Aplikasi Teori Bilangan di Dalam Masalah Kriptografi

Yosafat Eka Prasetya Pangalela
10107075
Program Studi Matematika
Fakultas Matematika dan Ilmu Pengetahuan Alam
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
yosafat@students.itb.ac.id

ABSTRAK

Teori Bilangan adalah salah satu cabang dari matematika yang khusus mempelajari sifat-sifat dari bilangan bulat. Di matematika sendiri, bilangan bulat adalah salah satu bentuk paling sederhana di dalam kekompleksitas matematika itu sendiri. Oleh karena itu, mempelajari teori bilangan secara khusus dapat dikatakan mempelajari miniatur dari matematika. Sebagai *mother of science*, matematika adalah ilmu yang merupakan cikal bakal dari ilmu-ilmu lainnya. Oleh karena itu, tidak heran apabila aplikasi dari ilmu matematika itu sendiri dapat menyentuh setiap sisi dari kehidupan kita. Di sini saya akan memberikan aplikasi dari teori bilangan, sebagai salah satu cabang ilmu matematika, di dalam Kriptografi. Kriptografi sendiri adalah ilmu yang mempelajari tentang persandian.

Kata kunci: Teori Bilangan, Fungsi Euler, Kriptografi, Cipher.

I. PENDAHULUAN

Sekarang ini, perkembangan teknologi sudah sangat maju, sehingga pertukaran informasi yang terjadi di masyarakat sangatlah cepat. Tetapi tidak semua informasi yang kita berikan, boleh dibaca ataupun diketahui oleh orang lain. Oleh karena itu, terkadang kita menerapkan semacam trik di dalam penulisan informasi, sehingga orang-orang yang tidak mengerti trik tersebut tidak mengerti isi informasi yang kita buat. Walaupun begitu, terkadang terdapat beberapa orang yang dapat memecahkan trik yang kita buat, sehingga informasi yang kita rahasiakan dapat tersebar secara luas. Contoh yang paling sederhana dalam masalah ini adalah fenomena *WikiLeaks* dengan *cablegate* nya.

Di sini saya akan memberikan beberapa jenis trik terkenal di dalam persandian, mulai yang sederhana sampai yang membutuhkan ilmu teori bilangan yang cukup tinggi. Istilah-istilah yang digunakan dalam kriptografi adalah *plain teks* untuk menyatakan "kalimat yang hendak disamarkan", *cipher teks* untuk menyatakan "kalimat yang udah disamarkan", *kunci* untuk menyatakan "penentu metode yang digunakan", *enkripsi* untuk menyatakan "proses perubahan dari plain teks menjadi cipher teks", dan *dekripsi* untuk menyatakan "proses perubahan dari cipher teks menjadi plain teks". Perhatikan bahwa bila kita memiliki kunci yang tidak sama dengan yang dimiliki pemberi informasi, maka bukan tidak mungkin kalau hasil dekripsi kita menghasilkan kalimat yang tidak memiliki arti ataupun berbeda arti dengan maksud pemberi informasi.

Di kriptografi peranan dari kunci sangatlah penting. Apabila kunci dari cipher teks kita terlalu mudah, maka bukan tidak mungkin kalau ada orang lain yang tidak seharusnya mengetahui informasi kita, berhasil memecahkan kunci kita. Oleh karena itu, peranan teori bilangan di dalam membuat kunci dan memecahkan kunci di kriptografi sangatlah penting.

II. PEMBAHASAN

Saya akan membagi pembahasan ini menjadi dua bagian. Bagian pertama, saya akan memberikan pengetahuan-pengetahuan yang berguna tentang teori bilangan di dalam kriptografi. Dan di bagian kedua, saya akan memberikan berbagai macam cipher yang sering digunakan di dalam masalah persandian.

II.1 TEORI BILANGAN

Saya akan mengulas beberapa teorema tentang teori bilangan, khususnya pengetahuan teori bilangan yang dapat diaplikasikan ke dalam masalah kriptografi.

Pertama-tama saya akan memperkenalkan beberapa istilah yang sering digunakan di dalam ilmu teori bilangan. Modulo atau biasa disingkat mod adalah sisa pembagian. Contoh: $3\ (mod\ 2) = 1$, karena 3 dibagi 2 bersisa 1. Bila a dan b memiliki sisa pembagian yang sama ketika dibagi oleh c, kita notasikan $a \equiv b\ (mod\ c)$. Bila $gcd(a,b) = 1$, maka a memiliki invers di dalam $mod\ b$, dengan kata lain terdapat bilangan a^{-1} sehingga $aa^{-1} \equiv 1\ (mod\ b)$. Selanjutnya a^{-1}disebut invers dari a di dalam $mod\ b$. Bilangan a dan b disebut saling relatif prima jika $gcd(a,b) = 1$.

II.1.1 FUNGSI EULER

Fungsi Euler dari n adalah banyak bilangan dari I sampai n yang saling prima dengan n. Selanjutnya kita notasikan fungsi Euler dari n sebagai $\phi(n)$. Contoh: $\phi(3) = 2$ dan $\phi(4) = 2$. Perhatikan bahwa setiap bilangan memiliki sebuah bentuk faktorisasi prima (atau perkalian dari bilangan-bilangan prima), dan bentuk ini tunggal.

TEOREMA: Jika $n > 1$ dan $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ dimana $a_i \geq 1$ untuk setiap $i = 1,2,\dots,n$ dan $p_i \neq p_j$ bila $i \neq j$. Maka $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$.

BUKTI: Bila n adalah bilangan prima, maka setiap bilangan asli yang kurang dari n akan relatif prima dengan n. Akibatnya $\phi(n) = n - 1$. Selanjutnya, andaikan n bilangan komposit, tulis $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$.. Misal P_i adalah himpunan yang berisi bilangan dari 1 sampai n yang habis dibagi oleh p_i, untuk setiap $i = 1,2,\dots,k$. Maka $|Pi| = \frac{n}{p_i}$ untuk setiap i=1,2,...,k. Kita juga mengetahui bahwa bila S adalah subset tak kosong dari $\{1,2,\dots,k\}$,maka $|\cup_{i \in S} P_i| = n \prod_{i \in S} \frac{1}{p_i}$. Jadi dengan prinsip inklusi eksklusi kita memperoleh banyak bilangan dari 1 sampai n yang relatif prima dengan n adalah $n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$.

Perhatikan bahwa $\phi(n)$ adalah fungsi multiplikatif, degan kata lain, bila $gcd(m,n) = 1$, maka $\phi(mn) = \phi(m)\phi(n)$. Selanjutnya saya akan memberikan sebuah teorema yang mengaitkan antara fungsi Euler dengan invers di modulo n.

LEMMA [1]: Let $n > 1$ and $gcd(a,n) = 1$. Jika $a_1, a_2, \dots, a_{\phi(n)}$ adalah bilangan positif kurang dari n dan relatif prima terhadap n, maka $aa_1, aa_2, \dots, aa_{\phi(n)}$ akan kongruen dalam modulo n terhadap $a_1, a_2, \dots, a_{\phi(n)}$ di suatu pengaturan.

BUKTI: Andaikan ada i, j sehingga $aa_i \equiv aa_j \pmod n$, dengan $1 \leq i < j \leq \phi(n)$. Karena $gcd(a,n) = 1$, maka dengan hukum pencoretan, kita memperoleh $a_i \equiv a_j \pmod n$, atau $a_i = a_j$, kontradiksi. Jadi tidak ada 2 bilangan di antara $aa_1, aa_2, \dots, aa_{\phi(n)}$ yang saling kongruen di modulo n. Lebih jauh, karena $gcd(a_i,n) = 1$ untuk setiap i dan $gcd(a,n) = 1$, maka $gcd(aa_i,n) = 1$ (hal ini dikarenakan $\phi(n)$ adalah fungsi multiplikatif). Pilih indeks i tetap, maka ada b dimana $0 \leq b < n$ sehingga $aa_i \equiv b \pmod n$. Karena $gcd(b,n) = gcd(aa_i,n) = 1$, maka b harus salah satu dari bilangan $a_1, a_2, \dots, a_{\phi(n)}$. Kesimpulan mengikuti.

TEOREMA [1]: Jika $n \geq 1$ dan $gcd(a,n) = 1$, maka $a^{\phi(n)} \equiv 1 \pmod n$.

BUKTI: Kasus $n = 1$ trivial, jadi andaikan $n > 1$. Misal $a_1, a_2, \dots, a_{\phi(n)}$ adalah bilangan positif kurang dari n dan relatif prima terhadap n. Karena $gcd(a,n) = 1$, maka dari lemma kita bisa menyimpulkan bahwa $aa_1, aa_2, \dots, aa_{\phi(n)}$ akan kongruen dalam modulo n terhadap $a_1, a_2, \dots, a_{\phi(n)}$. Akibatnya

$$\begin{aligned} aa_1 &\equiv a_1' \pmod n \\ aa_2 &\equiv a_2' \pmod n \\ &\vdots \quad \vdots \\ aa_{\phi(n)} &\equiv a_{\phi(n)}' \pmod n \end{aligned}$$

dimana $a_1', a_2', \dots, a_{\phi(n)}'$ adalah bilangan bulat $a_1, a_2, \dots, a_{\phi(n)}$ di suatu pengaturan. Jadi

$$(aa_1)(aa_2) \dots (aa_{\phi(n)}) \equiv a_1' a_2' \dots a_{\phi(n)}' \pmod n$$

atau

$$a^{\phi(n)}(a_1 a_2 \dots a_{\phi(n)}) \equiv a_1 a_2 \dots a_{\phi(n)} \pmod n$$

Karena $gcd(a_i,n) = 1$ untuk setiap i, maka $gcd(a_1 a_2 \dots a_{\phi(n)}, n) = 1$. Jadi kita memperoleh $a^{\phi(n)} \equiv 1 \pmod n$.

II.1.2 ORDER DARI BILANGAN MODULO N

DEFINISI: Jika $gcd(a,m) = 1$, maka bilangan asli terkecil x sehingga $a^x \equiv 1 \pmod m$ disebut order dari m. (ditulis $x = ord_m\, a$)
Contoh: Bila $a = 4$ dan $m = 5$, maka $2 = ord_5\, 4$.

Saya akan memberikan sebuah teorema yang mengaitkan konsep order dari modulo n dengan $\phi(n)$.

TEOREMA [1]: Misal bilangan bulat a memiliki order k modulo m. Maka $a^h \equiv 1 \pmod n$ jika dan hanya jika $k|h$.

BUKTI: Jika $k|h$, akan dibuktikan $a^h \equiv 1 \pmod n$. Tulis $h = jk$ untuk suatu bilangan bulat j. Karena $a^k \equiv 1 \pmod n$, maka $(a^k)^j \equiv 1^j \pmod n$, atau $a^h \equiv 1 \pmod n$.

Untuk arah sebaliknya, misal h adalah bilangan bulat positif sehingga $a^h \equiv 1 \pmod n$. Dengan algoritma pembagian, terdapat q dan r sehingga $h = ak + r$ dengan $0 \leq r < k$. Akibatnya,

$$a^h = a^{qk+r} = (a^k)^q a^r$$

Karena $a^h \equiv 1 \pmod n$ dan $a^k \equiv 1 \pmod n$maka $a^r \equiv 1 \pmod n$, dengan $0 \leq r < k$. Jadi $r = 0$. berdasarkan sifat keminimalan dari k. Akibatnya $k|h$.

TEOREMA [1]: Jika bilangan bulat a memiliki order k di modulo n, maka $a^i \equiv a^j \pmod n$ jika dan hanya *jika* $i \equiv j \pmod k$.

BUKTI: Andaikan $a^i \equiv a^j \pmod n$ dengan $i \geq j$. Karena $gcd(a,n) = 1$, maka dengan hukum pencoretan diperoleh $a^{i-j} \equiv 1 \pmod n$. Akibatnya $k|(i-j)$, jadi $i \equiv j \pmod k$.

Untuk arah sebaliknya, andaikan $i \equiv j \pmod k$. Maka kita mempunyai $i = qk + j$ untuk suatu bilangan

bulat q. Karena $a^k \equiv 1 \pmod n$, maka

$$a^i = a^{qk+j} = (a^k)^q a^j \equiv a^j \pmod n$$

Kesimpulan mengikuti.

II.2 JENIS-JENIS CIPHER

Sekarang saya akan memberikan beberapa jenis cipher yang sering dipakai, mulai dari yang sederhana sampai memerlukan ilmu teori bilangan yang cukup tinggi. Inti dari semua cipher yang ada adalah merubah huruf yang ada menjadi sebuah angka yang berkesusaian (A→ $0, B \rightarrow 1, C \rightarrow 2, \ldots, Z \rightarrow 25$) dan dilanjutkan dengan melakukan sebuah proses di angka-angka tersebut. Di sini saya akan menotasikan p sebagai plain teks, c sebagai cipher teks, dan k sebagai kunci.

1. Cipher Caesar [2]

Algoritma cipher:

1) Pilih bilangan bulat k
2) Setiap huruf diganti dengan angka yang berkesusaian
3) $c \equiv p + k \pmod{26}$
4) Ubah ke huruf yang berkesesuaian

Untuk dekripsi, kita menggunakan $p \equiv c - k \pmod{26}$.

Contoh: $k = 3$

Proses enkripsi:

Plain teks: *ANICANTIK*

↓

0 13 8 2 0 13 19 8 10

↓

3 16 11 5 3 16 22 11 13

↓

Cipher teks: *DQLFDQWLN*

Proses dekripsi:

Cipher teks: *DQLFDQWLN*

↓

3 16 11 5 3 16 22 11 13

↓

0 13 8 2 0 13 19 8 10

↓

Plain teks: *ANICANTIK*

2. Metode transformasi affine

Algoritma cipher:

1) Pilih bilangan bulat a, b dimana $gcd(a, 26) = 1$
2) Setiap huruf diganti dengan angka yang berkesusaian
3) $c \equiv ap + b \pmod{26}$
4) Ubah ke huruf yang berkesesuaian

Perhatikan bahwa $p \equiv a^{-1}(c - b) \pmod{26}$, atau $p \equiv a^{\phi(26)-1}(c - b) \pmod{26}$. Akibatnya $p \equiv a^{11}(c - b) \pmod{26}$. Jadi untuk dekripsi, kita menggunakan $p \equiv a^{11}(c - b) \pmod{26}$.

Contoh: $a = 25$ dan $b = 0$

Proses enkripsi:

Plain teks: *ANICANTIK*

↓

0 13 8 2 0 13 19 8 10

↓

0 13 18 24 0 13 7 18 16

↓

Cipher teks: *ANSYANHSQ*

Proses dekripsi: Karena $a = 25 \equiv -1 \pmod{26}$, maka $a^{11} \equiv (-1)^{11} \equiv -1 \pmod{26}$

Cipher teks: *ANSYANHSQ*

↓

0 13 18 24 0 13 7 18 16

↓

0 13 8 2 0 13 19 8 10

↓

Plain teks: *ANICANTIK*

3. Cipher Vigenēre [6]

Algoritma cipher:

1) Pilih n bilangan bulat
2) Pilih kata kunci, yaitu sebuah kata yang memiliki panjang n
3) Perubahan kata kunci menjadi angka yang berkesusaian (misal bilangan itu $k_1\ k_2\ \ldots\ k_n$)
4) Plain teks dikelompokkan menjadi kelompok-kelompok yang masing-masing terdiri dari n karakter (apabila kelompok terakhir tidak memiliki panjang n, tambahkan huruf apa saja sehingga panjangnya menjadi n)
5) Ubah ke n bilangan yang berkesesuaian (misal $p_1\ p_2\ \ldots\ p_n$)
6) Untuk setiap kelompok gunakan rumus $c_i \equiv p_i + k_i \pmod{26}$
7) Ubah ke huruf yang berkesesuaian

Untuk dekripsi, kita menggunakan $p_i \equiv c_i - k_i \pmod{26}$. Contoh: kunci *ITB* → 8 19 1

Proses enkripsi:

Plain teks: *ANI CAN TIK*

↓

(0 13 8) (2 0 13) (19 8 10)

↓

(8 6 9) (10 19 14) (1 1 11)

↓

Cipher teks: *IGJ KTO BBL*

Proses dekripsi:

Cipher teks *IGJ KTO BBL*

↓

(8 6 9) (10 19 14) (1 1 11)

↓

(0 13 8) (2 0 13) (19 8 10)

↓

Plain teks: *ANI CAN TIK*

4. Cipher Hill [7]

Algoritma cipher:

1) Pilih bilangan bulat a, b, c, d dimana $gcd(ad - bc, 26) = 1$ dan $0 \le a, b, c, d \le 25$
2) Plain teks dikelompokkan ke dalam grup yang memiliki panjang 2 (apabila kelompok terakhir

tidak memiliki panjang 2, tambahkan huruf apa saja sehingga panjangnya menjadi 2)

3) Ubah ke bilangan yang berkesesuaian
4) Untuk setiap kelompok gunakan rumus $c_1 \equiv ap_1 + bp_2 \ (mod\ 26)$ dan $c_2 \equiv cp_1 + dp_2 \ (mod\ 26)$
5) Ubah ke huruf yang berkesesuaian

Perhatikan bahwa kita dapat mengubah bentuk proses enkripsi tersebut menjadi

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} (mod\ 26)$$

Dari bentuk di atas, kita dapat mengetahui bahwa

$$\begin{pmatrix} p_1 \\ p_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} (mod\ 26)$$

atau

$$\begin{pmatrix} p_1 \\ p_2 \end{pmatrix} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} (mod\ 26)$$

Perhatikan bahwa $gcd(ad - bc, 26) = 1$, jadi $(ad - bc)^{-1}$ ada di modulo 26. Jadi untuk dekripsi, kita menggunakan $p_1 \equiv (ad - bc)^{-1}(dc_1 - bc_2) \ (mod\ 26)$ dan $p_2 \equiv (ad - bc)^{-1}(-cc_1 + ac_2) \ (mod\ 26)$.

Contoh: $a = 3, b = 5, c = 8$, dan $d = 17$

Proses enkripsi:

Plain teks: ANI
↓
$AN\ IC$
↓
(0 13) (8 2)
↓
(13 13) (8 20)
↓
Cipher teks: $NN\ IU$

Proses dekripsi: Perhatikan bahwa $ad - bc = -61 \equiv 17 \ (mod\ 26)$ dan $(ad - bc)^{-1} \equiv 23 \ (mod\ 26)$

Cipher teks: $NN\ IU$
↓
(13 13) (8 20)
↓
(0 13) (8 2)
↓
$AN\ IC$
↓
Plain teks: $ANI\ C$

5. Cipher autokey [4]

Algoritma cipher:

1) Pilih 1 huruf bibit kunci
2) Kunci untuk sebuah plain teks adalah plain teks tersebut yang telah ditambah satu karakter
3) Ubah plain teks menjadi bilangan yang berkesesuaian
4) Kunci ditambahkan dengan plain teks (huruf per huruf)
5) Ubah ke huruf yang berkesesuaian

Untuk proses deskripsi, langkahnya dilakukan huruf per huruf dan menggunakan proses pengurangan.

Contoh: plain teks: $INDAH \rightarrow$ 8 13 3 0 7 dan bibit kunci: $S \rightarrow$ 18. Jadi kunci adalah 18 8 13 3 0.

Proses enkripsi:

Plain teks: $INDAH$
↓
8 13 3 0 7
↓ + 18 8 13 3 0
0 21 16 3 7
↓
Cipher teks: $AVQDH$

Proses dekripsi:

Cipher teks: AVQ
↓
0 21 16
↓ − 18 0 0
8 21 16
↓ − 0 8 0
8 13 16
↓ − 0 0 13
8 13 13
↓
Plain teks: IND

6. Cipher eksponensial [3]

Algoritma cipher:

1) Misal k prima ganjil yang lebih besar dari 26 dan l (kunci) bilangan bulat, dimana $gcd(l, k - 1) = 1$
2) Setiap huruf plain teks diganti dengan angka yang berkesesuaian tetapi harus berdigit 2. Contoh: $A \rightarrow 00, B \rightarrow 01, C \rightarrow 02, \ldots, Z \rightarrow 25$
3) Pilih n dimana n menyatakan banyak unsur tiap kelompok. Selanjutnya kita pecah plain teks menjadi kelompok dengan panjang n (n harus kurang dari sama dengan banyak digit di k)
4) $c \equiv p^l \ (mod\ k)$

Karena k prima dan $gcd(k, p) = 1$, maka $ord_k\ p = k - 1$. Karena $gcd(l, k - 1) = 1$, maka ada l memiliki invers di modulo $k - 1$, misal invers nya itu adalah l^{-1}. Akibatnya

$$p = p^{ll^{-1}} = (p^l)^{l^{-1}} \equiv c^{l^{-1}} \ (mod\ k)$$

Jadi untuk dekripsi, kita menggunakan $p \equiv c^{l^{-1}} \ (mod\ k)$

Contoh: $k = 947, l = 53$ dan $n = 3$

Proses enkripsi:

Plain teks: DON
↓
04 15 14
↓
041514
↓
041 514
↓
$(14^{53} \ (mod\ 947))\ (514^{53} \ (mod\ 947))$
↓
Cipher teks: 544 390

Proses dekripsi: Karena $k = 947$ dan $l = 53$, maka $l^{-1} = 357$

Cipher teks: 544 390
↓

$(544^{357} \pmod{947})\ (390^{357} \pmod{947})$

↓

041 514

↓

041514

↓

04 15 14

↓

Plain teks: *DON*

7. Cipher knapsack [5]

Sebelum masuk ke algoritma cipher knapsocke, saya akan memperkenalkan beberapa definisi baru.

Diberikan bilangan asli $(a_1, a_2, \ldots, a_n)$ dan sebuah bilangan asli S. Tentukan (bila ada) $x_1, x_2, \ldots, x_n$ dimana x_i bernilai 0 atau 1 dengan $i = 1,2, \ldots, n$ sehingga $S = a_1x_1 + a_2x_2 + \cdots + a_nx_n$. Contoh: n=5, barisan $\{a_i\}$ nya 2,7,8,11,12 dan $S = 21$. Jadi $S = 2 + 7 + 12 = 2 + 8 + 11$ akibatnya S bisa ditulis (1,1,0,0,1) atau (1,0,1,1,0) terhadap barisan a_i. Jika $a_1 + a_2 + \cdots + a_{n-1} < a_n$ maka barisan $\{a_i\}$ disebut barisan super naik.

Algoritma untuk mencari x_i di barisan super naik:

1) x_n bernilai 1 jika $s \geq a_n$ dan 0 jika $s < a_n$
2) Untuk setiap $j = n-1, n-2, \ldots, 1$, x_j bernilai 1 jika $s - (a_{j+1}x_{j+1} + a_{j+2}x_{j+2} + \cdots + a_nx_n) \geq a_j$ dan 0 jika $s - (a_{j+1}x_{j+1} + a_{j+2}x_{j+2} + \cdots + a_nx_n) < a_j$

Algoritma cipher :

1) Misal $(a_1, a_2, \ldots, a_n)$ adalah barisan super naik, m bilangan asli dengan $m > 2a_n$. Misal w bilangan bulat dengan $gcd(w, m) = 1$
2) Bentuk barisan $(b_1, b_2, \ldots, b_n)$ dengan $b_j \equiv wa_j \pmod{m}$ dengan $0 \leq b_j \leq m$. Perhatikan bahwa barisan $(b_1, b_2, \ldots, b_n)$ bukan barisan super naik
3) Ubah setiap huruf di plain teks ke dalam basis 2, tetapi harus berdigit 5. Contoh: $A \rightarrow 00000, B \rightarrow 00001, C \rightarrow 00010, \ldots, Z \rightarrow 11001$
4) Gabung semua angka $0 - 1$ tersebut, kemudian pecah menjadi kelompok-kelompok yang beranggotakan n buah angka
5) Setiap kelompok, pandang angka yang di kelompok tersebut sebagai sebuah koordinat terhadap barisan $(b_1, b_2, \ldots, b_n)$

Untuk proses dekripsi gunakan algoritma berikut:

1) Misal w^{-1} adalah invers dari w di modulo m. Misal p adalah kelompok dari cipher teks dan misal $l \equiv pw^{-1} \pmod{m}$.
2) Nyatakan l sebagai kombinasi linear terhadap barisan $(a_1, a_2, \ldots, a_n)$, misalkan bentuk tersebut l'
3) Bila p adalah kelompok pertama, ambil n angka pertama dari l', dan sisa dari l' akan diberikan untuk kelompok berikutnya

Contoh: Misal $n = 7$ dan barisan $(a_1, a_2, \ldots, a_n)$ adalah $2, 11, 14, 29, 58, 119, 247$ dengan $m = 3837$ dan $w = 1001$. Kita memperoleh barisan $(b_1, b_2, \ldots, b_n)$ adalah $2002, 3337, 2503, 2170, 503, 172, 3347$.

Proses enkripsi:

Plain teks: *ANI*

↓

00000 01101 01000

↓

0000001 1010100 0000000

↓

Cipher teks: 3347 5068 0

Proses dekripsi: Karena $m = 3837$ dan $w = 1001$, maka $w^{-1} = 23$.

Cipher teks: 3347

↓

241

↓

0000001

↓

00000 01

↓

Plain teks: *A* 01

Selain cipher-cipher yang telah saya berikan di atas, tentu masih ada banyak cipher lainnya. Seperti cipher Diffie-Hellman dan cipher RSA (Rivest, Shamir, Aldermann). Saya tidak menjelaskan cipher-cipher tersebut karena menurut saya, inti dari ide cipher tersebut telah diakomodasi di cipher-cipher yang telah saya berikan. Anda juga dapat mebuat cipher buatan sendiri dengan menggabungkan beberapa bentuk cipher-cipher dasar yang telah saya berikan.

III. KESIMPULAN

Dari pembahasan, kita dapat menarik beberapa kesimpulan:

1) Teori bilangan adalah salah satu cabang matematika yang dapat diaplikasikan ke dalam kriptografi
2) Kriptografi sangat membutuhkan pengetahuan tentang teori bilangan, khususnya dalam proses dekripsi
3) Kita dapat mebuat cipher sendiri dengan melakukan kombinasi ataupun modifikasi dari cipher-cipher yang telah ada

REFERENSI

[1] Burton, David. M. "*Elementary Number Theory*", The McGraw-Hill Companies, 1998

[2] http://www.informatika.org/~rinaldi/Matdis/2008-2009/Teori%20Bilangan.ppt 11.30 PM 15/12/2010

[3] http://www.scribd.com/doc/35117715/Exponential-and-RSA-Ciphers 11.30 PM 15/12/2010

[4] http://en.wikipedia.org/wiki/Autokey_cipher 11.59 PM 15/12/2010

[5] http://deron.csie.ncue.edu.tw/security/Knapsack%20Cipher.ppt 11.59 PM 15/12/2010

[6] http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher 11.59 PM 15/12/2010

[7] http://en.wikipedia.org/wiki/Hill_cipher 11.59 PM 15/12/2010

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 16 Desember 2010

ttd

Yosafat Eka P. Pangalela (10107075)