BAB I
PENDAHULUAN

1.1 Latar Belakang

Kriptografi telah dikenal sejak zaman dahulu. Salah satu contoh awal kriptografi adalah pada tahun 2000 SM, saat hieroglip "rahasia" non-standar digunakan di Mesir kuno dalam bahasa tulis.

Pada zaman modern, kriptografi berkembang pesat seiring dengan ditemukannya komputer yang dapat melakukan penghitungan dengan sangat cepat. Kriptografi digunakan untuk mengamankan paket-paket data penting, baik yang dikirim melalui saluran komunikasi yang tidak aman maupun media yang tersedia bagi umum.

Sejak pertama kali dikenalkan, kriptografi menggunakan kunci simetris di mana kedua pihak memiliki metode enkripsi dan dekripsi yang sama sekaligus berbagi kunci rahasia. Pada tahun 1976, Diffie dan Hellman mengenalkan jenis baru *cipher*. Metode ini dinamakan kriptografi kunci publik. Dalam metode ini, seorang pengguna memiliki kunci rahasia seperti pada kriptografi simetris, namun juga kunci publik.

Pada awalnya kriptografi kunci publik lebih banyak menggunakan teori bilangan ataupun algoritma diskrit dalam metodenya. Hal ini termasuk algoritma Diffie-Hellman (1976) atau algoritma RSA (1978). Beberapa usaha telah dilakukan untuk mengembangkan sistem kriptografi tanpa berdasarkan teori bilangan, seperti kriptografi kuantum oleh Bennet dan Brassard (1984), kriptografi *lattice* oleh Goldreich (1997), maupun sistem pertukaran kunci oleh Anshel-Anshel-Goldfeld (1999) menggunakan masalah pencarian konjugasi pada grup Braid. Shilprain dan Ushakov (2008) mengajukan penggunaan masalah pencarian *double twisted conjugacy* (DTC) dalam sistem autentikasinya. Mereka juga mengenalkan *platform* grup baru yaitu matriks 2×2 terhadap polinomial terhadap *field* dengan dua anggota.

Dalam skripsi ini akan dibahas penyusunan protokol autentikasi menggunakan masalah konjugasi *twisted* dan *platform* yang dikenalkan Shilprain dan Ushakov, sekaligus memperkenalkan sistem pertukaran kunci menggunakan masalah konjugasi *twisted* dan modifikasi dari sistem pertukaran kunci Ko (Ko, dkk., 2000).

1.2 Rumusan Masalah

Rumusan masalah skripsi ini adalah sebagai berikut.

1. Bagaimana protokol autentikasi menggunakan masalah pencarian *double twisted conjugacy*?
2. Bagaimana protokol pertukaran kunci menggunakan masalah pencarian *double twisted conjugacy*?
3. Bagaimana cara menggunakan matriks 2×2 terhadap polinomial terhadap *field* dengan dua elemen dalam protokol autentikasi dan pertukaran kunci?

1.3 Tujuan

Tujuan dari skripsi ini adalah sebagai berikut.

1. Menjelaskan cara menyusun protokol autentikasi menggunakan masalah pencarian *double twisted conjugacy*.
2. Menjelaskan cara menyusun protokol pertukaran kunci menggunakan masalah pencarian *double twisted conjugacy*.
3. Menjelaskan cara menggunakan matriks 2×2 terhadap polinomial terhadap *field* dengan dua elemen dalam protokol autentikasi dan pertukaran kunci.

BAB II
TINJAUAN PUSTAKA

2.1 Relasi, Pemetaan, dan Operasi

Dalam struktur aljabar, dua buah anggota atau lebih dari suatu himpunan dapat dipasangkan, baik dengan suatu aturan tertentu ataupun sembarang aturan. Berikut akan diberikan definisi dari relasi dan turunannya.

Definisi 2.1.1 (Hasil Ganda Cartesius)
Misalkan A dan B adalah himpunan tidak kosong. Himpunan semua pasangan terurut (a, b) dengan $a \in A$ dan $b \in B$ disebut hasil ganda Cartesius *(Cartesian product)* antara himpunan A dan B, yang dinotasikan sebagai berikut:

$$A \times B = \{(a, b) | a \in A, b \in B\}.$$

(Bhattacharya, 1994)

Definisi 2.1.2 (Relasi)
Misalkan A dan B adalah himpunan tidak kosong dan R adalah himpunan bagian dari $A \times B$, maka R disebut relasi dari A ke B. Jika $(x, y) \in R$, maka dikatakan x berelasi R dengan y, dapat dituliskan xRy.

(Bhattacharya, 1994)

Definisi 2.1.3 (Relasi Ekuivalensi)
Misalkan R merupakan relasi biner (relasi dari dua elemen) pada himpunan A. R dikatakan merupakan relasi ekuivalensi jika memenuhi:

1. Refleksif : $(a, a) \in R$ untuk semua $a \in A$.
2. Simetris : Jika $(a, b) \in R$ maka $(b, a) \in R$ untuk semua $a, b \in A$.
3. Transitif : Jika $(a, b) \in R$ dan $(b, c) \in R$ maka $(a, c) \in R$.

(Cameron, 2008)

Definisi 2.1.4 (Pemetaan)
Misalkan A dan B adalah himpunan tidak kosong. Pemetaan f dari A ke B adalah suatu relasi sedemikian sehingga untuk setiap $a \in A$ terdapat satu $b \in B$ dengan $(a, b) \in f$, selanjutnya dituliskan sebagai $f(a) = b$. Pada pemetaan f dari A ke B himpunan A disebut daerah asal (domain) f dan himpunan B disebut daerah kawan (kodomain).

(Bhattacharya, 1994)

Definisi 2.1.5 (Operasi Biner)
Misalkan S adalah himpunan tidak kosong. Operasi biner $*$ pada himpunan S adalah pemetaan dari $S \times S$ ke S, atau dituliskan sebagai berikut:

$$*: S \times S \to S$$
$$(a, b) \mapsto * (a, b) = c \in S.$$

(Bhattacharya, 1994)

Bentuk lebih umum dari operasi biner adalah operasi n-er. Berikut adalah definisi operasi n-er.

Definisi 2.1.6 (Operasi n-er)
Misalkan S adalah himpunan tidak kosong. Operasi n-er dalam himpunan S adalah pemetaan *Cartesian product* $S^n = S \times S \times ... \times S$ sebanyak n kali ke S sendiri, atau dituliskan sebagai berikut:

$$* : S^n \to S$$
$$*: S \times S \times ... S \to S$$
$$(a_1, a_2, \dots, a_n) \mapsto * (a_1, a_2, \dots, a_n) = c \in S$$

(Grillet, 2000)

Definisi 2.1.7 (Sifat Operasi Biner)
Misalkan $*: S \times S \to S$ dan $\circ: S \times S \to S$ adalah dua buah operasi biner. Operasi $*: S \times S \to S$ pada himpunan S dikatakan,

1. komutatif, jika $a * b = b * a$, untuk setiap $a, b \in S$,
2. assosiatif, jika $a * (b * c) = (a * b) * c$, untuk setiap $a, b, c \in S$,
3. distributif kiri atas $\circ$, jika $a * (b \circ c) = (a * b) \circ (a * c)$, untuk setiap $a, b, c \in S$,
4. distributif kanan atas $\circ$, jika $(a \circ b) * c = (a * c) \circ (b * c)$, untuk setiap $a, b, c \in S$.

(Bhattacharya, 1994)

2.2 Grup dan Subgrup

Grup dan subgrup adalah salah satu struktur mendasar aljabar, karena keduanya menjadi dasar dari struktur aljabar yang lain, seperti ring, lapangan, dan modul. Berikut akan diberikan definisi dari semigrup dan grup.

Definisi 2.2.1 (Semigrup)
Misalkan S adalah himpunan tidak kosong yang di dalamnya didefinisikan sebuah operasi biner. $(S,*)$ disebut semigrup jika aksioma-aksioma berikut terpenuhi:
1. $(S,*)$ tertutup
   Untuk setiap $a, b \in S$ maka $a * b \in S$,
2. $(S,*)$ assosiatif
   Untuk setiap $a, b, c \in S$ maka $(a * b) * c = a * (b * c)$.

(Durbin, 1992)

Definisi 2.2.2 (Semigrup Komutatif)
Misalkan S adalah semigrup dengan operasi biner $*$. S disebut semigrup komutatif jika $a * b = b * a$ untuk semua $a, b \in S$.

(Durbin, 1992)

Definisi 2.2.3 (Grup)
Sebuah grup $(G,*)$ adalah himpunan tak kosong G dengan sebuah operasi biner $*$ yang memenuhi aturan berikut:
1. tertutup
   Untuk semua $g, h \in G$, $g * h \in G$,
2. assosiatif
   $g * (h * k) = (g * h) * k$ untuk semua $g, h, k \in G$,
3. elemen identitas
   Terdapat $e \in G$ sedemikian hingga $g * e = e * g = g$ untuk semua $g \in G$,
4. invers
   Untuk semua $g \in G$, terdapat $h \in G$ di mana $g * h = h * g = e$.

(Fraleigh, 1994)

Definisi 2.2.4 (Grup Komutatif)
Sebuah grup $(G,*)$ dikatakan komutatif (atau grup abelian) jika operasi biner $*$ bersifat komutatif.

(Fraleigh, 1994)

Contoh 2.2.5
Himpunan bilangan real $\mathbb{R}$ merupakan grup komutatif terhadap operasi biner penjumlahan, namun hanya merupakan semigrup terhadap operasi

pergandaan. Dengan kata lain, $(\mathbb{R}, +)$ merupakan grup komutatif dan $(\mathbb{R}, \times)$ merupakan semigrup.

Bukti

1. $(\mathbb{R}, +)$ merupakan grup
   a. Tertutup
      Dengan mengambil sebarang $a, b \in \mathbb{R}$, maka sesuai sifat aljabar dari $\mathbb{R}$, $a + b \in \mathbb{R}$.
   b. Assosiatif
      Ambil sebarang $a, b, c \in \mathbb{R}$. Sesuai dengan sifat penjumlahan pada himpunan $\mathbb{R}$ yang bersifat assosiatif, maka $a + (b + c) = (a + b) + c$.
   c. Elemen identitas
      Salah satu elemen di $\mathbb{R}$, yaitu 0, memiliki sifat khusus, yaitu untuk sebarang $r \in \mathbb{R}$, $r + 0 = 0 + r = r$. Dengan demikian 0 merupakan identitas dari himpunan $\mathbb{R}$ dengan operasi penjumlahan.
   d. Elemen invers
      Untuk setiap $r \in \mathbb{R}$, terdapat elemen lain, yaitu $-r \in \mathbb{R}$, sedemikian sehingga $r + (-r) = (-r) + r = 0$. Dengan demikian, setiap anggota $\mathbb{R}$ memiliki invers.
   e. Komutatif
      Sesuai dengan sifat penjumlahan pada bilangan real, maka untuk setiap $a, b \in \mathbb{R}$, berlaku $a + b = b + a$.

   Karena $(\mathbb{R}, +)$ memenuhi kelima sifat di atas, maka $\mathbb{R}$ merupakan grup komutatif terhadap operasi penjumlahan.
2. $(\mathbb{R}, \times)$ merupakan semigrup
   a. Tertutup
      Dengan mengambil sebarang $a, b \in \mathbb{R}$, sesuai sifat aljabar dari $\mathbb{R}$, maka $a \times b \in \mathbb{R}$.
   b. Assosiatif
      Ambil sebarang $a, b, c \in \mathbb{R}$. Karena pergandaan pada $\mathbb{R}$ bersifat assosiatif, maka $a \times (b \times c) = (a \times b) \times c$.
   c. Elemen Identitas
      Terdapat elemen 1 pada $\mathbb{R}$ yang memiliki sifat, untuk $r \in \mathbb{R}$, $r \times 1 = 1 \times r = r$.
   d. Invers
      Untuk $0 \in R$, tidak ada $r \in R$ sedemikian sehingga $0 \times r = 1$, karena untuk semua $r \in R$, $0 \times r = r \times 0 = 0$.

Karena $(\mathbb{R},\times)$ memiliki elemen yang tidak memiliki invers namun bersifat tertutup dan asssosiatif, maka $\mathbb{R}$ merupakan semigrup, namun bukan grup, terhadap operasi pergandaan.

Definisi 2.2.6 (Subgrup)
Misalkan $(G,*)$ adalah grup H adalah himpunan bagian dari G. H disebut subgrup dari G, ditulis $H < G$, jika H adalah grup terhadap operasi biner pada G.

(Bhattacharya, 1994)

2.3 Teori Ring

Ring merupakan bentuk lebih khusus dari grup dengan menambahkan satu operasi biner. Secara umum, operasi biner yang digunakan dalam ring disebut operasi biner penjumlahan dan pergandaan. Berikut diberikan definisi dari ring.

Definisi 2.3.1 (Ring)
Sebuah ring adalah pasangan terurut $(R,+,\times)$ dari himpunan tak kosong R dan dua operasi biner pada R, yaitu penjumlahan dan pergandaan, sedemikian sehingga

1. $(R,+)$ adalah grup komutatif;
2. $(R,\times)$ adalah semigrup (pergandaannya asosiatif);
3. Berlaku hukum distributif kiri dan kanan, yaitu untuk semua $a,b \in R$

$$a \times (b+c) = (a \times b) + (a \times c),$$
$$(a+b) \times c = (a \times c) + (b \times c).$$

(Grillet, 2007)

Definisi 2.3.2 (Ring dengan Identitas)
Ring dengan identitas adalah sebuah ring yang semigrup terhadap operasi pergandaannya memiliki identitas.

(Grillet, 2007)

Contoh 2.3.3
Himpunan semua bilangan real $\mathbb{R}$ dengan operasi penjumlahan dan pergandaan merupakan ring dengan identitas.

Bukti

Contoh 2.2.5 telah menjelaskan bahwa $\mathbb{R}$ merupakan grup komutatif terhadap penjumlahan dan semigrup terhadap pergandaan. Selain itu, $\mathbb{R}$ juga memiliki elemen identitas terhadap pergandaan, yaitu 1. Sekarang akan dibuktikan bahwa pada $\mathbb{R}$ berlaku hukum distibutif, yaitu untuk sebarang $x, y, z \in \mathbb{R}$ berlaku

$$x(y+z) = xy + xz, \text{dan}$$
$$(x+y)z = xz + yz$$

Hukum di atas berlaku untuk semua bilangan real $x, y, z \in \mathbb{R}$. Dengan demikian $\mathbb{R}$ merupakan ring dengan identitas.

Definisi 2.3.4 (Ring Komutatif)

Sebuah ring R dikatakan komutatif jika $(R,\times)$ adalah semigrup komutatif.

(Wisbauer, 1991)

Definisi 2.3.5 (Subring)

Misalkan $(R,+,\times)$ adalah sebuah ring, dan S adalah himpunan bagian dari R. S dikatakan subring dari R, jika $(S,+,\times)$ juga merupakan ring.

(Bhattacharya, 1994)

Definisi 2.3.6 (Ideal)

Sebuah himpunan tak kosong S dari ring R dinamakan ideal jika berlaku

1. $a - b \in S$ untuk semua $a, b \in S$,
2. $ar \in S$ dan $ra \in S$ untuk semua $a \in S$ dan $r \in R$.

(Bhattacharya, 1994)

Contoh 2.3.7

Diberikan $\mathbb{Z}$ di mana $\mathbb{Z}$ adalah himpunan semua bilangan bulat. Jika $3\mathbb{Z} = \{3x | x \in \mathbb{Z}\}$ maka $3\mathbb{Z}$ merupakan ideal.

Bukti:

Akan dibuktikan bahwa $3\mathbb{Z}$ merupakan ideal.

1. $a - b \in 3\mathbb{Z}$ untuk semua $a, b \in 3\mathbb{Z}$

   Ambil sebarang $a, b \in 3\mathbb{Z}$, maka terdapat $x, y \in \mathbb{Z}$ sehingga $a = 3x$ dan $b = 3y$. Dengan demikian

   $$a - b = 3x - 3y$$
   $$= 3(x - y) = 3c, c \in \mathbb{Z}$$

   Karena $a - b = 3c, c \in \mathbb{Z}$, maka $a - b \in 3\mathbb{Z}$.

2. $ar \in 3\mathbb{Z}$ dan $ra \in 3\mathbb{Z}$ untuk semua $a \in 3\mathbb{Z}$ dan $r \in \mathbb{Z}$.
Ambil sebarang elemen $3\mathbb{Z}$, misalkan a. Karena $a \in 3\mathbb{Z}$, maka terdapat $x \in \mathbb{Z}$ sedemikian sehingga $a = 3x$. Ambil pula sebarang $y \in \mathbb{Z}$. Maka

$$\begin{aligned} ay &= 3xy \\ &= 3(xy) \end{aligned}$$

Karena $xy \in \mathbb{Z}$ maka $ay \in 3\mathbb{Z}$. Demikian pula

$$\begin{aligned} ya &= y3x \\ &= 3yx \end{aligned}$$

Karena $yx \in \mathbb{Z}$ maka $ya \in 3\mathbb{Z}$.
Jadi terbukti bahwa $3\mathbb{Z}$ merupakan ideal.

Definisi 2.3.8 (*Field*)
Sebuah *field* (atau lapangan) adalah pasangan terurut $(F, +, \times)$ yang memenuhi aksioma berikut:

i. $(F, +)$ merupakan grup komutatif,
ii. $(F - \{0\}, \times)$ merupakan grup komutatif,
iii. Berlaku hukum distributif.

(Grillet, 2007)

Contoh 2.3.9
Himpunan semua bilangan real $\mathbb{R}$ dengan operasi penjumlahan dan pergandaan, merupakan field.

Bukti:
Sesuai Contoh 2.3.3, $\mathbb{R}$ merupakan ring dengan identitas. Selain itu:

- Operasi perkalian pada $\mathbb{R}$ bersifat komutatif, atau dengan kata lain $ab = ba$ untuk semua $a, b \in \mathbb{R}$.
- Untuk semua $x \in \mathbb{R}, x \neq 0$ maka terdapat $x^{-1} = 1/x \in \mathbb{R}$ sedemikian sehingga $xx^{-1} = x^{-1}x = 1$. Dengan demikian $\mathbb{R}\backslash\{0\}$ adalah grup komutatif.

Dengan demikian terbukti bahwa $\mathbb{R}$ merupakan field.

Terdapat himpunan yang merupakan ring, antara lain sebagai berikut.

Definisi 2.3.10 (Ring Polinomial Satu Peubah)
Misalkan R adalah ring dengan identitas. Misalkan pula x adalah peubah. Maka himpunan

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 | a_i \in R, i = 1,2, \ldots, n\}$$

dengan $n \geq 0$ dinamakan ring polinomial dalam peubah x dengan koefisien di dalam R. a_i dinamakan koefisien dari peubah x^i.Jika $a_n \neq 0$, maka polinomial tersebut dikatakan berderajat n.

(Dummit, 2004)

Definisi 2.3.11 (Operasi Penjumlahan dan Pergandaan Polinomial). Misalkan $p(x)$ dan $q(x)$ masing-masing adalah polinomial dalam peubah x di mana $p(x) = \sum_{i=0}^{n} a_i x^i =$ dan $q(x) = \sum_{i=0}^{n} b_i x^i$, maka operasi di dalam polinomial didefinisikan sebagai berikut:

1. Penjumlahan:

$$p(x) + q(x) = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$$
$$= (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_0 + b_0)$$

2. Pergandaan:

$$p(x) \times q(x) = \sum_{i=0}^{2n} \sum_{j=0}^{i} a_i b_{i-j} x^i$$
$$= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + (a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0)x^3 + \cdots$$

(Dummit, 2004)

Definisi 2.3.12 (Ring Matriks)

Misalkan R adalah ring dan n adalah bilangan bulat positif. Maka himpunan

$$M_n(R) = \left\{ (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} | a_{ij} \in R, i, j = 1,2, \ldots, n \right\}$$

merupakan ring matriks $n \times n$ dengan elemen dari R dan operasi penjumlahan dan pergandaan di dalam matriks didefinisikan sebagai berikut:

1. Penjumlahan:

$$(a_{ij}) + (b_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}$$

$$= \begin{pmatrix} (a_{11}+b_{11}) & (a_{12}+b_{12}) & \cdots & (a_{1n}+b_{1n}) \\ (a_{21}+b_{21}) & (a_{22}+b_{22}) & \cdots & (a_{2n}+b_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ (a_{n1}+b_{n1}) & (a_{n2}+b_{n2}) & \cdots & (a_{nn}+b_{nn}) \end{pmatrix}$$
$= (c_{ij})$, di mana $c_{ij} = a_{ij} + b_{ij} \in R$.

2. Pergandaan:

$$(a_{ij}) \times (b_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \times \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}$$
$$= \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix} = (c_{ij})$$
di mana $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$.

(Dummit, 2004)

Definisi 2.3.13 (Matriks Transposisi)
Misalkan R adalah ring dan $M_n(R)$ adalah ring matriks pada R. Misalkan (a_{ij}) adalah elemen dari $M_n(R)$, di mana

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$
maka $(a_{ij})^T$ dengan bentuk
$$(a_{ij})^T = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix}$$
dinamakan matriks transposisi dari (a_{ij}).

(Dummit, 2004)

2.4 Homomorfisma

Di dalam pembahasan tentang grup dan subgrup, pengetahuan tentang homomorfisma dan variasinya, seperti isomorfisma atau

endomorfisma, merupakan hal yang penting. Dalam subbab ini akan dibahas definisi dari homomorfisma dan beberapa jenisnya.

Definisi 2.4.1 (Homomorfisma Grup)
Misalkan $(G,*)$ dan $(H,\circ)$ masing-masing adalah grup. Homomorfisma grup adalah pemetaan $\varphi: G \to H$ sedemikian sehingga

$$\varphi(x * y) = \varphi(x) \circ \varphi(y), \text{ untuk semua } x, y \in G.$$

(Dummit, 2004)

Contoh 2.4.2
Misalkan $(\mathbb{R}^+,\times)$ adalah grup dengan himpunan bilangan real positif dan operasi biner pergandaan. Misalkan pula $(\mathbb{R},+)$ adalah grup dengan himpunan bilangan real dan operasi penjumlahan. Maka pemetaan $\theta: \mathbb{R}^+ \to \mathbb{R}$ di mana $\theta(x) = \log x$ untuk semua $x \in \mathbb{R}^+$ adalah homomorfisma grup.

Bukti:
Ambil sebarang $x, y \in \mathbb{R}^+$. Dengan demikian

$$\begin{aligned} \theta(x \times y) &= \log(x \times y) \\ &= \log x + \log y \\ &= \theta(x) + \theta(y) \end{aligned}$$

Dengan demikian θ merupakan homomorfisma.

Definisi 2.4.3 (Endomorfisma)
Endomorfisma pada grup $(G,*)$ adalah homomorfisma dari G ke G itu sendiri.

(Grillet, 2007)

Contoh 2.4.4
Misalkan $(G,*)$ adalah grup. Ambil sebuah elemen $a \in G$. Pemetaan $I_a: G \to G$ yang didefinisikan sebagai $I_a(x) = a^{-1}xa$ untuk semua $x \in G$ adalah endomorfisma.

Bukti
Akan dibuktikan bahwa I_a adalah endomorfsima. Pertama akan dibuktikan bahwa I_a memetakan G ke G itu sendiri. Ambil sebarang elemen $x \in G$. Karena $a^{-1} * x * a \in G$ untuk semua x, maka $I_a(x) \in G$. Selanjutnya akan dibuktikan bahwa I_a merupakan homomorfisma. Ambil sebarang elemen $x, y \in G$. Maka

$$\begin{aligned} I_a(x * y) &= a^{-1} * (x * y) * a \\ &= a^{-1} * x * a * a^{-1} * y * a \\ &= I_a(x) * I_a(y). \end{aligned}$$

Terlihat bahwa I_a merupakan homomorfisma. Dengan demikian I_a merupakan endomorfisma.

Definisi 2.4.5 (Antihomomorfisma)

Misalkan $(G,*)$ dan $(H,\circ)$ adalah grup. Antihomomorfisma adalah pemetaan $\omega: G \to H$ sedemikian sehingga

$$\omega(g * y) = \omega(y) \circ \omega(x), \text{ untuk semua } x, y \in G.$$

(Bhattacharya, 1994)

Contoh 2.4.6

Misalkan G adalah sebuah grup terhadap operasi penjumlahan dan $\omega: G \to G$ di mana $\omega(x) = x^{-1}$. Dengan demikian $*$ adalah antihomomorfisma.

Bukti:

Ambil dua buah sebarang elemen G, misal x dan y. Berdasarkan definisi pemetaan ω, maka $\omega(x) = x^{-1}$ dan $\omega(y) = y^{-1}$. Dengan demikian

$$\omega(x + y) = (x + y)^{-1}$$

Sekarang akan dihitung ruas kanan terlebih dahulu. Berdasarkan aksioma grup, maka

$$\begin{aligned} (x + y) + (x + y)^{-1} &= e \\ x + y + (x + y)^{-1} &= e \\ (x^{-1} + x) + y + (x + y)^{-1} &= x^{-1} + e = x^{-1} \\ (y^{-1} + y) + (x + y)^{-1} &= y^{-1} + x^{-1} \\ (x + y)^{-1} &= y^{-1} + x^{-1} \end{aligned}$$

Dengan demikian persamaan pertama menjadi

$$\begin{aligned} * (x + y) &= (x + y)^{-1} = y^{-1} + x^{-1} \\ &= \omega(y) + \omega(x) \end{aligned}$$

Dengan demikian ω merupakan antihomomorfisma.

Definisi 2.4.7 (Homomorfisma Ring)

Misalkan R dan S masing masing adalah ring. Homomorfisma ring adalah pemetaan $\varphi: R \to S$ yang memenuhi:

i. $\varphi(a + b) = \varphi(a) + \varphi(b)$ untuk semua $a, b \in R$, dan
ii. $\varphi(ab) = \varphi(a)\varphi(b)$ untuk semua $a, b \in R$.

(Dummit, 2004)

Contoh 2.4.8
Diberikan ring $\mathbb{Z}$ di mana $\mathbb{Z}$ adalah himpunan semua bilangan bulat, dan ring $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$ di mana $\mathbb{Z}_2$ merupakan himpunan dua buah bilangan modulo 2. Pemetaan $\psi: \mathbb{Z} \to \mathbb{Z}_2$ didefinisikan sebagai pengiriman bilangan genap pada $\mathbb{Z}$ ke 0 dan bilangan ganjil ke 1. Dengan demikian pemetaan ψ merupakan homomorfisma ring.

Bukti
Ambil sebarang $a, b \in \mathbb{Z}$. Masing-masing elemen dapat dinyatakan sebagai berikut: $a = 2x + r_1$ dan $b = 2y + r_2$, di mana x, y adalah suatu bilangan bulat dan $r_1, r_2 \in \{0,1\}$. Terdapat empat kemungkinan kasus:

i. Jika a, b genap, dengan $r_1 = r_2 = 0$. Maka

$$\begin{aligned} a + b &= 2x + 2y \\ &= 2(x + y) \\ &= 2c, c \in \mathbb{Z}, c = x + y, \text{dan} \\ ab &= 2x \cdot 2y \\ &= 2xy \\ &= 2d, d \in \mathbb{Z}, d = xy \end{aligned}$$

Karena $\psi(a) = \psi(b) = 0$ maka

$$\begin{aligned} \psi(a + b) &= \psi(2x + 2y) \\ &= \psi(2c), \text{c} = x + y \\ &= 0 \\ &= \psi(a) + \psi(b) \\ \psi(ab) &= \psi(2xy) \\ &= \psi(2d), d = xy \\ &= 0 \\ &= \psi(a)\psi(b) \end{aligned}$$

ii. Jika a, b ganjil. Dengan demikian $r_1 = r_2 = 1$. Maka

$$\begin{aligned} a + b &= 2x + 1 + 2y + 1 \\ &= 2(x + y + 1) \\ &= 2c \in \mathbb{Z}, c = x + y + 1, \text{dan} \\ ab &= (2x + 1)(2y + 1) \\ &= 2(x + y + 2xy) + 1 \\ &= 2d + 1, d \in \mathbb{Z}, d = x + y + 2xy. \end{aligned}$$

Karena $\psi(a) = \psi(b) = 1$ maka

$$\begin{aligned} \psi(a + b) &= \psi\big(2(x + y + 1)\big) \\ &= \psi(2c), c = x + y + 1 \\ &= 0 \end{aligned}$$

$$= 1 + 1$$
$$= \psi(a) + \psi(b)$$
$$\psi(ab) = \psi(2(x + y + 2xy) + 1)$$
$$= \psi(2d + 1), d = x + y + 2xy$$
$$= 1$$
$$= \psi(a)\psi(b).$$

iii. Jika a genap dan b ganjil. Dengan demikian $r_1 = 0$ dan $r_2 = 1$. Maka

$$a + b = 2x + 2y + 1$$
$$= 2(x + y) + 1$$
$$= 2c + 1, c \in \mathbb{Z}, c = x + y, \text{dan}$$
$$ab = 2x(2y + 1)$$
$$= 2(2xy + x)$$
$$= 2d, d \in \mathbb{Z}, d = 2xy + x.$$

Karena $\psi(a) = 0$ dan $\psi(b) = 1$, maka

$$\psi(a + b) = \psi(2(x + y) + 1)$$
$$= \psi(2c + 1), c = x + y$$
$$= 1$$
$$= 0 + 1$$
$$= \psi(a) + \psi(b), \text{dan}$$
$$\psi(ab) = \psi\big(2(xy + x)\big)$$
$$= \psi(2d), d = xy + x$$
$$= 0 = 0 \times 1$$
$$= \psi(a)\psi(b)$$

iv. Jika a ganjil dan b genap. Maka $r_1 = 1$ dan $r_2 = 0$ dan

$$a + b = 2x + 1 + 2y$$
$$= 2(x + y) + 1$$
$$= 2c + 1, c \in \mathbb{Z}, c = x + y, \text{dan}$$
$$ab = (2x + 1)2y$$
$$= 2(xy + y)$$
$$= 2d, d \in \mathbb{Z}, d = xy + x.$$

Karena $\psi(a) = 1$ dan $\psi(b) = 0$ maka

$$\psi(a + b) = \psi(2(x + y) + 1)$$
$$= \psi(2c + 1), c = x + y$$
$$= 1 = 1 + 0$$
$$= \psi(a) + \psi(b)$$
$$\psi(ab) = \psi\big(2(xy + y)\big)$$

$$= \psi(2d), d = xy + y$$
$$= 0 = 1 \times 0$$
$$= \psi(a)\psi(b)$$

Jadi untuk semua kemungkinan a, b berlaku

$$\psi(a + b) = \psi(a) + \psi(b)$$
$$\psi(ab) = \psi(a)\psi(b)$$

Maka ψ merupakan homomorfisma ring.

2.5 Masalah Konjugasi

Di dalam teori grup, terdapat relasi ekuivalensi dua elemen dalam himpunan yaitu konjugasi dengan definisi sebagai berikut.

Definisi 2.5.1 (Konjugasi)

Misalkan G adalah grup dengan $a, b \in G$. a dikatakan **konjugat** dengan b (ditulis $a \sim b$) jika $b = x^{-1}ax$ untuk suatu $x \in G$.

(Cameron, 2008)

Relasi konjugasi dikatakan merupakan relasi ekuivalensi. Sebelumnya akan diberikan definisi dari relasi ekuivalensi.

Teorema 2.5.2

Relasi konjugasi merupakan relasi ekuivalensi.

Bukti:

Misalkan R merupakan relasi konjugasi di grup G, di mana untuk $x, y \in G$, $(x, y) \in R \Leftrightarrow \exists a \in G \ni y = a^{-1}xa$. Akan dibuktikan bahwa R merupakan relasi ukuivalensi.

1. Refleksif

   Untuk sebarang elemen a pada grup G, maka $a = e^{-1}ae$ selalu terpenuhi. Dengan demikian $a \sim a$, atau $(a, a) \in R$.

2. Simetris

   Misalkan $a, b \in G$ di mana $a \sim b$. Dengan demikian, terdapat $x \in G$ sehingga $b = x^{-1}ax$. Bila kedua ruas dikalikan x pada sisi kiri dan x^{-1} pada sisi kanan, didapat

   $$xbx^{-1} = xx^{-1}axx^{-1}$$
   $$(x^{-1})^{-1}bx^{-1} = eae = a$$

   Karena $a = (x^{-1})^{-1}bx^{-1}$ dan $x^{-1} \in G$, maka $b \sim a$. Dengan kata lain, jika $(a, b) \in R$, maka $(b, a) \in R$.

3. Transitif
   Misalkan $a, b, c \in G$, $a \sim b$ dan $b \sim c$. Karena $a \sim b$, maka $b = x^{-1}ax$ untuk suatu $x \in G$. Demikian juga karena $b \sim c$, maka $c = y^{-1}by$ untuk suatu $y \in G$. Dengan mensubstitusikan persamaan $b = x^{-1}ax$ ke dalam $c = y^{-1}by$, didapat

$$\begin{aligned} c &= y^{-1}by \\ &= y^{-1}x^{-1}axy \\ &= (xy)^{-1}a(xy) \end{aligned}$$

   Karena $c = (xy)^{-1}a(xy)$, maka $a \sim c$. Dengan kata lain, jika $(a, b) \in R$, $(b, c) \in R$, maka $(a, c) \in R$.

Karena ketiga syarat terpenuhi, maka didapat bahwa konjugasi merupakan relasi ekuivalensi.■

Dalam perkembangannya, konjugasi bisa diimplementasikan ke dalam masalah keputusan dan masalah pencarian.

Definisi 2.5.3 (Masalah Keputusan)
Masalah keputusan adalah kejadian sebagai berikut: diberikan sebuah sifat $\mathcal{P}$ dan sebuah objek $\mathcal{O}$. Tentukan apakah objek $\mathcal{O}$ memiliki sifat $\mathcal{P}$.

(Shpilrain, 2007)

Contoh 2.5.4
Diberikan empat buah titik $(-3,8)$, $(1,0)$, $(2,3)$, dan $(2,-3)$ pada bidang Cartesius dua dimensi. Tentukan apakah terdapat parabola yang melalui setidaknya tiga titik di atas yang juga memotong sumbu x?

Penyelesaian
Masalah ini diselesaikan dengan mencari parabola yang mungkin. Salah satu parabola yang memenuhi sifat di atas adalah $y = x^2 - 1$, karena parabola tersebut melalui titik $(-3,8)$, $(1,0)$, dan $(2,3)$. Selain itu $y = x^2 - 1$ memotong sumbu x di dua titik yaitu $(-1,0)$ dan $(1,0)$. Dengan demikian diputuskan bahwa benar terdapat setidaknya satu parabola yang memenuhi sifat di atas.

Definisi 2.5.5 (Masalah Pencarian)
Masalah pencarian adalah kejadian sebagai berikut: diberikan sifat $\mathcal{P}$ dan informasi bahwa terdapat objek dengan sifat $\mathcal{P}$. Tentukan setidaknya satu objek dengan sifat $\mathcal{P}$.

(Shpilrain, 2007)

Contoh 2.5.6
Diberikan empat buah titik $(-3,8)$, $(1,0)$, $(2,3)$, dan $(2,-3)$ pada bidang Cartesius dua dimensi dan dijamin terdapat setidaknya satu buah parabola yang melewati setidaknya tiga di antara keempat titik tersebut. Cari parabola tersebut.

Penyelesaian
Menggunakan petunjuk pada contoh 2.5.4, didapat satu buah parabola yang memenuhi sifat tersebut, yaitu $y = x^2 - 1$.

Dengan demikian, masalah keputusan dan masalah pencarian konjugasi didefinisikan sebagai berikut.

Definisi 2.5.7 (Masalah Keputusan Konjugasi)
Diberikan $x, y \in G$ di mana G adalah grup. Tentukan apakah x dan y saling konjugat, atau dengan kata lain apakah terdapat sebuah $v \in G$ sedemikian sehingga $y = v^{-1}xv$.

(Garber, 2009)

Definisi 2.5.8 (Masalah Pencarian Konjugasi)
Diberikan sebuah grup G dan dua buah elemen yang konjugat, $x, y \in G$. Temukan setidaknya satu elemen $v \in G$ sedemikian sehingga $y = v^{-1}xv$.

(Shpilrain, 2008)

2.6 Kriptografi

Matematika, baik teori bilangan maupun struktur aljabar, memegang peranan yang penting pada kriptografi. Hal ini karena algoritma-algoritma yang ada pada kriptografi sebagian besar dikembangkan dari ilmu matematika, khususnya teori bilangan dan struktur aljabar.

Definisi 2.6.1 (Kriptografi)
Kriptografi adalah studi tentang teknik matematis berkaitan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, autentikasi entitas, dan autentikasi asal data. Kerahasiaan adalah layanan yang digunakan untuk menjaga isi informasi dari semua yang tidak berhak. Integritas data adalah layanan yang beralamatkan pada perubahan data

oleh pihak yang tidak berhak. Autentikasi adalah layanan yang berhubungan dengan identifikasi.

(Koblitz, 1996)

Di dalam bukunya, Mollin (2007) mengatakan bahwa kriptografi adalah studi tentang metode mengirim pesan secara rahasia (bernama, bentuk tersamarkan atau *enchipered*) sedemikian sehingga hanya penerima yang dimaksud yang bisa menghilangkan samaran dan membaca pesan tersebut (atau meng-*dechiper* pesan tersebut). Kriptografi sendiri berasal dari bahasa Yunani, *kryptos* artinya tersembunyi, dan *graphein* artinya menulis.

Lebih lanjut Mollin (2007) menjelaskan definisi dari beberapa hal yang berkaitan dengan kriptografi, antara lain:

- Pesan asli disebut *plaintext*, dan pesan yang tersamarkan disebut *chipertext*.
- Proses perubahan *plaintext* menjadi *chipertext* disebut enkripsi (*encryption*) atau *enchipering*.
- Proses sebaliknya yang merubah *chipertext* menjadi *plaintext*, yang bisa dilakukan hanya oleh pihak yang memiliki pengetahuan untuk menghilangkan penyamaran *plaintext*, disebut dekripsi (*decryption*) atau *dechipering*.
- Orang yang melaksanakan kriptografi disebut *kriptografer*.
- Studi tentang teknik matematis sebagai usaha untuk mengalahkan metode kriptografi disebut kriptanalisis (*cryptanalysis*).

Definisi 2.6.2 (Kriptosistem)
Kriptosistem (atau *chiper*) adalah lima tupel $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, yang masing-masing merupakan:

1. $\mathcal{M}$ adalah himpunan berhingga dari *plaintext*;
2. $\mathcal{C}$ adalah himpunan berhingga dari *chipertext*;
3. $\mathcal{K}$, atau ruang kunci (*keyspace*), adalah himpunan berhingga dari kunci yang mungkin;
4. Untuk setiap pasang elemen $e, d \in \mathcal{K}$, terdapat *aturan enkripsi* $E_e \in \mathcal{E}$ dan *aturan dekripsi* $D_d \in \mathcal{D}$. Setiap $E_e: \mathcal{M} \to \mathcal{C}$ dan $D_d: \mathcal{C} \to \mathcal{M}$ adalah fungsi sedemikian sehingga $d_K\big(e_K(z)\big) = z$ untuk setiap *plaintext* $z \in \mathcal{M}$.

(Stinson, 2006)

Contoh 2.6.3

Salah satu jenis kriptografi klasik adalah kriptografi substitusi. Misalnya diberikan sebuah tabel sebagai berikut:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
c	d	e	f	g	h	i	j	k	l	m	n	o	p	q

Seseorang yang ingin mengirim pesan rahasia akan mengganti huruf di tiap pesannya dengan huruf di bahwanya, sehingga bila ia hendak menyampaikan pesan "KAMI AMAN" kepada orang lain, pesan yang ia kirim berubah menjadi "mcok ckcp". Tentukan kelima tupel kriptosistemnya!

Penyelesaian

1. *Plaintext* dari kriptosistem di atas adalah semua kata yang mungkin dibentuk dari dua puluh karakter di baris pertama, atau dalam bentuk
$$\mathcal{M} = \{a_1 a_2 \dots a_n | a_i = \text{A, B, C, …, O}, i = 1,2, \dots n\}$$
2. *Chipertext* dari kriptosistem di atas adalah semua kata yang mungkin dibentuk dari dua puluh karakter di baris kedua, atau dalam bentuk
$$\mathcal{C} = \{b_1 b_2 \dots b_n | b_i = \text{c, d, e, …, q}, i = 1,2, \dots, n\}$$
3. *Keyspace* dari kriptosistem di atas adalah semua kombinasi yang mungkin dari susunan huruf-huruf di baris kedua, atau dalam bentuk
$$\mathcal{K} = \left\{ \begin{bmatrix} \text{A} & \text{B} & \text{C} & \cdots & \text{O} \\ k_1 & k_2 & k_3 & \cdots & k_{20} \end{bmatrix} | k_i = \text{c, d, e, …, q}, i = 1,2, \dots ,20 \right\}$$
4. Misalkan tabel di atas, yang merupakan elemen dari himpunan $\mathcal{K}$, dianggap sebagai k. Maka aturan enkripsi dan dekripsi untuk kriptosistem di atas adalah sebagai berikut:

Aturan Enkripsi	**Aturan Dekripsi**
$E_k(\text{A}) = \text{c}$	$D_k(\text{c}) = \text{A}$
$E_k(\text{B}) = \text{d}$	$D_k(\text{d}) = \text{B}$
⋮	⋮
$E_k(\text{O}) = \text{q}$	$D_k(\text{q}) = \text{O}$

Sedangkan $\mathcal{E}$ dan $\mathcal{D}$ masing-masing adalah himpunan semua aturan enkripsi dan dekripsi untuk semua jenis elemen *keyspace.*

Di dalam kriptografi, pihak-pihak yang berkaitan dalam skema kriptografi adalah sebagai berikut.

- *Entity* atau *party* adalah seseorang atau sesuatu yang mengirim, menerima, atau memanipulasi informasi. Sebuah *entity* bisa jadi adalah seseorang, terminal komputer, atau yang lain.
- *Pengirim* adalah sebuah *entity* di dalam komunikasi dua *entity* yang merupakan pengirim yang sah. Di dalam contoh pihak ini biasanya diwakili Alice.
- *Penerima* adalah sebuah *entity* di dalam komunikasi dua *entity* yang merupakan penerima yang dimaksud. Di dalam contoh pihak ini biasanya diwakili Bob.
- *Lawan* (*adversary*) adalah sebuah *entity* di dalam komunikasi dua *entity* yang bukan penerima ataupun pengirim, dan berusaha mengalahkan layanan keamanan informasi menjadi tersedia antara pengirim dan penerima. Seorang lawan bisa jadi berusaha memainkan peran sebagai pengirim atau penerima yang sah.

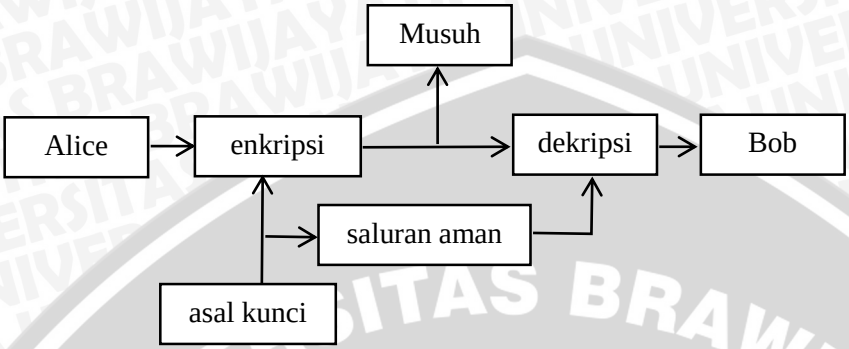
(Menezes, 1996)

Teknik kriptografi secara keseluruhan dibagi menjadi dua tipe umum, yaitu kriptografi kunci simetris (*symmetric-key*) dan kriptografi kunci publik (*public-key*). Definisi masing-masing teknik kriptografi adalah sebagai berikut.

Definisi 2.6.3 (Kriptografi Kunci Simetris)
Misalkan terdapat sebuah skema enkripsi terdiri dari himpunan transformasi enkripsi dan dekripsi, masing-masing $\{E_e | e \in \mathcal{K}\}$ dan $\{D_d | d \in \mathcal{K}\}$, di mana $\mathcal{K}$ adalah ruang kunci. Skema enkripsi tersebut dikatakan kunci simetris jika untuk setiap pasang kunci enkripsi/dekripsi (e, d), secara komputasional "mudah" menentukan d hanya dengan mengetahui e, dan menentukan e dari d.

(Menezes, 1996)

Di dalam kriptografi kunci simetris, biasanya $d = e$. Dengan demikian dibutuhkan saluran aman agar kedua pihak memiliki d dan e yang sama. Secara umum arus pertukaran informasi kriptografi kunci simetris digambarkan seperti di bawah ini.



Gambar 2.1 Alur pertukaran informasi menggunakan saluran aman untuk pertukaran kunci

Definisi 2.6.4 (Kriptografi Kunci Publik)
Misalkan terdapat sebuah skema enkripsi terdiri dari himpunan transformasi enkripsi dan dekripsi, masing-masing $\{E_e | e \in \mathcal{K}\}$ dan $\{D_d | d \in \mathcal{K}\}$, di mana $\mathcal{K}$ adalah ruang kunci. Metode enkripsi dikatakan skema enkripsi kunci publik jika untuk setiap kunci enkripsi/dekripsi (e, d), satu e (kunci publik) dibuat tersedia untuk umum, sedangkan d (kunci privat) tetap rahasia. Agar skema tersebut tetap rahasia, d tidak mungkin dapat dihitung melalui e.

(Menezes, 1996)

Definisi 2.6.5 (Protokol)
Di dalam kriptografi dikenal istilah protokol. Protokol dapat diartikan sebagai sistem dari aturan digital yang mengatur pertukaran data di dalam komputer atau komputer yang satu dengan yang lainnya. sedangkan protokol dalam kaitannya dengan kriptografi adalah protokol yang menjalankan fungsi yang berkaitan dengan sekuritas dan menggunakan metode kriptografis.

(Britannica, 2010)

Terdapat banyak jenis protokol dalam kriptografi. Dua di antaranya adalah protokol autentikasi dan protokol pertukaran kunci. (IRMA, 2014)

Definisi 2.6.6 (Autentikasi)
Autentikasi adalah salah satu tujuan paling penting dari keamanan informasi. Dengan autentikasi, seseorang bisa dengan yakin bahwa

entitas yang dia hubungi memang benar merupakan yang dia maksud, atau data yang ia terima belum dimanipulasi oleh kelompok yang tidak diinginkan.

(Menezes, 1996)

Autentikasi banyak digunakan di dalam komunikasi antara dua komputer atau lebih yang membutuhkan kepastian lawan komunikasi. Salah satu penggunaannya adalah autentikasi pada saat *login* ke dalam sebuah akun *email* atau penarikan uang di ATM. Autentikasi menjamin bahwa seseorang terhubung tepat ke akun yang ia tuju, atau menjamin akun yang ada tidak dapat diakses oleh pihak asing.

(Menezes, 1996)

Di dalam proses autentikasi, terdapat setidaknya tiga pihak yang terlibat, yaitu:

1) *Prover*, sebagai pihak pertama, yaitu pihak yang akan diautentikasi atau dicek kebenarannya bahwa ia benar merupakan pasangan komunikasi yang diinginkan pihak kedua. Dalam kaitannya dengan pihak-pihak di dalam kriptografi, *prover* adalah pengirim, atau diwakilkan Alice.
2) *Verifier*, sebagai pihak kedua, yaitu pihak yang akan mengautentikasi pihak pertama, atau dengan kata lain pihak yang akan memeriksa identitas *prover*. Dalam kaitannya dengan pihak-pihak di dalam kriptografi, *verifier* adalah penerima, atau diwakilkan sebagai Bob.
3) Pihak ketiga atau *adversary* sebagai pengganggu dalam proses komunikasi pihak pertama dan kedua, baik dengan berpura-pura sebagai *prover, verifier*, atau dengan cara lain.

(IRMA, 2014)

Definisi 2.6.7 (Pertukaran Kunci)
Pertukaran kunci merupakan bagian dari kriptografi di mana terdapat dua *entity* atau lebih bisa membangun (atau menghitung) sebuah kunci rahasia bersama. Dengan demikian, pihak ketiga tidak bisa mendapatkan kunci rahasia bersama yang dihitung oleh *entity* yang terlibat.

(Paar, 2010)

Salah satu protokol pertukaran kunci pertama yang dikenalkan adalah Pertukaran Kunci Diffie-Hellman pada tahun 1976. Salah satu

penerapan protokol Pertukaran Kunci Diffie-Hellman adalah sebagai berikut.

1. Grup yang digunakan adalah grup siklik G, yaitu grup yang semua elemennya dapat dinyatakan dalam bentuk p^a untuk suatu $p \in G$ dan $a \in \mathbb{Z}^+$.
2. Kunci publik yang digunakan adalah elemen $g \in G$ dan diketahui oleh kedua pihak. Kunci privat yang Alice gunakan adalah bilangan asli acak a, sedangkan kunci privat Bob adalah bilangan asli acak b.
3. Alice menghitung g^a dan mengirimkannya kepada Bob, sedangkan Bob menghitung g^b dan mengirimkannya kepada Alice.
4. Kunci bersama Alice dan Bob adalah g^{ab} di mana Alice dapat menghitungnya dari $\left(g^b\right)^a$, sedangkan Bob menghitungnya dari $(g^a)^b$.

(Diffie, 1976)

BAB III
PEMBAHASAN

3.1 Masalah Pencarian *Double Twisted Conjugacy*

Bentuk yang lebih umum dari masalah pencarian konjugasi adalah masalah konjugasi *twisted* yang menggunakan endomorfisma di dalamnya. Masalah keputusan *twisted conjugacy* didefinisikan sebagai berikut.

Definisi 3.1.1 (Masalah Keputusan *Twisted Conjugacy*)
Diberikan φ endomorfisma pada grup G dan $t, w \in G$. Tentukan apakah terdapat elemen $s \in G$ sedemikian sehingga $t = s^{-1}w\varphi(s)$.

(Shpilrain, 2008)

Shpilran dan Ushakov (2008) memberikan masalah yang lebih umum dari masalah keputusan konjugasi *twisted* tersebut, yang dinamakan masalah *double twisted conjugacy* (konjugasi *twisted* ganda), yang didefinisikan sebagai berikut.

Definisi 3.1.2 (Masalah Keputusan *Double Twisted Conjugacy*)
Diberikan φ, ψ dua buah endomorfisma pada grup G dan sepasang elemen $t, w \in G$. Tentukan apakah terdapat elemen $s \in G$ sedemikian sehingga $t = \varphi(s^{-1})w\psi(s)$.

Definisi 3.1.3 (Masalah Pencarian *Double Twisted Conjugacy*)
Diberikan φ, ψ dua buah endomorfisma pada grup G dan sepasang elemen $t, w \in G$. Temukan sebuah elemen $s \in G$ sedemikian sehingga $t = \varphi(s^{-1})w\psi(s)$ jika dipastikan setidaknya ada satu elemen s yang ada.

Shpilrain dan Ushakov mengajukan skema autentikasi yang keamanannya berdasarkan atas masalah pencarian *double twisted conjugacy*. Dalam skema autentikasi yang diberikan, G tidak harus merupakan grup, tapi bisa berupa sebuah semigrup. Untuk menggantikan invers s, digunakan sebuah antihomomorfisma $*: G \to G$ sedemikian sehingga $(ab)^* = b^*a^*$ untuk semua $a, b \in G$.

Skema pertukaran kunci dapat dibuat dengan sedikit modifikasi dari skema pertukaran kunci yang diusulkan oleh Shpilrain dan Ushakov

(2005). Skema pertukaran kunci yang diusulkan oleh Shpilrain dan Ushakov pada adalah sebagai berikut.

1. Kunci publik yang digunakan adalah (semi) grup W dan dua buah subgrupnya, yaitu A dan B sedemikian sehingga $ab = ba$ untuk semua $a \in A, b \in B$. Selain itu, kunci publik yang digunakan adalah sebuah elemen $w \in W$.
2. Kunci privat Alice adalah $a_1 \in A, b_1 \in B$, sedangkan kunci privat Bob adalah $a_2 \in A, b_2 \in B$.
3. Alice mengirim $u_1 = a_1 w b_1$ ke Bob, sedangkan Bob mengirim $u_2 = b_2 w a_2$ ke Alice.
4. Kunci rahasia bersama adalah $K = a_1 b_2 w a_2 b_1$.

K merupakan kunci rahasia bersama karena Alice bisa menghitung $K_1 = a_1 u_2 b_1$ dan Bob bisa menghitung $K_2 = b_2 u_1 a_2$. Nilai K_1 dan K_2 sama karena a_1, a_2 komutatif dengan b_1, b_2.

(Shpilrain, 2005)

3.2 Protokol Autentikasi dan Pertukaran Kunci menggunakan Masalah *Double Twisted Conjugacy*

3.2.1 Protokol Autentikasi

Berikut akan diberikan protokol autentikasi menggunakan masalah pencarian konjugasi *double twisted conjugacy*. Di sini Alice adalah *prover* dan Bob sebagai *verifier*. Misalkan G adalah sebuah semigrup, dengan $*$ merupakan sebuah antihomomorfisma pada G sehingga $(ab)^* = b^* a^*$.

1. Kunci publik Alice adalah sepasang endomorfisma φ, ψ pada semigrup G dan dua buah elemen $t, w \in G$ sedemikian sehingga $t = \varphi(s^*) w \psi(s)$, di mana $s \in G$ adalah kunci privatnya.
2. Untuk memulai autentikasi, Alice memilih sebuah elemen $r \in G$ dan mengirim elemen $u = \varphi(r^*) t \psi(r)$, yang dinamakan *commitment*, kepada Bob.
3. Bob kemudian memilih bilangan biner acak c dan mengirimkannya kepada Alice.
   - Jika $c = 0$, maka Alice mengirim $v = r$ ke Bob dan Bob mengecek apakah persamaan $u = \varphi(v^*) t \psi(v)$ terpenuhi. Jika ya, maka Bob menerima autentikasi Alice.
   - Jika $c = 1$, maka Alice mengirim $v = sr$ ke Bob dan Bob mengecek apakah persamaan $u = \varphi(v^*) w \psi(v)$ terpenuhi. Jika ya, maka Bob menerima autentikasi Alice.

Autentikasi Alice akan dipenuhi untuk kedua kasus c, karena:

- Jika $c = 0$, maka $v = r$ sehingga $\varphi(v^*)t\psi(v) = \varphi(r^*)t\psi(r) = u$.
- Jika $c = 1$, maka $v = sr$ sehingga $\varphi(v^*)w\psi(v)$
$= \varphi((sr)^*)w\psi(sr) = \varphi(r^*s^*)w\psi(sr)$
$= \varphi(r^*)\varphi(s^*)w\psi(s)\psi(r) = \varphi(r^*)t\psi(r) = u$.

Skema ini dianggap aman, karena walaupun pihak ketiga mampu mendapatkan informasi tentang φ, ψ, w, t, dan u, ia tidak bisa mendapatkan informasi mengenai s ataupun r dari skema tersebut.

3.2.2 Protokol Pertukaran Kunci

Berikut akan diberikan protokol pertukaran kunci menggunakan pencarian *double twisted conjugacy*. Misalkan G adalah sebuah semigrup, dengan $*$ merupakan sebuah antihomomorfisma pada G.

1. Kunci publik kedua pihak adalah sepasang endomorfisma φ, ψ pada semigrup G dan sebuah elemen $w \in G$. Alice dan Bob masing-masing memilih kunci privat $a, b \in G$ sedemikian sehingga a dan b komutatif, atau $ab = ba$.
2. Alice kemudian menghitung $t = \varphi(a^*)w\psi(a)$ dan mengirimkannya ke Bob, sedangkan Bob menghitung $u = \varphi(b^*)w\psi(b)$ dan mengirimkannya ke Alice.
3. Alice menghitung $k_1 = \varphi(a^*)u\psi(a)$, sedangkan Bob menghitung $k_2 = \varphi(b^*)t\psi(b)$.

Keduanya memiliki kunci yang sama (atau $k_1 = k_2$) karena:

- $k_1 = \varphi(a^*)u\psi(a)$
$= \varphi(a^*)\varphi(b^*)w\psi(b)\psi(a)$
$= \varphi((ba)^*)w\psi(ba)$.
- $k_2 = \varphi(b^*)t\psi(b)$
$= \varphi(b^*)\varphi(a^*)w\psi(a)\psi(b)$
$= \varphi((ab)^*)w\psi(ab)$
$= \varphi((ba)^*)w\psi(ba)$.

Skema ini dianggap aman, karena walaupun pihak ketiga mampu mendapatkan informasi tentang φ, ψ, t, dan u, ia tidak dapat menghitung nilai $k_1 = k_2$ dari persamaan tersebut.

3.3 Semigrup yang Digunakan dalam Protokol dan Parameternya

Di dalam menggunakan protokol autentikasi dan pertukaran kunci menggunakan *double twisted conjugacy* ini, semigrup yang digunakan haruslah semigrup non komutatif dan proses perhitungan tiap elemennya tergolong mudah. Syarat non komutatif digunakan agar nilai $t = \varphi(s^*)w\psi(s)$ tidak memiliki nilai yang sama dengan $t = \psi(s)w\varphi(s^*)$. Bila syarat ini dipenuhi, diharapkan penghitungan dalam proses pemecahan kunci menjadi lebih rumit. Syarat komputasi yang mudah dipakai agar dalam penerapannya komputer dapat dengan mudah memproses input hitungan.

Shpilrain dan Ushakov mengusulkan penggunaan semigrup matriks 2×2 terhadap ring sebagai *keyspace* dari protocol autentikasi mereka. Ring yang digunakan adalah polinomial terpotong n-suku di mana tiap koefisien dari polinomial tersebut diambil dari *field* dengan dua elemen, yaitu 0 dan 1. Dengan kata lain, jika $\mathbf{F}_2$ merupakan *field* dengan dua buah elemen, maka semigrup yang dipakai oleh Shpilrain dan Ushakov adalah ekspresi dari $\sum_{0 \le i \le n-1} a_i x^i$, di mana a_i adalah elemen dari $\mathbf{F}_2$ dan x^i merupakan variable.

Secara umum, himpunan semua *keyspace* adalah dalam bentuk

$$\mathcal{K} = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \middle| a_{ij} \in \boldsymbol{F_2}[x] \; mod \; x^n, \;\; i,j = 1,2 \right\}$$

Salah satu elemen dari himpunan di atas, dengan $n = 5$, adalah sebagai berikut.

$$a = \begin{pmatrix} 1 + x + x^3 & 1 + x + x^4 \\ x + x^2 & x^2 + x^4 \end{pmatrix}$$

Shpilrain dan Ushakov menggunakan semigrup bentuk ini karena semigrup ini memiliki banyak endomorfisma karena polinomial di dalam matriks tersebut memiliki banyak polinomial. Dengan menggunakan pemetaan dalam bentuk $x \to p(x)$, di mana $p(x)$ merupakan polinomial dengan $a_0 = 0$, didapat endomorfisma ring θ_p dalam bentuk $\theta_p(x^n) = \big(p(x)\big)^n$. Sebelumnya akan dibuktikan bahwa θ_p merupakan homomorfisma ring.

Teorema 3.3.1

Diberikan ring polinomial $R[x]$ dengan operasi penjumlahan dan pergandaan polinomial. Diberikan sebarang polinomial $p(x)$ dengan

$a_0 = 0$. Didefinisikan pemetaan θ_p di mana $\theta_p(x^n) = \big(p(x)\big)^n$. Maka θ_p merupakan homomorfisma ring.

Bukti

Akan ditunjukkan bahwa θ_p merupakan homomorfisma ring. Misalkan $a, b \in R[x]$ dalam bentuk:

$$a = \sum_{i=0}^{n-1} a_i x^i \qquad b = \sum_{i=0}^{n-1} b_i x^i$$

maka

$$\begin{aligned}\theta_p(a+b) &= \theta_p\left(\sum_{i=0}^{n}(a_i + b_i)x^i\right)\\ &= \sum_{i=0}^{n-1}(a_i + b_i)\big(p(x)\big)^i\\ &= \sum_{i=0}^{n-1} a_i\big(p(x)\big)^i + \sum_{i=0}^{n-1} b_i\big(p(x)\big)^i\\ &= \theta_p(a) + \theta_p(b).\end{aligned}$$

dan

$$\begin{aligned}\theta_p(a\times b) &= \theta_p\left(\sum_{i=0}^{2n-2}\sum_{j=0}^{i} a_i b_{i-j} x^i\right)\\ &= \sum_{i=0}^{2n-2}\sum_{j=0}^{i} a_i b_{i-j}\big(p(x)\big)^i\\ &= \sum_{i=0}^{n-1} a_i\big(p(x)\big)^i \times \sum_{i=0}^{n-1} b_i\big(p(x)\big)^i\\ &= \theta_p(a)\times\theta_p(b).\end{aligned}$$

Karena kedua sifat homomorfisma ring tersebut terpenuhi, maka θ_p merupakan homomorfisma ring. ■

Dengan demikian, karena θ_p merupakan homomorfisma penjumlahan dan pergandaan, maka θ_p meluas menjadi endomorfisma

semigrup semua matriks 2×2 terhadap polinomial satu peubah terpotong.

Secara umum, endomorfisma grup yang digunakan dalam protokol ini adalah dalam bentuk:

$$\begin{aligned} \varphi &: G \to G \\ g &\mapsto \varphi(g) \\ \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} &\mapsto \varphi \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} = \begin{pmatrix} \theta_p(g_{11}) & \theta_p(g_{12}) \\ \theta_p(g_{21}) & \theta_p(g_{22}) \end{pmatrix} \end{aligned}$$

di mana θ_p merupakan homomorfisma ring dan $p(x)$ merupakan polinomial dengan $a_0 = 0$.

Selain itu, operasi $*$ yang digunakan pada protokol diekspresikan sebagai matriks transposisi. Sesuai dengan sifat transposisi matriks, transposisi merupakan antihomomorfisma pada matriks, sehingga operasi $*$ dapat digunakan dalam protokol.

Dalam protokol autentikasi Shpilrain dan Ushakov, nilai n menyatakan parameter yang menentukan ukuran dari *keyspace*. Bila n dipilih bernilai 300, maka terdapat 2^{300} polinomial dengan derajat kurang dari n terhadap $\mathbf{F}_2$, sehingga terdapat $(2^{300})^4 = 2^{1200}$ matriks 2×2 matriks terhadap polinomial terpotong n. Dengan kata lain, terdapat 2^{1200} kemungkinan kunci privat, yang Ushakov dan Shpilrain anggap sudah cukup banyak.

Penghitungan polinomial terpotong terhadap $\mathbf{F}_2$ juga sangat efisien karena dapat dilakukan oleh komputer dalam waktu yang singkat.

(Bürgser dkk, 1997)

Ukuran dari *keyspace* publik juga tergolong besar. Salah satu kunci publik, w, juga merupakan matriks 2×2 terhadap polinomial terpotong n, sedangkan dua kunci publik lainnya adalah endomorfisma dalam bentuk $x \to p(x)$, di mana $p(x)$ adalah polinomial terpotong n dengan konstanta nol. Dengan demikian, terdapat sebanyak 2^{299} endomorfisma yang berbeda dalam bentuk tersebut, dan karena yang dibutuhkan adalah sepasang endomorfisma, maka terdapat 2^{598} pasangan endomorfisma yang berbeda.

Pemilihan kunci dilakukan dengan cara berikut.

1. Kunci w dipilih secara acak, yang merupakan matriks 2×2 dengan entri merupakan polinomial dengan derajat maksimal $n-1$. Koefisien polinomial dipilih acak dari angka 0 dan 1 dengan probabilitas masing-masing $1/2$.
2. Kunci privat s pada protokol autentikasi dipilih dengan acak dengan cara yang sama dengan pemilihan kunci public w. Terdapat pengecualian untuk konstanta polinomial, di mana konstanta yang dipilih adalah 1 untuk menjamin hasil kalinya tidak memiliki terlalu banyak angka 0.
3. Kunci privat a dan b pada protokol pertukaran kunci dipilih dengan cara yang sama dengan kunci privat s, dengan pengecualian matriks yang digunakan adalah matriks diagonal, atau dalam bentuk $\begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} \end{pmatrix}$ dan $\begin{pmatrix} b_{11} & 0 \\ 0 & b_{22} \end{pmatrix}$. Hal ini diperlukan karena syarat kekomutatifan pada protokol pertukaran kunci.

3.4 Contoh Penggunaan Semigrup Platform

Berikut akan diberikan contoh penggunaan semigrup dalam protokol autentikasi dan pertukaran kunci. Untuk memudahkan perhitungan dan penulisan, maka dipilih nilai n yang relatif kecil, yaitu $n = 5$. Untuk mempermudah penulisan, polinomial $a_0 + a_1 x + \cdots$ akan disingkat menjadi $a_0 a_1 \ldots$.

3.4.1 Protokol Autentikasi

Pada protokol ini, dipilih secara acak dua kunci publik yang berupa endomorfisma yaitu φ dan ψ, serta satu anggota semigrup G yaitu w, dan satu kunci privat $s \in G$. Pemilihan secara acak menghasilkan nilai w dan s yaitu

$$w = \begin{pmatrix} 1\,0\,0\,1\,1 & 1\,0\,1\,0\,0 \\ 0\,1\,0\,0\,1 & 1\,0\,1\,0\,1 \end{pmatrix} \qquad s = \begin{pmatrix} 1\,0\,0\,1\,1 & 1\,0\,1\,0\,1 \\ 1\,0\,0\,0\,1 & 1\,0\,1\,1\,1 \end{pmatrix}$$

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

dan polinomial $p(x)$ dan $q(x)$ yang digunakan yaitu

$\varphi(x) = x^2 + x^3 = (0\,0\,1\,1\,0)$ (digunakan dalam endomorfisma φ)

$\psi(x) = x + x^2 + x^4 = (0\,1\,1\,0\,1)$ (digunakan dalam endomorfisma ψ)

yang menghasilkan

$$s^* = s^T = \begin{pmatrix} 1\,0\,0\,1\,1 & 1\,0\,0\,0\,1 \\ 1\,0\,1\,0\,1 & 1\,0\,1\,1\,1 \end{pmatrix}$$

$$\varphi(s^*) = \begin{pmatrix} \theta_p(s_{11}^*) & \theta_p(s_{12}^*) \\ \theta_p(s_{21}^*) & \theta_p(s_{22}^*) \end{pmatrix} = \begin{pmatrix} 1\,0\,0\,0\,0 & 1\,0\,0\,0\,0 \\ 1\,0\,0\,0\,1 & 1\,0\,0\,0\,1 \end{pmatrix}$$

$$\psi(s) = \begin{pmatrix} \theta_q(s_{11}) & \theta_q(s_{12}) \\ \theta_q(s_{21}) & \theta_q(s_{22}) \end{pmatrix} = \begin{pmatrix} 1\,0\,0\,1\,0 & 1\,0\,1\,0\,0 \\ 1\,0\,0\,0\,1 & 1\,0\,1\,1\,1 \end{pmatrix}$$

$$t = \varphi(s^*)w\psi(s) = \begin{pmatrix} 1\,1\,0\,0\,0 & 1\,1\,1\,0\,1 \\ 1\,1\,0\,0\,1 & 1\,1\,1\,0\,0 \end{pmatrix}$$

$$u = \varphi(r^*)t\psi(s) = \begin{pmatrix} 0\,0\,0\,1\,0 & 0\,0\,0\,1\,0 \\ 0\,0\,0\,1\,0 & 0\,0\,0\,1\,0 \end{pmatrix}$$

Pada kasus $c = 0$ maka $v = r$, dengan demikian

$$\varphi(v^*)t\psi(v) = \varphi(r^*)t\psi(r) = \begin{pmatrix} 0\,0\,0\,1\,0 & 0\,0\,0\,1\,0 \\ 0\,0\,0\,1\,0 & 0\,0\,0\,1\,0 \end{pmatrix} = u$$

Pda kasus $c = 1$ maka $v = sr$, dengan demikian

$$\varphi(v^*)w\psi(v) = \varphi((sr)^*)w\psi(r) = \begin{pmatrix} 0\,0\,0\,1\,0 & 0\,0\,0\,1\,0 \\ 0\,0\,0\,1\,0 & 0\,0\,0\,1\,0 \end{pmatrix} = u$$

dengan proses perhitungan dapat dilihat pada lampiran.

Karena kedua persamaan terakhir menghasilkan nilai u maka Bob menerima autentikasi Alice untuk kedua kasus.

3.4.2 Protokol Pertukaran Kunci

Kunci publik yang digunakan dalam protokol pertukaran kunci adalah dua buah endomorfisma φ dan ψ pada semigrup G, dan satu elemen acak $w \in G$. Sedangkan kunci privat yang digunakan adalah dua buah elemen acak $a, b \in G$ sedemikian sehingga $ab = ba$, di mana kedua belah pihak hanya mempunyai satu kunci saja.

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

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

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

di mana polinomial yang digunakan adalah

$p(x) = x^2 + x^3 + x^4 = (0\,0\,1\,1\,1)$ (digunakan dalam φ)
$q(x) = x + x^2 + x^4 = (0\,1\,1\,0\,1)$ (digunakan dalam ψ)

yang menghasilkan

$$t = \varphi(a^*)w\psi(a) = \begin{pmatrix} 1\,1\,0\,1\,0 & 0\,1\,0\,0\,1 \\ 1\,0\,1\,1\,0 & 1\,1\,1\,0\,1 \end{pmatrix}$$

$$u = \varphi(b^*)w\psi(b) = \begin{pmatrix} 1\,0\,0\,1\,0 & 0\,1\,0\,0\,0 \\ 1\,1\,1\,1\,1 & 1\,1\,0\,1\,0 \end{pmatrix}$$

Kedua belah pihak mampu menghitung nilai k yang sama dengan cara yang berbeda, yaitu

$k = \varphi(a^*)u\psi(a) = \varphi(b^*)t\psi(b) = \begin{pmatrix} 1\,0\,0\,0\,0 & 0\,1\,1\,1\,1 \\ 1\,1\,0\,0\,1 & 1\,0\,1\,0\,0 \end{pmatrix}$.

dengan proses perhitungan dapat dilihat pada lampiran.

3.5 Kriptanalisis

Kriptanalisis (*cryptanalysis*) adalah studi tentang teknik matematis sebagai usaha untuk memecahkan teknik kriptografi, dan, secara lebih umum, layanan keamanan informasi. Seseorang yang merusaha melakukan kriptanalisis dinamakan kriptanalis (*cryptanalyst*). (Menezes, 1996)

Setiap kali sebuah teknik kriptografi dibuat, selalu ada pihak yang melakukan kriptanalisis. Hal ini dilakukan untuk mengetahui sebaik apa tingkat keamanan dari sistem yang ada. Secara umum, para penemu sistem kriptografi modern memaparkan cara kerja skema kriptografinya kepada publik agar publik bisa melakukan tes sebaik apa sistemnya. Dari tes tersebut biasanya didapatkan masukan-masukan untuk memperbaiki sistem kriptografi yang ada.

Shpilrain dan Ushakov, selain menawarkan skema autentikasi menggunakan *double twisted conjugacy*, mereka juga memaparkan kriptanalisis dari sistem tersebut. Secara umum kriptanalisis yang mereka tawarkan ada dua.

3.5.1 *Brute Force*

Secara umum, *brute force* dapat diartikan sebagai usaha melakukan dekripsi *(dechipering*) menggunakan semua kunci yang mungkin. Jika seseorang yang melakukan *brute force* akhirnya menemukan *plain text* yang sesuai dengan salah satu kunci yang ia miliki, maka ia dikatakan telah menemukan kunci yang tepat. (Paar, 2010)

Dengan mencoba semua kunci yang tersedia, seseorang diasumsikan pasti akan mampu menemukan paling tidak satu kunci yang cocok. Untuk mencegah masalah tersebut, sistem kriptografi biasanya memberi syarat parameter yang cukup besar, agar *keyspace* yang ada menjadi semakin

besar. Bila *keyspace* cukup besar, maka proses perhitungan akan membutuhkan waktu yang lama.

Pada skema autentikasi dan ini, secara normal parameter n yang dipakai adalah $n = 300$ atau lebih, yang menghasilkan jumlah kunci yang mungkin untuk s adalah sebanyak 2^{1200}, yang membutuhkan waktu yang sangat lama untuk dihitung. Dengan demikian proses pemecahan kriptografi dengan proses *brute force* dianggap tidak sesuai.

3.5.2 Penyelesaian Suku Awal

Skema ini didasarkan pada kenyataan bahwa pada perkalian dua buah polinomial, koefisien dari peubah dengan derajat yang lebih rendah dapat mempengaruhi hasil koeifisen dari peubah dengan derajat yang lebih tinggi. Hal ini tidak berlaku sebaliknya, di mana hasil kali koefisien dari peubah dengan derajat yang lebih tinggi tidak mempengaruhi koefisien dari variabel dengan derajat yang lebih rendah.

Pada skema autentikasi di atas, diketahui bahwa kunci $w, t, \varphi,$ dan ψ merupakan kunci yang diketahui oleh publik, sedangkan s hanya diketahui oleh Alice saja.

Proses pemecahan dilakukan dengan cara sebagai berikut. Matriks persamaan $t = \varphi(s^*)w\psi(s)$ diubah menjadi empat buah sistem persamaan polinomial terpotong terhadap $\mathbf{F}_2$, yaitu sebagai berikut:

$$t = \varphi(s^*)w\psi(s)$$

$$\begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} = \varphi \begin{pmatrix} s_{11} & s_{21} \\ s_{12} & s_{22} \end{pmatrix} \begin{pmatrix} w_{11} & w_{12} \\ w_{21} & w_{22} \end{pmatrix} \psi \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix}$$

$$= \begin{pmatrix} \varphi(s_{11}) & \varphi(s_{21}) \\ \varphi(s_{12}) & \varphi(s_{22}) \end{pmatrix} \begin{pmatrix} w_{11} & w_{12} \\ w_{21} & w_{22} \end{pmatrix} \begin{pmatrix} \psi(s_{11}) & \psi(s_{12}) \\ \psi(s_{21}) & \psi(s_{22}) \end{pmatrix}$$

yang kemudian diubah menjadi persamaan

$$\begin{aligned} t_{11} &= \varphi(s_{11})[w_{11}\psi(s_{11}) + w_{12}\psi(s_{12})] \\ &\quad +\varphi(s_{21})[w_{12}\psi(s_{11}) + w_{22}\psi(s_{21})] \\ t_{12} &= \varphi(s_{11})[w_{11}\psi(s_{12}) + w_{12}\psi(s_{22})] \\ &\quad +\varphi(s_{21})[w_{21}\psi(s_{12}) + w_{22}\psi(s_{22})] \\ t_{21} &= \varphi(s_{12})[w_{11}\psi(s_{11}) + w_{12}\psi(s_{21})] \\ &\quad +\varphi(s_{22})[w_{21}\psi(s_{11}) + w_{22}\psi(s_{21})] \\ t_{22} &= \varphi(s_{12})[w_{11}\psi(s_{12}) + w_{12}\psi(s_{22})] \\ &\quad +\varphi(s_{22})[w_{21}\psi(s_{12}) + w_{22}\psi(s_{22})] \end{aligned}$$

Proses penyelesaian dilakukan dalam langkah berikut.

a. Bagian yang akan dipecahkan (dicari) adalah nilai s di mana nilai $w, t, \varphi,$ dan ψ diketahui.

b. Konstanta polinomial pada matriks s dicoba satu persatu (misal: $s_{11} = 1, s_{12} = 1, s_{21} = 1, s_{22} = 0$) dan dimasukkan ke dalam persamaan di atas. Jika persamaan terpenuhi, nilai konstanta pada polinomial s disimpan.
c. Perhitungan dilanjutkan dengan mencoba koefisien pada peubah x dengan konstanta diambil dari langkah sebelumnya, misalnya nilai yang diuji adalah $s_{11} = (1\ 1)$, $s_{12} = (1\ 0)$, $s_{21} = (1\ 0)$, $s_{22} = (0\ 1)$. Bila persamaan terpenuhi, kedua nilai disimpan.
d. Perhitungan dilanjutkan dengan mencoba koefisien pada peubah x^2 dengan konstanta dan koefisien x diambil dari langkah lebelumnya, misal nilai yang diuji adalah $s_{11} = (1\ 1\ 0), s_{12} = (1\ 1\ 1), s_{21} = (1\ 0\ 0)$, dan $s_{22} = (0\ 1\ 0)$.
e. Perhitungan dilanjutkan dengan mencoba koefisien pada peubah dengan derajat yang besar sampai pada derajat maksimal, yaitu derajat n.

Proses perhitungan ini akan membuat sebuah *tree* yang bercabang maksimal sebanyak 16 (sesuai dengan banyaknya kombinasi kemungkinan koefisien tiap derajat yang dihitung, yaitu $2^4 = 16$), yang bila cabang-cabang tersebut tidak terlalu melebar (dalam artian jumlah cabangnya sedikit), diharapkan setelah selesai penghitungan pada derajat dengan derajat tertinggi, sistem persamaan tersebut dapat diselesaikan. Matriks dari hasil pencarian tersebut bisa jadi tidak sama dengan matriks s, namun kunci tersebut dianggap cukup untuk mewakili s.

Shpilrain dan Ushakov melakukan eksperimen dengan metode ini sebanyak lebih dari 1000 kali dengan parameter $n = 300$ dan menghabiskan waktu sebanyak dua minggu. Setiap kali melakukan eksperimen, hasil dari persamaan yang mungkin adalah maksimal sebanyak 16.384 buah. Dengan kata lain, ada 16.384 kunci yang mungkin. Namun dari semua kunci ini, tidak ada kunci yang sama persis dengan matriks kunci s. Dengan demikian, persentase keberhasilan dari pemecahan dengan metode ini adalah 0%.

BAB IV
PENUTUP

4.1 Kesimpulan

Kriptografi merupakan studi tentang teknik matematis berkaitan dengan aspek keamanan informasi. Kriptografi secara umum dibagi menjadi dua, yaitu kriptografi simetris dan kriptografi asimetris atau kunci publik. Penggunaan kriptografi kunci publik membiarkan seseorang menyebarkan kunci publik namun masih menyimpan kunci privat sendiri. Teori grup dapat digunakan pada sistem kriptografi kunci publik. Salah satu aspek yang dapat digunakan adalah adanya pencarian konjugasi pada teori grup. Dengan melakukan perluasan dari pencarian konjugasi, didapatkan konjugasi *twisted* dan konjugasi *twisted* ganda. Penggunaan pencarian konjugasi *twisted* ganda dan matriks polinomial sebagai semigrup yang digunakan menghasilkan skema autentikasi dan pertukaran kunci. Dengan paremeter yang cukup besar, skema ini dapat bertahan dari serangan *brute force* dan penyelesaian analitik dengan menyelesaikan suku awal.

4.2 Saran

Selain kedua metode kriptanalisis yang dipaparkan pada skripsi ini, perlu dipelajari lebih lanjut metode lain untuk memecahkan metode ini. Selain itu, diharapkan pada pengkajian selanjutnya, orde matriks yang digunakan lebih besar.

DAFTAR PUSTAKA

Bhattacharya, P.B., dkk. 1994. *Basic Abstract Algebra Second Edition.* Cambridge University Press. Australia.

Cameron, Peter J.. 2008. *Introduction to Algebra*. Oxford University Press. New York.

Diffie, Whitfield dan Martin E. Hellman. 1976. *New Directions in Cryptography*. Hal 644-647.

Dummit, David S. dan Foote, Richard M. *Abstract Algebra*. Prentice-Hall, Inc. USA.

Durbin, John R.. 1992. *Modern Algebra Sixth Edition: An Introduction.* John Wiley & Sons, Inc. USA.

Fraleigh, John B.. 1994. *A First Course in Abstract Algebra 5th Edition.* Addison-Wesley Publishing Company. USA.

Garber, David. 2009. *Braid Group Cryptography*. World Scientific Review hal 22.

Grillet, Pierre Antoine. 2000. *Abstract Algebra Second Edition*. Springer. USA.

Information Resources Management Association (IRMA). 2014. *Crisis Management: Concepts, Methodologies, Tools and Applications.* IGI Global. USA.

Ko, K., J. Birdman, dan S. Lee. 1998. *A New Approach to the Word Problem in the Braid Group.* Adv Math 139. Hal 322-353.

Koblitz, Neal. 1999. *Algebraic Aspect of Cryptography.* Springer. New York.

Menezes, Alfred J., Paul C. van Oorschot, dan Scott A. Vanstone. 1996. *Handbook of Applied Cryptography*. MIT Press. USA.

Mollin, Richard A.. 2007. *An Introduction to Cryptography 2nd Edition.* Taylor & Francis Group. USA.

Paar, Christof dan Jan Pelzl. 2010. *Understanding Cryptography: A Textbook for Students and Practitioners.* Springer. New York.

Shpilrain, Vladimir dan Alexander Ushakov. 2008. *An Authentication Scheme Based on the Twisted Conjugacy Problem.* Hal 1-6.

Shpilrain, Vladimir, Alexander Usakov, dan Alexei Myasnikov. 2007. *Group Based Cryptography*. Lecture notes for the Advanced Course of Group-Based Cryptography. New York.

Stinson, Douglas R.. 2006. *Crptography: Theory and Practice 6th Edition*. Taylor & Francis Group. USA.

Tim Penulis. 2010. *Encyclopædia Britannica 15th Edition*. Encyclopædia Britannica Inc. USA.

Wisbauer, Robert. 1991. *Foundation of Module and Ring Theory.* Gordon and Breach Science Publisher. USA.

LAMPIRAN

Lampiran 1: Perhitungan Contoh Protokol Autentikasi

Nilai awal:

$$w = \begin{pmatrix} 1\,0\,0\,1\,1 & 1\,0\,1\,0\,0 \\ 0\,1\,0\,0\,1 & 1\,0\,1\,0\,1 \end{pmatrix}$$
$$s = \begin{pmatrix} 1\,0\,0\,1\,1 & 1\,0\,1\,0\,1 \\ 1\,0\,0\,0\,1 & 1\,0\,1\,1\,1 \end{pmatrix}$$
$$r = \begin{pmatrix} 1\,0\,0\,1\,1 & 1\,0\,1\,1\,1 \\ 1\,1\,0\,0\,1 & 1\,1\,1\,0\,0 \end{pmatrix}$$
$$p(x) = x^2 + x^3 = (0\,0\,1\,1\,0)$$
$$q(x) = x + x^2 + x^4 = (0\,1\,1\,0\,1)$$
$$s^* = s^T = \begin{pmatrix} 1\,0\,0\,1\,1 & 1\,0\,0\,0\,1 \\ 1\,0\,1\,0\,1 & 1\,0\,1\,1\,1 \end{pmatrix}$$

a. Mencari nilai $\varphi(s^*)$

$$\theta_p(s_{11}^*) = \theta_p(1\,0\,0\,1\,1) = \theta_p(1 + x^3 + x^4)$$
$$= 1 + (x^2 + x^3)^3 + (x^2 + x^3)^4 \; mod\; x^5$$
$$= 1 = (1\,0\,0\,0\,0)$$
$$\theta_p(s_{12}^*) = \theta_p(1\,0\,0\,0\,1) = \theta_p(1 + x^4)$$
$$= 1 + (x^2 + x^4)^4 \; mod\; x^5$$
$$= 1 = (1\,0\,0\,0\,0)$$
$$\theta_p(s_{21}^*) = \theta_p(1\,0\,1\,0\,1) = \theta_p(1 + x^2 + x^4)$$
$$= 1 + (x^2 + x^3)^2 + (x^2 + x^3)^4 \; mod\; x^5$$
$$= 1 + x^4 = (1\,0\,0\,0\,1)$$
$$\theta_p(s_{22}^*) = \theta_p(1\,0\,1\,1\,1) = \theta_p(1 + x^2 + x^3 + x^4)$$
$$= 1 + (x^2 + x^3)^2 + (x^2 + x^3)^3 + (x^2 + x^3)^4 \; mod\; x^5$$
$$= 1 + x^4 = (1\,0\,0\,0\,1)$$

Dengan demikian

$$\varphi(s^*) = \begin{pmatrix} \theta_p(s_{11}^*) & \theta_p(s_{12}^*) \\ \theta_p(s_{21}^*) & \theta_p(s_{22}^*) \end{pmatrix} = \begin{pmatrix} 1\,0\,0\,0\,0 & 1\,0\,0\,0\,0 \\ 1\,0\,0\,0\,1 & 1\,0\,0\,0\,1 \end{pmatrix}$$

b. Mencari nilai $\psi(s)$

$$\theta_q(s_{11}) = \theta_q(1\,0\,0\,1\,1) = \theta_q(1 + x^3 + x^4)$$
$$= 1 + (x + x^2 + x^4)^3 + (x + x^2 + x^4)^4 \; mod\; x^5$$
$$= 1 + (x^3 + x^4) + (x^4) = 1 + x^3 = (1\,0\,0\,1\,0)$$
$$\theta_q(s_{12}) = \theta_q(1\,0\,1\,0\,1) = \theta_q(1 + x^2 + x^4)$$
$$= 1 + (x + x^2 + x^4)^2 + (x + x^2 + x^4)^4 \; mod\; x^5$$

$$= 1 + (x^2 + x^4) + (x^4) = 1 + x^2 = (1\,0\,1\,0\,0)$$

$$\theta_q(s_{21}) = \theta_q(1\,0\,0\,0\,1) = \theta_q(1 + x^4)$$
$$= 1 + (x + x^2 + x^4)^4 \; mod \; x^5$$
$$= 1 + x^4 = (1\,0\,0\,0\,1)$$

$$\theta_q(s_{22}) = \theta_q(1\,0\,1\,1\,1) = \theta_q(1 + x^2 + x^3 + x^4)$$
$$= 1 + (x + x^2 + x^4)^2 + (x + x^2 + x^4)^3 + (x + x^2 + x^4)^4 \; mod \; x^5$$
$$= 1 + (x^2 + x^4) + (x^3 + x^4) + (x^4)$$
$$= 1 + x^2 + x^3 + x^4 = (1\,0\,1\,1\,1)$$

Dengan demikian

$$\psi(s) = \begin{pmatrix} \theta_q(s_{11}) & \theta_q(s_{12}) \\ \theta_q(s_{21}) & \theta_q(s_{22}) \end{pmatrix} = \begin{pmatrix} 1\,0\,0\,1\,0 & 1\,0\,1\,0\,0 \\ 1\,0\,0\,0\,1 & 1\,0\,1\,1\,1 \end{pmatrix}$$

c. Mencari nilai $t = \varphi(s^*)w\psi(s)$

$$t = \varphi(s^*)w\psi(s)$$
$$= \underbrace{\begin{pmatrix} 1\,0\,0\,0\,0 & 1\,0\,0\,0\,0 \\ 1\,0\,0\,0\,1 & 1\,0\,0\,0\,1 \end{pmatrix}\begin{pmatrix} 1\,0\,0\,1\,1 & 1\,0\,1\,0\,0 \\ 0\,1\,0\,0\,1 & 1\,0\,1\,0\,1 \end{pmatrix}}_{\text{dihitung terlebih dahulu}}\begin{pmatrix} 1\,0\,0\,1\,0 & 1\,0\,1\,0\,0 \\ 1\,0\,0\,0\,1 & 1\,0\,1\,1\,1 \end{pmatrix}$$
$$= \begin{pmatrix} 1\,1\,0\,1\,0 & 0\,0\,0\,0\,1 \\ 1\,1\,0\,1\,1 & 0\,0\,0\,0\,1 \end{pmatrix}\begin{pmatrix} 1\,0\,0\,1\,0 & 1\,0\,1\,0\,0 \\ 1\,0\,0\,0\,1 & 1\,0\,1\,1\,1 \end{pmatrix}$$
$$= \begin{pmatrix} 1\,1\,0\,0\,0 & 1\,1\,1\,0\,1 \\ 1\,1\,0\,0\,1 & 1\,1\,1\,0\,0 \end{pmatrix}$$

d. Menghitung nilai $u = \varphi(r^*)t\psi(r)$

$$u = \varphi(r^*)t\psi(r)$$
$$= \begin{pmatrix} 1\,0\,0\,0\,0 & 1\,0\,1\,1\,0 \\ 1\,0\,0\,0\,1 & 1\,0\,1\,1\,1 \end{pmatrix}\begin{pmatrix} 1\,1\,0\,0\,0 & 1\,1\,1\,0\,1 \\ 1\,1\,0\,0\,1 & 1\,1\,1\,0\,0 \end{pmatrix}\begin{pmatrix} 1\,0\,0\,1\,0 & 1\,0\,1\,1\,1 \\ 1\,1\,1\,0\,0 & 1\,1\,0\,0\,0 \end{pmatrix}$$
$$= \begin{pmatrix} 0\,0\,1\,0\,0 & 0\,0\,1\,0\,1 \\ 0\,0\,1\,0\,0 & 0\,0\,1\,0\,1 \end{pmatrix}\begin{pmatrix} 1\,0\,0\,1\,0 & 1\,0\,1\,1\,1 \\ 1\,1\,1\,0\,0 & 1\,1\,0\,0\,0 \end{pmatrix}$$
$$= \begin{pmatrix} 0\,0\,0\,1\,0 & 0\,0\,0\,1\,0 \\ 0\,0\,0\,1\,0 & 0\,0\,0\,1\,0 \end{pmatrix}$$

e. Autentikasi untuk kasus $c = 0$

$v = r$ dan

$$\varphi(v^*)t\psi(v)$$
$$= \begin{pmatrix} 1\,0\,0\,0\,0 & 1\,0\,1\,1\,0 \\ 1\,0\,0\,0\,1 & 1\,0\,1\,1\,1 \end{pmatrix}\begin{pmatrix} 1\,1\,0\,0\,0 & 1\,1\,1\,0\,1 \\ 1\,1\,0\,0\,1 & 1\,1\,1\,0\,0 \end{pmatrix}\begin{pmatrix} 1\,0\,0\,1\,0 & 1\,0\,1\,1\,1 \\ 1\,1\,1\,0\,0 & 1\,1\,0\,0\,0 \end{pmatrix}$$
$$= \begin{pmatrix} 0\,0\,1\,0\,0 & 0\,0\,1\,0\,1 \\ 0\,0\,1\,0\,0 & 0\,0\,1\,0\,1 \end{pmatrix}\begin{pmatrix} 1\,0\,0\,1\,0 & 1\,0\,1\,1\,1 \\ 1\,1\,1\,0\,0 & 1\,1\,0\,0\,0 \end{pmatrix}$$

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

f. Autentikasi untuk kasus $c = 1$

$$v = sr = \begin{pmatrix} 1\,0\,0\,1\,1 & 1\,0\,1\,0\,1 \\ 1\,0\,0\,0\,1 & 1\,0\,1\,1\,1 \end{pmatrix} \begin{pmatrix} 1\,0\,0\,1\,1 & 1\,0\,1\,1\,1 \\ 1\,1\,0\,0\,1 & 1\,1\,1\,0\,0 \end{pmatrix}$$

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

$$\varphi(v^*) w \psi(v^*)$$

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

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

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

Lampiran 2: Perhitungan Contoh Protokol Pertukaran Kunci

Nilai awal:

$$a = \begin{pmatrix} 1\,0\,0\,1\,1 & 0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0 & 1\,1\,0\,1\,1 \end{pmatrix}$$
$$b = \begin{pmatrix} 1\,1\,1\,0\,0 & 0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0 & 1\,1\,1\,0\,1 \end{pmatrix}$$
$$w = \begin{pmatrix} 1\,1\,0\,0\,1 & 0\,1\,1\,0\,1 \\ 1\,0\,0\,1\,1 & 1\,0\,1\,0\,1 \end{pmatrix}$$
$$p(x) = x^2 + x^3 + x^4 = (0\,0\,1\,1\,1)$$
$$q(x) = x + x^2 + x^4 = (0\,1\,1\,0\,1)$$

a. Mencari $\varphi(a^*)$

$$\theta_p(a_{11}^*) = \theta_p(1\,0\,0\,1\,1) = \theta_p(1 + x^3 + x^4)$$
$$= 1 + (x^2 + x^3 + x^4)^3 + (x^2 + x^3 + x^4)^4 \; mod\; x^5$$
$$= 1 + x^4 = (1\,0\,0\,0\,1)$$
$$\theta_p(a_{12}^*) = \theta_p(0) = 0 = (0\,0\,0\,0\,0)$$
$$\theta_p(a_{21}^*) = \theta_p(0) = 0 = (0\,0\,0\,0\,0)$$
$$\theta_p(a_{22}^*) = \theta_p(1\,1\,0\,1\,1) = \theta_p(1 + x + x^3 + x^4)$$
$$= 1 + (x^2 + x^3 + x^4) + (x^2 + x^3 + x^4)^3 + (x^2 + x^3 + x^4)^4 \; mod\; x^5$$
$$= 1 + (x^2 + x^3 + x^4) = (1\,0\,1\,1\,1)$$

Dengan demikian

$$\varphi(a^*) = \begin{pmatrix} \theta_p(a_{11}^*) & \theta_p(a_{12}^*) \\ \theta_p(a_{21}^*) & \theta_p(a_{22}^*) \end{pmatrix} = \begin{pmatrix} 1\,0\,0\,0\,1 & 0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0 & 1\,0\,1\,1\,1 \end{pmatrix}$$

b. Mencari $\psi(a)$

$$\theta_q(a_{11}) = \theta_q(1\,0\,0\,1\,1) = \theta_q(1 + x^3 + x^4)$$
$$= 1 + (x + x^2 + x^4)^3 + (x + x^2 + x^4)^4 \; mod\; x^5$$
$$= 1 + (x^3 + x^4) + x^4 = 1 + x^3 = (1\,0\,0\,1\,0)$$
$$\theta_q(a_{12}) = \theta_q(0) = 0 = (0\,0\,0\,0\,0)$$
$$\theta_q(a_{21}) = \theta_q(0) = 0 = (0\,0\,0\,0\,0)$$
$$\theta_q(a_{22}) = \theta_q(1\,1\,0\,1\,1) = \theta_q(1 + x + x^3 + x^4)$$
$$= 1 + (x + x^2 + x^4) + (x + x^2 + x^4)^3 + (x + x^2 + x^4)^4 \; mod\; x^5$$

$$= 1 + (x + x^2 + x^4) + (x^3 + x^4) + x^4$$
$$= 1 + x + x^2 + x^3 + x^4 = (1\ 1\ 1\ 1\ 1)$$

Dengan demikian

$$\psi(a) = \begin{pmatrix} \theta_q(a_{11}) & \theta_q(a_{12}) \\ \theta_q(a_{21}) & \theta_q(a_{22}) \end{pmatrix} = \begin{pmatrix} 1\ 0\ 0\ 1\ 0 & 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0 & 1\ 1\ 1\ 1\ 1 \end{pmatrix}$$

c. Mencari $\varphi(b^*)$

$$\theta_p(b_{11}^*) = \theta_p(1\ 1\ 1\ 0\ 0) = \theta_p(1 + x + x^2)$$
$$= 1 + (x^2 + x^3 + x^4) + (x^2 + x^3 + x^4)^2 \ mod\ x^5$$
$$= 1 + (x^2 + x^3 + x^4) + x^4$$
$$= 1 + x^2 + x^3 = (1\ 0\ 1\ 1\ 0)$$
$$\theta_p(b_{12}^*) = \theta_p(0) = 0 = (0\ 0\ 0\ 0\ 0)$$
$$\theta_p(b_{21}^*) = \theta_p(0) = 0 = (0\ 0\ 0\ 0\ 0)$$
$$\theta_p(b_{22}^*) = \theta_p(1\ 1\ 1\ 0\ 1) = \theta_p(1 + x + x^2 + x^4)$$
$$= 1 + (x^2 + x^3 + x^4) + (x^2 + x^3 + x^4)^2$$
$$+ (x^2 + x^3 + x^4)^4 \ mod\ x^5$$
$$= 1 + (x^2 + x^3 + x^4) + x^4 = (1\ 0\ 1\ 1\ 0)$$

Dengan demikian

$$\varphi(b^*) = \begin{pmatrix} \theta_p(b_{11}^*) & \theta_p(b_{12}^*) \\ \theta_p(b_{21}^*) & \theta_p(b_{22}^*) \end{pmatrix} = \begin{pmatrix} 1\ 0\ 1\ 1\ 0 & 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0 & 1\ 0\ 1\ 1\ 0 \end{pmatrix}$$

d. Mencari $\psi(b)$

$$\theta_q(b_{11}) = \theta_q(1\ 1\ 1\ 0\ 0) = \theta_q(1 + x + x^2)$$
$$= 1 + (x + x^2 + x^4) + (x + x^2 + x^4)^2 \ mod\ x^5$$
$$= 1 + (x + x^2 + x^4) + (x^2 + x^4)$$
$$= 1 + x = (1\ 1\ 0\ 0\ 0)$$
$$\theta_q(b_{12}) = \theta_q(0) = 0 = (0\ 0\ 0\ 0\ 0)$$
$$\theta_q(b_{21}) = \theta_q(0) = 0 = (0\ 0\ 0\ 0\ 0)$$

$$\theta_q(b_{22}) = \theta_q(1\ 1\ 1\ 0\ 1) = \theta_q(1 + x + x^2 + x^4)$$
$$= 1 + (x + x^2 + x^4) + (x + x^2 + x^4)^2 + (x + x^2 + x^4)^4 \ mod\ x^5$$
$$= 1 + (x + x^2 + x^4) + (x^2 + x^4) + x^4$$
$$= 1 + x + x^4 = (1\ 1\ 0\ 0\ 1)$$

Dengan demikian

$$\psi(b) = \begin{pmatrix} \theta_q(b_{11}) & \theta_q(b_{12}) \\ \theta_q(b_{21}) & \theta_q(b_{22}) \end{pmatrix} = \begin{pmatrix} 1\ 1\ 0\ 0\ 0 & 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0 & 1\ 1\ 0\ 0\ 1 \end{pmatrix}$$

e. Penghitungan $t = \varphi(a^*)w\psi(a)$

$$t = \varphi(a^*)w\psi(a)$$
$$= \begin{pmatrix} 1\ 0\ 0\ 0\ 1 & 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0 & 1\ 0\ 1\ 1\ 1 \end{pmatrix} \begin{pmatrix} 1\ 1\ 0\ 0\ 1 & 0\ 1\ 1\ 0\ 1 \\ 1\ 0\ 0\ 1\ 1 & 1\ 0\ 1\ 0\ 1 \end{pmatrix} \begin{pmatrix} 1\ 0\ 0\ 1\ 0 & 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0 & 1\ 1\ 1\ 1\ 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1\ 1\ 0\ 0\ 1 & 0\ 1\ 1\ 0\ 1 \\ 1\ 0\ 1\ 0\ 0 & 1\ 0\ 0\ 1\ 1 \end{pmatrix} \begin{pmatrix} 1\ 0\ 0\ 1\ 0 & 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0 & 1\ 1\ 1\ 1\ 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1\ 1\ 0\ 1\ 0 & 0\ 1\ 0\ 0\ 1 \\ 1\ 0\ 1\ 1\ 0 & 1\ 1\ 1\ 0\ 1 \end{pmatrix}$$

f. Penghitungan $u = \varphi(b^*)w\psi(b)$

$$u = \varphi(b^*)w\psi(b)$$
$$= \begin{pmatrix} 1\ 0\ 1\ 1\ 0 & 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0 & 1\ 0\ 1\ 1\ 0 \end{pmatrix} \begin{pmatrix} 1\ 1\ 0\ 0\ 1 & 0\ 1\ 1\ 0\ 1 \\ 1\ 0\ 0\ 1\ 1 & 1\ 0\ 1\ 0\ 1 \end{pmatrix} \begin{pmatrix} 1\ 1\ 0\ 0\ 0 & 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0 & 1\ 1\ 0\ 0\ 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1\ 1\ 1\ 0\ 0 & 0\ 1\ 1\ 1\ 1 \\ 1\ 0\ 1\ 0\ 1 & 1\ 0\ 0\ 1\ 0 \end{pmatrix} \begin{pmatrix} 1\ 1\ 0\ 0\ 0 & 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0 & 1\ 1\ 0\ 0\ 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1\ 0\ 0\ 1\ 0 & 0\ 1\ 0\ 0\ 0 \\ 1\ 1\ 1\ 1\ 1 & 1\ 1\ 0\ 1\ 0 \end{pmatrix}$$

g. Penghitungan nilai k_1

$$k_1 = \varphi(a^*)u\psi(a)$$
$$= \begin{pmatrix} 1\ 0\ 0\ 0\ 1 & 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0 & 1\ 0\ 1\ 1\ 1 \end{pmatrix} \begin{pmatrix} 1\ 0\ 0\ 1\ 0 & 0\ 1\ 0\ 0\ 0 \\ 1\ 1\ 1\ 1\ 1 & 1\ 1\ 0\ 1\ 0 \end{pmatrix} \begin{pmatrix} 1\ 0\ 0\ 1\ 0 & 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0 & 1\ 1\ 1\ 1\ 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1\ 0\ 0\ 1\ 0 & 0\ 1\ 0\ 0\ 0 \\ 1\ 1\ 0\ 1\ 0 & 1\ 1\ 1\ 1\ 0 \end{pmatrix} \begin{pmatrix} 1\ 0\ 0\ 1\ 0 & 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0 & 1\ 1\ 1\ 1\ 1 \end{pmatrix}$$

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

h. Penghitungan nilai k_2

$$k_2 = \varphi(b^*)t\psi(b)$$
$$= \begin{pmatrix} 1\,0\,1\,1\,0 & 0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0 & 1\,0\,1\,1\,0 \end{pmatrix} \begin{pmatrix} 1\,1\,0\,1\,0 & 0\,1\,0\,0\,1 \\ 1\,0\,1\,1\,0 & 1\,1\,1\,0\,1 \end{pmatrix} \begin{pmatrix} 1\,1\,0\,0\,0 & 0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0 & 1\,1\,0\,0\,1 \end{pmatrix}$$
$$= \begin{pmatrix} 1\,1\,1\,1\,1 & 0\,1\,0\,1\,0 \\ 1\,0\,0\,0\,1 & 1\,1\,0\,0\,1 \end{pmatrix} \begin{pmatrix} 1\,1\,0\,0\,0 & 0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0 & 1\,1\,0\,0\,1 \end{pmatrix}$$
$$= \begin{pmatrix} 1\,0\,0\,0\,0 & 0\,1\,1\,1\,1 \\ 1\,1\,0\,0\,1 & 1\,0\,1\,0\,0 \end{pmatrix}$$

Lampiran 3. *Listing* Program Utama

Program utama untuk skema autentikasi dengan nama file *pautentikasi.m*

```
%input matriks
s11=[1 0 0 1 1];s12=[1 0 1 0 1];
s21=[1 0 0 0 1];s22=[1 0 1 1 1];

w11=[1 0 0 1 1];w12=[1 0 1 0 0];
w21=[0 1 0 0 1];w22=[1 0 1 0 1];

vpi=[0 0 1 1 0];psi=[0 1 1 0 1];
%transpos matriks s ke st;
st11=s11;st12=s21;st21=s12;st22=s22;
%penghitungan endomorfisma
k11=endomo2(st11,vpi);k12=endomo2(st12,vpi);
k21=endomo2(st21,vpi);k22=endomo2(st22,vpi);

l11=endomo2(s11,psi);l12=endomo2(s12,psi);
l21=endomo2(s21,psi);l22=endomo2(s22,psi);
%pencarian nilai t
[p11,p12,p21,p22]=kalimatriks(k11,k12,k21,k22,w11,w12
,w21,w22);
[t11,t12,t21,t22]=kalimatriks(p11,p12,p21,p22,l11,l12
,l21,l22);



%nilai acak r
r11=[1 0 0 1 1];r12=[1 0 1 1 1];
r21=[1 1 0 0 1];r22=[1 1 1 0 0];
%nilai endomorfisma pada r
vr11=endomo2(r11,vpi);vr12=endomo2(r21,vpi);
vr21=endomo2(r12,vpi);vr22=endomo2(r22,vpi);

pr11=endomo2(r11,psi);pr12=endomo2(r12,psi);
pr21=endomo2(r21,psi);pr22=endomo2(r22,psi);
%nilai u
[q11,q12,q21,q22]=kalimatriks(vr11,vr12,vr21,vr22,t11
,t12,t21,t22);
[u11,u12,u21,u22]=kalimatriks(q11,q12,q21,q22,pr11,pr
12,pr21,pr22);

%1. KASUS C=0
```

```
v1_11=r11;v1_12=r12;v1_21=r21;v1_22=r22;
%endomorfisma
vv11=endomo2(v1_11,vpi);vv12=endomo2(v1_21,vpi);
vv21=endomo2(v1_12,vpi);vv22=endomo2(v1_22,vpi);

vp11=endomo2(v1_11,psi);vp12=endomo2(v1_12,psi);
vp21=endomo2(v1_21,psi);vp22=endomo2(v1_22,psi);
%hasil kali
[z1,z2,z3,z4]=kalimatriks(vv11,vv12,vv21,vv22,t11,t12
,t21,t22);
[ua11,ua12,ua21,ua22]=kalimatriks(z1,z2,z3,z4,vp11,vp
12,vp21,vp22);

%2. KASUS C=1
[v2_11,v2_12,v2_21,v2_22]=kalimatriks(s11,s12,s21,s22
,r11,r12,r21,r22);
%endomorfisma
vv11=endomo2(v2_11,vpi);vv12=endomo2(v2_21,vpi);
vv21=endomo2(v2_12,vpi);vv22=endomo2(v2_22,vpi);

vp11=endomo2(v2_11,psi);vp12=endomo2(v2_12,psi);
vp21=endomo2(v2_21,psi);vp22=endomo2(v2_22,psi);
%hasil kali
[z1,z2,z3,z4]=kalimatriks(vv11,vv12,vv21,vv22,w11,w12
,w21,w22);
[ub11,ub12,ub21,ub22]=kalimatriks(z1,z2,z3,z4,vp11,vp
12,vp21,vp22);

%cek hasil
if (u11==ua11)&(u12==ua12)&(u21==ua21)&(u22==ua22)
    disp('Autentikasi dengan kondisi c=0 diterima')
end
if (u11==ub11)&(u12==ub12)&(u21==ub21)&(u22==ub22)
    disp('Autentikasi dengan kondisi c=1 diterima')
end
```

Program utama pertukaran kunci dengan nama file *pkunci.m*

```
%input matriks
a11=[1 0 0 1 1];a12=[0 0 0 0 0];
a21=[0 0 0 0 0];a22=[1 1 0 1 1];

b11=[1 1 1 0 0];b12=[0 0 0 0 0];
b21=[0 0 0 0 0];b22=[1 1 1 0 1];

w11=[1 1 0 0 1];w12=[0 1 1 0 1];
w21=[1 0 0 1 1];w22=[1 0 1 0 1];

vpi=[0 0 1 1 1];psi=[0 1 1 0 1];
%penghitungan endomorfisma
va11=endomo2(a11,vpi);va12=endomo2(a12,vpi);
va21=endomo2(a21,vpi);va22=endomo2(a22,vpi);

pa11=endomo2(a11,psi);pa12=endomo2(a12,psi);
pa21=endomo2(a21,psi);pa22=endomo2(a22,psi);

vb11=endomo2(b11,vpi);vb12=endomo2(b12,vpi);
vb21=endomo2(b21,vpi);vb22=endomo2(b22,vpi);

pb11=endomo2(b11,psi);pb12=endomo2(b12,psi);
pb21=endomo2(b21,psi);pb22=endomo2(b22,psi);
%penghitungan u dan t
[r11,r12,r21,r22]=kalimatriks(va11,va12,va21,va22,w11
,w12,w21,w22);
[t11,t12,t21,t22]=kalimatriks(r11,r12,r21,r22,pa11,pa
12,pa21,pa22);

[s11,s12,s21,s22]=kalimatriks(vb11,vb12,vb21,vb22,w11
,w12,w21,w22);
[u11,u12,u21,u22]=kalimatriks(s11,s12,s21,s22,pb11,pb
12,pb21,pb22);

%penghitungan nilai y=k1 dan z=k2
[c1,c2,c3,c4]=kalimatriks(va11,va12,va21,va22,u11,u12
,u21,u22);
[y11,y12,y21,y22]=kalimatriks(c1,c2,c3,c4,pa11,pa12,p
a21,pa22);
```

```
[d1,d2,d3,d4]=kalimatriks(vb11,vb12,vb21,vb22,t11,t12
,t21,t22);
[z11,z12,z21,z22]=kalimatriks(d1,d2,d3,d4,pb11,pb12,p
b21,pb22);

%hitung hasil
if (y11==z11)&(y12==z12)&(y21==z21)&(y22==z22)
    disp('Nilai k1 dan k2 sama, pertukaran kunci
berhasil')
end
```

Lampiran 4. *Listing* Program Pendukung

Program ini digunakan untuk mempermudah penghitungan dalam program utama, antara lain:

Program penghitungan matriks dengan nama *kalimatriks.m*

```
function [h11,h12,h21,h22] =
kalimatriks(a11,a12,a21,a22,b11,b12,b21,b22);
%penghitungan elemen
h11=gfadd(gfconv(a11,b11,2),gfconv(a12,b21,2),2);
h12=gfadd(gfconv(a11,b12,2),gfconv(a12,b22,2),2);
h21=gfadd(gfconv(a21,b11,2),gfconv(a22,b21,2),2);
h22=gfadd(gfconv(a21,b12,2),gfconv(a22,b22,2),2);
%pemotongan matriks
k=length(a11);
h11=fitmat(h11,k);
h12=fitmat(h12,k);
h21=fitmat(h21,k);
h22=fitmat(h22,k);
%k=length(a11)+1;
%l=length(h11);
%for i=k:l
%    h11(k)=[];h12(k)=[];h21(k)=[];h22(k)=[];
%end
end
```

Program penghitungan endomorfisma dengan nama file *endomo.m*

```
function blab = endomo2(a,b)
blab=a(1);
for i=2:length(a)
    k=1;
    if a(i)==1
       for j=1:i-1
          k=gfconv(k,b,2);
       end
    blab=gfadd(blab,k,2);
    end
end
blab=fitmat(blab,length(a));
end
```

Program pemotongan polinomial (agar polinomial ditulis menjadi vektor dengan panjang yang sama) disimpan dengan nama file *fitmat.m*

```
function matmat = fitmat(matriks,dimensi)

matmat=matriks;
s = dimensi;
if length(matriks)>s
    matmat=matriks(1:s);
end
if length(matriks)<s
    for i=length(matriks)+1:s
        matmat(i)=0;
    end
end
end
```

Lampiran 5. *Listing* Program Utama 2

Program Utama 2 secara umum sama dengan program utama, namun dengan nilai-nilai variabel yang berbeda dan lebih panjang.

Program utama 2 untuk autentikasi disimpan dengan nama *autentikasipanjang.m*

```
%input matriks
s11=[1 0 0 1 1 1 0 1 1 0 1 0 1 1 0];
s12=[1 0 1 0 1 0 1 0 1 1 1 0 0 0 1];
s21=[1 0 0 0 1 1 0 0 0 0 1 1 1 0 1];
s22=[1 0 1 1 0 1 0 1 1 1 0 1 0 0 1];

w11=[1 0 0 1 1 0 1 0 0 0 1 1 0 1 1];
w12=[1 0 1 0 0 0 1 0 0 1 0 1 1 1 1];
w21=[0 1 0 0 1 1 0 0 1 0 0 1 1 1 0];
w22=[1 0 1 0 1 1 0 0 1 0 0 1 1 1 0];

vpi=[0 0 1 1 0 1 0 1 0 1 1 1 1 0 0];
psi=[0 1 1 0 1 0 1 0 0 0 1 0 0 1 1];
%transpos matriks s ke st;
st11=s11;st12=s21;st21=s12;st22=s22;
%penghitungan endomorfisma
k11=endomo2(st11,vpi);k12=endomo2(st12,vpi);
k21=endomo2(st21,vpi);k22=endomo2(st22,vpi);

l11=endomo2(s11,psi);l12=endomo2(s12,psi);
l21=endomo2(s21,psi);l22=endomo2(s22,psi);
%pencarian nilai t
[p11,p12,p21,p22]=kalimatriks(k11,k12,k21,k22,w11,w12
,w21,w22);
[t11,t12,t21,t22]=kalimatriks(p11,p12,p21,p22,l11,l12
,l21,l22);


%nilai acak r
r11=[1 0 0 1 1 0 1 0 0 0 1 1 1 1 0];
r12=[1 0 1 1 1 0 0 1 1 0 0 0 0 1 1];
r21=[1 1 0 0 1 0 1 1 0 1 1 1 1 1 0];
r22=[1 1 1 0 0 0 1 1 1 0 0 1 1 0 0];
%nilai endomorfisma pada r
vr11=endomo2(r11,vpi);vr12=endomo2(r21,vpi);
```

```
vr21=endomo2(r12,vpi);vr22=endomo2(r22,vpi);

pr11=endomo2(r11,psi);pr12=endomo2(r12,psi);
pr21=endomo2(r21,psi);pr22=endomo2(r22,psi);
%nilai u
[q11,q12,q21,q22]=kalimatriks(vr11,vr12,vr21,vr22,t11
,t12,t21,t22);
[u11,u12,u21,u22]=kalimatriks(q11,q12,q21,q22,pr11,pr
12,pr21,pr22);

%1. KASUS C=0
v1_11=r11;v1_12=r12;v1_21=r21;v1_22=r22;
%endomorfisma
vv11=endomo2(v1_11,vpi);vv12=endomo2(v1_21,vpi);
vv21=endomo2(v1_12,vpi);vv22=endomo2(v1_22,vpi);

vp11=endomo2(v1_11,psi);vp12=endomo2(v1_12,psi);
vp21=endomo2(v1_21,psi);vp22=endomo2(v1_22,psi);
%hasil kali
[z1,z2,z3,z4]=kalimatriks(vv11,vv12,vv21,vv22,t11,t12
,t21,t22);
[ua11,ua12,ua21,ua22]=kalimatriks(z1,z2,z3,z4,vp11,vp
12,vp21,vp22);

%2. KASUS C=1
[v2_11,v2_12,v2_21,v2_22]=kalimatriks(s11,s12,s21,s22
,r11,r12,r21,r22);
%endomorfisma
vv11=endomo2(v2_11,vpi);vv12=endomo2(v2_21,vpi);
vv21=endomo2(v2_12,vpi);vv22=endomo2(v2_22,vpi);

vp11=endomo2(v2_11,psi);vp12=endomo2(v2_12,psi);
vp21=endomo2(v2_21,psi);vp22=endomo2(v2_22,psi);
%hasil kali
[z1,z2,z3,z4]=kalimatriks(vv11,vv12,vv21,vv22,w11,w12
,w21,w22);
[ub11,ub12,ub21,ub22]=kalimatriks(z1,z2,z3,z4,vp11,vp
12,vp21,vp22);

%cek hasil
if (u11==ua11)&(u12==ua12)&(u21==ua21)&(u22==ua22)
    disp('Autentikasi dengan kondisi c=0 diterima')
end
```

```
if (u11==ub11)&(u12==ub12)&(u21==ub21)&(u22==ub22)
    disp('Autentikasi dengan kondisi c=1 diterima')
end
```

Program utama 2 untuk pertukaran kunci disimpan dengan nama *pkuncipanjang.m*

```
%input matriks
a11=[1 0 0 1 1 1 0 0 1 1 0 1 0 0 1];
a12=[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0];
a21=[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0];
a22=[1 1 0 1 1 1 0 0 1 0 1 1 0 0 1];

b11=[1 1 1 0 0 1 0 1 1 0 0 0 1 1 1];
b12=[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0];
b21=[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0];
b22=[1 1 1 0 1 1 1 0 0 1 0 1 0 0 0];

w11=[1 1 0 0 1 0 1 1 0 0 1 0 1 1 1];
w12=[0 1 1 0 1 0 0 0 1 1 1 1 0 0 0];
w21=[1 0 0 1 1 1 1 1 0 0 1 1 0 0 1];
w22=[1 0 1 0 1 1 0 0 0 1 1 0 1 0 1];

vpi=[0 0 1 1 1 1 0 0 1 0 1 1 0 0 1];
psi=[0 1 1 0 1 1 1 0 0 0 1 1 1 1 0];
%penghitungan endomorfisma
va11=endomo2(a11,vpi);va12=endomo2(a12,vpi);
va21=endomo2(a21,vpi);va22=endomo2(a22,vpi);

pa11=endomo2(a11,psi);pa12=endomo2(a12,psi);
pa21=endomo2(a21,psi);pa22=endomo2(a22,psi);

vb11=endomo2(b11,vpi);vb12=endomo2(b12,vpi);
vb21=endomo2(b21,vpi);vb22=endomo2(b22,vpi);

pb11=endomo2(b11,psi);pb12=endomo2(b12,psi);
pb21=endomo2(b21,psi);pb22=endomo2(b22,psi);
%penghitungan u dan t
[r11,r12,r21,r22]=kalimatriks(va11,va12,va21,va22,w11
,w12,w21,w22);
[t11,t12,t21,t22]=kalimatriks(r11,r12,r21,r22,pa11,pa
12,pa21,pa22);
```

```
[s11,s12,s21,s22]=kalimatriks(vb11,vb12,vb21,vb22,w11
,w12,w21,w22);
[u11,u12,u21,u22]=kalimatriks(s11,s12,s21,s22,pb11,pb
12,pb21,pb22);

%penghitungan nilai y=k1 dan z=k2
[c1,c2,c3,c4]=kalimatriks(va11,va12,va21,va22,u11,u12
,u21,u22);
[y11,y12,y21,y22]=kalimatriks(c1,c2,c3,c4,pa11,pa12,p
a21,pa22);

[d1,d2,d3,d4]=kalimatriks(vb11,vb12,vb21,vb22,t11,t12
,t21,t22);
[z11,z12,z21,z22]=kalimatriks(d1,d2,d3,d4,pb11,pb12,p
b21,pb22);

%hitung hasil
if (y11==z11)&(y12==z12)&(y21==z21)&(y22==z22)
    disp('Nilai k1 dan k2 sama, pertukaran kunci
berhasil')
end
```