UNIVERSITAS INDONESIA

METODE IMAI-MATSUMOTO PADA LAPANGAN HINGGA $GF(2^m)$

SKRIPSI

DIMAS TRISNADI

0305010173

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

PROGRAM STUDI MATEMATIKA

DEPOK

JULI 2010

UNIVERSITAS INDONESIA

METODE IMAI-MATSUMOTO PADA LAPANGAN HINGGA $GF(2^m)$

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana sains

DIMAS TRISNADI

0305010173

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
PROGRAM STUDI MATEMATIKA

DEPOK

JULI 2010

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri,

dan semua sumber baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar.

Nama	: Dimas Trisnadi
NPM	: 0305010173
Tanda Tangan	: 
Tanggal	: 13 Juli 2010

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh
Nama : Dimas Trisnadi
NPM : 0305010173
Program Studi : Matematika
Judul Skripsi : Metode Imai-Matsumoto pada Lapangan Hingga $GF\left(2^m\right)$

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Sains pada Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Indonesia

DEWAN PENGUJI

Pembimbing I : Dr. Sri Mardiyati, M. Kom ( )

Pembimbing II : Helen Burhan, M.Si ( )

Penguji : Dra. Suarsih Utama ( )

Penguji : Dhian Widya, M. Kom ( )

Ditetapkan di : Depok
Tanggal : 13 Juli 2010

KATA PENGANTAR

Alhamdulillah, segala puji dan syukur penulis panjatkan kepada Allah SWT, dzat yang telah melimpahkan berbagai nikmat dan karunia-Nya kepada penulis serta karena rahmat-Nya, penulis dapat menyelesaikan skripsi ini.

Penulis menyadari bahwa, tanpa bantuan, bimbingan, dan dukungan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi penulis untuk menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

(1) Orang tua penulis yaitu Tatang Sutrisno dan Sumarni yang telah merawat, mendidik, dan membesarkan penulis dengan penuh kasih sayang. Jasa kalian tak akan pernah dapat penulis balas dan skripsi ini adalah salah satu upaya kecil untuk membahagiakan kalian;

(2) Bu Sri Mardiyati dan Bu Helen Burhan, selaku pembimbing I dan II yang telah bersedia menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan skripsi ini;

(3) Pak Suryadi MT, Pembimbing Akademik yang selalu memberi nasihat dan arahan kepada penulis selama kuliah di depatemen Matematika UI;

(4) Pak Yudi Satria dan Bu Dian, yang telah membuka kuliah Analisis II pada semester yang tidak semestinya dibuka, serta penulis ucapkan terima kasih pula kepada Pak Ari Wibowo selaku dosen Analisi II;

(5) Zawjati Aisyah Setyowati As-Salafy yang telah begitu sabar dan setia menemani penulis dalam menghadapi masa-masa sulit serta tidak henti-hentinya memberikan dukungan dan semangat sehingga akhirnya penulis dapat menyelesaikan skripsi ini. Uhibbuki fillah habibaty;

(6) Mba Yunda, Angga, Mas Ari, sikecil Sultan, dan Pakde, terima kasih telah mengisi hari-hari penulis dengan keceriaan disaat penulis pulang ke rumah;

(7) Bapak Djoko Suripto dan Ibu Sri Wahyuni, orang yang sangat penulis kagumi karena kelemah lembutan akhlak dan lisan mereka serta begitu tawakal dan tawadhu dalam menjalani kehidupan, semoga penulis dapat

mencontoh kalian dan semoga Allah senantiasa mengumpulkan kita dalam kebaikan;

(8) Anak-anak kontrakan yang hidup serba seadanya yaitu: Arif Wirawan, Ridwan Setiawan, Ashari Nurhidayat, dan Sigap Pamungkas;

(9) Hamdan, Hairu, dan Latif teman seperjuangan yang sama-sama terlantar saat daftar seminar kolokium;

(10) Anak-anak ABEL: Maulana, uun, Rifkos, Ridwan lagi, Aris, Hamdan lagi, Hairu lagi, Udin, Trian, Asep, Cupz, dan Imba;

Semoga Allah SWT membalas kebaikan kalian dengan balasan yang baik. Akhir kata, penulis berharap semoga skripsi ini membawa manfaat bagi pengembangan ilmu.

Penulis

2010

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama	: Dimas Trisnadi
NPM	: 0305010173
Program Studi	: Matematika
Departemen	: Matematika
Fakultas	: Matematika dan Ilmu Pengetahuan Alam
Jenis Karya	: Skripsi

Demi pengembangan ilmu pengetahuan, meyetujui untuk memberikan kepada Universitas Indonesia Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul :

Metode Imai-Matsumoto Pada Lapangan Hingga $GF\left(2^m\right)$

Beserta perangkat yang ada. Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikia pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 13 Juli 2010
Yang menyatakan

(Dimas Trisnadi)

ABSTRAK

Nama : Dimas Trisnadi
Program Studi : Matematika
Judul : Metode Imai-Matsumoto pada Lapangan Hingga $GF\left(2^m\right)$

Metode dalam kriptografi dibedakan menjadi dua berdasarkan jenis kunci yang digunakan, yaitu metode simetris dan metode asimetris. Salah satu metode asimetris dalam kriptografi adalah metode Imai-Matsumoto. Dalam tugas akhir ini akan dibahas tentang cara kerja metode Imai-Matsumoto yang bekerja pada lapangan hingga $GF\left(2^m\right)$. Metode ini menggunakan dua jenis kunci yang berbeda yaitu kunci pribadi dan kunci umum. Kunci umum pada metode ini dibentuk dari kunci pribadi yang dipilih oleh sipengguna metode.

Kata kunci : metode simetris, metode asimetris, lapangan, kunci pribadi, Kunci umum.
ix + 35 Halaman.
Daftar Pustaka : 8 (1990 - 2005)

ABSTRACT

Name : Dimas Trisnadi
Program Study : Mathematics
Title : Imai-Matsumoto Method on Finite Field $GF\left(2^m\right)$

Cryptographic methods are distinguished into two types based on the type of key used, namely symmetric method and asymmetric method. One of the asymmetric methods is the Imai-Matsumoto method. This mini thesis will discuss the Imai-Matsumoto method that works on the finite field $GF\left(2^m\right)$. This method uses two different types of keys those are private key and public key. The public key is formed by the private keys selected by user.

Key Word : symmetric method, asymmetric method, field, private key, public key.
ix + 35 Pages.
Bibliography : 8 (1990 - 2005)

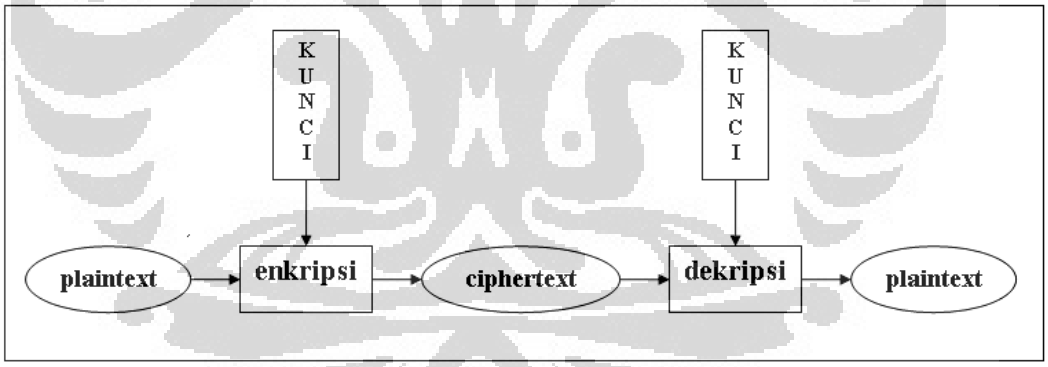
DAFTAR ISI

BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Dalam dunia teknologi dan komputerisasi, pengamanan suatu informasi merupakan hal yang penting, oleh karena itu dibutuhkan suatu metode atau cara agar suatu informasi yang bersifat rahasia tidak dapat diketahui oleh pihak yang tidak berhak mengetahui informasi tersebut.

Ilmu yang mempelajari tentang penulisan rahasia atau pengkodean suatu pesan/teks disebut kriptografi. Proses untuk mengubah suatu teks asli (*plaintext*) menjadi teks yang dikodekan (*ciphertext*), disebut enkripsi, atau proses sebaliknya yang disebut dekripsi, dibutuhkan suatu kunci (William Stalling, 2005). Secara umum proses suatu metode kriptografi dapat digambarkan sebagai berikut :



Gambar 1.1

Berdasarkan gambar di atas terlihat bahwa untuk melakukan enkripsi dan dekripsi masing-masing digunakan suatu kunci. Jika kunci yang digunakan untuk kedua proses tersebut sama maka metode tersebut disebut metode simetris, dan jika kunci yang digunakan dalam proses enkripsi dan dekripsi berbeda maka metode tersebut disebut metode asimetris (William Stalling, 2005).

Pada metode asimetris terdapat dua jenis kunci berbeda yang digunakan, yaitu kunci yang digunakan untuk enkripsi yang biasa disebut kunci umum dan kunci untuk dekripsi yang biasa disebut kunci pribadi.

Salah satu metode asimetris dalam kriptografi adalah metode Imai-Matsumoto. Pada metode ini kunci umumnya berupa himpunan persamaan polinomial nonlinier dan kunci pribadinya adalah sejumlah parameter yang dipilih oleh user untuk membentuk persamaan polinomial nonlinier tersebut. Metode ini bekerja pada lapangan hingga $GF\left(2^m\right)$ atau dengan kata lain *plaintext* dan *ciphertext* dalam metode ini berupa elemen dari lapangan hingga $GF\left(2^m\right)$.

1.2 PERUMUSAN MASALAH

Masalah yang dibahas pada tugas akhir ini adalah:

Bagaimana sistem kerja metode Imai-Matsumoto pada lapangan hingga $GF\left(2^m\right)$?

1.3 TUJUAN PENULISAN

Tujuan penulisan tugas akhir ini adalah:

Menjelaskan sistem kerja metode Imai-Matsumoto pada lapangan hingga $GF\left(2^m\right)$.

1.4 METODE PENELITIAN

Metode penelitian yang digunakan dalam proses pembuatan tugas akhir ini adalah studi literatur, yaitu dengan cara mempelajari buku-buku referensi yang berhubungan dengan topik tugas akhir serta mengambil referensi lainnya melalui internet.

1.5 SISTEMATIKA PENULISAN

Penulisan tugas akhir ini dibagi dalam empat bagian, yang dimulai dengan Bab I Pendahuluan, yang berisi tentang latar belakang, tujuan penulisan, perumusan masalah, metode penelitian dan sistematika penulisan.

Selanjutnya adalah Bab II Landasan Teori, yang berisi pengertian-pengertian, teorema-teorema, serta sifat-sifat yang diperlukan pada pembahasan tentang metode Imai-Matsumoto.

Pada Bab III akan dibahas tentang cara kerja metode Imai-Matsumoto beserta contohnya. Terakhir Bab IV Penutup berisi kesimpulan yang dapat ditarik oleh penulis dari keseluruhan isi tugas akhir dan saran dari penulis tentang tugas akhir ini.

BAB II
LANDASAN TEORI

Pada bab ini akan dibahas pengertian lapangan, ruang vektor atas suatu lapangan, serta sifat-sifat yang diperlukan pada pembahasan bab selanjutnya.

Untuk memberikan pengertian lapangan dan ruang vektor atas suatu lapangan terlebih dahulu akan diberikan definisi suatu sistem matematika.

Definisi 2.1

Misalkan S suatu himpunan tak kosong dan terdapat operasi $*$ pada S, yaitu pemetaan

$$*: S \times S \to S$$

maka $(S,*)$ disebut sistem matematika.

Suatu sistem matematika juga dapat didefinisikan oleh dua operasi + dan $*$, ditulis $(S,+,*)$.

(Achmad Arifin, 2001)

Selanjutnya akan diberikan pengertian grup serta sifat-sifat dalam suatu grup.

Definisi 2.2

Suatu sistem matematika $(G,*)$ disebut grup jika :

1. $a,b \in G$ maka $a*b \in G$
2. memenuhi sifat assosiatif, yaitu untuk setiap $a,b,c \in G$ berlaku
   $a*(b*c) = (a*b)*c$
3. terdapat elemen identitas $e \in G$ sedemikian sehingga $a*e = e*a = a$ untuk setiap $a \in G$
4. untuk setiap $a \in G$ terdapat invers $a^{-1} \in G$ sedemikian sehingga
   $a*a^{-1} = a^{-1}*a = e$

(I.N. Herstein, 1996)

Definisi 2.3

Suatu grup G disebut grup abelian atau grup komutatif jika $a*b=b*a$ untuk setiap $a,b\in G$.

(I.N. Herstein, 1996)

Definisi 2.4

Suatu grup G disebut grup siklik jika terdapat elemen $g\in G$ sedemikian sehingga $G=\left\{g^n \mid n\in\mathbb{Z}\right\}$. Elemen g disebut generator dari G.

(Bhattacharya, Jain, Nagpaul, 1994)

Berikut ini diberikan penamaan suatu grup berdasarkan jumlah elemen yang ada pada grup tersebut.

Definisi 2.5

Suatu grup G dikatakan grup hingga jika banyaknya elemen G berhingga. Banyaknya elemen di G disebut order dari G dan dinotasikan dengan |G|.

(I.N. Herstein, 1996)

Berikut ini diberikan definisi order elemen dari suatu grup.

Definisi 2.6

Misal G adalah grup hingga, order dari $a\in G$, dilambangkan $o(a)$, adalah bilangan bulat terkecil m sedemikian sehingga $a^m=e$, dimana e adalah elemen identitas terhadap operasi di G.

(I.N. Herstein, 1996)

Teorema berikut menunjukkan hubungan antara order suatu grup dengan order elemen suatu grup.

Teorema 2.7

Jika G grup hingga dan $a \in G$, maka $o(a) \mid |G|$.

(I.N. Herstein, 1996)

Teorema 2.8

Jika G grup hingga berorder n, maka $a^n = e$ untuk setiap $a \in G$

(I.N. Herstein, 1996).

Selanjutnya akan diberikan definisi pemetaan dari dua buah grup yang memiliki sifat khusus.

Definisi 2.9

Misal G dan G' adalah grup, maka pemetaan $\varphi : G \to G'$ dikatakan homomorfisma jika $\varphi(ab) = \varphi(a)\varphi(b)$ untuk setiap $a, b \in G$.

(I.N. Herstein, 1996).

Definisi 2.10

Jika φ adalah homomorfisma dari G ke G', maka kernel φ didefinisikan $\ker \varphi = \{a \in G \mid \varphi(a) = e'\}$

(I.N. Herstein, 1996).

Teorema 2.11

Jika φ adalah homomorfisma dari G ke G', maka φ satu-satu jika dan hanya jika $\ker \varphi = (e)$.

(I.N. Herstein, 1996).

Suatu grup adalah sistem matematika dengan satu buah operasi. Berikut ini akan diberikan pengertian tentang lapangan, yaitu suatu sistem matematika dengan dua buah operasi didalamnya.

Definisi 2.12

Suatu sistem matematika $(F,+,*)$ disebut lapangan jika :

1. $(F,+)$ merupakan grup komutarif
2. $(F-\{0\},*)$ merupakan grup komutatif
3. $(F,+,*)$ memenuhi sifat distributif, artinya $a*(b+c)=a*b+a*c$ untuk setiap $a,b,c \in F$.

(Achmad Arifin, 2001)

Berdasarkan jumlah elemennya, lapangan dapat dibedakan menjadi dua, yaitu lapangan hingga dan lapangan tak hingga.

Suatu lapangan $(F,+,*)$ disebut lapangan hingga jika banyak elemen di F berhingga, yang biasa disebut dengan *Galois Field*. *Galois Field* dengan q elemen biasa ditulis $GF(q)$. Jika suatu lapangan memiliki jumlah elemen tak berhingga maka lapangan tersebut disebut lapangan tak hingga.
(Bhattacharya, Jain, Nagpaul, 1994)

Himpunan bilangan riil $\mathbb{R}$ beserta operasi penjumlahan dan perkalian yang umum padanya, dinotasikan dengan $(\mathbb{R},+,\times)$ merupakan contoh lapangan tak hingga. Sedangkan untuk memberikan contoh suatu lapangan hingga, terlebih dahulu akan diberikan definisi tentang kelas modulo.

Definisi 2.13

Himpunan semua bilangan bulat yang menghasilkan sisa a jika dibagi dengan $n \in \mathbb{Z}$ disebut kelas a modulo n, dinotasikan $[a]_n$.

Dengan kata lain, $[a]_n = \{a+nk \mid k \in \mathbb{Z}\}$.

(Alexander Bogomolny, 1996)

Sekarang pandang $\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{Z}\}$, himpunan bilangan bulat modulo n, $n \in$ dengan dua operasi didefinisikan padanya, yaitu:

Operasi tambah $+ : [a]_n + [b]_n = [a+b]_n$

Operasi kali $* : [a]_n * [b]_n = [a*b]_n$

Berdasarkan pengertian di atas maka diperoleh:

1. $(\mathbb{Z}_n, +)$ merupakan grup komutatif.
2. $(\mathbb{Z}_n, +, *)$ memenuhi sifat distributif, karena
   $[a]_n * ([b]_n + [c]_n) = [a]_n * [b]_n + [a]_n * [c]_n$ untuk setiap $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$
3. $(\mathbb{Z}_n, *)$ memenuhi sifat assosiatif dan komutatif.
4. $(\mathbb{Z}_n, *)$ mempunyai elemen identitas yaitu $[1]_n$.

Untuk sembarang n belum tentu untuk setiap elemen $\mathbb{Z}_n$ yang tidak sama dengan $[0]_n$ mempunyai invers. Contoh pada $\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$ terdapat elemen yang tidak sama dengan $[0]_n$ yang tidak punya invers yaitu $[2]_4$.

Jika $n = p$, dimana p adalah bilangan prima, maka $\mathbb{Z}_p$ merupakan suatu lapangan. Untuk menunjukkan kebenarannya, akan digunakan teorema berikut.

Teorema 2.14 (Teorema Fermat)

Jika p adalah bilangan prima dan $p \nmid a$, maka $a^{p-1} \equiv 1 \bmod p$.

Untuk suatu bilangan bulat b, jika $p \mid b$ maka $b^p \equiv b \bmod p$.

(I.N. Herstein, 1996)

Perhatikan jika $[a]_p \neq [0]_p \in \mathbb{Z}_p$ berarti $p \nmid a$, dengan demikian berdasarkan Teorema Fermat

$a^{p-1} \equiv 1 \bmod p$

Dari definisi kelas [.] didapat

$[a^{p-1}]_p = [1]_p$

Karena

$$[a^{p-1}]_p = [a]_p^{p-1}$$

Maka

$$[a]_p^{p-1} = [1]_p$$

Sehingga

$$[a]_p^{p-2} * [a]_p = [1]_p$$

Yang berarti bahwa untuk setiap $[a]_p \neq [0]_p \in \mathbb{Z}_p$ memiliki invers, yaitu $[a]_p^{p-2}$.

Berdasarkan empat hal di atas dan terdapatnya invers untuk setiap elemen di $\left(\mathbb{Z}_p - [0]_p, *\right)$, maka $\left(\mathbb{Z}_p, +, *\right)$ merupakan suatu lapangan.

Karena $\mathbb{Z}_p = \left\{[0]_p, [1]_p, ..., [p-1]_p\right\}$, merupakan suatu himpunan dengan banyaknya elemen adalah p, maka $\left(\mathbb{Z}_p, +, *\right)$ merupakan contoh untuk suatu lapangan hingga.

Berikut ini akan diberikan pengertian mengenai karakteristik suatu lapangan.

Definisi 2.15

Suatu lapangan F dikatakan mempunyai karakteristik $p \neq 0$ jika untuk setiap $a \in F$ terdapat bilangan bulat positif p sedemikian sehingga $pa = 0$, dan tidak ada bilangan bulat positif lain yang lebih kecil dari p memenuhi sifat tersebut.
(I.N. Herstein, 1996)

Jika suatu lapangan tidak mempunyai karakteristik $p \neq 0$ untuk suatu bilangan bulat positif p, maka lapangan tersebut dikatakan mempunyai karakteristik 0.

Berikut diberikan contoh lapangan dan karakteristik dari masing-masing lapangan tersebut.

1. Lapangan $\mathbb{Q}$, $\mathbb{R}$, dan $\mathbb{C}$ adalah lapangan dengan karakteristik 0, karena tidak ada bilangan bulat positif p yang memenuhi $pa = 0$ untuk setiap elemen dalam lapangan $\mathbb{Q}$, $\mathbb{R}$, dan $\mathbb{C}$ tersebut.
2. Lapangan $\mathbb{Z}_p$ adalah lapangan dengan karakteristik p, karena

   $p[a]_p = \underbrace{[a]_p + [a]_p + ... + [a]_p}_{p} = [0]_p$ untuk setiap $[a]_p \in \mathbb{Z}_p$, dimana

   $[0]_p$ adalah elemen identitas terhadap operasi penjumlahan di $\mathbb{Z}_p$.

Berkaitan dengan definisi di atas, diberikan teorema berikut.

Teorema 2.16

Karakteristik dari suatu lapangan adalah 0 atau suatu bilangan prima p
(I.N. Herstein, 1996)

Berikut akan diberikan pengertian sublapangan dari suatu lapangan.

Definisi 2.17

Himpunan bagian U dari suatu lapangan F disebut sublapangan dari F jika U adalah lapangan dengan operasi-operasi dalam F.
(Rudolf Lidl & Guntler Pilz, 1994)

Selanjutnya akan kita lihat hubungan suatu lapangan F dengan suatu himpunan lain, yaitu himpunan polinomial dalam x atas F yang dilambangkan $F[x]$. Berikut ini diberikan pengertian dari $F[x]$.

Definisi 2.18

Misal F lapangan, maka elemen dari himpunan $F[x]$ adalah polinomial $f(x) = a_0 + a_1 x + ... + a_n x^n$ dimana $a_i \in F$, $i = 0,1,...,n$.
(I.N. Herstein, 1996)

Definisi 2.19

Polinomial $f(x) \in F[x]$ disebut polinomial monik jika koefisien dari pangkat tertingginya adalah 1. atau dengan kata lain

$f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, dimana $n \geq 1$.

(I.N. Herstein, 1996)

Definisi 2.20

Misal $f(x) \in F[x]$. Jika $f(x) = a_0 + a_1 x + ... + a_n x^n$ dan $a_n \neq 0$, maka derajat dari $f(x)$, dinotasikan $\deg f(x)$, adalah n.

(I. N. Herstein, 1996)

Dalam $F[x]$ terdapat operasi pembagian. Berikut diberikan suatu teorema dan definisi yang berkaitan dengan operasi pembagian dalam $F[x]$.

Teorema 2.21 (Divisor Algorithm)

Untuk setiap $f(x), g(x) \in F[x]$ dengan $g(x) \neq 0$, terdapat $q(x), r(x) \in F[x]$ sedemikian sehingga:

$f(x) = q(x)g(x) + r(x)$; dimana $r(x) = 0$ atau $\deg r(x) < \deg g(x)$.

(I. N. Herstein, 1996)

Definisi 2.22

Misal $f(x), g(x) \in F[x]$ dengan $g(x) \neq 0$. $g(x)$ dikatakan membagi $f(x)$, ditulis $g(x) \mid f(x)$, jika $f(x) = a(x)g(x)$, untuk suatu $a(x) \in F[x]$.

(I. N. Herstein, 1996)

Polinomial dalam $F[x]$ yang mempunyai bentuk khusus adalah polinomial yang tak tereduksi. Pengertian tentang suatu polinomial yang tak tereduksi dalam $F[x]$ dimulai dengan pengertian tentang *greatest common divisor* dari suatu polinomial dalam $F[x]$ dan definisi relatif prima dalam $F[x]$.

Definisi 2.23

Misal $f(x), g(x) \in F[x]$ dimana tidak keduanya nol. Polinomial monik $d(x) \in F[x]$ disebut *greatest common divisor* dari $f(x)$ dan $g(x)$ jika:

(a) $d(x) \mid f(x)$ dan $d(x) \mid g(x)$.

(b) Jika $h(x) \mid f(x)$ dan $h(x) \mid g(x)$, maka $h(x) \mid d(x)$.

(I. N. Herstein, 1996)

Dari definisi 2.23, dapat dilihat hubungan antara dua polinomial dalam $F[x]$ sebagai berikut.

Definisi 2.24

Polinomial $f(x), g(x) \in F[x]$ dikatakan saling relatif prima jika *greatest common divisor* dari $f(x)$ dan $g(x)$ adalah 1.

(I. N. Herstein, 1996)

Berdasarkan definisi 2.23 dan 2.24 diperoleh definisi berikut.

Definisi 2.25

Polinomial $p(x) \in F[x]$ dengan $\deg p(x) \geq 1$ disebut tak tereduksi dalam $F[x]$ jika untuk sebarang $f(x) \in F[x]$ berlaku $p(x) \mid f(x)$ atau $p(x)$ dan $f(x)$ relatif prima.

(I. N. Herstein, 1996)

Selanjutnya diberikan pengertian suatu akar dari polinomial dalam $F[x]$.

Definisi 2.26

Suatu elemen a disebut akar dari suatu polinomial $f(x) \in F[x]$ jika $f(a) = 0$.

(I. N. Herstein, 1996)

Berikut ini akan dibahas tentang perluasan lapangan dari suatu lapangan yang dimulai dengan memberikan definisi perluasan lapangan sebagai berikut.

Definisi 2.27

Misal F dan K lapangan, maka K disebut perluasan lapangan dari F jika F adalah sublapangan dari K.

(I.N. Herstein, 1996)

Berikut akan diberikan definisi suatu ruang vektor atas suatu lapangan dan definisi-definisi lain yang berhubungan dengan ruang vektor.

Definisi 2.28

Misal V himpunan tak kosong dimana dua operasi didefinisikan padanya, yaitu operasi penjumlahan $+ : V \times V \to V$ dan operasi perkalian dengan skalar $* : F \times V \to V$. Maka sistem matematika $(V, +, *)$ disebut ruang vektor atas lapangan F jika:

1. $(V, +)$ adalah grup komutatif
2. untuk setiap $a \in F$ dan setiap $x \in V$ berlaku $ax \in V$
3. $a(x + y) = ax + ay$ untuk setiap $a \in F$ dan $x, y \in V$
4. $(a + b)x = ax + bx$ untuk setiap $a, b \in F$ dan $x \in V$
5. $a(bx) = (ab)x$ untuk setiap $a, b \in F$ dan $x \in V$
6. $1x = x$ untuk setiap $x \in V$, dimana $1 \neq 0$ adalah elemen satuan di F.

(I.N. Herstein, 1996)

Selanjutnya akan diberikan definisi tentang basis dari suatu ruang vektor V atas lapangan F yang dimulai dengan memberikan definisi tentang pembangun ruang vektor V atas lapangan F sebagai berikut.

Definisi 2.29

Subhimpunan $X = \{x_1, x_2, ..., x_n\} \subseteq V$ dikatakan membangun V jika setiap $y \in V$ merupakan kombinasi linier dari X.

Dengan kata lain, $y = a_1x_1 + a_2x_2 + ... + a_nx_n$ dimana $a_i \in F$.

(Achmad Arifin, 2001)

Berikut ini diberikan definisi bebas linier dari suatu himpunan.

Definisi 2.30

Subhimpunan $X = \{x_1, x_2, ..., x_n\} \subseteq V$ dikatakan bebas linier jika penulisan vektor nol sebagai kombinasi linier dari X bersifat tunggal.

Dengan kata lain, kombinasi linier $a_1x_1 + a_2x_2 + ... + a_nx_n = 0$ hanya dipenuhi oleh $a_i = 0 \in F$ untuk setiap $x_i \in X$.

(Achmad Arifin, 2001)

Berdasarkan definisi-definisi di atas, diberikan definisi basis dari suatu ruang vektor V atas lapangan F sebagai berikut.

Definisi 2.31

Subhimpunan $X = \{x_1, x_2, ..., x_n\} \subseteq V$ disebut basis ruang vektor V jika X membangun V dan bebas linier di V.

(Achmad Arifin, 2001)

Berkaitan dengan definisi basis dari suatu ruang vektor V atas lapangan F diperoleh definisi dimensi dari suatu ruang vektor V atas lapangan F sebagai berikut.

Definisi 2.32

Banyaknya elemen dalam suatu basis dari ruang vektor V disebut dimensi ruang vektor V atas lapangan F.

(Achmad Arifin, 2001)

Suatu ruang vektor V atas lapangan F disebut ruang vektor berdimensi hingga jika banyaknya elemen dalam suatu basisnya berhingga.

Berikut ini akan diberikan pengertian suatu pemetaan dari dua ruang vektor yang memiliki sifat khusus.

Definisi 2.33

Misal V dan W adalah ruang vektor atas suatu lapangan yang sama yaitu F. Transformasi linier dari V ke W adalah suatu fungsi $T:V \to W$ yang memenuhi:

1. jika $u,v \in V$, maka $T(u+v)=T(u)+T(v)$
2. jika $v \in V$ dan $k \in F$, maka $T(kv)=kT(v)$.

(Bill Jacob, 1990)

Selanjutnya akan diberikan teorema yang menunjukkan hubungan antara suatu perluasan lapangan K dari F dengan suatu ruang vektor atas suatu lapangan F.

Teorema 2.34

Jika K adalah perluasan lapangan dari F, maka K merupakan suatu ruang vektor atas lapangan F.

(I.N. Herstein, 1996)

Bukti:

Untuk membuktikan bahwa K adalah ruang vektor atas F, maka K harus memenuhi sifat-sifat ruang vektor atas suatu lapangan seperti pada definisi 2.28.

Karena K adalah lapangan, maka $(K,+,*)$ merupakan suatu sistem matematika dengan operasi penjumlahan dan perkalian dalam K dan $(K,+)$ adalah grup komutatif.

Karena $K \supset F$, maka untuk setiap $\alpha,\beta \in F$, berlaku $\alpha,\beta \in K$. Sehingga untuk setiap skalar $\alpha,\beta \in F$ dan vektor $a,b \in K$ maka syarat kedua sampai keenam

dari definisi 2.28 akan langsung terpenuhi. Sehingga terbukti bahwa K merupakan ruang vektor atas F.

Dengan memandang K sebagai ruang vektor atas F, maka dikenal juga dimensi dari ruang vektor K atas F. Berkaitan dengan pengertian dimensi ruang vektor K dan K sebagai perluasan lapangan dari F, maka diberikan definisi berikut.

Definisi 2.35

Dimensi dari K sebagai ruang vektor atas F disebut derajat dari perluasan lapangan K atas F, dinotasikan $[K:F]$.

(I.N. Herstein, 1996)

Selanjutnya akan dijelaskan secara ringkas bagaimana cara membentuk suatu perluasan lapangan dari suatu lapangan hingga $\mathbb{F}$ yang diberikan. Langkah-langkah yang harus dilakukan adalah:

1. Cari suatu polinomial monik $p(x)$ berderajat n yang tak tereduksi dalam $\mathbb{F}[x]$
2. Temukan akar α dari $p(x)$ dengan $\alpha \notin \mathbb{F}$
3. Bentuk $\mathbb{F}(\alpha)$, yaitu himpunan yang memuat semua kombinasi linier dari α^k, $k = 1, 2, ..., n-1$ dan elemen-elemen di $\mathbb{F}$.

Maka $\mathbb{F}(\alpha)$ inilah yang menjadi perluasan lapangan dari $\mathbb{F}$.

Berikut akan diberikan contoh perluasan lapangan yang dibentuk dari $\mathbb{Z}_2$.

1. Misal kita pilih polinomial monik $p(x)$ berderajat 3 yang tak tereduksi dalam $\mathbb{Z}_2[x]$ adalah $p(x) = x^3 + x + 1$.
2. misal $\alpha \notin \mathbb{Z}_2$ adalah akar dari $p(x)$.
3. maka diperoleh $\square_2(\alpha) = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$ dimana banyak elemen di $\square_2(\alpha)$ adalah $2^3 = 8$.

Jadi $\mathbb{Z}_2(\alpha)$ adalah perluasan lapangan dari $\mathbb{Z}_2$.

Akar α merupakan generator dari $\mathbb{Z}_2(\alpha)$ karena memenuhi kondisi berikut.

- $\alpha^1 = \alpha$
- $\alpha^2 = \alpha^2$
- $\alpha^3 = -\alpha - 1 = \alpha + 1$
- $\alpha^4 = \alpha^2 + \alpha$ (2.1)
- $\alpha^5 = \alpha^3 + \alpha^2 = (\alpha + 1) + \alpha^2 = \alpha^2 + \alpha + 1$
- $\alpha^6 = \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1$
- $\alpha^7 = \alpha^3 + \alpha = (\alpha + 1) + \alpha = 1$

Berikut ini diberikan tabel penjumlahan dan perkalian dalam $\mathbb{Z}_2(\alpha)$ dengan $p(x) = x^3 + x + 1$. Operasi penjumlahan adalah operasi penjumlahan biasa dalam $\mathbb{Z}_2[x]$.

Tabel 2.1. Penjumlahan dalam $\mathbb{Z}_2(\alpha)$

	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

Operasi perkalian dalam $\mathbb{Z}_2(\alpha)$ adalah operasi perkalian modulo $p(x) = x^3 + x + 1$, yaitu operasi perkalian antar dua buah elemen dalam $\mathbb{Z}_2(\alpha)$ yang hasilnya merupakan sisa pembagian dengan $x^3 + x + 1$. Sebagai contoh, misal $x + 1$ dikalikan dengan $x^2 + 1$, maka diperoleh

$(x+1)(x^2+1)=x^3+x^2+x+1$, lalu kita bagi dengan x^3+x+1. Dengan operasi pembagian biasa dalam $\mathbb{Z}_2[x]$ akan didapat sisa x^2. Sehingga $(x+1)(x^2+1)=x^2$.

Cara lainnya adalah dengan menggunakan persamaan (2.1). Misal kita gunakan contoh yang sama pada cara sebelumnya, yaitu
$(x+1)(x^2+1)=x^3+x^2+x+1$. Karena $x^3=x+1$, maka
$x^3+x^2+x+1=(x+1)+x^2+x+1=x^2+2x+2$. Dalam $\mathbb{Z}_2$ $x^2+2x+2=x^2$.
Sehingga diperoleh $(x+1)(x^2+1)=x^2$.

Tabel 2.2. Perkalian dalam $\mathbb{Z}_2(\alpha)$.

	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

Dari tabel terlihat bahwa $\{\mathbb{Z}_2(\alpha)-\{0\}\}$ merupakan grup terhadap perkalian modulo $p(x)=x^3+x+1$. Dengan elemen identitas adalah 1.

Misal $GF(q)$ adalah perluasan lapangan yang dibentuk berdasarkan akar dari polinomial berderajat n yang tak tereduksi di $\mathbb{Z}_p[x]$. Berdasarkan cara pembentukan perluasan lapangan, didapat bahwa
$GF(q)=\{a_0+a_1x+...+a_{n-1}x^{n-1} \mid a_i \in \mathbb{Z}_p\}$, dimana x adalah akar dari polinomial $p(x)$. Sehingga $X=\{1,x,x^2,...,x^{n-1}\} \subseteq GF(q)$ dapat dipilih sebagai basis dari ruang vektor $GF(q)$ atas $\mathbb{Z}_p$. Dengan mengambil basis tersebut, maka elemen-

elemen dalam $GF(q)$ dapat dinyatakan sebagai kombinasi linier dari vektor basis X. Sebagai contoh untuk $y \in GF(q)$ maka $y = a_0 + a_1 x + ... + a_{n-1} x^{n-1}$, $a_i \in \mathbb{Z}_p$, atau y dapat ditulis sebagai n-tuple elemen-elemen dalam $\mathbb{Z}_p$ yaitu $[y]_X = (a_0, a_1, ..., a_{n-1})$. Dengan demikian didapat korespondensi satu-satu antara elemen-elemen dalam $GF(q)$ dan himpunan semua n-tuple elemen-elemen dalam $\mathbb{Z}_p$. Sehingga diperoleh bahwa banyak elemen dalam suatu perluasan lapangan dari $\mathbb{Z}_p$ yang dibentuk berdasarkan akar dari polinomial $p(x)$ berderajat n adalah $q = p^n$.

Selanjutnya akan diberikan sifat-sifat yang berlaku pada suatu perluasan lapangan berderajat hingga.

Teorema 2.36

Jika $GF(q)$ adalah suatu lapangan dengan $q = p^n$ elemen, maka berlaku $u^q - u = 0$, untuk setiap $u \in GF(q)$.

(Neil Koblitz,1997)

Bukti:

Jika $u = 0$ maka jelas berlaku $0^n - 0 = 0$. Misal $K^* = \{GF(q) - \{0\}\}$, berdasarkan definisi lapangan, K^* adalah grup terhadap operasi perkalian di $GF(q)$, dan order K^* adalah $q-1$. Berdasarkan teorema 2.8 maka berlaku $u^{q-1} = 1$, untuk setiap $u \in K^*$, dimana 1 adalah elemen satuan di K^*, atau dengan kata lain berlaku $u^q - u = 0$ untuk setiap $u \in K^*$.

Lemma 2.37

Jika F adalah suatu lapangan berkarakteristik p, maka berlaku $(a+b)^p = a^p + b^p$ untuk setiap $a, b \in F$.

(Neil Koblitz,1997)

Bukti:

Perhatikan ekspansi binomial

$$(a+b)^p = \sum_{j=0}^{p} \binom{p}{j} a^{p-j} b^j = a^p + \frac{p!}{(p-1)!} a^{p-1} b + \frac{p!}{2!(p-2)!} a^{p-2} b^2 + \ldots + b^p$$

Untuk $0 < j < p$, $\binom{p}{j} = \frac{p!}{j!(p-j)!}$ selalu dapat dibagi dengan p, sehingga untuk $0 < j < p$ nilai suku-suku akan sama dengan 0. Maka didapat $(a+b)^p = a^p + b^p$.

Berdasarkan pengembangan lemma di atas didapat $(a+b)^{p^n} = a^{p^n} + b^{p^n}$, karena untuk $0 < j < p^n$, $\binom{p^n}{j} = \frac{p^n!}{j!(p^n - j)!}$ selalu dapat dibagi dengan p.

Lemma 2.38

Jika $GF(q)$ adalah suatu lapangan dengan $q = p^n$ elemen, maka pemetaan $T : GF(q) \to GF(q)$ yang didefinisikan $T : u \mapsto u^h$ akan bersifat satu-satu jika $\gcd(h, p^n - 1) = 1$.

Bukti:

Misal $K^* = \{GF(q) - \{0\}\}$, berdasarkan definisi lapangan, K^* adalah grup terhadap operasi perkalian di $GF(q)$, dan order K^* adalah $p^n - 1$.

Pandang pemetaan

$T : K^* \to K^*$

$T(u) = u^h$, dengan $g.c.d.(h, p^n - 1) = 1$

Ambil sebarang $u, v \in K^*$

$T(uv) = (uv)^h = u^h v^h = T(u)T(v)$

$\therefore T$ homomorfisma

Jika $g.c.d.(h, p^n - 1) = 1$, berarti h tidak membagi $p^n - 1$, maka tidak terdapat elemen di K^* dengan order h, atau dengan kata lain $\forall u \neq e \in K^*$ tidak berlaku

$u^h = e$, dimana e adalah elemen satuan di $K*$ terhadap operasi perkalian. Satu-satunya elemen $K*$ yang memenuhi $u^h = e$ adalah e

$\therefore \ker T = \{e\}$

Karena T homomorfisma dan ker $T = \{e\}$, maka berdasarkan teorema 2.11 T satu-satu.

Lemma 2.39

Jika $GF(q)$ adalah suatu lapangan dengan $q = p^r$ dan K adalah perluasan lapangan berderajat n dari $GF(q)$ atau $K = GF\left(q^n\right)$, maka pemetaan $T : K \to K$ yang didefinisikan $T : u \mapsto u^{q^k}$ untuk $1 \le k \le n$, adalah suatu transformasi linier.

Bukti:

Pandang pemetaan

$T : K \to K$

$T\left(u\right) = u^{q^k}$

1. Ambil sebarang $u, v \in K$

   Berdasarkan pengembangan lemma 2.37 didapat $\left(u+v\right)^{q^k} = u^{q^k} + v^{q^k}$ sehingga

   $T\left(u+v\right) = \left(u+v\right)^{q^k} = u^{q^k} + v^{q^k} = T\left(u\right) + T\left(v\right)$

2. Ambil sebarang $u \in K$ dan $a \in GF\left(q\right)$. Akan ditunjukkan $T(au) = aT(u)$.

   $T(au) = \left(au\right)^{q^k}$

   $= a^{q^k} u^{q^k}$

   Sesuai dengan teorema 2.36 untuk setiap $a \in GF\left(q\right)$ berlaku $a^q = a$.

   $a^{q^k} = \left(a^q\right)^{\underbrace{q.q...q}_{k-1}} = a$, maka

   $T(au) = \left(au\right)^{q^k} = a^{q^k} u^{q^k} = au^{q^k} = aT(v)$.

Karena pemetaan T memenuhi dua hal di atas maka terbukti bahwa T transformasi linier.

BAB III
METODE IMAI-MATSUMOTO
PADA LAPANGAN HINGGA GF(2^m)

Pada bab ini akan dibahas sistem kerja metode Imai-Matsumoto yang bekerja pada lapangan hingga $GF(2^m)$. Sebelumnya akan dijelaskan terlebih dahulu metode Imai-Matsumoto secara umum.

3.1 METODE IMAI-MATSUMOTO

Metode Imai-Matsumoto adalah salah satu metode asimetris dalam kriptografi yang pertama kali ditemukan oleh Imai dan Matsumoto pada tahun 1989. Metode ini menggunakan dua kunci yang berbeda, yaitu kunci umum yang digunakan untuk enkripsi dan kunci pribadi yang digunakan untuk dekripsi. Kunci pribadi pada metode ini adalah dua buah matriks, dua buah vektor, dan satu parameter yang memiliki sifat dan aturan tertentu yang dipilih oleh si pengguna metode. Selanjutnya dari kunci pribadi tersebut dibentuk kunci umum yang berbentuk himpunan persamaan polinomial nonlinier. Kunci umum pada metode ini akan diberikan kepada orang-orang yang ingin mengirimkan pesan rahasia kepada si pengguna metode, sedangkan kunci pribadi hanya diketahui oleh si pembuat kunci yaitu si pengguna metode itu sendiri.

Jika Alice akan menggunakan metode Imai-Matsumoto, maka setiap orang yang akan mengirim pesan ke Alice akan mengenkripsi pesan tersebut menjadi *ciphertext* dengan menggunakan kunci umum yang telah diberikan oleh Alice. Setelah Alice menerima *ciphertext* tersebut, ia akan mendekripsi *ciphertext* menggunakan kunci pribadi yang hanya diketahui oleh Alice. Dengan demikian hanya Alice yang dapat membaca *ciphertext* tersebut.

Untuk metode Imai-Matsumoto yang bekerja pada lapangan hingga $GF\left(2^m\right)$, maka *plaintext* dan *ciphertext* pada metode ini adalah anggota dari lapangan hingga $GF\left(2^m\right)$. Sebelum membahas Metode Imai-Matsumoto yang bekerja pada lapangan hingga $GF\left(2^m\right)$, berikut ini akan dijelaskan terlebih dahulu pengertian-pengertian pada lapangan hingga $GF\left(2^m\right)$ yang akan digunakan pada metode Imai-Matsumoto.

3.2 LAPANGAN HINGGA GF(2^m)

Berdasarkan lapangan hingga $\mathbb{Z}_2$ dapat dibentuk perluasan lapangan hingga dengan banyaknya elemen 2^r dengan cara seperti dijelaskan pada bab II. Lapangan hingga dengan jumlah elemen 2^r biasa dinotasikan $GF\left(2^r\right)$ atau $GF\left(q\right)$ dengan $q = 2^r$.

Berdasarkan lapangan $GF\left(q\right)$ dapat dibentuk lagi perluasan lapangan hingga dengan jumlah elemen q^n atau $\left(2^r\right)^n$. Lapangan hingga dengan jumlah elemen $\left(2^r\right)^n$ biasa dinotasikan $GF\left(2^{rn}\right)$ atau $GF\left(2^m\right)$ dengan $m = rn$.

Operasi penjumlahan dalam $GF\left(2^m\right)$ adalah operasi penjumlahan biasa dalam $GF\left(2^m\right)$. Sedangkan operasi perkalian dalam $GF\left(2^m\right)$ adalah operasi perkalian modulo $p(x)$, dimana $p(x)$ adalah polinomial monik berderajat n yang tak tereduksi dalam $GF\left(q\right)$ yang dipilih saat membentuk $GF\left(2^m\right)$.

Karena $GF\left(2^m\right)$ adalah perluasan lapangan dari $GF\left(q\right)$ dengan jumlah elemen q^n maka $GF\left(2^m\right)$ dapat kita pandang sebagai ruang vektor berdimensi n atas $GF\left(q\right)$. Karena $GF\left(2^m\right)$ adalah ruang vektor atas $GF\left(q\right)$ berdimensi n maka $GF\left(2^m\right)$ mempunyai basis, misal $\beta = \{\beta_1, \beta_2, ..., \beta_n\} \subseteq GF\left(2^m\right)$, adalah basis dari $GF\left(2^m\right)$, $\beta_i \in GF\left(2^m\right)$ adalah vektor basis dari $GF\left(2^m\right)$.

Dengan mengambil basis tersebut, maka untuk setiap $\mathbf{u} \in GF\left(2^m\right)$ dapat ditulis sebagi kombinasi linier dari $\beta = \{\beta_1, \beta_2, ..., \beta_n\}$, yaitu

$\mathbf{u} = u_1\beta_1 + ... + u_n\beta_n \in GF\left(2^m\right)$, $u_i \in GF(q)$.

Untuk setiap $\mathbf{u} \in GF\left(2^m\right)$ dimana $\mathbf{u} = u_1\beta_1 + ... + u_n\beta_n \in GF\left(2^m\right)$, $\mathbf{u}$ juga dapat dinyatakan sebagai n-tuple elemen-elemen dalam $GF(q)$ yaitu $[\mathbf{u}]_\beta = (u_1, u_2, ..., u_n)$, atau dengan kata lain $[\mathbf{u}]_\beta$ adalah penulisan lain dari $\mathbf{u}$. Untuk pembahasan selanjutnya $[\mathbf{u}]_\beta$ dinotasikan dengan $\bar{u}$.

Berikut ini akan dibahas metode Imai-Matsumoto yang bekerja pada perluasan lapangan hingga $GF\left(2^m\right)$.

3.3 METODE IMAI-MATSUMOTO PADA LAPANGAN HINGGA GF(2^m)

Misalkan Alice akan menerapkan metode Imai-Matsumoto pada $GF\left(2^m\right)$. Untuk menggunakan metode Imai-Matsumoto ini Alice harus menentukan terlebih dahulu lima parameter yang akan menjadi kunci pribadinya. Kelima parameter ini terdiri dari dua buah matriks invertible $n \times n$ yaitu $A = \{a_{ij}\}_{1 \le i, j \le n}$ dan $B = \{b_{ij}\}_{1 \le i, j \le n}$ dengan $a_{ij}, b_{ij} \in GF(q)$, dua vektor $\bar{c} = (c_1, ..., c_n) \in GF\left(2^m\right)$ dan $\bar{d} = (d_1, ..., d_n) \in GF\left(2^m\right)$ serta sebuah parameter h. Parameter h dipilih yang memenuhi $h = q^\theta + 1$, dengan $0 < h < q^n$ dan memenuhi kondisi $g.c.d.(h, q^n - 1) = 1$.

Kondisi $g.c.d.(h, q^n - 1) = 1$ diperlukan agar pemetaan $\mathbf{u} \mapsto \mathbf{u}^h$ di $GF\left(2^m\right)$ adalah pemetaan satu-satu sesuai dengan yang disyaratkan oleh lemma 2.38. Karena $GF\left(2^m\right)$ berdimensi hingga dan pemetaan $\mathbf{u} \mapsto \mathbf{u}^h$ satu-satu, maka pemetaan ini mempunyai invers yaitu pemetaan $\mathbf{u} \mapsto \mathbf{u}^{h'}$ dengan h' adalah invers perkalian dari h modulo $q^n - 1$.

Misalkan vektor $\bar{x} = (x_1, ..., x_n) \in GF\left(2^m\right)$ adalah notasi untuk *plaintext*, $\bar{y} = (y_1, ..., y_n) \in GF\left(2^m\right)$ notasi untuk *ciphertext*, dan $\beta = \{\beta_1, \beta_2, ..., \beta_n\} \subseteq GF\left(2^m\right)$ adalah basis dari ruang vektor $GF\left(2^m\right)$ atas $GF(q)$.

Setelah kunci pribadi $h, A, B, \bar{c}$, dan $\bar{d}$ dipilih, berikut akan digambarkan proses merubah *plaintext* $\bar{x} \in GF\left(2^m\right)$ menjadi *ciphertext* $\bar{y} \in GF\left(2^m\right)$.

$$\bar{x} = \left(x_1, ..., x_n\right)$$
$$\Downarrow$$
$$\bar{u}^t = A\bar{x}^t + \bar{c}^t$$
$$\Downarrow$$
$$\mathbf{u} = \sum u_i \beta_i \quad , \qquad \beta_i \text{ basis dari } GF\left(2^m\right)$$
$$\Downarrow$$
$$\mathbf{v} = \mathbf{u}^h$$
$$\Downarrow$$
$$\bar{y}^t = B^{-1}\left(\bar{v}^t - \bar{d}^t\right)$$

Proses di atas masih melibatkan $h, A, B, \bar{c}$, dan $\bar{d}$ untuk merubah *plaintext* $\bar{x} \in GF\left(2^m\right)$ menjadi *ciphertext* $\bar{y} \in GF\left(2^m\right)$, sedangkan $h, A, B, \bar{c}$, dan $\bar{d}$ akan digunakan Alice sebagai kunci pribadinya. Maka selanjutnya Alice akan membentuk kunci umum yang tidak mengandung $h, A, B, \bar{c}$, dan $\bar{d}$ untuk merubah *plaintext* $\bar{x} \in GF\left(2^m\right)$ menjadi *ciphertext* $\bar{y} \in GF\left(2^m\right)$. Berikut akan dijelaskan proses pembentukkan kunci umum tersebut.

Lemma 2.39 menjelaskan bahwa suatu pemetaan $T : GF\left(2^m\right) \to GF\left(2^m\right)$ dengan $T(\mathbf{u}) = \mathbf{u}^{q^k}$ untuk $1 \le k \le n$ merupakan transformasi linier.

Untuk setiap $\mathbf{u} \in GF\left(2^m\right)$ dapat dituliskan sebagai $\mathbf{u} = u_1\beta_1 + ... + u_n\beta_n$ dengan $u_i \in GF(q)$ dan $\beta_i \in GF\left(2^m\right)$, $i = 1, 2, ...n$. Karena T transformasi linier, maka $T(\mathbf{u}) = T\left(u_1\beta_1 + ... + u_n\beta_n\right)$ dapat ditulis

$T(\mathbf{u}) = u_1 T(\beta_1) + ... + u_n T(\beta_n)$. Karena $\beta_i \in GF(2^m)$ untuk $i = 1,2,...n$, maka $T(\beta_i) = \beta_i^{q^k}$, $\forall i = 1,2,...,n$. Sehingga didapat $\mathbf{u}^{q^k} = u_1(\beta_1)^{q^k} + ... + u_n(\beta_n)^{q^k}$.

Karena $\beta_i^{q^k}$, $i = 1,2,...n$ adalah juga anggota dari $GF(2^m)$, maka dapat ditulis berikut ini:

$$\begin{aligned}(\beta_1)^{q^k} &= p_{11}^{(k)}\beta_1 + p_{12}^{(k)}\beta_2 + ... + p_{1n}^{(k)}\beta_n \\ &\vdots \qquad\qquad p_{ij}^{(k)} \in GF(q) \\ (\beta_n)^{q^k} &= p_{n1}^{(k)}\beta_1 + p_{n2}^{(k)}\beta_2 + ... + p_{nn}^{(k)}\beta_n\end{aligned}$$

Sehingga matriks transformasi T relatif terhadap basis $\beta = \{\beta_1, \beta_2, ..., \beta_n\}$ adalah

$$\begin{aligned}[T]_\beta = P^{(k)} &= \begin{pmatrix} p_{11}^{(k)} & \cdots & p_{1n}^{(k)} \\ \vdots & \ddots & \vdots \\ p_{n1}^{(k)} & \cdots & p_{nn}^{(k)} \end{pmatrix} \\ &= \left\{ p_{ij}^{(k)} \right\}, \ i, j = 1,2,...,n\end{aligned}$$

Berikut akan dilihat hasil perkalian antara vektor di basis $\beta = \{\beta_1, \beta_2, ..., \beta_n\}$ dengan $\beta_i \in GF(2^m)$. Karena $GF(2^m)$ merupakan grup terhadap operasi perkalian di $GF(2^m)$, maka perkalian $\beta_i \beta_j$ juga merupakan anggota dari $GF(2^m)$ atau dapat ditulis

$$\beta_i \beta_j = \sum_{l=1}^{n} m_{ijl} \beta_l \ , \tag{3.1}$$

dengan $m_{ijl} \in GF(q)$ dan $i, j = 1,2,...,n$.

Pada proses perubahan *plaintext* menjadi *ciphertext* terdapat formula $\mathbf{v} = \mathbf{u}^h$ dengan $h = q^\theta + 1$, maka dapat ditulis

$$\mathbf{v} = \mathbf{u}^{q^\theta}\mathbf{u} \ , \qquad \mathbf{v}, \mathbf{u}, \mathbf{u}^{q^\theta} \in GF(2^m)$$

Atau

$$\begin{aligned}\sum_{1 \le l \le n} v_l \beta_l &= \left(\sum_{i=1}^{n} u_i \beta_i^{q^\theta} \right) \left(\sum_{j=1}^{n} u_j \beta_j \right) \\ &= \left(\sum_{1 \le i, \mu \le n} p_{i\mu}^{(\theta)} u_i \beta_\mu \right) \left(\sum_{j=1}^{n} u_j \beta_j \right)\end{aligned} \tag{3.2}$$

Pada persamaan (3.2) ini akan terdapat perkalian antar basis. Jika perkalian antar basis ini kita tulis seperti pada persamaan (3.1) maka persamaan (3.2) akan menjadi:

$$\sum_{1\le l\le n} v_l\beta_l = \sum_{1\le i,j,\mu,l\le n} p_{i\mu}^{(\theta)} m_{\mu jl} u_i u_j \beta_l$$

Sehingga untuk setiap $l = 1, 2, ..., n$ didapat

$$v_l = \sum_{1\le i,j,\mu\le n} p_{i\mu}^{(\theta)} m_{\mu jl} u_i u_j \tag{3.3}$$

dengan $m_{\mu jl}$ dan $p_{i\mu}^{(\theta)}$ dapat diketahui oleh Alice.

Karena

$$\bar{u}^t = A\bar{x}^t + \bar{c}^t, \qquad \text{dan} \qquad \bar{v}^t = B\bar{y}^t + \bar{d}^t$$

maka dapat ditulis

$$u_i = c_i + \sum_{\rho} a_{i\rho} x_\rho \text{ dan } v_l = d_l + \sum_{\sigma} b_{l\sigma} y_\sigma \tag{3.4}$$

Dengan mensubtitusikan (3.4) pada persamaan (3.3) dan mengumpulkan koefisien dari masing-masing perkalian $x_i x_j$ akan didapat n persamaan, yang masing-masing persamaan berbentuk polinomial berderajat maksimal 2 dalam $x_1, ..., x_n$ di ruas kanan dan berbentuk ekspresi linier dalam $y_1, ..., y_n$ di ruas kiri. Dengan menggunakan aljabar linier akan didapat n persamaan yang masing-masing y_i berbentuk polinomial berderajat maksimal 2 dalam $x_1, ..., x_n$ atau $y_i = GF(q)[x_1, x_2, ..., x_n]$.

Dengan demikian n persamaan inilah yang menjadi kunci umum dari metode ini. Jadi, jika Bob ingin mengirim pesan *plaintext* kepada Alice, ia akan mensubtitusikan x_i ke dalam persamaan ini untuk mendapatkan y_i.

Ketika Alice menerima pesan dari Bob berupa *ciphertext* y_i, maka ia akan menggunakan kunci pribadinya yaitu $A, B, \bar{c}, \bar{d}$, dan h untuk merubahnya menjadi *plaintext* x_i. Karena h' adalah invers perkalian dari h modulo $q^n - 1$ maka pemetaan $\mathbf{u} \mapsto \mathbf{u}^{h'}$ akan membalik pemetaan $\mathbf{u} \mapsto \mathbf{u}^h$.

Diagram berikut menunjukkan proses dekripsi dari y_i menjadi x_i

$$\bar{y} = (y_1, ..., y_n)$$
$$\Downarrow$$
$$\bar{v}^t = B\bar{y}^t + \bar{d}^t$$
$$\Downarrow$$
$$\mathbf{v} = \sum v_i \beta_i \quad , \qquad \beta_i \text{ basis dari } GF\left(2^m\right)$$
$$\Downarrow$$
$$\mathbf{u} = \mathbf{v}^{h'}$$
$$\Downarrow$$
$$\bar{x}^t = A^{-1}\left(\bar{u}^t - \bar{c}^t\right)$$

Berikut ini akan diberikan contoh sederhana untuk menggambarkan cara kerja metode Imai-Matsumoto.

3.4 CONTOH

Misal kita pilih $GF(q) = \mathbb{Z}_2$, maka $q = 2$. Dengan mengambil $p(x) = x^3 + x + 1$ sebagai polinomial monik berderajat 3 yang tak tereduksi dalam $\mathbb{Z}_2[x]$ maka dapat dibentuk $GF\left(2^3\right)$. Misal $\alpha \notin \mathbb{Z}_2$ adalah akar dari $p(x) = x^3 + x + 1$, maka elemen-elemen di $GF\left(2^3\right)$ adalah $GF\left(2^3\right) = \left\{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\right\}$, sehingga basis dari $GF\left(2^3\right)$ sebagai ruang vektor atas $\mathbb{Z}_2$ adalah $\left\{1, \alpha, \alpha^2\right\}$. Akar α merupakan generator dari $GF\left(2^3\right)$ karena memenuhi kondisi berikut.

$$\left.\begin{array}{l} \bullet\ \alpha^1 = \alpha \\ \bullet\ \alpha^2 = \alpha^2 \\ \bullet\ \alpha^3 = -\alpha - 1 = 1 + \alpha \\ \bullet\ \alpha^4 = \alpha + \alpha^2 \\ \bullet\ \alpha^5 = \alpha^2 + \alpha^3 = \alpha^2 + (1+\alpha) = 1 + \alpha + \alpha^2 \\ \bullet\ \alpha^6 = \alpha + \alpha^2 + \alpha^3 = 1 + \alpha^2 \\ \bullet\ \alpha^7 = \alpha + \alpha^3 = \alpha + (\alpha + 1) = 1 \end{array}\right\} \qquad (3.5)$$

Karena $GF\left(2^3\right)$ dibentuk dengan mengambil suatu polinomial monik berderajat 3, maka dipilih matriks A dan B yang berukuran 3×3. Entri-entri dari matriks A dan B adalah anggota dari $GF\left(q\right) = \mathbb{Z}_2$.

Misal dipilih:

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \qquad \bar{c} = \begin{pmatrix} 1 & 1 & 0 \end{pmatrix} \qquad \bar{d} = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}$$

Dipilih juga $h = q^{\theta} + 1$ yang memenuhi $g.c.d.(h, q^n - 1) = 1$. Dengan memilih $\theta = 2$ didapat $h = 2^2 + 1 = 5$ dan $h' = 3$.

Dengan memilih matriks A dan B seperti di atas maka didapat

$$A^{-1} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \qquad B^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Selanjutnya kita bentuk:

$$\bar{u}^t = A\bar{x}^t + \bar{c}^t = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x_1 + x_3 + 1 \\ x_2 + 1 \\ x_1 + x_2 \end{pmatrix}$$

Didapat $\begin{array}{l} u_1 = x_1 + x_3 + 1 \\ u_2 = x_2 + 1 \\ u_3 = x_1 + x_2 \end{array}$ sehingga $\mathbf{u} = u_1 + u_2\alpha + u_3\alpha^2 \in GF\left(2^3\right)$

$$\mathbf{v} = \mathbf{u}^5 = \mathbf{u}\mathbf{u}^4 = \left(u_1 + u_2\alpha + u_3\alpha^2\right)\left(u_1 + u_2\alpha + u_3\alpha^2\right)^4 \qquad (3.6)$$

Berdasarkan teorema 2.39 pemetaan $T : GF\left(2^3\right) \to GF\left(2^3\right)$ yang didefinisikan $T\left(\mathbf{u}\right) = \mathbf{u}^{2^k}$ untuk $1 \le k \le 3$ adalah transformasi linier, sehingga dapat ditulis $\mathbf{u}^4 = \left(u_1 + u_2\alpha + u_3\alpha^2\right)^4 = \left(u_1 + u_2\alpha^4 + u_3\alpha^8\right)$. Maka persamaan (3.6) dapat ditulis menjadi $\mathbf{v} = \left(u_1 + u_2\alpha + u_3\alpha^2\right)\left(u_1 + u_2\alpha^4 + u_3\alpha^8\right)$.

Dengan menggunakan persamaan (3.5) maka didapat

$$\begin{aligned}
\mathbf{v} &= \left(u_1 + u_2\alpha + u_3\alpha^2\right)\left(u_1 + u_2\left(\alpha + \alpha^2\right) + u_3\alpha\right) \\
&= \left(u_1 + u_2\alpha + u_3\alpha^2\right)\left(u_1 + \left(u_2 + u_3\right)\alpha + u_2\alpha^2\right) \\
&= u_1{}^2 + \left(u_1u_2 + u_1u_3 + u_1u_2\right)\alpha + \left(u_1u_2 + u_2{}^2 + u_2u_3 + u_1u_3\right)\alpha^2 \\
&\quad + \left(u_2{}^2 + u_2u_3 + u_3{}^2\right)\alpha^3 + \left(u_2u_3\right)\alpha^4 \\
&= u_1{}^2 + \left(u_1u_2 + u_1u_3 + u_1u_2\right)\alpha + \left(u_1u_2 + u_2{}^2 + u_2u_3 + u_1u_3\right)\alpha^2 \\
&\quad + \left(u_2{}^2 + u_2u_3 + u_3{}^2\right)\left(1 + \alpha\right) + \left(u_2u_3\right)\left(\alpha + \alpha^2\right) \\
&= \left(u_1{}^2 + u_2{}^2 + u_2u_3 + u_3{}^2\right) + \left(u_1u_3 + u_2{}^2 + u_3{}^2\right)\alpha + \left(u_1u_2 + u_2{}^2 + u_1u_3\right)\alpha^2
\end{aligned}$$

Karena $\left\{1, \alpha, \alpha^2\right\}$ merupakan basis dari $GF\left(2^3\right)$ maka $\mathbf{v} = \left(u_1{}^2 + u_2{}^2 + u_2u_3 + u_3{}^2\right) + \left(u_1u_3 + u_2{}^2 + u_3{}^2\right)\alpha + \left(u_1u_2 + u_2{}^2 + u_1u_3\right)\alpha^2$ dapat ditulis sebagai n-tuple dari elemen $GF\left(q\right) = \mathbb{Z}_2$, yaitu $\bar{v} = \left(v_1, v_2, v_3\right)$ dengan

$$
\begin{aligned}
v_1 &= u_1^{\,2} + u_2^{\,2} + u_2u_3 + u_3^{\,2} \\
&= \left(x_1 + x_3 + 1\right)^2 + \left(x_2 + 1\right)^2 + \left(x_2 + 1\right)\left(x_1 + x_2\right) + \left(x_1 + x_2\right)^2 \\
&= \left(x_1^{\,2} + x_3^{\,2} + 1\right) + \left(x_2^{\,2} + 1\right) + \left(x_1x_2 + x_2^{\,2} + x_1 + x_2\right) + \left(x_1^{\,2} + x_2^{\,2}\right) \\
&= 2x_1^{\,2} + x_3^{\,2} + 2 + 3x_2^{\,2} + x_1x_2 + x_1 + x_2 \\
&= x_3^{\,2} + x_2^{\,2} + x_1x_2 + x_1 + x_2 \\
v_2 &= u_1u_3 + u_2^{\,2} + u_3^{\,2} \\
&= \left(x_1 + x_3 + 1\right)\left(x_1 + x_2\right) + \left(x_2 + 1\right)^2 + \left(x_1 + x_2\right)^2 \\
&= \left(x_1^{\,2} + x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2\right) + \left(x_2^{\,2} + 1\right) + \left(x_1^{\,2} + x_2^{\,2}\right) \\
&= 2x_1^{\,2} + x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2 + 2x_2^{\,2} + 1 \\
&= x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2 + 1 \\
v_3 &= u_1u_2 + u_2^{\,2} + u_1u_3 \\
&= \left(x_1 + x_3 + 1\right)\left(x_2 + 1\right) + \left(x_2 + 1\right)^2 + \left(x_1 + x_3 + 1\right)\left(x_1 + x_2\right) \\
&= \left(x_1x_2 + x_1 + x_2x_3 + x_3 + x_2 + 1\right) + \left(x_2^{\,2} + 1\right) + \left(x_1^{\,2} + x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2\right) \\
&= 2x_1x_2 + 2x_1 + 2x_2x_3 + x_3 + 2x_2 + 2 + x_2^{\,2} + x_1^{\,2} + x_1x_3 \\
&= x_3 + x_2^{\,2} + x_1^{\,2} + x_1x_3
\end{aligned}
\qquad (3.7)
$$

Karena $\bar{y}^t = B^{-1}\left(\bar{v}^t - \bar{d}^t\right)$ maka

$$
\bar{v}^t = B\bar{y}^t + \bar{d}^t = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} y_1 + 1 \\ y_3 \\ y_1 + y_2 + 1 \end{pmatrix}
$$

Sehingga didapat:

$$
\begin{aligned}
v_1 &= y_1 + 1 \\
v_2 &= y_3 \\
v_3 &= y_1 + y_2 + 1
\end{aligned}
\qquad (3.8)
$$

Dengan mensubtitusikan (3.8) pada (3.7) maka akan didapat:

$$
\begin{aligned}
y_1 &= x_3^{\,2} + x_2^{\,2} + x_1x_2 + x_1 + x_2 + 1 \\
y_2 &= x_3 + x_1^{\,2} + x_1x_3 + x_3^{\,2} + x_1x_2 + x_1 + x_2 \\
y_3 &= x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2 + 1
\end{aligned}
\qquad (3.9)
$$

Sehingga tiga persamaan inilah yang menjadi kunci umum dari metode Imai-Matsumoto jika kita memilih kunci pribadinya yaitu:

$A=\begin{pmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 1 & 1 & 0\end{pmatrix}$, $B=\begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 1\\ 1 & 1 & 0\end{pmatrix}$, $\bar{c}=\begin{pmatrix}1 & 1 & 0\end{pmatrix}$, $\bar{d}=\begin{pmatrix}1 & 0 & 1\end{pmatrix}$, dan

$h=2^2+1=5$

Misalkan ada suatu *plaintext* $\bar{x}=(1,0,1)$, dengan mensubtitusikan ke persamaan (3.9) akan didapat *ciphertext* dari $\bar{x}=(1,0,1)$, yaitu:

$y_1=1^2+0^2+1.0+1+0+1=3=1$
$y_2=1+1^2+1.1+1^2+1.0+1+0=5=1$
$y_3=1.0+1.1+0.1+1+0+1=3=1$

Atau $\bar{y}=(1,1,1)$.

Untuk mengembalikan *ciphertext* $\bar{y}=(1,1,1)$ menjadi *plaintext*, digunakan cara sebagai berikut:

$$\bar{v}^t=B\bar{y}^t+\bar{d}^t=\begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 1\\ 1 & 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 1\\ 1\end{pmatrix}+\begin{pmatrix}1\\ 0\\ 1\end{pmatrix}=\begin{pmatrix}0\\ 1\\ 1\end{pmatrix}$$

Maka didapat:

$$\mathbf{v}=0+\alpha+\alpha^2$$

Kemudian bentuk $\mathbf{u}=\mathbf{v}^{h'}$, yaitu.

$$\begin{aligned}\mathbf{u}=\mathbf{v}^3&=\left(0+\alpha+\alpha^2\right)^2\left(0+\alpha+\alpha^2\right)\\ &=\left(0+\alpha^2+\alpha^4\right)\left(0+\alpha+\alpha^2\right)\\ &=\left(0+\alpha^2+\left(\alpha+\alpha^2\right)\right)\left(0+\alpha+\alpha^2\right)\\ &=\left(0+\alpha+0\right)\left(0+\alpha+\alpha^2\right)\\ &=\alpha^2+\alpha^3=\alpha^2+1+\alpha\\ &=1+\alpha+\alpha^2\end{aligned}$$

Maka didapat

$$\bar{u}=(1,1,1)$$

Selanjutnya langkah terakhir yaitu:

$$\bar{x}^t = A^{-1}\left(\bar{u}^t - \bar{c}^t\right) = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}\left[\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}\right]$$

$$= \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

Sehingga didapat *plaintext* $\bar{x} = (1,0,1)$.

BAB IV
PENUTUP

4.1 KESIMPULAN

Dalam tugas akhir ini telah dibahas sistem kerja metode Imai-Matsumoto yang bekerja pada lapangan hingga $GF\left(2^m\right)$, serta cara pembentukan kunci umum metode Imai-Matsumoto. Agar tingkat keamanan dari metode ini menjadi lebih tinggi, maka dipilih lapangan hingga $GF\left(2^r\right)^n$ dengan r, n bilangan bulat positif yang besar.

4.2 SARAN

Tingkat keamanan dari metode Imai-Matsumoto akan semakin tinggi dengan memilih lapangan hingga $GF\left(2^r\right)^n$ dengan r, n bilangan bulat positif yang besar. Semakin besar nilai r, n maka penghitungan dalam proses enkripsi dan dekripsi akan semakin sulit. Maka dari itu diharapkan dapat dibuat suatu program untuk melakukan penghitungan proses enkripsi dan dekripsi metode ini agar tugas akhir ini menjadi lebih bermanfaat.

DAFTAR PUSTAKA

Arifin, Achmad. (2001). *Aljabar Linier* (Ed. Ke-2). Bandung: Penerbit ITB Bandung.

Bhattacharya, P.B., S.K. Jain., & S.R. Nagpaul. (1994). *Basic Abstract Algebra* (2nd ed). Cambridge: Cambridge University Press.

Bogomolny, Alexander. (1996). *Modular Arithmetic*. April 22, 2010. http://www.cut-the-knot.org/blue/Modulo.shtml.

Herstein, I.N. (1996). *Abstract Algebra* (3rd ed). New Jersey: Prentice-Hall.

Jacob, Bill. (1990). *Linier Algebra*. New York: W.H. Freeman and Company.

Koblitz, Neil. (1997). *Algebraic Aspects of Cryptography* (vol. 3). Berlin: Springer-Verlag.

Lidl, R. & G. Pilz. (1994). *Applied Abstract Algebra* (2nd ed). Berlin: Springer-Verlag.

Stalling, William. (2005). *Cryptography and Network Security Principles and Practices* (4th ed). New Jersey: Prentice-Hall.