay
Alamat Tinggal : Perumahan graha Absolut Sedayu, Sumberan, Argodadi, Sedayu, Bantul, DIY
Email : Shobariah35@gmail.com
No. Hp : 085210506915

B. Latar Belakang Pendidikan Formal

Jenjang	Nama Sekolah	Tahun
TK	TK-A Awwaliyah Tasikmalaya	2001-2002
SD	SD Negeri Sukarindik 1 Tasikmalaya	2002-2008
SMP	SMP Negeri 16 Tasikmalaya	2008-2011
SMA	MAN Godean Sleman	2011-2014
S1	UIN Sunan Kalijaga Yogyakarta	2014-2020