SKRIPSI

PENGAMANAN PESAN RAHASIA DENGAN SANDI ALIRAN BERDASARKAN TRANSFORMASI PADA QUASIGROUP ATAS $\mathbb{Z}_P^*$

M. ADIB JAUHARI DWI PUTRA

NIM 08610009

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2013

PENGAMANAN PESAN RAHASIA DENGAN SANDI ALIRAN BERDASARKAN TRANSFORMASI PADA QUASIGROUP ATAS $\mathbb{Z}_P^*$

Skripsi
Sebagai salah satu persyaratan
untuk memperoleh derajat Sarjana S-1
Program Studi Matematika

diajukan oleh
M. ADIB JAUHARI DWI PUTRA
NIM 08610009

Kepada

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
YOGYAKARTA

2013

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi
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 saya selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : M. Adib Jauhari Dwi Putra
NIM : 08610009
Judul Skripsi : Pengamanan Pesan Rahasia dengan Sandi Aliran Berdasarkan Transformasi pada Quasigroup atas $\mathbb{Z}_p^*$

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 saya mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya saya ucapkan terima kasih.

Wassalamu'alaikum wr. Wb

Yogyakarta, 2 Mei 2013

Pembimbing I	Pembimbing II
Muhamad Zaki Riyanto, S.Si., M.Sc.	Malahayati, S.Si., M.Sc.
NIDN. 0513018402	NIP. 19840412 201101 2 010

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-07/R0

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : UIN.02/D.ST/PP.01.1/1617/2013

Skripsi/Tugas Akhir dengan judul : Pengamanan Pesan Rahasia dengan Sandi Aliran Berdasarkan Transformasi pada Quasigroup atas Z*p

Yang dipersiapkan dan disusun oleh :
Nama : M. Adib Jauhari Dwi Putra
NIM : 08610009
Telah dimunaqasyahkan pada : 20 Mei 2013
Nilai Munaqasyah : A/B

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

TIM MUNAQASYAH :

Ketua Sidang

Muhamad Zaki Riyanto,S.Si., M.Sc
NIDN. 0513018402

Penguji I

Dra. Khurul Wardati, M.Si.
NIP.19660731 200003 2 001

Penguji II

Malahayati, M.Sc
NIP.19840412 201101 2 010

Yogyakarta, 03 Juni 2013
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

KEMENTERIAN AGAMA FAKULTAS SAINS DAN TEKNOLOGI YOGYAKARTA UIN SUNAN KALIJAGA

Prof. Drs. H. Akh. Minhaji, M.A, Ph.D
NIP. 19580919 198603 1 002

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini :

Nama : M. Adib Jauhari Dwi Putra

NIM : 08610009

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Menyatakan dengan sesungguhnya bahwa skripsi ini merupakan hasil pekerjaan penulis sendiri dan sepanjang pengetahuan penulis tidak berisi materi yang dipublikasikan atau ditulis orang lain, dan atau telah digunakan sebagai persyaratan penyelesaian Tugas Akhir di Perguruan Tinggi lain, kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 6 Mei 2013

Yang menyatakan

M. Adib Jauhari Dwi Putra

NIM. 08610009

iv

Karya sederhana ini penulis persembahkan untuk

▷ Ibu dan Ayah tercinta

▷ Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta

▷ Pecinta matematika dan pemerhati perkembangan ilmu kriptologi di seluruh Indonesia

"Dan Dialah Allah (yang disembah), baik di langit maupun di bumi; Dia mengetahui apa yang kamu rahasiakan dan apa yang kamu lahirkan dan mengetahui (pula) apa yang kamu usahakan."

(QS. 6:3)

"Has a secret make a boy be a man"

(quotes)

"No matter how gifted, you alone can not change the world"

(L Death note)

ABSTRAK

Sandi aliran berdasarkan transformasi pada *quasigroup* atas $\mathbb{Z}_p^*$ atau dinamakan *quasigroup* stream cipher termasuk dalam klasifikasi algoritma kunci simetris, yaitu kunci yang digunakan untuk enkripsi dan dekripsi pesan sama. Algoritma ini bekerja dalam $\mathbb{Z}_p^*$ (dimana p merupakan bilangan prima), dengan mendefinisikan *quasigroup* berorder $p-1$ dan melakukan transformasi string *quasigroup*.

Algoritma sandi aliran berdasarkan transformasi pada *quasigroup* atas $\mathbb{Z}_p^*$ memiliki dua buah kunci, yaitu bilangan K dan sejumlah leader l. Dalam mengenkripsi dan mendekripsi pesan rahasia, bilangan K selalu tetap, sedangkan leader l selalu berubah. Enkripsi dilakukan pada setiap blok-blok plainteks dan menghasilkan cipherteks yang sama panjang dengan plainteksnya.

Pada tugas akhir ini pembahasan terfokus pada algoritma sandi aliran berdasarkan transformasi pada *quasigroup* atas $\mathbb{Z}_p^*$ beserta konsep matematis yang melandasinya. Kemudian dibuat sebuah program sederhana untuk mengenkripsi dan mendekripsi pesan rahasia berdasarkan algortima tersebut.

Kata kunci: dekripsi, enkripsi, quasigroup, stream cipher

KATA PENGANTAR

Alhamdulillahirobil'alamin syukur kehadirat Allah SWT atas limpahan rahmat serta hidayah-Nya kepada penulis atas terselesaikannya tugas akhir ini. Sholawat dan salam semoga senantiasa tercurah kepada junjungan, suri teladan yang mulia, Nabi Muhammad SAW yang telah memberikan tuntunan yang sangat bijaksana pada kehidupan umat manusia umumnya dan pada penulis khususnya.

Tak bisa dipungkiri bahwa penyusunan tugas akhir ini tak lepas dari dukungan berbagai pihak berupa bimbingan, arahan dan bantuan baik moral maupun material. Oleh karena itu penulis haturkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Drs. Akh. Minhaji, M.A.,Ph.D. selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
2. Bapak M. Abrori, S.Si, M.Kom. selaku Ketua Program Studi Matematika.
3. Bapak Muhamad Zaki Riyanto, S.Si, M.Sc. selaku Dosen Pembimbing yang telah bersedia meluangkan waktu dan pikiran, serta memberikan pemahaman tentang dunia kriptografi hingga terselesaikannya penulisan tugas akhir ini.
4. Ibu Malahayati, S.Si. M.Sc. selaku Dosen Pembimbing yang telah bersedia meluangkan waktu dan pikiran demi terselesaikannya penulisan tugas

akhir ini.

5. Ibu Dra. Khurul Wardati, M.Si. selaku dosen Pengantar Struktur Aljabar sehingga penulis tertarik untuk mendalami aljabar.

6. Bapak Sugiyanto S.T., M.Si. selaku Dosen Penasehat Akademik Program Studi Matematika yang telah memberikan motivasi dan pengarahan kepada penulis.

7. Seluruh Dosen Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta yang telah memberikan wawasan dan ilmunya kepada penulis sebagai bekal di masa depan.

8. Ibu dan Ayah tersayang, serta kakak dan adik tercinta yang selalu memberikan semangat dan doa kepada penulis setiap hari.

9. Sahabat masa kecil dan teman-teman dari SDN Mlatiharjo, SMPN 2 Bringin dan SMAN 3 Salatiga yang telah memberikan kenangan dan pelajaran berharga dalam hidupku.

10. Nindita Yuda, teman bermain di Salatiga yang selalu mensuport dan mendoakanku.

11. Kakak pertama (Imron) dan kakak kedua (Ial), semoga misi kita berhasil dan jangan lupa janji Imron.

12. Okta, Tatar, Ranto, ayo mancing lagi. Ria, Aesa, Septa, mbako (Mariana), Lia, ketua Himaho (Jajang), wakil ketua Himaho (Bayu), sesepuh

(simbah Riyanto), B-tela (Bowo), Najib, Santosa, Rifqi dan teman-teman Matematika 2008 yang lain yang selalu memberi semangat, semoga tali silaturahmi kita tetap terjaga, dan semoga kesuksesan menyertai kita semua.

13. Segenap pihak yang telah membantu penulis dari pembuatan proposal, sampai terselesaikannya penulisan tugas akhir ini yang tidak dapat penulis sebutkan satu persatu.

Tentunya masih banyak kekurangan dan kesalahan dalam penulisan tugas akhir ini. Masukan, saran dan kritik demi kemajuan dan kesempurnaan tulisan ini sangat penulis harapkan. Semoga karya ini dapat memberikan manfaat dan sumbangan bagi kemajuan dan perkembangan ilmu pengetahuan terutama dalam bidang kriptografi.

Yogyakarta, 16 April 2013

Penulis

M. Adib Jauhari Dwi Putra

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG DAN SINGKATAN

$x \in A$	: x anggota A
$\mathbb{Z}$	: himpunan semua bilangan bulat
$\mathbb{R}$	: himpunan semua bilangan real
$\blacksquare$	: akhir suatu bukti
$\sum_{i=1}^{n} a_i$	: penjumlahan $a_1 + a_2 + \cdots + a_n$
$p \Rightarrow q$	: jika p maka q
$\Leftrightarrow$	: jika dan hanya jika
$x \leftarrow a$	: nilai a dimasukkan ke x
$\forall a \in G$	: untuk semua nilai a dalam G
C_r^n	: r kombinasi dari n unsur yang berbeda
$a \mid b$	: a membagi habis b
$(\Rightarrow)$	: syarat perlu
$(\Leftarrow)$	: syarat cukup
$\mathbb{Z}_p^*$	: Himpunan bilangan bulat $\{1, 2, \cdots, p-1\}$ dimana p adalah bilangan prima
$a \backslash b$	: operasi left parastrophe quasigroup dari operasi quasigroup $a * b$

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Matematika sering disebut sebagai *Queen of the Sciences* yang melayani berbagai disiplin ilmu. Sangat banyak penerapan atau aplikasi dari matematika dalam bidang keilmuan lain sehingga matematika menduduki peran yang sangat penting dalam perkembangan ilmu-ilmu pengetahuan. Kriptografi atau secara umum disebut ilmu dan seni untuk menjaga kerahasiaan berita, merupakan salah satu ilmu yang dalam perkembangannya menggunakan banyak sekali konsep-konsep matematika. Cabang matematika seperti aljabar abstrak menyumbang berbagai teori yang digunakan untuk merancang suatu algoritma kriptografi.

Sebelumnya perlu diketahui bahwa ide menyandikan pesan telah ada sejak lebih dari 2000 tahun yang lalu(Wikipedia,2013). Hal ini dilakukan untuk melindungi pesan atau berita terhadap ancaman penyerangan dan kebocoran dari pihak-pihak tertentu yang tidak memiliki hak mengetahui isi pesan tersebut. Untuk itu, diperlukan suatu metode yang dapat merahasiakan isi pesan agar tidak terjadi hal-hal tersebut. Proses merahasiakan isi pesan atau penyandian dinamakan proses enkripsi. Beberapa diantara enkripsi atau sandi kuno yaitu Caesar cipher dari Romawi dan Kamasutra cipher dari India yang menggunakan proses substitusi.

Dari sudut pandang bagaimana algoritma enkripsi mengenkripsi informasi yang berulang beberapa kali selama tahap komunikasi, algoritma enkripsi dibagi pada stream cipher dan block cipher. Block cipher selalu memberikan output yang sama dari cipher teks untuk input yang sama dari plainteks, sedangkan stream cipher memberikan output yang berbeda dari urutan yang sama dari plainteks (Gligoroski,2004). Stream cipher mengenkripsi data per satuan data, seperti bit, byte, nible atau per lima bit. Setiap mengenkripsi satu satuan data digunakan kunci yang merupakan hasil pembangkitan dari kunci sebelum. Berdasarkan tipe kunci yang digunakan dalam algoritma kriptografi, dan cara kerja kunci, algoritma enkripsi diklasifikasikan menjadi algoritma kunci simetris dan asimetris. Pada algoritma kunci simetris, digunakan satu kunci untuk mengenkripsi data dan kunci yang sama untuk mendekripsi data. Sedangkan algoritma kunci asimetris, digunakan dua kunci, kunci publik dan kunci rahasia. Kunci publik digunakan untuk mengenkripsi pesan, dan kunci rahasia digunakan untuk mendeskripsi pesan. Pengirim hanya mengetahui kunci publik, sedangkan penerima pesan mengetahui keduanya.

Salah satu teori aljabar abstrak yang digunakan dalam dunia kriptografi saat ini adalah quasigroup. Himpunan tak kosong Q, dan suatu operasi biner $*$ di Q disebut quasigrup jika untuk semua $a, b \in Q$ terdapat dengan tunggal $x, y \in Q$ sedemikian sehingga $a * x = b \quad$ dan $\quad y * a = b$. Sifat ketunggalan inilah yang digunakan dalam algoritma kriptogafi. Dalam tugas akhir ini dibahas mengenai sandi aliran berdasarkan transformasi quasigroup atas $\mathbb{Z}_p^*$ yang

merupakan salah satu penerapan konsep quasigroup. Algoritma ini termasuk dalam klasifikasi algoritma kunci simetris.

1.2. Rumusan Masalah

Rumusan masalah yang dibahas dalam skripsi ini adalah:

1. Bagaimana proses penyandian pesan rahasia menggunakan algoritma sandi aliran berdasarkan transformasi quasigroup atas $\mathbb{Z}_p^*$?

2. Bagaimana program komputer sederhana yang digunakan untuk memahami cara kerja algoritma sandi aliran berdasarkan transformasi quasigroup atas $\mathbb{Z}_p^*$?

1.3. Batasan Masalah

Tugas akhir ini hanya membahas tentang algoritma sandi aliran berdasarkan transformasi quasigroup atas $\mathbb{Z}_p^*$ dan konsep matematis yang melandasinya. Serta diberikan contoh kasus dan implementasinya dalam suatu program komputer menggunakan bahasa pemrograman Matlab.

1.4. Tujuan Penelitian dan Manfaat

Berdasarkan latar belakang dan perumusan masalah yang dikemukakan di atas, tujuan utama penelitian ini yaitu menunjukkan proses penyandian algoritma sandi aliran berdasarkan transformasi quasigroup atas $\mathbb{Z}_p^*$. Sebelumnya, terlebih dahulu dikenalkan konsep matematis yang melandasi pem-

bentukan algoritma sandi tersebut. Selain itu, dibuat pula program komputer sederhana untuk memahami cara kerja algoritma sandi aliran berdasarkan transformasi quasigroup atas $\mathbb{Z}_p^*$. Penelitian ini diharapkan dapat memberikan kontribusi di bidang kriptografi dan meningkatkan minat untuk mempelajari kriptografi.

1.5. Tinjauan Pustaka

Penelitian mengenai kriptografi telah banyak dilakukan oleh para akademisi dan menghasilkan banyak algoritma penyandian baru dengan efektifitas dan keamanan yang lebih baik. Zaki,(2007) dalam skripsinya yang berjudul *Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi ElGamal Atas Grup Pergandaan* $\mathbb{Z}_p^*$ membahas tentang algoritma ElGamal. Namun, kekurangan algoritma ini yaitu dalam hal efisiensi karena kecepatan enkripsi maupun dekripsinya berjalan lambat.

Gligoroski (2004) dalam jurnalnya yang berjudul *Stream Cipher Based on Quasigroup String Transformation in* $\mathbb{Z}_p^*$ memberikan penjelasan tentang algoritma Stream Cipher berdasarkan transformasi quasigroup pada $\mathbb{Z}_p^*$ yang merupakan penerapan dari teori quasigroup. Kelebihan dari algoritma ini yaitu dalam hal efisiensi dan kecepatan enkripsi maupun dekripsi, serta tidak memerlukan perangkat keras yang berspesifikasi tinggi. Tetapi konsep matematis algoritma ini belum dijelaskan secara mendetail.

Menezes, dkk. (1996) dalam bukunya yang berjudul *Handbook of Applied Cryptography* membahas tentang dasar-dasar kriptografi dan terapannya.

Hoffstein, dkk, (2008) memberikan penjelasan tentang penghitungan modulo. Sedangkan penjelasan mengenai bilangan bulat dan dasar struktur aljabar pada kriptografi dijelaskan Buchmann (2000) pada bukunya yang berjudul *Introduction to Cryptography.*

Penelitian yang dilakukan penulis yaitu menjelaskan mengenai dasar-dasar kriptografi tentang algoritma ini, konsep matematis yang melandasinya, serta merancang dan membuat suatu program komputer untuk mensimulasikan algoritma ini.

1.6. Metodologi Penelitian

Penelitian ini dilakukan dengan metode studi literatur hasil penelitian dari D. Gligoroski yang membahas tentang sandi aliran berdasarkan transformasi pada quasigroup atas $\mathbb{Z}_p^*$. Terlebih dahulu dipelajari apa itu kriptografi, jenis-jenis kriptografi dan sebagainya. Kemudian dipelajari pula konsep bilangan bulat, penghitungan modulo serta quasigroup dan teorema-teorema yang digunakan dalam pokok pembahasan. Pada pokok pembahasan, diberikan materi tentang sandi aliran berdasarkan transformasi pada quasigroup atas $\mathbb{Z}_p^*$. Langkah terakhir adalah melakukan perancangan program komputer untuk mensimulasikan cara kerja algoritma tersebut dengan menggunakan bahasa pemrograman Matlab.

1.7. Sistematika Penulisan

Pembahasan materi disusun menjadi empat bab dengan sistematika sebagai berikut: pada bab I berisi pendahuluan yang meliputi latar belakang, perumusan masalah, batasan masalah, maksud dan tujuan penulisan skripsi, tinjauan pustaka, metode penulisan, sertasistematika penulisan skripsi. Bab II khusus memuat landasan teori yang berhubungan dengan topik bahasan. Beberapa hal yang akan dibahas antara lain pengertian umum kriptografi, definisi quasigroup dan beberapa teorema yang dipakai dalam algoritma kriptografi. Bab III merupakan inti dari tugas akhir ini, berisi tentang pembahasan masalah tentang penerapan quasigroup dalam kriptografi yaitu pada sandi aliran berdasarkan transformasi quasigroup atas $\mathbb{Z}_p^*$ serta contoh proses enkripsi dan deskripsinya. Bab ini juga mencakup tentang langkah-langkah pembuatan program komputer untuk mensimulasikan cara kerja algoritma sandi aliran berdasarkan transformasi quasigroup atas $\mathbb{Z}_p^*$ dalam menyandikan pesan. Kemudian dilakukan uji coba dan pembahasan hasil uji coba program tersebut. Sedangkan bab IV merupakan kesimpulan dan saran-saran yang dapat diambil berdasarkan materi-materi yang telah dibahas pada bab-bab sebelumnya.

BAB IV

PENUTUP

Berdasarkan materi-materi yang telah dibahas pada bab-bab sebelumnya, diperoleh kesimpulan dan saran-saran yang dapat diambil .

4.1. Kesimpulan

Kesimpulan yang dapat diambil penulis setelah menyelesaikan penyusunan skripsi ini adalah :

1. Aljabar abstrak, khususnya quasigroup, dapat diterapkan pada algoritma kriptografi karena memiliki sifat invers kiri dan kanan tunggal.

2. Kemampuan enkripsi dan dekripsi pada sandi kunci simetris, atau dalam hal ini sandi aliran berdasarkan transformasi pada quasigroup atas $\mathbb{Z}_p^*$, berjalan cepat sehingga sangat efisien untuk memproses data yang besar.

3. Semakin besar bilangan prima p yang digunakan dan semakin banyak jumlah leader yang dipakai, kekuatan algoritma sandi semakin meningkat.

4. Kelemahan algoritma sandi kunci simetris yaitu dalam hal distribusi kunci, karena hanya pihak pengirim dan penerima pesan yang boleh mengetahui kunci rahasia.

4.2. Saran

Setelah membahas dan mengimplementasikan algoritma sandi aliran berdasarkan transformasi pada quasigroup atas $\mathbb{Z}_p^*$, penulis menyampaikan beberapa saran.

1. Diperlukan suatu metode untuk mendistribusikan kunci secara aman.
2. Untuk menjaga keaslian pesan rahasia, diperlukan suatu cara untuk mengantisipasi perubahan pesan.
3. Penyempurnaan program komputer sangat diperlukan, terutama agar dapat menggunakan sejumlah n buah leader.

DAFTAR PUSTAKA

Achmad, Ikhwanudin, 2007, *Aplikasi Invers Matriks Tergeneralisasi pada Cipher Hill*, Skripsi, Yogyakarta: Fakultas Matematika dan Ilmu Pengetahuan Alam UGM.

Buchmann, J. A., 2000, *Introduction to Cryptography*, Springer-Verlag New York, Inc., USA.

Gligoroski, D., 2004, *Stream Cipher Based on Quasigroup String Transformation in* $\mathbb{Z}_p^*$, University St. Cyril and Methodious, Republic of Macedonia.

Hoffstein, J., Pipher, J., Silverman, J. H., *An Introduction to Mathematical Cryptography*, Springer Science+Business Media, New York, USA.

Malik, D. S., Mordeson, J. N., Sen, M. K., 2007, *Introduction to Abstrack Algebra*, United States of America.

Markovski, S., Gligoroski, D., Andova, S., 1997, *Using quasigroups for one-one secure encoding*, University St. Cyril and Methodious, Republic of Macedonia.

Menezes, Oorcshot, Vanstone, 1996, *Handbook of Applied Cryptography*, CRC Press, Inc. USA.

Stinson, Douglas R., 2006, *Cryptography Theory and Practice Third Edition*, University of Waterloo, Ontario, Canada.

Wikipedia, 2013, *Cryptography*, http://en.wikipedia.org/wiki/Cryptography, 22 Januari 2013, 22:13.

Wikipedia, 2013, *Frequency analysis*, https://en.wikipedia.org/wiki/Frequency_analysis, 22 Januari 2013, 23:05.

Riyanto, M. Zaki, 2007, *Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi ElGamal Atas Grup Pergandaan Zp**, Skripsi, Yogyakarta : Fakultas Matematika dan Ilmu Pegetahuan Alam UGM.

LAMPIRAN

SKRIP PROGRAM

```
%program utama quasigroup stream cipher
function streamcipher3leader
clc;
clear all;
ulang=true;
while ulang
disp('==========================================================');
disp('Simulasi Program Pengamanan Pesan Rahasia');
disp('Stream Cipher Based on Quasigroup in Zp');
disp('');
disp('M. Adib Jauhari Dwi Putra');
disp('==========================================================');

disp('Pilih menu: ');
disp('1. enkripsi');
disp('2. dekripsi');
disp('3. keluar')
disp(' ');
pilih=input('pilihan anda (1-2-3)-->> ');
switch pilih
    case 1
        disp(' ');
        disp('=====================================');
```

```
24          disp('Enkripsi Pesan Rahasia');
25          disp('==========================');
26          enkripsi3leader
27          disp('Tekan sembarang tombol untuk lanjut');
28          pause
29      case 2
30          disp(' ');
31          disp('==========================');
32          disp('Dekripsi Pesan Rahasia');
33          disp('==========================');
34          dekripsi3leader
35          disp('Tekan sembarang tombol untuk lanjut');
36          pause
37      case 3
38          disp(' ');
39          disp('Terima kasih');
40          ulang=false;
41      otherwise
42          disp('Pilihan Tidak Ada');
43          disp('Tekan sembarang tombol untuk lanjut');
44          pause
45  end;
46  end
```

```
1  function y=invmodn(b,p);
2  %fungsi ini digunakan untuk mencari nilai invers dari b mod n
3  %dasar program: Algoritma Euclid yang diperluas
```

```
%sumber: Skripsi Ikhwanudin Achmad {Aplikasi Invers Matriks
%Tergeneralisasipada Cipher Hill}
n0=p;
b0=b;
t0=0;
t=1;

q=floor(n0/b0);
r=n0-q*b0;
while r>0,
    temp=t0-q*t;
    if(temp >=0),
        temp=mod(temp,p);
    end;
    if (temp < 0),
        temp=p - ( mod(-temp,p));
    end;
    t0=t;
    t=temp;
    n0=b0;
    b0=r;
    q=floor(n0/b0);
    r=n0-q*b0;
end;
 if b0~=1,
    y=[];
    %disp('No Inverse');
```

```
31 else
32     y=mod(t,p);
33 end;
```

```
1  %program enkripsi pesan rahasia dengan menggunakan 3 leader
2  function enkripsi3leader
3  prima_ke=input('Bilangan prima ke berapa yang akan digunakan? ');
4  pri=primes(10000000);
5  pr=pri(prima_ke);
6  if pr>10000000
7      disp('Prima terlalu besar');
8  else prima=pr;
9      disp(['Bilangan prima yang dipakai adalah ', num2str(prima)]);
10 end
11 batas=prima-1;
12 batas2=prima-2;
13 K=input(['Masukkan sembarang K, 1<=K<=',num2str(batas),'= ']);
14 leader1=input(['masukkan leader ke-1,  1<=leader 1<=',
15     num2str(batas2),'='] );
16 leader2=input(['masukkan leader ke-2,  1<=leader 2<=',
17     num2str(batas2),'=']);
18 leader3=input(['masukkan leader ke-3,  1<=leader 3<=',
19     num2str(batas2),'=']);
20 pesan=input('masukkan karakter pesan yang akan di enkripsi ');
21
22 jml=length(pesan);
23
```

```
24 message=pesan(1);
25
26 s=(K+message);
27 c=prima-1;
28 r=mod (s,c);
29 b= 1+r;
30 y=invmodn (b,prima);
31 as=leader1*y;
32 m_enkrip1=mod (as,prima);
33
34 s=(K+m_enkrip1);
35 c=prima-1;
36 r=mod (s,c);
37 b= 1+r;
38 y=invmodn (b,prima);
39 as=leader2*y;
40 m_enkrip2=mod (as,prima);
41
42 s=(K+m_enkrip2);
43 c=prima-1;
44 r=mod (s,c);
45 b= 1+r;
46 y=invmodn (b,prima);
47 as=leader3*y;
48 m_enkrip3(1)=mod (as,prima);
49
50 for n=1:(jml-1)
```

```
51
52      leader3=1+mod((m_enkrip1+m_enkrip2+m_enkrip3(n)),prima-1);
53      pesan(n+1);
54      s=([K+pesan(n+1)]);
55      c=prima-1;
56      r=mod (s,c);
57      b= 1+r;
58      y=invmodn (b,prima);
59      as=m_enkrip1*y;
60      m_enkrip1=mod (as,prima);
61
62      s=(K+m_enkrip1);
63      c=prima-1;
64      r=mod (s,c);
65      b= 1+r;
66      y=invmodn (b,prima);
67      as=m_enkrip2*y;
68      m_enkrip2=mod (as,prima);
69
70      s=(K+m_enkrip2);
71      c=prima-1;
72      r=mod (s,c);
73      b= 1+r;
74      y=invmodn (b,prima);
75      as=leader3*y;
76      m_enkrip3(n+1)=mod (as,prima);
77  end
```

```
78 disp(['Cipherteksnya adalah ',num2str(m_enkrip3)])
79 return
```

```
1  %program dekripsi pesan rahasia dengan menggunakan 3 leader
2  function dekripsi3leader
3  prima_ke=input('Bilangan prima ke berapa yang akan digunakan? ');
4  pri=primes(10000000);
5  pr=pri(prima_ke);
6  if pr>10000000
7      disp('Prima terlalu besar');
8  else prima=pr;
9      disp(['Bilangan prima yang dipakai adalah ', num2str(prima)]);
10 end
11 batas=prima-1;
12 batas2=prima-2;
13 K=input(['Masukkan sembarang K, 1<=K<=',num2str(batas),'= ']);
14 leader3=input(['masukkan leader ke-1,  1<=leader 1<=',
15     num2str(batas2),'='] );
16 leader2=input(['masukkan leader ke-2,  1<=leader 2<=',
17     num2str(batas2),'=']);
18 leader1=input(['masukkan leader ke-3,  1<=leader 3<=',
19     num2str(batas2),'=']);
20 cipher=input('Masukkan karakter cipherteks yang akan di dekripsi ')
21
22 jml=length(cipher);
23
24 c2=invmodn(cipher(1),prima);
```

```
25 ij=leader1*c2;
26 ijp=mod(ij,prima);
27 cipher2=mod([ijp-1-K],[prima-1]);
28
29 c2=invmodn(cipher2,prima);
30 ij=leader2*c2;
31 ijp=mod(ij,prima);
32 cipher1=mod([ijp-1-K],[prima-1]);
33
34 c2=invmodn(cipher1,prima);
35 ij=leader3*c2;
36 ijp=mod(ij,prima);
37 plainteks(1)=mod([ijp-1-K],[prima-1]);
38
39 for n=1:(jml-1)
40
41     leader1=1+mod((cipher1+cipher2+cipher(n)),prima-1);
42     leader2=cipher2;
43     leader3=cipher1;
44     c2=invmodn(cipher(n+1),prima);
45     ij=leader1*c2;
46     ijp=mod(ij,prima);
47     cipher2=mod([ijp-1-K],[prima-1]);
48
49     c2=invmodn(cipher2,prima);
50     ij=leader2*c2;
51     ijp=mod(ij,prima);
```

```
52        cipher1=mod([ijp-1-K],[prima-1]);
53
54        c2=invmodn(cipher1,prima);
55        ij=leader3*c2;
56        ijp=mod(ij,prima);
57        plainteks(n+1)=mod([ijp-1-K],[prima-1]);
58  end
59  plainteks=char(plainteks);
60  disp(['Plainteksnya adalah= ',num2str(plainteks)]);
61  return
```

LAMPIRAN

TABEL KODE ASCII

Kode ASCII (0 - 127)

No.	Kode	No.	Kode	No.	Kode	No.	Kode
0	NULL	32	SP (*Space*)	64	@	96	`
1	SOH (*Start of Heading*)	33	!	65	A	97	a
2	STX (*Start of Text*)	34	"	66	B	98	b
3	ETX (*End of Text*)	35	#	67	C	99	c
4	EOT (*End of Transmission*)	36	$	68	D	100	d
5	ENQ (*Enquiry*)	37	%	69	E	101	e
6	ACK (*Acknowledge*)	38	&	70	F	102	f
7	BEL (*Bell*)	39	'	71	G	103	g
8	BS (*Backspace*)	40	(	72	H	104	h
9	HT (*Horizontal Tab*)	41	)	73	I	105	i
10	NL (*New Line*)	42	*	74	J	106	j
11	VT (*Vertical Tab*)	43	+	75	K	107	k
12	NP (*New Page*)	44	,	76	L	108	l
13	CR (*Carriage Return*)	45	-	77	M	109	m
14	SO (*Shift Out*)	46	.	78	N	110	n
15	SI (*Shift In*)	47	/	79	O	111	o
16	DLE (*Data Link Escape*)	48	0	80	P	112	p
17	DC1 (*Device Control 1*)	49	1	81	Q	113	q
18	DC2 (*Device Control 2*)	50	2	82	R	114	r
19	DC3 (*Device Control 3*)	51	3	83	S	115	s
20	DC4 (*Device Control 4*)	52	4	84	T	116	t
21	NAK (*Negative Acknowledge*)	53	5	85	U	117	u
22	SYN (*Synchronus Idle*)	54	6	86	V	118	v
23	ETB (*End of Trans. Blok*)	55	7	87	W	119	w
24	CAN (*Cancel*)	56	8	88	X	120	x
25	EM (*End of Medium*)	57	9	89	Y	121	y
26	SUB (*Substitute*)	58	:	90	Z	122	z
27	ESC (*Escape*)	59	;	91	[	123	{
28	FS (*File Separator*)	60	<	92	\	124	|
29	GS (*Group Separator*)	61	=	93	]	125	}
30	RS (*Record Separator*)	62	>	94	^	126	~
31	US (*Unit Separator*)	63	?	95	_	127	DEL

Kode ASCII *Extended* (128 - 255)

128	Ç	144	É	161	í	177	▒	193	┴	209	╤	225	ß	241	±
129	ü	145	æ	162	ó	178	▓	194	┬	210	╥	226	Γ	242	≥
130	é	146	Æ	163	ú	179	│	195	├	211	╙	227	π	243	≤
131	â	147	ô	164	ñ	180	┤	196	─	212	╘	228	Σ	244	⌠
132	ä	148	ö	165	Ñ	181	╡	197	┼	213	╒	229	σ	245	⌡
133	à	149	ò	166	ª	182	╢	198	╞	214	╓	230	µ	246	÷
134	å	150	û	167	º	183	╖	199	╟	215	╫	231	τ	247	≈
135	ç	151	ù	168	¿	184	╕	200	╚	216	╪	232	Φ	248	°
136	ê	152	ÿ	169	⌐	185	╣	201	╔	217	┘	233	Θ	249	∙
137	ë	153	Ö	170	¬	186	║	202	╩	218	┌	234	Ω	250	·
138	è	154	Ü	171	½	187	╗	203	╦	219	█	235	δ	251	√
139	ï	156	£	172	¼	188	╝	204	╠	220	▄	236	∞	252	ⁿ
140	î	157	¥	173	¡	189	╜	205	═	221	▌	237	φ	253	²
141	ì	158	₧	174	«	190	╛	206	╬	222	▐	238	ε	254	■
142	Ä	159	ƒ	175	»	191	┐	207	╧	223	▀	239	∩	255	
143	Å	160	á	176	░	192	└	208	╨	224	α	240	≡		