APLIKASI ALJABAR *MIN-PLUS* UNTUK MENGAMANKAN INFORMASI RAHASIA

SKRIPSI

Diajukan kepada Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Negeri Yogyakarta
untuk Memenuhi Sebagian Persyaratan
Guna Memperoleh Gelar Sarjana Sains

Oleh :

Dimas Ridwan Wicaksono

10305141025

PROGRAM STUDI MATEMATIKA
JURUSAN PENDIDIKAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS NEGERI YOGYAKARTA

2014

PERSETUJUAN

Skripsi yang berjudul:

APLIKASI ALJABAR *MIN-PLUS* UNTUK MENGAMANKAN INFORMASI RAHASIA

yang disusun oleh:

Dimas Ridwan Wicaksono

10305141025

telah disetujui oleh dosen pembimbing pada tanggal 24 Oktober 2014

untuk diujikan dihadapkan dewan penguji Skripsi

Menyetujui,

Dosen Pembimbing

Musthofa, M.Sc.

NIP. 19801107 200604 1 001

PERNYATAAN

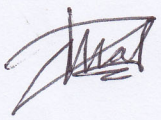
Yang bertanda tangan di bawah ini, saya:

Nama	: Dimas Ridwan Wicaksono
NIM	: 10305141025
Prodi	: Matematika
Jurusan	: Pendidikan Matematika
Fakultas	: MIPA
Judul TAS	: Aplikasi Aljabar *Min-Plus* untuk Mengamankan Informasi Rahasia

dengan ini menyatakan bahwa skripsi ini merupakan hasil karya saya sendiri dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang ditulis atau diterbitkan oleh orang atau institusi lain kecuali pada bagian tertentu yang memang diambil sebagai pedoman, acuan atau kutipan dengan mengikuti tata penulisan karya ilmiah yang telah lazim. Apabila ternyata terbukti pernyataan ini tidak benar maka sepenuhnya menjadi tanggungjawab saya sebagai penulis dan bersedia menerima sanksi sesuai peraturan yang berlaku.

Yogyakarta, 24 Oktober 2014

Yang menyatakan,



Dimas Ridwan Wicaksono

NIM. 10305141025

PENGESAHAN

Skripsi yang berjudul "APLIKASI ALJABAR *MIN-PLUS* UNTUK MENGAMANKAN INFORMASI RAHASIA" yang disusun oleh Dimas Ridwan Wicaksono, NIM 10305141025 ini telah dipertahankan di depan Dewan Penguji pada tanggal 31 Oktober 2014 dan dinyatakan lulus.

DEWAN PENGUJI

Nama	Jabatan	Tanda Tangan	Tanggal
Musthofa, M.Sc 19801107200604100 1	Ketua Penguji	.....	10-11-2014
Nur Hadi W., M.Eng 197801192003121002	Sekretaris Penguji	.....	10-11-2014
Bambang S.H.M., M.Kom 196802101998121001	Penguji Utama	.....	10-11-2014
Kuswari H., M.Kom 197604142005012002	Penguji Pendamping	.....	7-11-2014

Yogyakarta, 12 November 2014
Fakultas Matematika dan Ilmu Pengetahuan Alam
Dekan,

Dr. Hartono
NIP 196203291987021002

MOTTO

Berusahalah jangan sampai terlengah walau sedetik saja, karena atas kelengahan kita tak akan bisa dikembalikan seperti semula

Sesuatu yang belum dikerjakan, seringkali tampak mustahil, kita baru yakin kalau kita telah berhasil melakukannya dengan baik. (Evelyn Underhill)

Rasa percaya diri adalah kunci rahasia pertama dari sukses seseorang (Ralph waldo Emerson)

Orang yang murah senyum akan menambah deretan relasi, rejeki, dan prestasi

PERSEMBAHAN

Segala puji syukur kepada Allah SWT

Kupersembahkan karya sederhana ini untuk

"Kedua orang tuaku, Hardilan dan Sri Maryatin"

yang telah memberikan makna dalam hidupku.

Ucapan terima kasih yang dalam atas segala doa, kasih sayang, pengertian,

dukungan dan kesabaran

Rizal, Aryo, Bayu, Ikfan, Nanang, Lina dan rekan-rekan Matsub 2010

Untuk kebersamaan, dalam berjuang bersama

Salam sayang untuk kalian, untuk segalanya.

Sungguh, aku beruntung memiliki kalian.

Aplikasi Aljabar *Min-Plus* untuk Mengamankan Informasi Rahasia

Oleh:

Dimas Ridwan Wicaksono

10305141025

ABSTRAK

Protokol perjanjian kunci merupakan suatu skema dalam kriptografi yang digunakan untuk mengatasi masalah pengiriman informasi yang bersifat rahasia. Dalam mengamankan informasi tersebut dibutuhkan suatu kunci. Kedua belah pihak yang saling bertukar informasi harus menyepakati kunci yang sama. Kunci tersebut digunakan pada proses enkripsi dan dekripsi diantara dua pihak yang saling berkomunikasi.

Pada penelitian ini protokol perjanjian kunci yang digunakan tingkat keamanannya didasarkan pada operasi matriks dalam aljabar *min-plus* atas $\mathbb{Z}$. Aljabar *min-plus* atas $\mathbb{Z}$ merupakan himpunan $\mathbb{Z} \cup \{+\infty\}$ dengan $\mathbb{Z}$ adalah himpunan semua bilangan bulat yang dilengkapi operasi minimum, dinotasikan dengan $\oplus$, dan operasi penjumlahan yang dinotasikan dengan $\otimes$. Selanjutnya ($\mathbb{Z} \cup \{+\infty\}, \oplus, \otimes$) dinotasikan dengan $\mathbb{Z}_{min}$.

Hasil penelitian menunjukkan bahwa sifat perkalian matriks atas aljabar *min-plus* dapat diterapkan untuk menentukan kunci pada proses pengamanan informasi secara rahasia dengan algoritma pembentukan kunci. Diperoleh kunci yang sama antara pihak 1 dan pihak 2, yaitu $K = K_1 = K_2$. Kunci tersebut digunakan pada proses enkripsi dan dekripsi. Proses enkripsi dilakukan dengan cara mengubah *plaintext* ke dalam bentuk *ciphertext* dan dilakukan perhitungan dengan modulo 94 dengan rumus $C_i = (K + P_i)$ mod 94, sedangkan proses dekripsi dilakukan dengan cara mengubah *ciphertext* ke dalam bentuk *plaintext* dan dilakukan perhitungan dengan modulo 94 dengan rumus $P_i = (C_i - K)$ mod 94 dengan C_i adalah *ciphertext*, P_i adalah *plaintext*, serta K adalah kunci.

Kata kunci: Kriptografi, Kunci, Aljabar *Min-Plus*

KATA PENGANTAR

Segala puji bagi Allah SWT, Tuhan semesta alam atas segala rahmat, hidayah, dan inayah-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan lancar. Skripsi yang berjudul "Aplikasi Aljabar *Min-Plus* untuk Mengamankan Informasi Rahasia" ini disusun untuk memenuhi salah satu syarat kelulusan meraih gelar sarjana sains pada Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Negeri Yogyakarta. Dalam penyusunan skripsi ini, penulis tidak lepas dari bimbingan, dukungan, dan bantuan berbagai pihak. Berbagai dukungan, kritik, saran, semangat, dan motivasi, penulis dapatkan demi terselesaikannya skripsi ini. Oleh karena itu dalam kesempatan ini dengan segala kerendahan hati, penulis ingin menyampaikan terimakasih kepada:

1. Bapak Dr. Hartono selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Negeri Yogyakarta.
2. Bapak Dr. Sugiman selaku Ketua Jurusan Pendidikan Matematika FMIPA UNY.
3. Bapak Dr. Agus Maman Abadi, selaku Koordinator Program Studi Matematika Jurusan Pendidikan Matematika FMIPA UNY dan selaku Pembimbing Akademik.
4. Bapak Musthofa, M.Sc., selaku Dosen Pembimbing tugas akhir skripsi yang dengan penuh kesabaran telah memberikan arahan dan bimbingan kepada penulis.

5. Seluruh Dosen Jurusan Pendidikan Matematika FMIPA UNY dan guru-guru almamater yang selama masa studi ini telah memberikan banyak ilmu, motivasi dan pengalaman hidup yang berharga kepada penulis.
6. Teman-teman Matematika 2010 yang selalu memberikan keceriaan, dukungan, dan motivasi kepada penulis dalam proses penyusunan skripsi ini.
7. Semua pihak yang tidak dapat penulis sebutkan satu per satu.

Penulis menyadari bahwa dalam pembuatan tugas akhir skripsi ini masih terdapat banyak kekurangan. Oleh karena itu, saran dan kritik sangat diharapkan sebagai koreksi demi kesempurnaan skripsi ini. Terakhir penulis berharap semoga tugas akhir skripsi ini dapat memberi manfaat bagi semua pihak yang membacanya.

Yogyakarta, 24 Oktober 2014

Penulis,

Dimas Ridwan Wicaksono

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

DAFTAR SIMBOL

$(S, +, \times)$	: Himpunan tak kosong S yang dilengkapi dengan dua operasi biner $+$ dan $\times$
$\mathcal{E}$	: elemen netral terhadap operasi *minium*$(\mathcal{E} \coloneqq +\infty)$
$\mathbb{Z}_{\mathcal{E}}$	: $\mathbb{Z} \cup \{\mathcal{E}\}$
$\oplus$	: operasi penjumlahan dalam aljabar *min-plus*
$\otimes$	: operasi perkalian dalam aljabar *min-plus*
$\mathbb{Z}_{min}$	: $(\mathbb{Z}_{\mathcal{E}}, \oplus, \otimes)$
$\mathbb{Z}$	: himpunan bilangan bulat
$\mathbb{Z}_{\mathcal{E}}$	: $\mathbb{Z} \cup \{\mathcal{E}\}$
P	: *plaintext*
C	: *ciphertext*
K	: kunci

BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi dewasa ini sangat berpengaruh besar terhadap segala aspek kehidupan, salah satunya di bidang informasi dan komunikasi seperti dalam proses pengiriman pesan. Banyak sekali manfaat yang didapat dengan adanya teknologi yang terus berkembang sehingga memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi secara jarak jauh. Seiring dengan berkembangnya teknologi dan informasi, tuntutan akan keamanan terhadap kerahasiaan informasi juga semakin meningkat. Tidak menutup kemungkinan adanya pihak ketiga yang ingin merubah isi pesan saat proses pengiriman tersebut. Hal inilah yang seringkali ditakutkan oleh pihak-pihak yang saling ingin bertukar informasi. Keamanan dan kerahasiaan sebuah data atau informasi dalam komunikasi menjadi hal yang sangat penting. Apabila informasi yang dikirim bersifat rahasia, maka jaminan keamanan informasi menjadi faktor utama yang harus dipenuhi. Berbagai hal telah dilakukan untuk mendapatkan jaminan keamanan informasi rahasia ini. Salah satu cara untuk mengatasi masalah tersebut adalah menggunakan kriptografi.

Kriptografi berasal dari bahasa Yunani, yang terdiri dari dua kata yaitu *cryptos* dan *graphein*. *Cryptos* berarti rahasia, dan *graphein* berarti tulisan. Sehingga menurut bahasa, kriptografi berarti tulisan rahasia.

Sedangkan definisi kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (Menezes, Oorcshot, and Vanstone, 1996). Secara umum, kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan berita (Bruce Schneier). Kriptografi memiliki dua konsep utama yaitu enkripsi dan dekripsi. Enkripsi adalah sebuah proses penyandian yang melakukan perubahan kode dari yang dapat dimengerti (*plaintext*) menjadi sebuah kode yang tidak dapat dimengerti (*ciphertext*), sedangkan proses kebalikannya yaitu mengubah *ciphertext* menjadi *plaintext* disebut dekripsi (Rinaldi, 2006). Proses enkripsi dan dekripsi memerlukan suatu kunci rahasia yang disepakati oleh kedua belah pihak.

Setiap komunikasi informasi apapun yang dilakukan sangat memerlukan adanya keamanan, termasuk komunikasi informasi secara elektronik. Di sinilah salah satu peran kriptografi dalam upaya mengamankan informasi, baik yang dilakukan secara *off-line* maupun *on-line*. Jadi hubungan kriptografi dan teknologi informasi adalah pada aplikasinya, dimana kriptografi bersifat membangun komunikasi lebih aman meskipun pada saat tertentu bisa mengurangi kecepatan dalam proses komunikasi. Protokol perjanjian kunci merupakan suatu metode dalam kriptografi yang digunakan untuk mengatasi masalah tersebut. Pada metode ini, kedua belah pihak saling menukarkan parameter yang dapat

diketahui oleh umum, akan tetapi dari parameter tersebut dapat dibentuk suatu kunci rahasia yang sama dan tidak diketahui oleh umum.

Protokol perjanjian kunci pernah dibahas sebelumnya oleh Muhammad Zaki Riyanto (2012) dalam penelitiannya yang berjudul *Protokol Perjanjian Kunci Berdasarkan Masalah Faktorisasi Atas Semigrup Non-Komutatif*. Dalam penelitian ini penentuan semigrup yang non-komutatif dan order yang besar turut menentukan tingkat kesulitan dalam menyelesaikan masalah faktorisasi. Penelitian tersebut kemudian dikembangkan oleh Musthofa, Dwi Lestari (2013) dalam penelitian yang berjudul *Metode Perjanjian Password Berdasarkan Operasi Matriks atas Aljabar Min-Plus untuk Keamanan Pengiriman Informasi Rahasia.* Dalam penelitian ini dibahas tentang pengamanan informasi rahasia pada protokol perjanjian *password* dapat menggunakan operasi matriks atas aljabar *min-plus*. Rininda Ulfa Arizka (2011) dalam skripsi berjudul *Penerapan Sistem Kriptografi ElGamal atas* $\mathbb{Z}_p^*$ *Dalam Pembuatan Tanda Tangan Digital* menjelaskan tentang bagaimana menjaga keotentikan suatu dokumen dengan cara pembuatan tanda tangan digital dengan menggunakan sistem kriptografi ElGamal atas $\mathbb{Z}_p^*$.

Pembahasan mengenai protokol perjanjian kunci sekarang ini sudah banyak dibahas dan dikembangkan. Protokol perjanjian kunci Diffie-Hiellman merupakan salah satu contoh perjanjian kunci yang paling sederhana. Namun protokol ini memiliki kelemahan yaitu tidak adanya otentikasi dari pertukaran kunci sehingga rentan terhadap serangan (Decky

Hendarsyah dan Retantyo Wardoyo, 2011). Pada protokol perjanjian kunci Diffie-Hiellman digunakan grup siklik yang merupakan grup komutatif. Tingkat kemanan dari protokol perjanjian kunci Diffie-Hiellman didasarkan pada masalah logaritma diskrit pada grup siklik (Myasnikov dkk, 2008). Pada penelitian Stickel (2005) dalam Myasnikov dkk (2008) diperkenalkan konsep mengenai protokol perjanjian kunci yang menggunakan grup non-komutatif. Untuk dapat menggunakan grup tidak komutatif, protokol perjanjian kunci harus dapat dikonstruksi menggunakan suatu permasalahan matematis yang ada pada grup non-komutatif. Salah satu contoh grup yang dapat digunakan pada protokol perjanjian kunci Stickel adalah grup perkalian matriks atas suatu lapangan hingga. Penggunaan grup pada Protokol Stickel ini dapat diperumum menjadi sebarang *semiring*. Pada penulisan skripsi ini semiring yang digunakan adalah himpunan semua matriks $n\,x\,n$ atas $\mathbb{Z}$ dengan operasi penjumlahan biasa dan perkaliannya didefinisikan atas suatu aljabar *min-plus*, yaitu $(\mathbb{Z}_{min})^{n\times n}$.

Berdasarkan uraian tersebut, pada skripsi ini akan dibahas mengenai pengamanan informasi rahasia dimana dalam perhitungannya menggunakan operasi matriks atas aljabar min-plus. Implementasi algoritma dalam mengamankan pesan ini menggunakan perangkat lunak matlab. Program ini dapat digunakan untuk meningkatkan keamanan informasi sehingga menjadi lebih aman setelah diubah ke dalam bentuk kode, karena informasi hanya dapat dibaca oleh pihak yang berhak.

B. Batasan Masalah

Dalam skripsi ini, pembahasan algoritma yang digunakan pada proses pembentukan kunci digunakan protokol perjanjian kunci Stickel yang perhitungannya didasarkan pada operasi matriks dalam aljabar *min-plus* atas $\mathbb{Z}_{min}^{2x2}$. Untuk mempermudah perhitungan pada proses pembuatan kunci, enkripsi dan dekripsi digunakan perangkat lunak *Matlab*.

C. Rumusan Masalah

Berdasarkan latar belakang masalah, maka dirumuskan pokok permasalahan yang akan menjadi kajian dari skripsi ini, yaitu "Bagaimana menerapkan konsep-konsep dalam aljabar *min-plus* pada proses pengamanan informasi rahasia?".

D. Tujuan Penulisan

Berdasarkan rumusan masalah, tujuan dari penulisan skripsi ini adalah menjelaskan penerapan konsep-konsep dalam aljabar *min-plus* pada proses pengamanan informasi rahasia.

E. Manfaat Penulisan

Penulisan ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Solusi bagi pihak-pihak yang menggunakan sarana informasi dan komunikasi untuk dapat melakukan pengiriman informasi yang bersifat rahasia secara aman.
2. Memperoleh metode-metode baru dalam protokol perjanjian kunci menggunakan Aljabar *Min-Plus*.

3. Memberi informasi tentang Aljabar *Min-Plus* sebagai salah satu metode yang dapat digunakan untuk pengaplikasian dalam mengamankan informasi rahasia**.**

BAB II

DASAR TEORI

Pada bab ini akan dibahas tentang konsep dasar yang berhubungan dengan kriptografi. Adapun yang dibahas adalah tentang sistem kriptografi dan Aljabar *Min-Plus*.

A. Kriptografi

1. Definisi kriptografi

Kriptografi berasal dari bahasa Yunani, *cryptos* yang berarti rahasia dan *graphein* yang berarti tulisan. Jadi menurut bahasa, kriptografi merupakan tulisan rahasia. Ada beberapa definisi kriptografi yang telah dikemukakan di berbagai literatur. Bruce Schneier dalam bukunya yang berjudul *Applied Cryptography* mendefinisikan kriptografi sebagai ilmu dan seni untuk menjaga keamanan pesan. Menurut Rinaldi Munir (2006) kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas suatu data, serta otentikasi.

2. Terminologi Kriptografi

Di dalam kriptografi akan sering ditemukan berbagai istilah atau terminologi. Ada beberapa istilah penting yang sering digunakan yaitu:

a. Pesan, *Plaintext*, dan *Ciphertext*

Pesan adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah *Plaintext*, atau tak jelas (*cleartext*) (Schneier, 1996). Agar pesan tidak dapat dimengerti

maknanya oleh pihak lain, maka pesan perlu disandikan ke bentuk yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut *ciphertext* (Stamp, 2007).

Contoh 2.1 (contoh *plaintext*)

Hari itu saya pergi dengan mengendarai mobil berwarna merah.

Contoh 2.2 (contoh ciphertext)

t4e=o5 ?ye4| 1?y]4]?i z4e 12 e4l4e, 5yt4s s3ey4 84?4]+-84?4]+ ^4]+ 4@4 @1 @4l4e]^4.

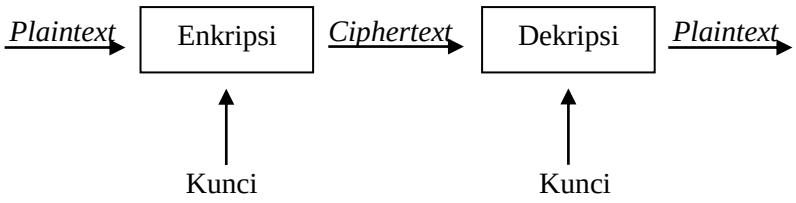
b. Pengirim dan Penerima

Suatu aktifitas komunikasi data akan melibatkan pertukaran pesan antara dua entitas, yaitu pengirim dan penerima. Pengirim adalah entitas dalam komunikasi yang mengirim informasi kepada entitas lainnya. Penerima adalah entitas dalam komunikasi yang diharapkan menerima informasi dari entitas lainnya (Rinaldi, 2006). Entitas yang dimaksud adalah orang atau sesuatu yang mengirim, menerima dan memanipulasi informasi. Entitas dapat berupa orang, mesin, dan sebagainya.

c. Enkripsi dan Dekripsi (Rinaldi, 2006)

Enkripsi adalah proses penyandian yang melakukan perubahan sebuah kode dari yang dapat dimengerti (*plaintext)* menjadi sebuah kode yang tidak dapat dimengerti (*ciphertext*), sedangkan proses mengembalikan

ciphertext menjadi *plaintext* disebut dekripsi. Skema enkripsi dan dekripsi disajikan pada gambar 2.1.



Gambar 2.1 Skema enkripsi dan dekripsi

d. Algoritma dan Kunci

Algoritma kriptografi disebut juga *cipher* yaitu aturan yang digunakan untuk enkripsi dan dekripsi (Schneier, 1996). Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yang berisi elemen-elemen *plaintext*. Dalam hal ini, enkripsi dan dekripsi merupakan suatu pesan yang memetakan elemen-elemen antara kedua himpunan tersebut. Misalkan *P* menyatakan *plaintext* dan *C* menyatakan *ciphertext*, maka fungsi enkripsi *E* memetakan *P* ke *C* atau dapat ditulis $E(P)=C$ dan fungsi dekripsi *D* memetakan *C* ke *P* atau dapat ditulis $D(C)=P$. Pengiriman pesan dalam kriptografi modern membutuhkan kunci yang harus dijaga kerahasiaannya. Kunci adalah parameter yang digunakan untuk mentransformasi proses pengenkripsian dan pendekripsian pesan. Kunci biasanya berupa deretan bilangan maupun *string*. Dengan menggunakan kunci *K*, maka fungsi enkripsi dan dekripsi dapat ditulis $E_k(P)=C$ dan $D_K(C)=P$ dan kedua fungsi tersebut memenuhi $D_k(E_k(P))=P$.

e. Sistem Kriptografi

Sistem kriptografi merupakan kumpulan yang terdiri dari *plaintext*, *ciphertext*, kunci, enkripsi serta dekripsi (Stinson, 2006).

f. Penyadap

Penyadap adalah orang yang berusaha menangkap pesan selama ditransmisikan dengan tujuan mendapatkan informasi sebanyak-banyaknya mengenai sistem kriptografi yang digunakan untuk berkomunikasi dengan maksud untuk memecahkan *ciphertext*.

g. Kriptanalisis

Kriptanalisis adalah ilmu dan seni untuk memecahkan *ciphertext* menjadi *plaintext* tanpa mengetahui kunci yang digunakan (Stamp, 2007). Pelakunya disebut kriptanalis.

3. Tujuan Kriptografi (Menezes, 1996)

Tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi adalah sebagai berikut

a. Kerahasiaan (*confidentiality*) merupakan layanan yang digunakan untuk menjaga isi informasi dari semua pihak yang tidak berhak untuk mendapatkannya kecuali pihak yang memiliki kunci rahasia untuk membuka informasi yang telah disandi.

b. Integritas Data (*data integrity)* merupakan layanan yang menjamin bahwa pesan masih asli. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-

pihak yang tidak berhak antara lain penyisipan, penghapusan, dan penggantian data lain ke data yang sebenarnya.

c. Autentikasi (*authentication*) merupakan suatu layanan yang berhubungan dengan identifikasi, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.

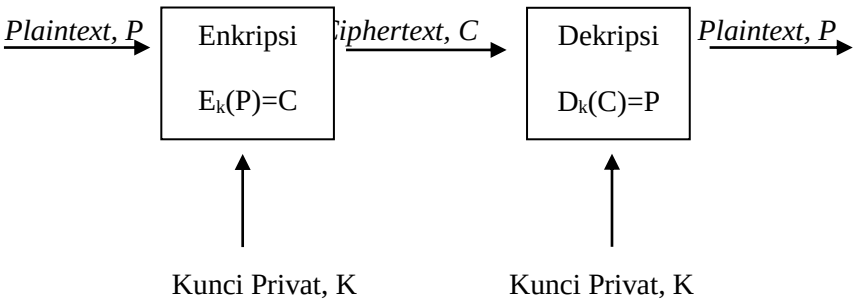
d. Nirpenyangkalan (*non-repudiation*) merupakan layanan untuk mencegah terjadinya penyangkalan terhadap pengirim maupun penerima yang saling berkomunikasi.

4. Jenis Algoritma Kriptografi

Berdasarkan jenis kunci yang digunakan dalam proses enkripsi dan dekripsi, kriptografi dibedakan menjadi kriptografi kunci simetri dan kriptografi kunci asimetri (Schneier, 1996) (Rinaldi, 2006) (Menezes, 1996).

a. Kriptografi Kunci Simetris

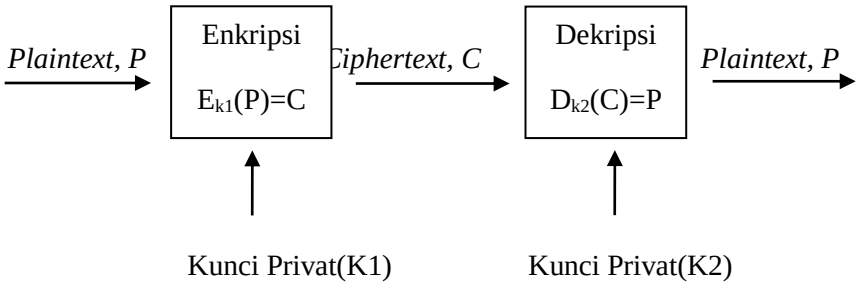
Pada sistem kriptografi simetri, kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Keamanan sistem kriptografi simetri terletak pada kerahasiaan kunci. Istilah lain untuk kriptografi simetri adalah kriptografi kunci privat. Skema kriptografi simetris disajikan pada gambar 2.2.



Gambar 2.2 Skema kriptografi simetris

b. Kriptografi Kunci Asimetri

Pada sitem kriptografi asimetri, kunci untuk proses enkripsi tidak sama dengan kunci untuk proses dekripsi. Kriptografi asimetri juga disebut dengan kunci publik, sebab kunci untuk enkripsi tidak rahasia dan dapat diketahui oleh siapapun, sementara untuk kunci dekripsi hanya diketahui oleh penerima pesan. Skema kriptografi asimetri disajikan pada gambar 2.3.



Gambar 2.3 Skema kriptografi asimetri

B. Protokol Perjanjian Kunci

Protokol perjanjian kunci merupakan skema dalam kriptografi yang digunakan untuk mengatasi masalah perjanjian kunci rahasia. Kunci tersebut digunakan pada proses enkripsi dan dekripsi diantara dua pihak yang saling berkomunikasi. Tingkat keamanan dari protokol perjanjian kunci diletakkan pada tingkat kesulitan dari suatu permasalahan matematis dan bertujuan agar kedua belah pihak dapat menentukan kunci yang sama. Protokol perjanjian kunci Diffie-Hiellman merupakan salah satu contoh perjanjian kunci yang paling sederhana yang dipublikasikan pada tahun 1976. Skema protokol perjanjian kunci Diffie-Hiellman disajikan pada gambar 2.4.

<table>
<tr><td colspan="2">Pihak 1 atau Pihak 2 mempublikasikan suatu grup siklik G
dengan elemen pembangun $g \in G$.</td></tr>
<tr><td>Pihak 1</td><td>Pihak 2</td></tr>
<tr><td>1. Memilih secara rahasia suatu bilangan positif a
2. Menghitung g^a
3. Mengirim g^akepada pihak 2
4. Menerima g^bdari pihak 2
5. Menghitung $K_1 = (g^a)^b = g^{ab}$</td><td>1. Memilih secara rahasia suatu bilangan positif b
2. Menghitung g^b
3. Mengirim g^b kepada pihak 1
4. Menerima g^a dari pihak 1
5. Menghitung $K_2=(g^b)^a= g^{ba}$</td></tr>
<tr><td colspan="2">Pihak 1 dan Pihak 2 telah menyepakati kunci rahasia $K = K_1 = K_2$</td></tr>
</table>

Gambar 2.4 Skema Protokol Perjanjian Kunci Diffie-Hiellman (Myasnikov dkk, 2008)

Setiap grup siklik merupakan grup komutatif, maka $ab = ba$, sehingga diperoleh $K = K_1 = K_2$. Misalkan Pihak 1 dan Pihak 2 telah berhasil menyepakati kunci rahasia yang sama yaitu *K*. Kemudian, kunci rahasia *K* yang telah disepakati digunakan untuk melakukan proses enkripsi dan dekripsi. Di lain pihak, Pihak 3 sebagai pihak penyerang hanya dapat mengetahui nilai *g*, g^a dan g^b. Untuk mendapatkan kunci yang telah disepakati Pihak 1 dan Pihak 2, Pihak 3 harus menentukan nilai *a* atau *b.* Dengan kata lain, Pihak 3 harus menyelesaikan masalah logaritma diskrit pada *G*, yaitu menentukan *a* apabila nilai g dan g^a diketahui. Tingkat kemanan dari protokol perjanjian kunci Diffie-Hiellman didasarkan pada masalah logaritma diskrit pada grup siklik (Myasnikov dkk, 2008).

Pada protokol perjanjian kunci Diffie-Hiellman digunakan grup siklik yang merupakan grup komutatif. Akan tetapi, pada penelitian Stickel (2005) dalam Myasnikov dkk (2008) diperkenalkan konsep mengenai protokol perjanjian kunci yang menggunakan grup non-komutatif. Myasnikov, dkk (2008) memberikan skema protokol perjanjian kunci Stickel yang didasarkan atas grup non-komutatif disajikan pada gambar 2.5.

Pihak 1 atau pihak 2 mempublikasikan suatu grup non-komutatif Gdan $a, b \in G, ab \neq ba$, dengan N dan M berturut-turut adalah order dari a dan b.	
Pihak 1	**Pihak 2**
1. Memilih secara rahasia $n < N$ dan $m < M$ 2. Menghitung $U = a^n b^m$ 3. Mengirim U kepada pihak 2 4. Menerima V dari pihak 2 5. Menghitung $K_1 = a^n V b^m$	1. Memilih secara rahasia $r < N$ dan $s < M$ 2. Menghitung $V = a^r b^s$ 3. Mengirim V kepad pihak 1 4. Menerima U dari pihak 1 5. Menghitung $K_2 = a^r U b^s$
Pihak 1 dan pihak 2 telah menyepakati kunci rahasia $K = K_1 = K_2$	

Gambar 2.5 Skema Protokol Perjanjian Kunci Stickel (Myasnikov dkk, 2008)

Ditunjukkan bahwa pihak 1 dan pihak 2 telah berhasil menyepakati kunci yang sama yaitu

$$K_1 = a^n V b^m = a^n a^r b^s b^m = a^{n+r} b^{s+m} = a^r a^n b^m b^s = a^r U b^s = K_2$$

Grup perkalian matriks atas suatu lapangan hingga merupakan salah satu contoh grup yang dapat digunakan pada protokol perjanjian kunci Stickel. Penggunaan grup pada Protokol Stickel ini dapat diperumum menjadi sebarang semigrup, juga dapat diperumum menjadi sebarang semiring. Pada penulisan skripsi ini semiring yang digunakan adalah himpunan semua matriks$n\ x\ n$ atas $\mathbb{Z}$ dengan operasi penjumlahan biasa dan perkaliannya didefinisikan atas suatu aljabar *min-plus*, yaitu $(\mathbb{Z}_{min})^{n \times n}$.

C. Aljabar *Min-Plus*

Pada subbab ini dibahas pengertian aljabar *min-plus* dan sifat-sifatnya. Pada bagian ini aljabar *min-plus* yang digunakan didefinisikan atas himpunan $\mathbb{Z}$.

Aljabar *min-plus* atas $\mathbb{Z}$ merupakan himpunan $\mathbb{Z} \cup \{+\infty\}$ yang dilengkapi dengan operasi minimum, dinotasikan dengan $\oplus$, dan operasi penjumlahan yang dinotasikan dengan $\otimes$. Selanjutnya $(\mathbb{Z} \cup \{+\infty\}, \oplus, \otimes)$ dinotasikan dengan $\mathbb{Z}_{min}$.(Musthofa, 2013).

Definisi 2.1 (Subiono, 2010)

Suatu *semiring* $(S, +, \times)$, adalah suatu himpunan tak kosong S disertai dengan dua operasi biner $+$ dan $\times$, yang memenuhi aksioma berikut:

1) $(S, +)$ merupakan semigrup komutatif dengan elemen netral 0, yaitu $\forall x, y, z \in S$ memenuhi

$$x + y = y + x$$

$$(x + y) + z = x + (y + z)$$

$$x + 0 = 0 + x = x,$$

2) $(S, \times)$ adalah semigrup dengan elemen satuan 1, yaitu $\forall x, y, z \in S$memenuhi

$$(x \times y) \times z = x \times (y \times z)$$

$$x \times 1 = 1 \times x = x,$$

3) sifat penyerapan elemen netral 0 terhadap operasi $\times$, yaitu $\forall x \epsilon S$ memenuhi

$$x \times 0 = 0 \times x = 0.$$

4) Operasi $\times$ distributif terhadap $+$, yaitu $\forall x, y, z \epsilon S$ berlaku

$$(x + y) \times z = (x \times z) + (y \times z),$$

$$x \times (y + z) = (x \times y) + (x \times z)$$

Suatu *semiring* (S, +, $\times$) dikatakan komutatif jika operasi $\times$ bersifat komutatif, yaitu $\forall x, y \in \boldsymbol{S}, x \times y = y \times x$.

Definisi 2.2 (Subiono, 2010)

Bila suatu *semiring* $(S, +, \times)$ terhadap operasi $\times$ berlaku$\forall x, y \epsilon S$, $x \times y = y \times x$, maka dikatakan *semiring* komutatif.

Definisi 2.3 (Subiono, 2010)

Bila suatu *semiring* $(S, +, \times)$ mempunyai sifat idempoten terhadap operasi $+$ yaitu untuk setiap x di S berlaku $x + x = x$, maka dikatakan *semiring* idempoten atau dioid.

Contoh 2.3

Semiring $\mathbb{Z}_{min}$ merupakan *semiring* komutatif yang sekaligus idempoten, sebab untuk setiap $x, y \epsilon \mathbb{Z}_{\varepsilon}$ berlaku $xy = x + y = y + x = y \otimes x$ dan $x \oplus x = min\{x, x\} = x$

Definisi 2.4(Subiono, 2010)

Suatu *semiring* komutatif $(S, +, \times)$ dinamakan *semifield* bila setiap elemen x di $S - \{0\}$ mempunyai invers terhadap operasi $\times$, yaitu untuk setiap x di $S - \{0\}$ ada x^{-1} sehingga $x \times x^{-1} = x^{-1} \times x = 1$.

Contoh 2.4

Semiring komutatif $\mathbb{Z}_{min}$ merupakan *semifield*, sebab untuk setiap $x \in \mathbb{Z}$ ada $-x$, sehingga berlaku $x\ (-x) = x + (-x) = 0$

Dari Contoh **2.3** dan **2.4** di atas terlihat bahwa $\mathbb{Z}_{min}$ merupakan *semifield* idempoten. Elemen-elemen $\mathbb{Z}_{min}$ akan disebut juga dengan skalar. Seperti halnya dalam aljabar biasa, prioritas urutan operasi $\otimes$ lebih dulu atas operasi $\oplus$. Misalnya,

1) $10 \otimes -7 \oplus 6 \otimes 2$, mempunyai arti

   $(10 \otimes -7) \oplus (6 \otimes 2) = 3 \oplus 8 = max\{3, 8\} = 8$

2) $5 \oplus 10 \otimes 6 \otimes 2$, mempunyai arti

   $5 \oplus (10 \otimes 6) \otimes 2 = 5 \oplus (16 \otimes 2) = 5 \oplus 18 = min\{5, 18\} = 5$

Teorema 2.1

Diberikan *semiring* $\mathbb{Z}_{min}$= $(\mathbb{Z}, \oplus, \otimes)$. Idempoten dari $\oplus$ berakibat bahwa elemen invers terhadap $\oplus$ tidak ada.

Bukti :

Misalkan $a \neq \varepsilon$ mempunyai suatu invers terhadap $\oplus$ yaitu b, didapat

$a \oplus b = \varepsilon$

Tambahkan a pada kedua ruas persamaan, didapat

$a \oplus a \oplus b = a \oplus \varepsilon$

Dengan sifat idempotent, persamaan menjadi

$a \oplus b = a$

maka hal ini bertentangan dengan $a \oplus b = \varepsilon$.

Teorema 2.2

$\mathbb{Z}_{min}$ merupakan *semifield* yang komutatif dan idempotent.

Bukti:

I. $\mathbb{Z}_{min}$ merupakan *semifield*.

1. Sistem matematika $(\mathbb{Z}_{min}, \oplus)$ memenuhi aksioma-aksioma berikut:

   a. Bersifat asosiatif

   $$x \oplus (y \oplus z) = \min(x, \min(y, z)) = \min(\min(x, y), z)$$
   $$= (x \oplus y) \oplus z, \qquad \forall x, y, z \in \mathbb{Z}_{min}$$

   Jadi operasi $\oplus$ bersifat asosiatif di $\mathbb{Z}_{min}$.

   b. Bersifat komutatif

   $$x \otimes y = \min(x, y) = \min(y, x) = y \otimes x, \qquad \forall x, y \in \mathbb{Z}_{min}.$$

   Jadi operasi $\oplus$ bersifat komutatif di $\mathbb{Z}_{min}$.

   c. Terdapat elemen nol $\varepsilon = +\infty$ di $\mathbb{Z}_{min}$

   $$x \otimes \varepsilon = \min(x, +\infty) = \min(+\infty, x) = \varepsilon \otimes x, \qquad \forall x \in \mathbb{Z}_{min}.$$

   Jadi $\varepsilon = +\infty$ adalah elemen nol di $\mathbb{Z}_{min}$terhadap operasi $\otimes$.

2. Sistem matematika$(\mathbb{Z}_{min} + \{\varepsilon\}, \otimes)$ membentuk suatu grup.

   a. Bersifat asosiatif

   $$x \otimes (y \otimes z) = x + (y + z) = (x + y) + z$$
   $$= (x \otimes y) \otimes z, \qquad \forall x, y, z \in \mathbb{Z}_{min} + \{\varepsilon\}$$

   Jadi operasi $\otimes$ bersifat asosiatif di $\mathbb{Z}_{min} + \{\varepsilon\}$.

b. Terdapat elemen kesatuan $e = 0$ di $\mathbb{Z}_{min} + \{\varepsilon\}$

$x \otimes e = \mathrm{x} + 0 = 0 + \mathrm{x} = 0 \otimes x\,, \qquad \forall x \in \mathbb{Z}_{min} + \{\varepsilon\}.$

Jadi $e = 0$ adalah elemen kesatuan di $\mathbb{Z}_{min} + \{\varepsilon\}$ terhadap operasi $\otimes$.

c. Untuk setiap $x = \mathbb{Z}_{min} + \{\varepsilon\}$, terdapat $x^{-1} = -x \in \mathbb{Z}_{min} + \{\varepsilon\}$

$x^{-1} \otimes x = -\mathrm{x} + \mathrm{x} = \mathrm{x} + (-\mathrm{x}) = x \otimes x^{-1} = e.$

Jadi $-x$ adalah invers (kebalikan) dari $x \in \mathbb{Z}_{min} + \{\varepsilon\}$ terhadap operasi $\otimes$.

3. Operasi $\otimes$ bersifat distributif kanan terhadap $\otimes$.

$x \otimes (y \oplus z) = x + \min(y, z) = \min(x + y, x + z)$

$= (x \otimes y) \oplus (x \otimes z), \qquad \forall x, y, z \in \mathbb{Z}_{min} + \{\varepsilon\}$

Jadi operasi $\otimes$ bersifat distributif kanan terhadap operasi $\oplus$ di $\mathbb{Z}_{min} + \{\varepsilon\}$.

4. Operasi $\otimes$ bersifat distributif kiri terhadap $\otimes$.

$(x \oplus y) \otimes z = \min(x, y) + z = \min(x + z, y + z)$

$= (x \otimes z) \oplus (y \otimes z), \qquad \forall x, y, z \in \mathbb{Z}_{min} + \{\varepsilon\}.$

Jadi operasi $\otimes$ bersifat distributif kiri terhadap operasi $\oplus$ di $\mathbb{Z}_{min} + \{\varepsilon\}$.

Jadi berdasar 1 sampai 4 $\mathbb{Z}_{min}$ merupakan suatu *semilfield.*

II. Selanjutnya $\mathbb{Z}_{min}$ *semifield* dikatakan komutatif dan idempotent jika,

1. Terhadap operasi $\otimes$ bersifat komutatif

$x \otimes y = x + y = y + x = y \otimes x\,, \qquad \forall x, y \in \mathbb{Z}_{min}.$

Jadi terhadap operasi $\otimes$ bersifat komutatif di $\mathbb{Z}_{min}$.

2. Terhadap operasi $\oplus$ bersifat idempotent di $\mathbb{Z}_{min}$

   $x \oplus x = \min(x, x) = x$, $\quad \forall x \in \mathbb{Z}_{min}$.

   Jadi operasi $\oplus$ bersifat idempotent di $\mathbb{Z}_{min}$.

Jadi berdasarkan I dan II $\mathbb{Z}_{min}$ adalah *semifield* yang komutatif dan idempotent.

Adapun sifat-sifat yang berlaku dalam $\mathbb{Z}_{min}$ antara lain:

1) $x \oplus (y \oplus z) = \min(x, \min(y, z)) = \min(\min (x,y), z) = (x \oplus y) \oplus z$
2) $x \oplus \{+\infty\} = \min (x, +\infty) = x$
3) $x \otimes \{+\infty\} = x + \{+\infty\} = \{+\infty\}$
4) $x \otimes 0 = x + 0 = x$
5) $x \otimes (y \otimes z) = x + (y + z) = (x + y) + z = (x \otimes y) \otimes z$
6) $x \otimes y = x + y = y + x = y \otimes x$
7) $x \otimes (-x) = x + (-x) = 0$
8) $x \otimes (y \oplus z) = x + (\min (y, z)) = \min (x + y, x + z) = (x \otimes y) \oplus (x \otimes z)$

Dari sifat –sifat di atas, terlihat bahwa $+\infty$ merupakan elemen identitas (elemen netral) terhadap operasi $\oplus$ dan 0 merupakan elemen identitas (elemen satuan) terhadap operasi $\otimes$. Oleh karena itu, ditinjau dari struktur aljabar $\mathbb{Z}_{min}$ merupakan *semiring*, yaitu:

1) $(Z \cup \{+\infty\}, \oplus)$ merupakan monoid komutatif dengan elemen netral $+\infty$
2) $(Z \cup \{+\infty\}, \otimes)$ merupakan monoid dengan elemen satuan 0
3) Operasi $\otimes$ terhadap $\oplus$ bersifat distributif

4) Elemen netral terhadap operasi $\oplus$, yaitu $\{+\infty\}$ bersifat menyerap terhadap operasi $\otimes$. Jadi $x \otimes +\infty = +\infty \otimes x = +\infty$, $\forall x \in \mathbb{Z}_{min}$

Selanjutnya karena operasi $\oplus$ bersifat idempotent, yaitu $x \oplus x = x$, $\forall x \in \mathbb{Z}_{min}$, maka $\mathbb{Z}_{min}$ merupakan *semiring* idempoten dan $\forall x \in \mathbb{Z}_{min}$ tidak mempunyai invers terhadap operasi $\oplus$ dalam aljabar *min-plus*. Kemudian karena operasi kedua yaitu $\otimes$ memiliki invers, maka $\mathbb{Z}_{min}$ merupakan *semifield* idempotent.

D. Matriks dalam Aljabar *Min-Plus* atas $\mathbb{Z}$

Pada subbab ini dibahas tentang konsep dasar matriks dalam aljabar *min-plus*. Jika diberikan suatu *semifield idempotent* $\mathbb{Z}_{min}$ dapat dibentuk matriks dengan entri-entrinya adalah elemen-elemen $\mathbb{Z}_{min}$. Operasi $\oplus$ dan $\otimes$ pada matriks yang telah terbentuk didefinisikan sebagai berikut:

1) $(A \oplus B)_{ij} = A_{ij} \oplus B_{ij}$

2) $(A \otimes B)_{ij} = \underset{k}{\oplus}(A_{ik} \otimes B_{kj})$

Contoh 2.5

Jika $A = \begin{bmatrix} 1 & 0 \\ 3 & 2 \end{bmatrix}$ dan $B = \begin{bmatrix} 2 & -1 \\ 2 & 3 \end{bmatrix}$, maka

$$A \oplus B = \begin{bmatrix} 1 & 0 \\ 3 & 2 \end{bmatrix} \oplus \begin{bmatrix} 2 & -1 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} 1 \oplus 2 & 0 \oplus -1 \\ 3 \oplus 2 & 2 \oplus 3 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 2 & 2 \end{bmatrix}$$

$$A \otimes B = \begin{bmatrix} 1 & 0 \\ 3 & 2 \end{bmatrix} \otimes \begin{bmatrix} 2 & -1 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} (1+2) \oplus (0+2) & (1+(-1)) \oplus (0+3) \\ (3+2) \oplus (2+2) & (3+(-1)) \oplus (2+3) \end{bmatrix}$$

$$= \begin{bmatrix} 2 & 0 \\ 4 & 2 \end{bmatrix}$$

Selanjutnya didefinisikan $(\mathbb{Z}_{min})^{n \times n}$ sebagai himpunan semua matriks berukuran $n \times n$ dengan entri-entrinya elemen $\mathbb{Z}_{min}$. Elemen netral terhadap

operasi + dan elemen netral terhadap operasi x dalam $(\mathbb{Z}_{min})^{n\ x\ n}$ berturut-turut adalah matriks E dengan $(E)_{ij}=\begin{cases} 0, \text{jika } i=j \\ +\infty, \text{jika } i\neq j \end{cases}$ dan matriks $\varepsilon\epsilon(\mathbb{Z}_{min}^{mxn})$ dengan $(\varepsilon)_{ij} = +\infty$, untuk setiap i dan j. Jadi,

1) $(E\otimes A) = (A\otimes E) = A$ untuk setiap $A\ \epsilon(\mathbb{Z}_{min})^{n\ x\ n}$
2) $(\varepsilon \oplus A) = (A\oplus\varepsilon) = A$, untuk setiap $A\ \epsilon(\mathbb{Z}_{min})^{n\ x\ n}$.

Beberapa sifat berikut merupakan sifat matriks atas aljabar *min-plus* dan berlaku untuk sebarang matriks $A,B,C\ \epsilon(\mathbb{Z}_{min})^{n\ x\ n}$ dengan ukuran yang bersesuaian dan operasi matriks tersebut terdefinisi:

i. $A\oplus(B \oplus C) = (A\oplus B) \oplus C$

ii. $A \oplus B = B \oplus A$

iii. $A \otimes (B \otimes C) = (A \otimes B) \otimes C$

iv. $A \otimes (B\oplus C) = (A \otimes B)\oplus(A \otimes C)$

v. $(A \oplus B)\otimes C = (A \otimes C)\oplus(B \otimes C)$

vi. $A \oplus A = A$

Bukti

i. $[A\oplus (B\oplus C)]_{ij} = A_{ij}\oplus(B_{ij} \oplus C_{ij})$

$= (A_{ij} \oplus B_{ij})\oplus C_{ij} = [(A\oplus B)\oplus C]_{ij}$

ii. $[A \oplus B]_{ij} = A_{ij}\oplus B_{ij} = B_{ij}\oplus A_{ij} = [B \oplus A]_{ij}$

iii. $[A \otimes (B \otimes C)]_{ij} = \bigoplus_{k=1}^{n} A_{ik}\left(\bigoplus_{l=1}^{n} B_{kl} \otimes C_{lj}\right)$

$= \bigoplus_{k=1}^{n}\bigoplus_{l=1}^{n} A_{ik} \otimes B_{kl} \otimes C_{lj}$

$$= \bigoplus_{k=1}^{n}\left(\bigoplus_{l=1}^{n} A_{ik} \otimes B_{kl}\right)\otimes C_{lj}$$

$$= [(A \otimes B) \otimes C]_{ij}$$

iv. $[A\otimes (B\oplus C)]_{ij}= \bigoplus_{k=1}^{n} A_{ik}\left(B_{kj} \oplus C_{kj}\right)$

$$= \bigoplus_{k=1}^{n}\left(\left(A_{ik} \otimes B_{kj}\right)\oplus\left(A_{ik} \otimes C_{kj}\right)\right)$$

$$= \left(\bigoplus_{k=1}^{n}\left(A_{ik} \otimes B_{kj}\right)\right)\oplus\left(\bigoplus_{k=1}^{n} A_{ik} \otimes C_{kj}\right)$$

$$= [(A\otimes B) \oplus (A\otimes C)]_{ij}$$

v. $[(A\oplus B)\otimes C]_{ij} = \bigoplus_{k=1}^{n}\left(A_{ik} \oplus B_{ik}\right)C_{kj}$

$$= \bigoplus_{k=1}^{n}\left(\left(A_{ik} \otimes C_{kj}\right)\oplus\left(B_{ik} \otimes C_{kj}\right)\right)$$

$$= \bigoplus_{k=1}^{n}\left(A_{ik} \otimes C_{kj}\right)\oplus\bigoplus_{k=1}^{n}\left(B_{ik} \otimes C_{kj}\right)$$

$$= [(A\otimes C) \oplus (B\otimes C)]_{ij}$$

vi. $[A\oplus A]_{ij} = A_{ij}\oplus A_{ij}= A_{ij}$

Jadi berdasarkan sifat-sifat diatas $\mathbb{Z}_{min}$ merupakan *semiring* idempotent.

BAB III

PEMBAHASAN

Sistem kriptografi atau sering disebut dengan *cipher* 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 dalam M. Zaki Riyanto, 2011).

Berdasarkan pernyataan-pernyataan tersebut maka ketentuan-ketentuan yang digunakan pada algoritma sistem kriptografi ini adalah sebagai berikut:

a. Proses pembentukan kunci digunakan algoritma pembentukan kunci Stickel (2005) yang tercantum pada bab II,
b. Pada proses pembentukan kunci, perhitungannya berdasarkan operasi matriks atas aljabar *min-plus*,
c. Penambahan kode <*space*> untuk kasus yang jumlah karakter pesan tidak habis dibagi 4,

d. Proses enkripsi dan dekripsi dilakukan dengan perhitungan modulo 94,
e. Pada proses enkripsi, perhitungannya dilakukan berdasarkan penjumlahan matriks biasa,
f. Pada proses dekripsi, perhitungannya dilakukan berdasarkan pengurangan matriks biasa.

A. Operasi Perkalian Matriks atas Aljabar *Min-Plus*

Pada perkalian operasi matriks atas aljabar *min-plus* telah dibuktikan bahwa perkalian operasi matriks atas aljabar *min-plus* bersifat asosiatif, sehingga dapat diperoleh sifat berikut:

Teorema 3.1

Jika A merupakan matriks atas aljabar *min-plus* maka berlaku

$$A^m \otimes A^n = A^n \otimes A^m$$

Bukti 3.1

Perkalian matriks atas aljabar *min-plus* memenuhi sifat asosiatif..

Contoh

Diberikan matriks atas aljabar *min-plus* $A=\begin{pmatrix}3 & 10\\ 5 & 2\end{pmatrix}$dengan $m = 2, n = 3$

Diperoleh $A^2=\begin{pmatrix}3 & 10\\ 5 & 2\end{pmatrix} \otimes \begin{pmatrix}3 & 10\\ 5 & 2\end{pmatrix}= \begin{pmatrix}6 & 5\\ 7 & 4\end{pmatrix}$

$A^3=\begin{pmatrix}3 & 10\\ 5 & 2\end{pmatrix} \otimes \begin{pmatrix}3 & 10\\ 5 & 2\end{pmatrix} \otimes \begin{pmatrix}3 & 10\\ 5 & 2\end{pmatrix}=\begin{pmatrix}9 & 7\\ 9 & 6\end{pmatrix}$

$A^2 \otimes A^3=\begin{pmatrix}6 & 5\\ 7 & 4\end{pmatrix} \otimes \begin{pmatrix}9 & 7\\ 9 & 6\end{pmatrix}=\begin{pmatrix}14 & 11\\ 13 & 10\end{pmatrix}=\begin{pmatrix}9 & 7\\ 9 & 6\end{pmatrix} \otimes \begin{pmatrix}6 & 5\\ 7 & 4\end{pmatrix}=A^3 \otimes A^2$

B. Penerapan Operasi Perkalian Matriks atas Aljabar *Min-Plus* pada Protokol Perjanjian Kunci

1. Pembentukan Kunci

Kunci (*key*) adalah parameter yang digunakan untuk mentransformasi proses pengenkripsian dan pendekripsian pesan. Pada permasalahan ini, digunakan skema protokol perjanjian kunci Stickel yang didasarkan atas grup non-komutatif untuk menjaga keamanan kunci tersebut. Berdasarkan sifat operasi matriks atas aljabar *Min-Plus*, dapat diterapkan algoritma untuk melakukan pembentukan kunci seperti pada gambar 2.5. Berdasarkan sifat perkalian matriks atas aljabar *min-plus*, maka diperoleh:

$$K_1=A^m VB^n=A^m A^r B^s B^n=A^r A^m B^n B^s=A^r UB^s=K_2$$

Pihak 1 dan pihak 2 berhasil menyepakati kunci yang sama, yaitu $K=K_1=K_2$. Misalkan pihak 1 ingin mengirimkan pesan rahasia kepada pihak 2 menggunakan sistem kriptografi simetris. Apabila pihak 1 mengenkripsi pesan tersebut menggunakan suatu kunci dan menghasilkan *ciphertext*, maka *ciphertext* yang dikirimkan kepada pihak 2 tidak dapat dibuka oleh pihak 2, sebab pihak 2 tidak mengetahui kunci yang digunakan oleh pihak 1. Pihak 1 tidak boleh mengirimkan kunci kepada pihak 2, karena ada pihak 3 sebagai pihak penyerang yang dapat menyadap dan mendapatkan apapun yang melewati jalur komunikasi. Oleh karena itu, pihak 1 dan pihak 2 harus melakukan suatu perjanjian kunci. Misalkan diberikan dalam gambar 2.6.

Pihak 1 atau pihak 2 mempublikasikan suatu semiring $(\mathbb{Z}_{min})^{2x2}$ dan A,B$\in(\mathbb{Z}_{min})^{2x2}$

Misal: $A = \begin{bmatrix} 3 & 5 \\ 2 & 1 \end{bmatrix}$ dan $B = \begin{bmatrix} 1 & 4 \\ 4 & 2 \end{bmatrix}$

Pihak 1	Pihak 2
1. Memilih secara rahasia bilangan asli m dan n. Misal: $m = 2$ dan $n = 2$	1. Memilih secara rahasia bilangan asli r dan s. Misal: $r = 2$ dan $s = 1$
2. Menghitung $U = A^2B^2$ $U = \begin{bmatrix} 3 & 5 \\ 2 & 1 \end{bmatrix}^2 \begin{bmatrix} 1 & 4 \\ 4 & 2 \end{bmatrix}^2$ $= \begin{bmatrix} 6 & 6 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 2 & 5 \\ 5 & 4 \end{bmatrix}$ $= \begin{bmatrix} 8 & 10 \\ 5 & 6 \end{bmatrix}$	2. Menghitung $V = A^2B^1$ $V = \begin{bmatrix} 3 & 5 \\ 2 & 1 \end{bmatrix}^2 \begin{bmatrix} 1 & 4 \\ 4 & 2 \end{bmatrix}^1$ $= \begin{bmatrix} 6 & 6 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 4 & 2 \end{bmatrix}$ $= \begin{bmatrix} 7 & 8 \\ 4 & 4 \end{bmatrix}$
3. Mengirim *U* kepada pihak 2	3. Mengirim *V* kepada pihak 1
4. Menerima *V* dari pihak 2	4. Menerima *U* kepada pihak 1
5. Menghitung $K_1 = A^m V B^n$ $K_1 = \begin{bmatrix} 3 & 5 \\ 2 & 1 \end{bmatrix}^2 \begin{bmatrix} 7 & 8 \\ 4 & 4 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 4 & 2 \end{bmatrix}^2$ $= \begin{bmatrix} 6 & 6 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 7 & 8 \\ 4 & 4 \end{bmatrix} \begin{bmatrix} 2 & 5 \\ 5 & 4 \end{bmatrix}$ $= \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix}$	5. Menghitung $K_2 = A^r U B^s$ $K_2 = \begin{bmatrix} 3 & 5 \\ 2 & 1 \end{bmatrix}^2 \begin{bmatrix} 8 & 10 \\ 5 & 6 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 4 & 2 \end{bmatrix}^1$ $= \begin{bmatrix} 6 & 6 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 8 & 10 \\ 5 & 6 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 4 & 2 \end{bmatrix}$ $= \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix}$

Pihak 1 dan pihak 2 berhasil menyepakati kunci yang sama $K = K_1 = K_2$

$$K = K_1 = K_2 = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix}$$

Gambar 2.6 Perhitungan Protokol Perjanjian Kunci Stickel atas $(\mathbb{Z}_{min})^{2x2}$

C. Implementasi Algoritma Untuk Pengamanan Pesan

1. Proses Enkripsi

Pada pengenkripsian sebuah *plaintext*, dibutuhkan kunci K yang sebelumnya telah dibuat oleh penerima pesan. Pada proses ini pihak 1 akan mengirimkan suatu pesan kepada pihak 2 yang telah diubah menjadi blok-blok yang terdiri dari 4 karakter. Setiap blok kemudian diubah ke dalam angka-angka sesuai dengan tabel kode (terlampir pada lampiran 1) dan ditulis dalam bentuk matriksP_{2x2}. Selanjutnya proses pengenkripsian dilakukan dengan cara menambakan kunci K pada tiap blok serta dilakukan perhitungan dengan modulo 94, sehingga didapat suatu *ciphertext* sebagai berikut:

$$C_i = (K + P_i) \bmod 94,$$

dengan

C_i= *Ciphertext*

K= *Kunci*

P_i= *Plaintext*

$i = 1,2,3, \dots, n.$

a. **Kasus 1**: jumlah karakter pesan habis dibagi 4.

Andre dan Bayu adalah teman akrab. Andre ingin mengirimkan uang kepada Bayu. Setelah uangnya berhasil ditransfer, kemudian Andre mengirimkan pesan rahasia kepada Bayu yang isinya adalah

Uangnya sudah saya transfer ke rekening anda sebesar 200 juta rupiah, TOLONG DI CEK!

Pesan tersebut kemudian dienkripsi terlebih dahulu oleh Andre dan dipecah menjadi blok-blok 4 huruf yaitu:

Uang	**nya<*space*>**	**suda**
h<*space*>sa	**ya<*space*>t**	**rans**
fer<*space*>	**ke<*space*>r**	**eken**
ing<*space*>	**anda**	**<*space*>seb**
esar	**<*space*>200**	**<*space*> jut**
a<*space*>ru	**piah**	**, <*space*>TO**
LONG	**<*space*>DI<*space*>**	**CEK!**

Setiap blok kemudian diubah ke dalam angka-angka sesuai dengan tabel kode (terlampir pada lampiran 1) dan ditulis dalam bentuk matriks P_{2x2}. Misalkan pada pesan blok pertama yaitu **Uang**, maka dikonversi dengan tabel kode (terlampir pada lampiran 1) didapat U=56, a=0, n=13, g=6 sehingga diperoleh *plaintext* $P_1 = \begin{bmatrix} 56 & 0 \\ 13 & 6 \end{bmatrix}$ dan seterusnya sampai pada pesan blok terakhir, sehingga diperoleh *plaintext* sebagai berikut:

$$P_1 = \begin{bmatrix} 56 & 0 \\ 13 & 6 \end{bmatrix}; \quad P_2 = \begin{bmatrix} 13 & 24 \\ 0 & 93 \end{bmatrix}; \quad P_3 = \begin{bmatrix} 18 & 20 \\ 3 & 0 \end{bmatrix}$$

$$P_4 = \begin{bmatrix} 7 & 93 \\ 18 & 0 \end{bmatrix}; \quad P_5 = \begin{bmatrix} 24 & 0 \\ 93 & 19 \end{bmatrix}; \quad P_6 = \begin{bmatrix} 17 & 0 \\ 13 & 18 \end{bmatrix}$$

$P_7 = \begin{bmatrix} 5 & 4 \\ 17 & 93 \end{bmatrix}$; $P_8 = \begin{bmatrix} 10 & 4 \\ 93 & 17 \end{bmatrix}$; $P_9 = \begin{bmatrix} 4 & 10 \\ 4 & 13 \end{bmatrix}$

$P_{10} = \begin{bmatrix} 8 & 13 \\ 6 & 93 \end{bmatrix}$; $P_{11} = \begin{bmatrix} 0 & 13 \\ 3 & 0 \end{bmatrix}$; $P_{12} = \begin{bmatrix} 93 & 18 \\ 4 & 1 \end{bmatrix}$

$P_{13} = \begin{bmatrix} 4 & 18 \\ 0 & 17 \end{bmatrix}$; $P_{14} = \begin{bmatrix} 93 & 27 \\ 35 & 35 \end{bmatrix}$; $P_{15} = \begin{bmatrix} 93 & 9 \\ 20 & 19 \end{bmatrix}$

$P_{16} = \begin{bmatrix} 0 & 93 \\ 17 & 20 \end{bmatrix}$; $P_{17} = \begin{bmatrix} 15 & 8 \\ 0 & 7 \end{bmatrix}$; $P_{18} = \begin{bmatrix} 90 & 93 \\ 55 & 50 \end{bmatrix}$

$P_{19} = \begin{bmatrix} 47 & 50 \\ 49 & 42 \end{bmatrix}$; $P_{20} = \begin{bmatrix} 93 & 39 \\ 44 & 93 \end{bmatrix}$; $P_{21} = \begin{bmatrix} 38 & 40 \\ 46 & 63 \end{bmatrix}$

Pesan tersebut kemudian dienkripsi menggunakan kunci yang telah disepakati yaitu $K = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix}$ dan dilakukan perhitungan dengan rumus $C_i = (K + P_i) \bmod 94$, sehingga diperoleh:

$C_1 = \mathrm{K} + P_1 = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} + \begin{bmatrix} 56 & 0 \\ 13 & 6 \end{bmatrix} = \begin{bmatrix} 68 & 14 \\ 21 & 16 \end{bmatrix}$

$C_2 = \mathrm{K} + P_2 = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} + \begin{bmatrix} 13 & 24 \\ 0 & 93 \end{bmatrix} = \begin{bmatrix} 25 & 38 \\ 8 & 9 \end{bmatrix}$

$C_3 = \mathrm{K} + P_3 = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} + \begin{bmatrix} 18 & 20 \\ 3 & 0 \end{bmatrix} = \begin{bmatrix} 30 & 34 \\ 11 & 10 \end{bmatrix}$

$C_4 = \mathrm{K} + P_4 = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} + \begin{bmatrix} 7 & 93 \\ 18 & 0 \end{bmatrix} = \begin{bmatrix} 19 & 13 \\ 26 & 10 \end{bmatrix}$

$C_5 = \mathrm{K} + P_5 = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} + \begin{bmatrix} 24 & 0 \\ 93 & 19 \end{bmatrix} = \begin{bmatrix} 36 & 14 \\ 7 & 29 \end{bmatrix}$

$C_6 = \mathrm{K} + P_6 = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} + \begin{bmatrix} 17 & 0 \\ 13 & 18 \end{bmatrix} = \begin{bmatrix} 29 & 14 \\ 21 & 28 \end{bmatrix}$

$C_7 = \mathrm{K} + P_7 = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} + \begin{bmatrix} 5 & 4 \\ 17 & 93 \end{bmatrix} = \begin{bmatrix} 17 & 18 \\ 25 & 9 \end{bmatrix}$

$C_8 = \mathrm{K} + P_8 = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} + \begin{bmatrix} 10 & 4 \\ 93 & 17 \end{bmatrix} = \begin{bmatrix} 22 & 18 \\ 7 & 27 \end{bmatrix}$

$$C_9 = \mathrm{K} + P_9 = \begin{bmatrix}12 & 14\\ 8 & 10\end{bmatrix} + \begin{bmatrix}4 & 10\\ 4 & 13\end{bmatrix} = \begin{bmatrix}16 & 24\\ 12 & 23\end{bmatrix}$$

$$C_{10} = \mathrm{K} + P_{10} = \begin{bmatrix}12 & 14\\ 8 & 10\end{bmatrix} + \begin{bmatrix}8 & 13\\ 6 & 93\end{bmatrix} = \begin{bmatrix}20 & 27\\ 14 & 9\end{bmatrix}$$

$$C_{11} = \mathrm{K} + P_{11} = \begin{bmatrix}12 & 14\\ 8 & 10\end{bmatrix} + \begin{bmatrix}0 & 13\\ 3 & 0\end{bmatrix} = \begin{bmatrix}12 & 27\\ 11 & 10\end{bmatrix}$$

$$C_{12} = \mathrm{K} + P_{12} = \begin{bmatrix}12 & 14\\ 8 & 10\end{bmatrix} + \begin{bmatrix}93 & 18\\ 4 & 1\end{bmatrix} = \begin{bmatrix}11 & 32\\ 12 & 11\end{bmatrix}$$

$$C_{13} = \mathrm{K} + P_{13} = \begin{bmatrix}12 & 14\\ 8 & 10\end{bmatrix} + \begin{bmatrix}4 & 18\\ 0 & 17\end{bmatrix} = \begin{bmatrix}16 & 32\\ 8 & 27\end{bmatrix}$$

$$C_{14} = \mathrm{K} + P_{14} = \begin{bmatrix}12 & 14\\ 8 & 10\end{bmatrix} + \begin{bmatrix}93 & 27\\ 35 & 35\end{bmatrix} = \begin{bmatrix}11 & 41\\ 43 & 45\end{bmatrix}$$

$$C_{15} = \mathrm{K} + P_{15} = \begin{bmatrix}12 & 14\\ 8 & 10\end{bmatrix} + \begin{bmatrix}93 & 9\\ 20 & 19\end{bmatrix} = \begin{bmatrix}11 & 23\\ 28 & 29\end{bmatrix}$$

$$C_{16} = \mathrm{K} + P_{16} = \begin{bmatrix}12 & 14\\ 8 & 10\end{bmatrix} + \begin{bmatrix}0 & 93\\ 17 & 20\end{bmatrix} = \begin{bmatrix}12 & 13\\ 25 & 30\end{bmatrix}$$

$$C_{17} = \mathrm{K} + P_{17} = \begin{bmatrix}12 & 14\\ 8 & 10\end{bmatrix} + \begin{bmatrix}15 & 8\\ 0 & 7\end{bmatrix} = \begin{bmatrix}27 & 22\\ 8 & 17\end{bmatrix}$$

$$C_{18} = \mathrm{K} + P_{18} = \begin{bmatrix}12 & 14\\ 8 & 10\end{bmatrix} + \begin{bmatrix}90 & 93\\ 55 & 50\end{bmatrix} = \begin{bmatrix}8 & 13\\ 63 & 60\end{bmatrix}$$

$$C_{19} = \mathrm{K} + P_{19} = \begin{bmatrix}12 & 14\\ 8 & 10\end{bmatrix} + \begin{bmatrix}47 & 50\\ 49 & 42\end{bmatrix} = \begin{bmatrix}59 & 64\\ 57 & 52\end{bmatrix}$$

$$C_{20} = \mathrm{K} + P_{20} = \begin{bmatrix}12 & 14\\ 8 & 10\end{bmatrix} + \begin{bmatrix}93 & 39\\ 44 & 93\end{bmatrix} = \begin{bmatrix}11 & 53\\ 52 & 9\end{bmatrix}$$

$$C_{21} = \mathrm{K} + P_{21} = \begin{bmatrix}12 & 14\\ 8 & 10\end{bmatrix} + \begin{bmatrix}38 & 40\\ 46 & 63\end{bmatrix} = \begin{bmatrix}50 & 54\\ 54 & 73\end{bmatrix}$$

Hasil perhitungan selanjutnya diubah ke dalam huruf sesuai dengan tabel kode (terlampir pada lampiran 1) sehingga diperoleh suatu kode (*ciphertext*) yang merupakan suatu pesan yang akan dikirim kepada Bayu yaitu:

^ovqzCij59lktn1kAoh44ov3rszjwsh2qymxu2ojm2lkl7ml q7i2lFHJlx34mnz52wirin!YX@VQlRQjOSS_

b. **Kasus 2**: jumlah karakter pesan tidak habis dibagi 4.

Misalkan Tomi ingin mengirim barang ke rumah Udin. Tetapi ia tidak tahu alamat rumahnya, sehingga Udin memberitahukan alamat rumahnya lewat pesan rahasia. Isi pesan tersebut adalah

Jl. Anggrek No. 9, Klaten

Pada kasus ini jumlah karakter pesan yaitu 25 dan tidak habis dibagi 4, sehingga memiliki sisa 1 karakter. Pesan tersebut kemudian dienkripsi terlebih dahulu oleh Tomi dan dipecah menjadi blok-blok 4 huruf yaitu:

Jl.<*space*>	**Angg**	**rek<*space*>**
No. <*space*>	**9, <*space*>K**	**late**
n<*space*><*space*><*space*>		

Setiap blok kemudian diubah ke dalam angka-angka sesuai dengan tabel kode (terlampir pada lampiran 1) dan ditulis dalam bentuk matriks P_{2x2}. Misalkan pada pesan blok pertama yaitu **Jl.<*space*>** , maka dikonversi dengan tabel kode (terlampir pada lampiran 1) didapat J=45, l=11, .=91, <*space*>=93 sehingga diperoleh *plaintext*

$P_1 = \begin{bmatrix} 45 & 11 \\ 91 & 93 \end{bmatrix}$ dan seterusnya sampai pada pesan blok terakhir, sehingga diperoleh *plaintext* sebagai berikut:

$$P_1 = \begin{bmatrix} 45 & 11 \\ 91 & 93 \end{bmatrix}; \quad P_2 = \begin{bmatrix} 36 & 13 \\ 6 & 6 \end{bmatrix}; \quad P_3 = \begin{bmatrix} 17 & 4 \\ 10 & 93 \end{bmatrix}$$

$$P_4 = \begin{bmatrix} 49 & 14 \\ 91 & 93 \end{bmatrix}; \quad P_5 = \begin{bmatrix} 34 & 90 \\ 93 & 46 \end{bmatrix}; \quad P_6 = \begin{bmatrix} 11 & 0 \\ 19 & 4 \end{bmatrix}$$

$$P_7 = \begin{bmatrix} 13 & 93 \\ 93 & 93 \end{bmatrix}$$

Pesan tersebut kemudian dienkripsi menggunakan kunci yang telah disepakati yaitu $K = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix}$ dan dilakukan perhitungan dengan rumus $C_i = (K + P_i) \bmod 94$, sehingga diperoleh:

$$C_1 = \mathrm{K} + P_1 = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} + \begin{bmatrix} 45 & 11 \\ 91 & 93 \end{bmatrix} = \begin{bmatrix} 57 & 25 \\ 5 & 9 \end{bmatrix}$$

$$C_2 = \mathrm{K} + P_2 = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} + \begin{bmatrix} 36 & 13 \\ 6 & 6 \end{bmatrix} = \begin{bmatrix} 48 & 27 \\ 14 & 16 \end{bmatrix}$$

$$C_3 = \mathrm{K} + P_3 = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} + \begin{bmatrix} 17 & 4 \\ 10 & 93 \end{bmatrix} = \begin{bmatrix} 29 & 18 \\ 18 & 9 \end{bmatrix}$$

$$C_4 = \mathrm{K} + P_4 = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} + \begin{bmatrix} 49 & 14 \\ 91 & 93 \end{bmatrix} = \begin{bmatrix} 61 & 28 \\ 5 & 9 \end{bmatrix}$$

$$C_5 = \mathrm{K} + P_5 = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} + \begin{bmatrix} 34 & 90 \\ 93 & 46 \end{bmatrix} = \begin{bmatrix} 46 & 10 \\ 7 & 56 \end{bmatrix}$$

$$C_6 = \mathrm{K} + P_6 = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} + \begin{bmatrix} 11 & 0 \\ 19 & 4 \end{bmatrix} = \begin{bmatrix} 23 & 14 \\ 27 & 14 \end{bmatrix}$$

$$C_7 = \mathrm{K} + P_7 = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} + \begin{bmatrix} 13 & 93 \\ 93 & 93 \end{bmatrix} = \begin{bmatrix} 25 & 13 \\ 7 & 9 \end{bmatrix}$$

Hasil perhitungan selanjutnya diubah ke dalam huruf sesuai dengan tabel kode (terlampir pada lampiran 1) sehingga diperoleh suatu

kode (*ciphertext*) yang merupakan suatu pesan yang akan dikirim kepada Tomi yaitu:

VzfjM2oq4ssjZ3fjKkhUxo2oznhj

2. Proses Dekripsi

Proses selanjutnya adalah dekripsi. Setelah memperoleh *ciphertext* dari pihak 1, maka pihak kedua atau penerima pesan mengubahnya menjadi *plaintext*. Pada proses ini juga dibutuhkan kunci K untuk mendekripsikan pesan tersebut. Pesan tersebut selanjutnya diubah ke dalam blok-blok yang terdiri dari 4 karakter, lalu setiap blok diubah ke dalam angka-angka sesuai dengan tabel kode (terlampir pada lampiran 1) dan ditulis dalam bentuk matriks C_{2x2}. Berbeda dengan proses enkripsi, pada proses ini pendekripsian pesan dilakukan dengan cara mengurangi dengan kunci K pada setiap blok serta dilakukan perhitungan dengan modulo 94 sehingga diperoleh rumus *plaintext* sebagai berikut:

$$P_i = (C_i - K) \bmod 94,$$

dengan

P_i= *Plaintext*

C_i= *Ciphertext*

K= *Kunci*

$i = 1,2,3, \dots, n.$

a. Berdasarkan (**Kasus 1**) dihasilkan suatu pesan rahasia (*ciphertext*) berupa:

^ovqzCij59lktn1kAoh44ol3rszjwsh2qjmxu2ojm2lkl7mlq7i 2lFHJlx34mnz52wirin!YX@VQlRQjOSS_

Pesan tersebut akan diubah menjadi pesan aslinya. Oleh karena itu, pesan terlebih dahulu diubah menjadi blok-blok 4 karakter sehingga diperoleh sebagai berikut:

^ovq	**zCij**	**59lk**	**tn1k**
Aoh4	**4ol3**	**rszj**	**wsh2**
qjmx	**u2oj**	**m2lk**	**l7ml**
q7i2	**lFHJ**	**lx34**	**mnz5**
2wir	**in!Y**	**X@VQ**	**lRQj**
OSS_			

Setiap blok kemudian diubah ke dalam angka-angka sesuai dengan tabel kode (terlampir pada lampiran 1) dan ditulis dalam bentuk matriks C_{2x2}. Misalkan pada pesan blok pertama yaitu **^ovq**, maka dikonversi dengan tabel kode (terlampir pada lampiran 1) didapat ^=68, o=14, v=21, q=16 sehingga diperoleh *ciphertext* C_1=

$\begin{bmatrix}68 & 14\\21 & 16\end{bmatrix}$ dan seterusnya sampai pada pesan blok terakhir sehingga diperoleh *ciphertext* sebagai berikut:

$$C_1=\begin{bmatrix}68 & 14\\21 & 16\end{bmatrix};\ C_2=\begin{bmatrix}25 & 38\\8 & 9\end{bmatrix};\ C_3=\begin{bmatrix}30 & 34\\11 & 10\end{bmatrix}$$

$$C_4=\begin{bmatrix}19 & 13\\26 & 10\end{bmatrix};\ C_5=\begin{bmatrix}36 & 14\\7 & 29\end{bmatrix};\ C_6=\begin{bmatrix}29 & 14\\11 & 28\end{bmatrix}$$

$$C_7=\begin{bmatrix}17 & 18\\25 & 9\end{bmatrix};\ C_8=\begin{bmatrix}22 & 18\\7 & 27\end{bmatrix};\ C_9=\begin{bmatrix}16 & 24\\12 & 23\end{bmatrix}$$

$$C_{10}=\begin{bmatrix}20 & 27\\14 & 9\end{bmatrix};\ C_{11}=\begin{bmatrix}12 & 27\\11 & 10\end{bmatrix};\ C_{12}=\begin{bmatrix}11 & 32\\12 & 11\end{bmatrix}$$

$$C_{13}=\begin{bmatrix}16 & 32\\8 & 27\end{bmatrix};\ C_{14}=\begin{bmatrix}11 & 41\\43 & 45\end{bmatrix};\ C_{15}=\begin{bmatrix}11 & 23\\28 & 29\end{bmatrix}$$

$$C_{16}=\begin{bmatrix}12 & 13\\25 & 30\end{bmatrix};\ C_{17}=\begin{bmatrix}27 & 22\\8 & 17\end{bmatrix};\ C_{18}=\begin{bmatrix}8 & 13\\63 & 60\end{bmatrix}$$

$$C_{19}=\begin{bmatrix}59 & 64\\57 & 52\end{bmatrix};\ C_{20}=\begin{bmatrix}11 & 53\\52 & 9\end{bmatrix};\ C_{21}=\begin{bmatrix}50 & 54\\54 & 73\end{bmatrix}$$

Pesan tersebut kemudian didekripsi menggunakan kunci yang telah disepakati yaitu $K=\begin{bmatrix}12 & 14\\8 & 10\end{bmatrix}$ dan dilakukan perhitungan dengan rumus $P_i=(C_i-K) \bmod 94$, sehingga diperoleh:

$$P_1=C_1-K=\begin{bmatrix}68 & 14\\21 & 16\end{bmatrix}-\begin{bmatrix}12 & 14\\8 & 10\end{bmatrix}=\begin{bmatrix}56 & 0\\13 & 6\end{bmatrix}$$

$$P_2=C_2-K=\begin{bmatrix}25 & 38\\8 & 9\end{bmatrix}-\begin{bmatrix}12 & 14\\8 & 10\end{bmatrix}=\begin{bmatrix}13 & 24\\0 & 93\end{bmatrix}$$

$$P_3=C_3-K=\begin{bmatrix}30 & 34\\11 & 10\end{bmatrix}-\begin{bmatrix}12 & 14\\8 & 10\end{bmatrix}=\begin{bmatrix}18 & 20\\3 & 0\end{bmatrix}$$

$$P_4 = C_4 - K = \begin{bmatrix} 19 & 13 \\ 26 & 10 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 7 & 93 \\ 18 & 0 \end{bmatrix}$$

$$P_5 = C_5 - K = \begin{bmatrix} 36 & 14 \\ 7 & 29 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 24 & 0 \\ 93 & 19 \end{bmatrix}$$

$$P_6 = C_6 - K = \begin{bmatrix} 29 & 14 \\ 11 & 28 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 17 & 0 \\ 3 & 18 \end{bmatrix}$$

$$P_7 = C_7 - K = \begin{bmatrix} 17 & 18 \\ 25 & 9 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 5 & 4 \\ 17 & 93 \end{bmatrix}$$

$$P_8 = C_8 - K = \begin{bmatrix} 22 & 18 \\ 7 & 27 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 10 & 4 \\ 93 & 17 \end{bmatrix}$$

$$P_9 = C_9 - K = \begin{bmatrix} 16 & 24 \\ 12 & 23 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 4 & 10 \\ 4 & 13 \end{bmatrix}$$

$$P_{10} = C_{10} - K = \begin{bmatrix} 20 & 27 \\ 14 & 9 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 8 & 13 \\ 6 & 93 \end{bmatrix}$$

$$P_{11} = C_{11} - K = \begin{bmatrix} 12 & 27 \\ 11 & 10 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 0 & 13 \\ 3 & 0 \end{bmatrix}$$

$$P_{12} = C_{12} - K = \begin{bmatrix} 11 & 32 \\ 12 & 11 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 93 & 18 \\ 4 & 1 \end{bmatrix}$$

$$P_{13} = C_{13} - K = \begin{bmatrix} 16 & 32 \\ 8 & 27 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 4 & 18 \\ 0 & 17 \end{bmatrix}$$

$$P_{14} = C_{14} - K = \begin{bmatrix} 11 & 41 \\ 43 & 45 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 93 & 27 \\ 35 & 35 \end{bmatrix}$$

$$P_{15} = C_{15} - K = \begin{bmatrix} 11 & 23 \\ 28 & 29 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 93 & 9 \\ 20 & 19 \end{bmatrix}$$

$$P_{16} = C_{16} - K = \begin{bmatrix} 12 & 13 \\ 25 & 30 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 0 & 93 \\ 17 & 20 \end{bmatrix}$$

$$P_{17} = C_{17} - K = \begin{bmatrix} 27 & 22 \\ 8 & 17 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 15 & 8 \\ 0 & 7 \end{bmatrix}$$

$$P_{18} = C_{18} - K = \begin{bmatrix} 8 & 13 \\ 63 & 60 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 90 & 93 \\ 55 & 50 \end{bmatrix}$$

$$P_{19} = C_{19} - K = \begin{bmatrix} 59 & 64 \\ 57 & 52 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 47 & 50 \\ 49 & 42 \end{bmatrix}$$

$$P_{20} = C_{20} - K = \begin{bmatrix} 11 & 53 \\ 52 & 9 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 93 & 39 \\ 44 & 93 \end{bmatrix}$$

$$P_{21} = C_{21} - K = \begin{bmatrix} 50 & 54 \\ 54 & 73 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 38 & 40 \\ 46 & 63 \end{bmatrix}$$

Hasil perhitungan selanjutnya diubah ke dalam huruf sesuai dengan tabel kode (terlampir pada lampiran 1) sehingga diperoleh suatu *plaintext* yaitu:

Uangnya sudah saya transfer ke rekening anda sebesar 200 juta rupiah, TOLONG DI CEK!

b. Berdasarkan (**Kasus 2**) dihasilkan suatu pesan rahasia (*chipertext*) berupa:

VzfjM2oq4ssjZ3fjKkhUxo2oznhj

Pesan tersebut terlebih dahulu diubah menjadi blok-blok 4 karakter sehingga diperoleh sebagai berikut:

Vzfj	**M2oq**	**4ssj**	**Z3fj**
KkhU	**xo2o**	**znhj**	

Setiap blok kemudian diubah ke dalam angka-angka sesuai dengan tabel kode (terlampir pada lampiran 1) dan ditulis dalam bentuk matriks C_{2x2}. Misalkan pada pesan blok pertama yaitu **Vzfj**, maka dikonversi dengan tabel kode (terlampir pada lampiran 1) didapat V=57, z=25, f=5, j=9 sehingga diperoleh *ciphertext* $C_1 = \begin{bmatrix} 57 & 25 \\ 5 & 9 \end{bmatrix}$ dan seterusnya sampai pada pesan blok terakhir sehingga diperoleh *ciphertext* sebagai berikut:

$C_1 = \begin{bmatrix} 57 & 25 \\ 5 & 9 \end{bmatrix}$; $C_2 = \begin{bmatrix} 48 & 27 \\ 14 & 16 \end{bmatrix}$; $C_3 = \begin{bmatrix} 29 & 18 \\ 18 & 9 \end{bmatrix}$

$C_4 = \begin{bmatrix} 61 & 28 \\ 5 & 9 \end{bmatrix}$; $C_5 = \begin{bmatrix} 46 & 10 \\ 7 & 56 \end{bmatrix}$; $C_6 = \begin{bmatrix} 23 & 14 \\ 27 & 14 \end{bmatrix}$

$C_7 = \begin{bmatrix} 25 & 13 \\ 7 & 9 \end{bmatrix}$

Pesan tersebut kemudian didekripsi menggunakan kunci yang telah disepakati yaitu $K = \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix}$ dan dilakukan perhitungan dengan rumus $P_i = (C_i - K) \bmod 94$, sehingga diperoleh

$P_1 = C_1 - K = \begin{bmatrix} 57 & 25 \\ 5 & 9 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 45 & 11 \\ 91 & 93 \end{bmatrix}$

$P_2 = C_2 - K = \begin{bmatrix} 48 & 27 \\ 14 & 16 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 36 & 13 \\ 6 & 6 \end{bmatrix}$

$P_3 = C_3 - K = \begin{bmatrix} 29 & 18 \\ 18 & 9 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 17 & 4 \\ 10 & 93 \end{bmatrix}$

$P_4 = C_4 - K = \begin{bmatrix} 61 & 28 \\ 5 & 9 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 49 & 14 \\ 91 & 93 \end{bmatrix}$

$P_5 = C_5 - K = \begin{bmatrix} 46 & 10 \\ 7 & 56 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 34 & 90 \\ 93 & 46 \end{bmatrix}$

$P_6 = C_6 - K = \begin{bmatrix} 23 & 14 \\ 27 & 14 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 11 & 0 \\ 19 & 4 \end{bmatrix}$

$P_7 = C_7 - K = \begin{bmatrix} 25 & 13 \\ 7 & 9 \end{bmatrix} - \begin{bmatrix} 12 & 14 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 13 & 93 \\ 93 & 93 \end{bmatrix}$

Hasil perhitungan selanjutnya diubah ke dalam huruf sesuai dengan tabel kode (terlampir pada lampiran 1) sehingga diperoleh suatu *plaintext* yaitu:

Jl. Anggrek No. 9, Klaten

BAB IV

PENUTUP

A. Kesimpulan

Kesimpulan yang dapat diambil dalam skripsi ini yaitu sifat perkalian matriks atas aljabar *min-plus* dapat diterapkan untuk menentukan kunci pada proses pengamanan informasi rahasia. Adapun algoritma untuk pembentukan kunci tersebut yaitu:

<table>
<tr><td colspan="2">Pihak 1 atau pihak 2 mempublikasikan suatu semiring $(\mathbb{Z}_{min})^{n\,x\,n}$ dan A,B$\in(\mathbb{Z}_{min})^{n\,x\,n}$</td></tr>
<tr><td>Pihak 1</td><td>Pihak 2</td></tr>
<tr><td>1. Memilih secara rahasia bilangan asli m dan n.
2. Menghitung $U = A^m B^n$
3. Mengirim U kepada pihak 2
4. Menerima V dari pihak 2
5. Menghitung $K_1 = A^m V B^n$</td><td>1. Memilih secara rahasia bilangan asli r dan s.
2. Menghitung $V = A^r B^s$
3. Mengirim V kepada pihak 1
4. Menerima U dari pihak 1
5. Menghitung $K_2 = A^r U B^s$</td></tr>
<tr><td colspan="2">Pihak 1 dan pihak 2 menyepakati kunci yang sama $K = K_1 = K_2$</td></tr>
</table>

Dari proses pembentukan kunci, diperoleh kunci yang sama antara pihak 1 dan pihak 2 yaitu $K = K_1 = K_2$. Kunci tersebut digunakan pada proses enkripsi dan dekripsi. Proses enkripsi dilakukan oleh pihak 1 atau pihak pengirim pesan dengan cara mengubah pesan yang akan dikirim atau

plaintext ke dalam bentuk *ciphertext* dengan rumus $C_i = (K + P_i) \bmod 94$, sedangkan proses dekripsi dilakukan oleh pihak 2 atau pihak penerima pesan dengan cara mengubah pesan yang telah diterima atau *ciphertext* ke dalam bentuk *plaintext* dengan menggunakan rumus $P_i = (C_i - K) \bmod 94$,

dengan

C_i= *Ciphertext*

K= *Kunci*

P_i= *Plaintext*

$i = 1,2,3,\dots,n.$

B. Saran

Berdasarkan hasil penulisan skripsi ini, penulis memberikan beberapa saran untuk mengembangkan skripsi ini menjadi lebih baik, antara lain:

1. Dalam sistem kriptografi ini, pembentukan kunci sangat penting untuk proses pengamanan pesan. Kunci harus dijaga keamanannya dengan membuat kunci yang baru setiap melakukan komunikasi agar tidak mudah dimanipulasi oleh pihak-pihak yang tidak bertanggungjawab.
2. Dalam skripsi ini belum membahas tingkat keamanan algoritma pembentukan kunci yang dipakai dan jenis sistem kriptografinya. Bagi pembaca yang ingin mengembangkan skripsi ini dapat menggunakan algoritma lain yang tingkat keamanannya lebih tinggi.

DAFTAR PUSTAKA

Chung, Misoo. 1995. *Eigenvalues and Eigenvectors in the Max-Plus Algebra*. Thesis. University of Colorado.

Decky Hendarsyah dan Retantyo Wardoyo. 2011. Implementasi Protokol Diffie-Hiellman Dan Algoritma RC4 Untuk Keamanan Pesan SMS. *Jurnal IJCCS.* Volume 5. No. 1.

Le Boudec, J.Y, Thiran, P. Tanpa tahun. *Min-Plus System Theory Applied to Communication Network*. Swiss.

Menezes, Oorcshot, and Vanstone. 1996. *Handbook of Applied Cryptography*.

Florida: CRC Press.

Mulyadi. 2011. Perbandingan Sistem Persamaan Linier Dalam Aljabar Klasik dan Aljabar Max-Plus. Tesis. FMIPA, Univ.Indonesia.

Musthofa. 2011. Sistem Persamaan Linier pada Aljabar Min-Plus, dipresentasikan pada Seminar Nasional MIPA, FMIPA UNY Yogyakarta, 14 Mei 2011

Musthofa, Dwi Lestari. 2013. Metode Perjanjian Password Berdasarkan Operasi Matriks atas Aljabar Min-Plus untuk Keamanan Pengiriman Informasi Rahasia. Penelitian. FMIPA, UNY

Myasnikov Alexei, Vladimir Shpilrain and Alexander Ushakov. 2008. *Group-based Cryptography*. Basel Switzerland: Birkhauser Verlag.

M. Zaki Riyanto, 2011. Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi atas Grup Non-komutatif, dipresentasikan pada Seminar Nasional MIPA, FMIPA UNY Yogyakarta, 14 Mei 2011.

Rinaldi Munir. 2006. Kriptografi. Bandung: Informatika Bandung.

Rininda Ulfa Arizka. 2011. Penerapan Sistem Kriptografi ElGamal atas $\mathbb{Z}_p^*$ Dalam Pembuatan Tanda Tangan Digital. *Skripsi*. Universitas Negeri Yogyakarta.

Schneier, Bruce. 1996. *Applied Cryptography.* Second Edition, New Jersey: John Wiley & Sons, Inc.

Stallings, Williams. 2005. *Cryptography and Network Security.* New Jersey: Pearson.

Stickel, E. 2005. *A New Method for Exchanging Secret Keys*. Proceedings of The Third International Conference on Information Technology and Applications (ICITA05), Contemporary Mathematics 2, pp. 426-430. IEEE Computer Society.

Stinson Douglas, R. 2006.*Cryptography: Theory and Practice Third Edition*. Florida: CRC Press.

Subiono. 2010. Aljabar *Maxplus* dan Terapannya. Surabaya: Institut Teknologi Sepuluh November.

LAMPIRAN

Lampiran 1: Tabel Kode (0-93)

No	Kode
0	a
1	b
2	c
3	d
4	e
5	f
6	g
7	h
8	i
9	j
10	k
11	l
12	m
13	n
14	o
15	p
16	q
17	r
18	s
19	t
20	u
21	v
22	w
23	x
24	y
25	z
26	1
27	2
28	3
29	4
30	5
31	6
32	7

No	Kode
33	8
34	9
35	0
36	A
37	B
38	C
39	D
40	E
41	F
42	G
43	H
44	I
45	J
46	K
47	L
48	M
49	N
50	O
51	P
52	Q
53	R
54	S
55	T
56	U
57	V
58	W
59	X
60	Y
61	Z
62	~
63	!
64	@
65	#

No	Kode
66	$
67	%
68	^
69	&
70	*
71	(
72	)
73	_
74	+
75	`
76	=
77	-
78	{
79	}
80	|
81	[
82	]
83	\
84	:
85	"
86	;
87	<
88	>
89	?
90	,
91	.
92	/
93	<*space*>

Lampiran 2.

Program untuk Proses Pembentukan Kunci

```
function k=minmult(A,B)
syms  p q r s;
disp('masukkan matriks n x n');
disp('awali dan akhiri dengan []');
X=input('A= ');
[p,q]=size(X);
while p>q | p<q
pdisp('masukkan matriks n x n');
X=input('A= ');
[p,q]=size(X);
end
Y=input('B= ');
[r,s]=size(Y);
while r>s | r<s
disp('masukkan matriks n x n');
Y=input('B= ');
[r,s]=size(Y);
end
disp('pilih sebarang bilangan m dan n dari pihak 1');
m=input('m= ');
n=input('n= ');
%mencari E dan F
switch m
    case {4}
    if q==p E=inf*ones(p,q);
            for i=1:p;
                for j=1:q;
                    for k=1:q;
                        for l=1:q;
                            for t=1:q;
```

```
        E(i,t)=min(E(i,t),(X(i,k)+X(k,j)+X(j,l)+X(l,t)));
                        end
                    end
                end
            end
        end
end
case {3}
if q==p E=inf*ones(p,q);
        for i=1:p;
            for j=1:q;
                for k=1:q;
                    for l=1:q;
            E(i,l)=min(E(i,l),(X(i,k)+X(k,j)+X(j,l)))
                    end
                end
            end
        end
end
case {2}
if q==p E=inf*ones(p,q);
    for i=1:p;
        for j=1:q;
            for k=1:q;
                 E(i,j)=min(E(i,j),(X(i,k)+X(k,j)));
            end
        end
    end
end
case {1}
if q==p E=inf*ones(p,q);
    for i=1:p;
        for j=1:q;
              E(i,j)=min(E(i,j),(X(i,j)));
```

```
            end
        end
    end
end
switch n
    case {4}
    if s==r F=inf*ones(r,s);
            for i=1:r;
                for j=1:s;
                    for k=1:s;
                        for l=1:s;
                            for t=1:s;
          F(i,t)=min(F(i,t),(Y(i,k)+Y(k,j)+Y(j,l)+Y(l,t)));
                            end
                        end
                    end
                end
            end
    end
    case {3}
    if s==r F=inf*ones(r,s);
            for i=1:r;
                for j=1:s;
                    for k=1:s;
                        for l=1:s;
                 F(i,l)=min(F(i,l),(Y(i,k)+Y(k,j)+Y(j,l)));
                        end
                    end
                end
            end
    end

    case {2}
    if s==r F=inf*ones(r,s);
```

```
        for i=1:r;
            for j=1:s;
                for k=1:s;
                     F(i,j)=min(F(i,j),(Y(i,k)+Y(k,j)));
                end
            end
        end
    end
    case {1}
    if s==r F=inf*ones(r,s);
        for i=1:r;
            for j=1:s;
                  F(i,j)=min(F(i,j),(Y(i,j)));
            end
        end
    end
end
%mencari matriks U
if q==r U=inf*ones(p,s);
    for i=1:p;
        for j=1:s;
            for k=1:q;
                U(i,j)=min(U(i,j),(E(i,k)+F(k,j)))
            end
        end
    end
else disp('Ukuran matriks A dan B harus sama!');
end
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
disp('pilih sebarang bilangan r dan s dari pihak 2');
r1=input('r= ');
s1=input('s= ');
%mencari G dan H
switch r1
```

```
case {4}
if q==p E1=inf*ones(p,q);
        for i=1:p;
            for j=1:q;
                for k=1:q;
                    for l=1:q;
                        for t=1:q;
 E1(i,t)=min(E1(i,t),(X(i,k)+X(k,j)+X(j,l)+X(l,t)));
                        end
                    end
                end
            end
        end
end
case {3}
if q==p E1=inf*ones(p,q);
        for i=1:p;
            for j=1:q;
                for k=1:q;
                    for l=1:q;
       E1(i,l)=min(E1(i,l),(X(i,k)+X(k,j)+X(j,l)));
                    end
                end
            end
        end
end
case {2}
if q==p E1=inf*ones(p,q);
    for i=1:p;
        for j=1:q;
            for k=1:q;
                 E1(i,j)=min(E1(i,j),(X(i,k)+X(k,j)));
            end
        end
```

```
        end
    end
    case {1}
    if q==p E1=inf*ones(p,q);
        for i=1:p;
            for j=1:q;
                  E1(i,j)=min(E1(i,j),(X(i,j)));
            end
        end
    end
end
switch s1
    case {4}
    if s==r F1=inf*ones(r,s);
            for i=1:r;
                for j=1:s;
                    for k=1:s;
                        for l=1:s;
                            for t=1:s;
     F1(i,t)=min(F1(i,t),(Y(i,k)+Y(k,j)+Y(j,l)+Y(l,t)));
                            end
                        end
                    end
                end
            end
    end
    case {3}
    if s==r F1=inf*ones(r,s);
            for i=1:r;
                for j=1:s;
                    for k=1:s;
                        for l=1:s;
           F1(i,l)=min(F1(i,l),(Y(i,k)+Y(k,j)+Y(j,l)));
                        end
```

```
                    end
                end
            end
        end
        case {2}
        if s==r F1=inf*ones(r,s);
            for i=1:r;
                for j=1:s;
                    for k=1:s;
                         F1(i,j)=min(F1(i,j),(Y(i,k)+Y(k,j)));
                    end
                end
            end
        end
        case {1}
        if s==r F1=inf*ones(r,s);
            for i=1:r;
                for j=1:s;
                      F1(i,j)=min(F1(i,j),(Y(i,j)));
                end
            end
        end
    end
    %mencari matriks V
    if q==r V=inf*ones(p,s);
        for i=1:p;
            for j=1:s;
                for k=1:q;
                    V(i,j)=min(V(i,j),(E1(i,k)+F1(k,j)));
                end
            end
        end
    else disp('Ukuran matriks A dan B harus sama!');
    end
```

```
[a,b]=size(X);
[e,f]=size(V);

%mencari matriks Kunci
if b==e K1=inf*ones(a,f);
    for i=1:a
        for j=1:f
            for k=1:b
                K1(i,j)=min(K1(i,j),(E(i,k)+V(k,j)));
            end
        end
    end
end
[c,d]=size(Y);
[g,h]=size(K1);

if d==g K=inf*ones(c,h);
    for i=1:c;
        for j=1:h;
            for k=1:d;
                K(i,j)=min(K(i,j),(K1(i,k)+F(k,j)))
            end
        end
    end
end
```

Lampiran 3.

Program untuk mengubah huruf menjadi angka

```
function [angka] = hurufkeangka(huruf)
angka = [];
for i=1:size(huruf,2)
    angka(i) = Ubah(huruf(i));
```

```
end

function [angka] = Ubah(huruf)
if strcmp(huruf,'a')==1
    angka=0;
elseif strcmp(huruf,'b')==1
    angka=1;
elseif strcmp(huruf,'c')==1
    angka=2;
elseif strcmp(huruf,'d')==1
    angka=3;
elseif strcmp(huruf,'e')==1
    angka=4;
elseif strcmp(huruf,'f')==1
    angka=5;
elseif strcmp(huruf,'g')==1
    angka=6;
elseif strcmp(huruf,'h')==1
    angka=7;
elseif strcmp(huruf,'i')==1
    angka=8;
elseif strcmp(huruf,'j')==1
    angka=9;
elseif strcmp(huruf,'k')==1
    angka=10;
elseif strcmp(huruf,'l')==1
    angka=11;
elseif strcmp(huruf,'m')==1
    angka=12;
elseif strcmp(huruf,'n')==1
    angka=13;
elseif strcmp(huruf,'o')==1
    angka=14;
elseif strcmp(huruf,'p')==1
```

```
    angka=15;
elseif strcmp(huruf,'q')==1
    angka=16;
elseif strcmp(huruf,'r')==1
    angka=17;
elseif strcmp(huruf,'s')==1
    angka=18;
elseif strcmp(huruf,'t')==1
    angka=19;
elseif strcmp(huruf,'u')==1
    angka=20;
elseif strcmp(huruf,'v')==1
    angka=21;
elseif strcmp(huruf,'w')==1
    angka=22;
elseif strcmp(huruf,'x')==1
    angka=23;
elseif strcmp(huruf,'y')==1
    angka=24;
elseif strcmp(huruf,'z')==1
    angka=25;
elseif strcmp(huruf,'1')==1
    angka=26;
elseif strcmp(huruf,'2')==1
    angka=27;
elseif strcmp(huruf,'3')==1
    angka=28;
elseif strcmp(huruf,'4')==1
    angka=29;
elseif strcmp(huruf,'5')==1
    angka=30;
elseif strcmp(huruf,'6')==1
    angka=31;
elseif strcmp(huruf,'7')==1
```

```
    angka=32;
elseif strcmp(huruf,'8')==1
    angka=33;
elseif strcmp(huruf,'9')==1
    angka=34;
elseif strcmp(huruf,'0')==1
    angka=35;
elseif strcmp(huruf,'A')==1
    angka=36;
elseif strcmp(huruf,'B')==1
    angka=37;
elseif strcmp(huruf,'C')==1
    angka=38;
elseif strcmp(huruf,'D')==1
    angka=39;
elseif strcmp(huruf,'E')==1
    angka=40;
elseif strcmp(huruf,'F')==1
    angka=41;
elseif strcmp(huruf,'G')==1
    angka=42;
elseif strcmp(huruf,'H')==1
    angka=43;
elseif strcmp(huruf,'I')==1
    angka=44;
elseif strcmp(huruf,'J')==1
    angka=45;
elseif strcmp(huruf,'K')==1
    angka=46;
elseif strcmp(huruf,'L')==1
    angka=47;
elseif strcmp(huruf,'M')==1
    angka=48;
elseif strcmp(huruf,'N')==1
```

```
    angka=49;
elseif strcmp(huruf,'O')==1
    angka=50;
elseif strcmp(huruf,'P')==1
    angka=51;
elseif strcmp(huruf,'Q')==1
    angka=52;
elseif strcmp(huruf,'R')==1
    angka=53;
elseif strcmp(huruf,'S')==1
    angka=54;
elseif strcmp(huruf,'T')==1
    angka=55;
elseif strcmp(huruf,'U')==1
    angka=56;
elseif strcmp(huruf,'V')==1
    angka=57;
elseif strcmp(huruf,'W')==1
    angka=58;
elseif strcmp(huruf,'X')==1
    angka=59;
elseif strcmp(huruf,'Y')==1
    angka=60;
elseif strcmp(huruf,'Z')==1
    angka=61;
elseif strcmp(huruf,'~')==1
    angka=62;
elseif strcmp(huruf,'!')==1
    angka=63;
elseif strcmp(huruf,'@')==1
    angka=64;
elseif strcmp(huruf,'#')==1
    angka=65;
elseif strcmp(huruf,'$')==1
```

```
    angka=66;
elseif strcmp(huruf,'%')==1
    angka=67;
elseif strcmp(huruf,'^')==1
    angka=68;
elseif strcmp(huruf,'&')==1
    angka=69;
elseif strcmp(huruf,'*')==1
    angka=70;
elseif strcmp(huruf,'(')==1
    angka=71;
elseif strcmp(huruf,')')==1
    angka=72;
elseif strcmp(huruf,'_')==1
    angka=73;
elseif strcmp(huruf,'+')==1
    angka=74;
elseif strcmp(huruf,'`')==1
    angka=75;
elseif strcmp(huruf,'-')==1
    angka=76;
elseif strcmp(huruf,'=')==1
    angka=77;
elseif strcmp(huruf,'{')==1
    angka=78;
elseif strcmp(huruf,'}')==1
    angka=79;
elseif strcmp(huruf,'|')==1
    angka=80;
elseif strcmp(huruf,'[')==1
    angka=81;
elseif strcmp(huruf,']')==1
    angka=82;
elseif strcmp(huruf,'\')==1
```

```
    angka=83;
elseif strcmp(huruf,':')==1
    angka=84;
elseif strcmp(huruf,'"')==1
    angka=85;
elseif strcmp(huruf,';')==1
    angka=86;
elseif strcmp(huruf,'<')==1
    angka=87;
elseif strcmp(huruf,'>')==1
    angka=88;
elseif strcmp(huruf,'?')==1
    angka=89;
elseif strcmp(huruf,',')==1
    angka=90;
elseif strcmp(huruf,'.')==1
    angka=91;
elseif strcmp(huruf,'/')==1
    angka=92;
elseif strcmp(huruf,' ')==1
    angka=93;
end
```

Lampiran 4.

Program untuk Proses Enkripsi

```
kunci=input('Kunci= ')
m=input('tulis pesan= ','s')
n=length(m);
o=hurufkeangka(m)
if mod(n,4)==0
   for e=0:((n/4)-1)
       b=4*e;
```

```
        k=1;
        P=[o(k+b) o(k+b+1); o(k+b+2) o(k+b+3)];

C='abcdefghijklmnopqrstuvwxyz1234567890ABCDEFGHIJKLMNOPQRSTU
VWXYZ~!@#$%^&*()_+`-={}|[]\:";<>?,./ ';
    q=mod(P+kunci+1,94);
    mat=C(q);
    a=mat(1,1:2);
    b=mat(2,1:2);
    ciphertext=[a b]
   end
else if mod(n,4)==3
        t=[93];
        t1=[o t];
        r=length(t1);
        for e=0:((r/4)-1)
            b=4*e;
            k=1;
            P=[t1(k+b) t1(k+b+1); t1(k+b+2) t1(k+b+3)];

C='abcdefghijklmnopqrstuvwxyz1234567890ABCDEFGHIJKLMNOPQRSTU
VWXYZ~!@#$%^&*()_+`-={}|[]\:";<>?,./ ';
    p=mod(P,94);
    q=mod(p+kunci+1,94);
    mat=C(q);
        a=mat(1,1:2);
        b=mat(2,1:2);
        ciphertext=[a b]
        end
 else if mod(n,4)==2
            t=[93 93];
            t1=[o t];
            r=length(t1);
            for e=0:((r/4)-1)
```

```
                b=4*e;
                k=1;
                P=[t1(k+b) t1(k+b+1); t1(k+b+2) t1(k+b+3)];

C='abcdefghijklmnopqrstuvwxyz1234567890ABCDEFGHIJKLMNOPQRSTU
VWXYZ~!@#$%^&*()_+`-={}|[]\:";<>?,./ ';
    p=mod(P,94);
    q=mod(p+kunci+1,94);
    mat=C(q);
            a=mat(1,1:2);
            b=mat(2,1:2);
            ciphertext=[a b]
            end
else if mod(n,4)==1
                t=[93 93 93];
                t1=[o t];
                r=length(t1);
                for e=0:((r/4)-1)
                    b=4*e;
                    k=1;
                    P=[t1(k+b) t1(k+b+1); t1(k+b+2)
t1(k+b+3)];

C='abcdefghijklmnopqrstuvwxyz1234567890ABCDEFGHIJKLMNOPQRSTU
VWXYZ~!@#$%^&*()_+`-={}|[]\:";<>?,./ ';
    p=mod(P,94);
    q=mod(p+kunci+1,94);
    mat=C(q);
                a=mat(1,1:2);
                b=mat(2,1:2);
                ciphertext=[a b]
                end
            end
        end
```

```
    end
end
```

Lampiran 5.

Program untuk Proses Dekripsi

```
kunci=input('Kunci= ')
m=input('tulis pesan= ','s')
n=length(m);
o=hurufkeangka(m)
   for e=0:((n/4)-1)
       b=4*e;
       k=1;
       C=[o(k+b) o(k+b+1); o(k+b+2) o(k+b+3)];
    c='
abcdefghijklmnopqrstuvwxyz1234567890ABCDEFGHIJKLMNOPQRSTUVWX
YZ~!@#$%^&*()_+`-={}|[]\:";<>?,./';
    q=mod(C-kunci+2,94);
    mat=c(q);
    a=mat(1,1:2);
    b=mat(2,1:2);
    plaintext=[a b]
    end
```

Lampiran 6.

Hasil Perhitungan Pembentukan Kunci

```
>> key

masukkan matriks n x n

awali dan akhiri dengan []
```

```
A= [3 5;2 1]

B= [1 4;4 2]

pilih sebarang bilangan m dan n

m= 2

n= 2

U =

     8    10

     5     6

masukkan V dari pihak 2

V= [7 8; 4 4]

K =

    12    14

     8    10
```

Lampiran 7.

Hasil Proses Enkripsi (kasus 1)

```
>> enk

Kunci= [12 14; 8 10]

kunci =

    12    14
```

```
     8    10

tulis pesan= Uangnya sudah saya transfer ke rekening anda
sebesar 200 juta rupiah, TOLONG DI CEK!

Ciphertext=

^ovqzCij59lktn1kAoh44ov3rszjwsh2qymxu2ojm2lkl7mlq7i2lFHJlx34
mnz52wirin!YX@VQlRQjOSS_
```

Lampiran 8.

Hasil Proses Enkripsi (kasus 2)

```
>> enk

Kunci= [12 14; 8 10]

kunci =

    12    14

     8    10

tulis pesan= Jl. Anggrek No. 9, Klaten

ciphertext = VzfjM2oq4ssjZ3fjKkhUxo2oznhj
```

Lampiran 9.

Hasil Proses Dekripsi (kasus 1)

```
>> dek

Kunci= [12 14; 8 10]
```

```
kunci =

    12    14

     8    10

tulis pesan=
^ovqzCij59lktn1kAoh44ov3rszjwsh2qymxu2ojm2lkl7mlq7i2lFHJlx34
mnz52wirin!YX@VQlRQjOSS_

Plaintext = Uangnya sudah saya transfer ke rekening anda
sebesar 200 juta rupiah, TOLONG DI CEK!
```

Lampiran 10.

Hasil Proses Dekripsi (kasus 2)

```
>> dek

Kunci= [12 14; 8 10]



kunci =

    12    14

     8    10

tulis pesan= VzfjM2oq4ssjZ3fjKkhUxo2oznhj

plaintext= Jl. Anggrek No. 9, Klaten
```