Kelompok 8

PMAT C

KRIPTOLOGI

Disusun Guna Memenuhi Tugas Mata Kuliah Teori Bilangan

Dosen Pengampu Dr. Agus Maman Abadi

oleh:

Nadzifah Ajeng Daniyati (11709251039)

Muhammad Irfan Rumasoreng (10709259023)

PROGRAM PASCASARJANA

JURUSAN PENDIDIKAN MATEMATIKA

UNIVERSITAS NEGERI YOGYAKARTA

2011

KRIPTOLOGI

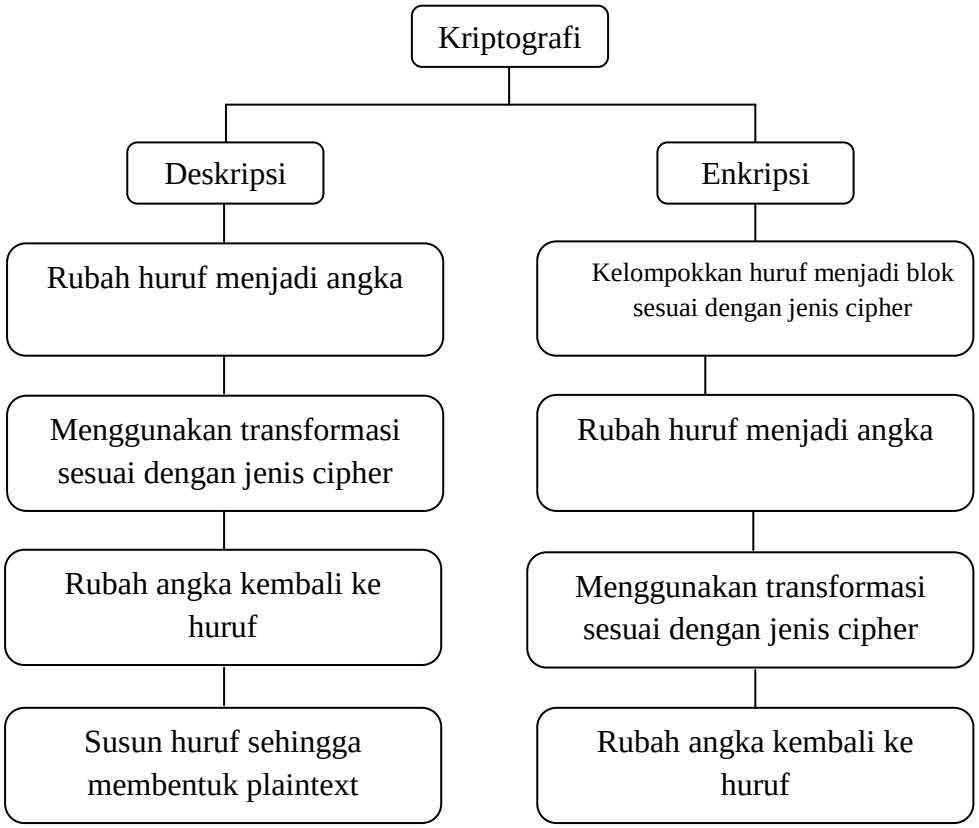
A. Pendahuluan

Dari zaman kuno, pesan rahasia telah dikirim. Kebutuhan untuk komunikasi rahasia telah terjadi di dalam urusan diplomasi dan militer. Sekarang, dengan masuknya komunikasi elektronik digunakan secara luas, kerahasiaan menjadi penting. Baru-baru ini, dengan munculnya perbankan elektronik, kerahasiaan telah menjadi diperlukan bahkan untuk transaksi keuangan. Dalam makalah ini akan di bahas macam- macam karakter cipher, antara lain: Cipher Caesar, Transformasi Affine, Cipher Vigenere, Cipher Hill, Cipher Stream.

B. Pembahasan

1. Karakter Cipher

Sebelum membahas sistem kerahasiaan khusus, akan di bahas beberapa pengertian terlebih dahulu. Disipin ilmu yang membahas sistem kerahasiaan disebut kriptologi. Kriptografi merupakan bagian dari kriptologi. Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi. Enkripsi adalah proses mengubah suatu pesan, data, atau informasi asli (plaintext) menjadi suatu pesan, data, atau informasi dalam bahasa sandi (ciphertext). Sedangkan dekripsi adalah proses mengubah pesan, data, atau informasi dalam suatu bahasa sandi (ciphertext) kembali menjadi pesan, data, atau informasi asli (plaintext). Skema permasalahan dalam kriptografi:



Dalam bab ini, menyajikan sistem kerahasiaan berdasarkan aritmatika modular. Yang pertama berasal dari Julius Caesar. Dalam sistem ini, kita mulai dengan menerjemahkan huruf menjadi angka. Kami mengambil sebagai standar, alfabet huruf bahasa Inggris dan menerjemahkan ke dalam integer dari 0 ke 25, seperti yang ditunjukkan pada Tabel 8.1.

Huruf	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Angka	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Tabel 8 .1. Huruf Setara Angka

Tentu saja, jika kita mengirim pesan Rusia, Yunani, Ibrani atau bahasa lain kita akan menggunakan berbagai bilangan bulat yang sesuai abjad. Kita mungkin juga ingin memasukkan tanda baca, simbol untuk menunjukkan kosong, dan mungkin untuk mewakili digit nomor sebagai bagian dari pesan. Namun, demi kesederhanaan, kita membatasi diri pada huruf-huruf alfabet Inggris.

Pertama, kita bahas berdasarkan sistem kerahasiaan mengubah setiap huruf dari pesan plaintext menjadi huruf yang berbeda untuk menghasilkan ciphertext. Cipher seperti ini disebut cipher karakter atau monografi, karena setiap huruf

berubah secara individu dengan huruf lain dengan substitusi. Secara keseluruhan, ada 26! cara yang mungkin untuk menghasilkan transformasi monografi. Kita akan membahas yang didasarkan pada aritmatika modular.

Sebuah cipher, yang digunakan oleh Julius Caesar, didasarkan pada substitusi di mana setiap huruf digantikan dengan huruf tiga bagian bawah abjad, dengan tiga huruf terakhir bergeser ke tiga huruf pertama dari alfabet. Untuk menggambarkan cipher ini menggunakan aritmatika modular, biarkan P menjadi setara numerik huruf dalam plaintext dan C setara numerik dari huruf ciphertext yang sesuai. Kemudian

$$C \equiv P + 3(Mod\,26), 0 \le C \le 25$$

Korespondensi antara plaintext dan ciphertext diberikan dalam Tabel 8.2.

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
ciphertext	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2
	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Tabel 8 .2. Korespondensi huruf untuk Cipher Caesar

Untuk menulis dalam kode pesan menggunakan transformasi ini, pertama diubah ke setara angkanya, dengan pengelompokan huruf dengan lima blok. Kemudian kita mengubah setiap angka. Langkah ini disebut dengan enkripsi pesan.

Secara singkat, langkah- langkah untuk mengenkripsi pesan dari cipher caesar sebagai berikut:

a. Kelompokkan pesan menjadi 5 huruf,
b. Huruf diubah menjadi angka (lihat tabel 8.1),
c. Menggunakan transformasi $C \equiv P + 3(Mod\,26)$ untuk memperoleh pesan ciphertext,
d. Angka diubah menjadi huruf.

Contoh:

(Rosen, K.H. 2011. *Elementary Number Theory and Its Application Sixth Edition. Monmouth University*. Hal. 293)

Enkripsikan pesan :

THIS MESSAGE IS TOP SECRET

Kelompokkan pesan menjadi lima huruf, pesan menjadi

THISM ESSAG EISTO PSECR ET

Mengubah huruf menjadi angka, kita memperoleh

19 7 8 18 12 4 18 18 0 6 4 8 18 19 14

15 18 4 2 17 4 19

Menggunakan transformasi Caesar $C \equiv P + 3(Mod\,26)$ ini menjadi

22 10 11 21 15 7 21 21 3 9 7 11 21 22 17

18 21 7 5 20 7 22

Penerjemahan kembali ke huruf, diperoleh

WKLVP HVVDJ HLVWR SVHGU HW.

Ini adalah pesan yang dikirim.

Untuk mendeskripsikan pesan, pertama terlebih dahulu pesan dikonversi ke angka. Kemudian, hubungan $C \equiv P + 3(Mod\,26), 0 \le C \le 25$ digunakan untuk mengubah ciphertext kembali ke plaintext.

Secara singkat, langkah- langkah untuk mendeskripsi pesan dari cipher caesar sebagai berikut:

a. Ubah huruf menjadi angka (lihat tabel 8.1),
b. Menggunakan transformasi $P \equiv C - 3(Mod\,26)$ untuk memperoleh pesan plaintext,
c. Ubah angka kembali menjadi huruf,
d. Susun huruf sehingga mempunyai arti.

Contoh:

(Rosen, K.H. 2011. *Elementary Number Theory and Its Application Sixth Edition. Monmouth University*. Hal. 294)

Deskripsi pesan:

WKLVL VKPZZ HGHFL SKHU

Pertama, mengubah huruf menjadi angka, diperoleh

22 10 11 21 11 21 l0 17 25 25 7 6 7 5 11 18 10 7 20.

Selanjutnya, melakukan transformasi $P \equiv C - 3(Mod\,26)$ untuk mengubah menjadi plaintext, dan diperoleh

19 7 8 18 8 18 7 14 22 22 4 3 4 2 8 15 7 4 17.

Megubah angka kembali ke huruf,

THISI SHOWW EDECI PHER.

Dengan menggabungkan huruf-huruf yang sesuai dengan kata-kata, kita menemukan bahwa pesan tersebut

THIS IS HOW WE DECIPHER.

2. Transformasi Affine

Cipher Caesar adalah salah satu dari keluarga cipher serupa digambarkan oleh shift transformasi:

$$C \equiv P + k(Mod\,26), 0 \le C \le 25$$

di mana k adalah kunci yang mewakili ukuran pergeseran huruf dalam alfabet. Ada 26 transformasi yang berbeda dari jenis ini, termasuk kasus k = 0 (mod 26), di mana huruf tidak berubah, karena dalam hal ini $C \equiv P(Mad\,26)$.

Secara umum,

$$C \equiv aP + b(Mod\,26), 0 \le C \le 25$$

dimana a dan b adalah bilangan bulat dengan (a, 26) = 1. Ini disebut transformasi affine. Shift transformasi adalah transformasi affine dengan a=1 . Mengharuskan (a, 26) = 1, sehingga P berjalan melalui sistem residu lengkap modulo 26, demikian juga dengan C. Ada $\Phi(26) = 12$ pilihan untuk a, dan 26 pilihan untuk b, memberikan total $12 \times 26 = 312$ transformasi jenis ini (salah satunya adalah C = P (mod 26) diperoleh bila a = 1 dan b = 0. Jika hubungan antara plaintext dan ciphertext dijelaskan oleh (8.1), maka hubungan terbalik diberikan oleh

$$P \equiv \bar{a}(C - b)(Mad\,26), 0 \le P \le 25$$

Dimana $\bar{a}$ merupakan invers dari (mod 26).

Contoh:

(Rosen, K.H. 2011. *Elementary Number Theory and Its Application Sixth Edition. Monmouth University*. Hal. 295)

a = 7 dan b = 10, sehingga $C \equiv 7P + 10(Mod\,26)$ Oleh karena itu, $P \equiv 15(C - 10) \equiv 15C + 6(Mod\,26)$. 15 adalah invers dari 7 modulo 26.

Korespondensi antara huruf diberikan dalam Tabel 8.3.

Plaintext	A 0	B 1	C 2	D 3	E 4	F 5	G 6	H 7	I 8	J 9	K 10	L 11	M 12	N 13	O 14	P 15	Q 16	R 17	S 18	T 19	U 20	V 21	W 22	X 23	Y 24	Z 25
ciphertext	10 K	17 R	24 Y	5 F	12 M	19 T	0 A	7 H	14 O	21 V	2 C	9 J	16 Q	23 X	4 E	11 L	18 S	25 Z	6 G	13 N	20 U	1 B	8 I	15 P	22 W	3 D

Table 8 .3. Korespondensi huruf untuk Cipher dengan $C \equiv 7P + 10(Mod\,26)$

Untuk menggambarkan memperoleh korespondensi tersebut, perhatikan bahwa huruf plaintext L dengan setara angka 11 sesuai dengan huruf J pada ciphertext, $7 \times 11 + 10 = 87 \equiv 9(Mod\,26)$ dan 9 setara dengan J.

Langkah- langkah untuk mengenkripsi pesan dari transformasi affine sebagai berikut:

a. Kelompokkan pesan menjadi 5 huruf
b. Huruf diubah menjadi angka (lihat tabel 8.1)
c. Menggunakan transformasi $C \equiv 7P + 10(Mod\,26)$ untuk memperoleh pesan ciphertext
d. Angka diubah menjadi huruf

Langkah- langkah untuk mendeskripsi pesan dari transformasi affine sebagai berikut:

a. Ubah huruf menjadi angka (lihat tabel 8.1),
b. Menggunakan transformasi P ≡ 15 C + 6 (mod 26) untuk memperoleh pesan plaintext,
c. Ubah angka kembali menjadi huruf,
d. Susun huruf sehingga mempunyai arti.

Contoh :

(Rosen, K.H. 2011. *Elementary Number Theory and Its Application Sixth Edition. Monmouth University*. Hal. 295)

1. Enkripsikan pesan:

PLEASE SEND MONEY

Kelompokkan pesan menjadi lima huruf, pesan menjadi

PLEAS ESEND MONEY

Mengubah huruf menjadi angka, selanjutnya menggunakan transformasi $C \equiv 7P + 10(Mod\,26)$, sehingga diperoleh

P = 15 maka C = 7. 15 + 10 = 115 ≡ 11 (mod 26), sehingga P menjadi L.

L = 11 maka C = 7. 11 + 10 = 87 ≡ 9 (mod 26), sehingga L menjadi J.

.

.

dst

Sehigga di peroleh

LJMKG MGMXF QEXMW.

2. Deskripsikan pesan:

FEXEN ZMBMK JNHMG MYZMN

Menggunakan rumus P ≡ 15 C + 6 (mod 26) di peroleh

F = 5 maka P = 15. 5 + 6 = 81 ≡3 (mod 26), sehingga F menjadi D.

E = 4 maka P = 15. 4 + 6 = 66 ≡ 14 (mod 26), sehingga E menjadi O.

.

.

dst

Menjadi

DONOT REVEA LTHES ECRET

atau pada plaintext

DO NOT REVEAL THE SECRET.

Sekarang kita membahas beberapa teknik yang diarahkan pada pembacaan sandi dari cipher berdasarkan transformasi affine. Dalam upaya memecahkan cipher monografi, frekuensi huruf dalam ciphertext dibandingkan dengan frekuensi pada teks biasa. Ini memberikan informasi mengenai kesesuaian antara huruf. Dalam

perhitungan berbagai macam frekuensi pada teks English, salah satunya menemukan persentase yang terdapat dalam tabel 8.4 untuk kejadian ke 26 huruf.

Huruf	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frekuensi(%)	7	1	3	4	13	3	2	3	8	<1	<1	4	3	8	7	3	<1	8	6	9	3	1	1	<1	2	<1

Tabel 8.4. Frekuensi dari kejadian huruf pada alfabet.

Dari tabel ini didapatkan bahwa frekuensi yang sering muncul pada teks English adalah E, T, N, R, I, O dan A. Kita dapat menggunkan informasi ini untuk membedakan chiper yang mana pada sebuah transformasi affine yang telah digunakan untuk menulis pesan.

Contoh :

(Rosen, K.H. 2011. *Elementary Number Theory and Its Application Sixth Edition. Monmouth University*. Hal. 296)

Deskripsikan pesan:

YFXMP CESPZ CJTDF DPQFW QZCPY

NTASP CTYRX PDDLR PD

Pertama-tama dengan menghitung huruf yang muncul dalam chipertext, yaitu

Huruf	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Angka yang muncul	1	0	4	5	1	3	0	0	0	1	0	1	1	1	0	7	2	2	2	3	0	0	1	2	3	2

Dari tabel didapatkan bahwa huruf yang sering muncul : P, C, D, F, T dan Y.

P menggambarkan huruf E karena E adalah huruf yang sering muncul dalam teks English. Jika demikian maka

P = 15 (ciphertext)

E = 4 (plaintext)

$C \equiv P + k \ (mod\ 26)$

$15 \equiv 4 + k \pmod{26}$

$k \equiv 11 \pmod{26}$.

$C \equiv P + 11 \pmod{26}$

Dan $P \equiv C - 11 (\mathrm{mod}\ 26)$, maka didapatkan kesamaan

chipertext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
plain text	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

Dari kesamaan ini maka:

YFXMP CESPZ CJTDF DPQFW QZCPY NTASP CTYRX PDDLR PD sama dengan

NUMBE RTHEO RYISU SEFUL FOREN CIPHE RINGM ESSAG ES

atau

NUMBER THEORY IS USEFUL FOR ENCIPHERING MESSAGES.

Jika kita telah mencoba transformasi, namun menghasilkan bukan plaintext dan teks kacau, maka coba transformasi lain berdasarkan jumlah frekuensi huruf dalam ciphertext.

Transformasi affine dari bentuk $C \equiv aP + b (mod\ 26), 0 \leq C \leq 25$ digunakan dalam penerjemahan.

Contoh :

(Rosen, K.H. 2011. *Elementary Number Theory and Its Application Sixth Edition. Monmouth University*. Hal. 297)

USLEL	JUTCC	YRTPS	URKLT	YGGFV
ELYUS	LRYXD	JURTU	ULVCU	URJRK
QLLQL	YXSRV	LBRYZ	CYREK	LVEXB
RYZDG	HRGUS	LJLLM	LYPDJ	LJTJU
FALGU	PTGVT	JULYU	SLDAL	TJRWU
SLJFE	OLPU			

Huruf	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Angka yang muncul	2	2	4	4	5	3	6	1	0	10	3	22	1	0	1	4	2	12	7	8	16	5	1	3	10	2

Dari tabel didapatkan huruf L adalah sering muncul dalam chipertext dan hal ini sama dengan huruf E. Sedang huruf U sama dengan T. Sehingga

$C \equiv 4a + b \equiv 11(mod26)$

$C \equiv 19a + b \equiv 20(mod26)$

didapatkan $a \equiv 11(mod26)$ dan $b \equiv 19(mod26)$

$C \equiv aP + b(mod\ 26)$

$C \equiv 11\ P + 19\ (\text{mod } 26)$

$P \equiv 19(C - 19) \equiv 19C - 361 \equiv 19C + 3(mod26), 0 \leq P \leq 25$; sehingga di dapatkan

chipertext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
plaintext	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7	0	19	12	5	24	17	10
	D	W	P	I	B	U	N	G	Z	S	L	E	X	Q	J	C	V	O	H	A	T	M	P	Y	R	K

Maka

USLEL	JUTCC	YRTPS	URKLT	YGGFV
ELYUS	LRYXD	JURTU	ULVCU	URJRK
QLLQL	YXSRV	LBRYZ	CYREK	LVEXB
RYZDG	HRGUS	LJLLM	LYPDJ	LJTJU
FALGU	PTGVT	JULYU	SLDAL	TJRWU
SLJFE	OLPU			

Sama dengan

THEBE	STAPP	ROACH	TOLEA	RNNUM
BERTH	EORYI	STOAT	TEMPT	TOSOL
VEEVE	RYHOM	EWORK	PROBL	EMBYW
ORKIN	GONTH	ESEEX	ERCIS	ESAST
UDENT	CANMA	STER	HEIDE	ASOFT
HESUB	JECT			

atau

THE BEST APPROACH TO LEARN NUMBER THEORY IS TO ATTEMPT TO SOLVE EVERY HOM EWORK PROBLEM BY WORKIN G ON THESE EXERCISES A STUDENT CAN MASTER HE IDEAS OF THE SUBJECT.

Latihan:

a. Dengan menggunakan caesar chiper, enkripsikan pesan ATTACK AT DAWN.
(Rosen, K.H. 2011. *Elementary Number Theory and Its Application Sixth Edition. Monmouth University*. Hal. 298, No 1).

Jawab:

ATTACK AT DAWN

Kelompokkan lima huruf, pesan menjadi

ATTAC KATDA WN

Mengubah huruf menjadi angka, kita memperoleh

0 19 19 0 2 10 0 19 3 0 22 13

Menggunakan transformasi Caesar $C \equiv P + 3(Mod\,26)$ ini menjadi

3 22 22 3 5 13 3 22 6 3 25 16

Penerjemahan kembali ke huruf, diperoleh

DWWDF NDWGD ZQ

Jadi, pesan yang di maksud DWWDF NDWGD ZQ.

b. Deskripsikan pesan RTOLK TOIK dengan menggunakan rumus
$C \equiv 3P + 24\ (mod\ 26)$.

(Rosen, K.H. 2011. *Elementary Number Theory and Its Application Sixth Edition. Monmouth University*. Hal. 298, No 4).

Jawab:

RTOLK TOIK

Menggunakan rumus $C \equiv 3P + 24 \ (mod\ 26)$

Pertama, mengubah huruf menjadi angka, diperoleh

17 19 14 11 10 19 l4 8 10

Selanjutnya, kita melakukan transformasi, untuk mengubah plaintext, dan diperoleh

$C \equiv 3P + 24 \ (mod\ 26)$

$3P \equiv C - 24 \ (mod\ 26)$

$3P \equiv 27(C - 24) \ (mod\ 26)$

$P \equiv 9\ (C - 24) \ (mod\ 26)$

$P \equiv 9C - 216 \ (mod\ 26)$

$P \equiv 9C + 18 \ (mod\ 26)$

Menggunakan transformasi $P \equiv 9C + 18 \ (mod\ 26)$ menjadi

Untuk 17

$P \equiv 9C + 18 \ (mod\ 26)$

$P \equiv 9(17) + 18 \ (mod\ 26)$

$P \equiv 171 \ (mod\ 26)$

$P \equiv 15 \ (mod\ 26)$

Jadi, R = 17 setelah di transformasi menjadi 15

Dengan cara yang sama, diperoleh

15 7 14 13 4 7 14 12 4

Menerjrmahkan angka ini kembali ke huruf dan mengembalikan pesan plaintext, diperoleh

PHONE HOME

3. Cipher Vigenere

Untuk mengenkripsi pesan plaintext, pertama kita membagi menjadi blok dengan panjang n. Sebuah blok yang terdiri dari pesan dengan setara numerik p_1, p_2,

... p_n berubah menjadi blok ciphertext dengan huruf setara numerik c_1, c_2,..., c_n menggunakan cipher pergeseran urutan dengan

$c_i \equiv p_i + k_i \pmod{26}$, $0 \leq c_i \leq 25$,

untuk i = 1 2, ... , n. Vigenère cipher adalah algoritma enkripsi dimana huruf plaintext dengan panjang n, dienkripsi pesan ciphertext yang sama panjang. Vigenere cipher dapat dianggap sebagai cipher yang beroperasi dengan panjang n menggunakan kunci dengan panjang n.

Langkah – langkah untuk mengenkripsikan pesan dari cipher vigenere sebagai berikut:

a. Pesan dan kunci diubah menjadi angka (lihat tabel 8.1),
b. Huruf- huruf yang ada di pesan (p_1, p_2, p_3, p_4.....) dan huruf di kunci (k_1,k_2, k_3, k_4, k_5,....),
c. Menggunakan Cipher Vigenere $c_i \equiv p_i + k_i$ (mod 26),
d. Angka tersebut diartikan ke dalam huruf menggunakan tabel 8.1,
e. Huruf di kelompokkan menjadi 5 huruf.

Contoh:

(Rosen, K.H. 2011. *Elementary Number Theory and Its Application Sixth Edition. Monmouth University*. Hal. 301)

Enkripsikan pesan MILLENNIUM dengan kunci YTWOK menggunakan Cipher Vigenere.

Pertama, artikan pesan dan kunci ke dalam angka (tabel 8.1)

M	I	L	L	E	N	N	I	U	M
12	8	11	11	4	13	13	8	20	12
p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}

Dan

Y	T	W	O	K
24	19	22	14	10
k_1	k_2	k_3	k_4	k_5

Menggunakan Cipher Vigenere:

$c_i \equiv p_i + k_i$ (mod 26)

di peroleh:

$c_1 = p_1 + k_1 = 12 + 24 \equiv 10 \pmod{26}$

$c_2 = p_2 + k_2 = 8 + 19 \equiv 1 \pmod{26}$

$c_3 = p_3 + k_3 = 11 + 22 \equiv 7 \pmod{26}$

$c_4 = p_4 + k_4 = 11 + 14 \equiv 25 \pmod{26}$

$c_5 = p_5 + k_5 = 4 + 10 \equiv 14 \pmod{26}$

$c_6 = p_6 + k_6 = 13 + 24 \equiv 11 \pmod{26}$

$c_7 = p_7 + k_7 = 13 + 19 \equiv 6 \pmod{26}$

$c_8 = p_8 + k_8 = 8 + 22 \equiv 4 \pmod{26}$

$c_9 = p_9 + k_9 = 20 + 14 \equiv 8 \pmod{26}$

$c_{10} = p_{10} + k_{10} = 12 + 10 \equiv 22 \pmod{26}$

Angka tersebut diartikan ke dalam huruf menggunakan tabel 8.1, kita peroleh KBHZO LGEIW.

Langkah – langkah untuk mengdeskripsikan pesan dari cipher vigenere sebagai berikut:

a. Pesan dan kunci diubah menjadi angka (lihat tabel 8.1),
b. Huruf- huruf yang ada di pesan (c_1, c_2, c_3, c_4.....) dan huruf di kunci (k_1, k_2, k_3, k_4, k_5,....),
c. Menggunakan Cipher Vigenere $p_i \equiv c_i - k_i \pmod{26}$,
d. Angka tersebut diartikan ke dalam huruf menggunakan tabel 8.1,
e. Susun huruf sehingga mempunyai arti.

Contoh:

(Rosen, K.H. 2011. *Elementary Number Theory and Its Application Sixth Edition. Monmouth University*. Hal. 302)

Deskripsikan pesan FFFLB CVFX menggunakan Cipher Vigenere dengan kunci ZORRO.

Artikan pesan tersebut dengan angka (lihat tabel 8.1)

F	F	F	L	B	C	V	F	X
5	5	5	11	1	2	21	5	23

c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9

dan

Z	O	R	R	O
25	14	17	17	14
k_1	k_2	k_3	k_4	k_5

Menggunakan Cipher Vigenere:

$c_i \equiv p_i + k_i \pmod{26}$

$p_i \equiv c_i - k_i \pmod{26}$

di peroleh:

$p_1 = c_1 - k_1 = 5 - 25 \equiv 6 \pmod{26}$

$p_2 = c_2 - k_2 = 5 - 14 \equiv 17 \pmod{26}$

$p_3 = c_3 - k_3 = 5 - 17 \equiv 14 \pmod{26}$

$p_4 = c_4 - k_4 = 11 - 17 \equiv 20 \pmod{26}$

$p_5 = c_5 - k_5 = 1 - 14 \equiv 13 \pmod{26}$

$p_6 = c_6 - k_6 = 2 - 25 \equiv 3 \pmod{26}$

$p_7 = c_7 - k_7 = 21 - 14 \equiv 7 \pmod{26}$

$p_8 = c_8 - k_8 = 5 - 17 \equiv 14 \pmod{26}$

$p_9 = c_9 - k_9 = 23 - 17 \equiv 6 \pmod{26}$

Angka tersebut di kembalikan ke dalam huruf dengan menggunakan tabel 8.1, diperoleh pesan GROUNDHOG.

4. Cipher Hill

Cipher Hill diciptakan oleh Lester Hill di tahun 1929. Untuk memperkenalkan cipher Hill, pertama-tama setiap blok dari dua huruf dari plaintext digantikan oleh sebuah blok dari dua huruf ciphertext (menambahkan huruf boneka X, pada akhir pesan, jika perlu, sehingga blok akhir memiliki dua huruf).

Langkah – langkah untuk mengenkripsikan pesan dari cipher hill sebagai berikut:

a. Kelompokkan pesan menjadi 2 huruf (menambahkan huruf boneka X, pada akhir pesan, jika perlu, sehingga blok akhir memiliki dua huruf),

b. Huruf-huruf ini diterjemahkan ke dalam setara numerik (Tabel 8.1),
c. Menggunakan transformasi yang ditentukan,
d. Ubah angka tersebut menjadi huruf.

Contoh:

(Rosen, K.H. 2011. *Elementary Number Theory and Its Application Sixth Edition. Monmouth University*. Hal. 306)

Enkripsikan pesan dengan Chiper Hill.

THE GOLD IS BURIED IN ORONO

Pertama kita bagi pesan menjadi dua huruf (menambahkan huruf boneka X, pada akhir pesan, jika perlu, sehingga blok akhir memiliki dua huruf).

TH EG OL DI SB UR IE DI NO RO NO

Berikutnya, huruf-huruf ini diterjemahkan ke dalam setara numerik (Tabel 8.1), diperoleh

19 7 4 6 14 11 3 8 18 1 20 17 8 4 3 8 13 14

17 14 13 14

Misal,

$C_1 \equiv 5P_1 + 17P_2 \pmod{26}, \quad 0 \leq C_1 < 26$

$C_2 \equiv 4P_1 + 15P_2 \pmod{26}, \quad 0 \leq C_2 < 26$

Untuk 19 dan 7

$C_1 \equiv 5 \cdot 19 + 17 \cdot 7 \equiv 6 \pmod{26}, \quad 0 \leq C_1 < 26$

$C_2 \equiv 4 \cdot 19 + 15 \cdot 7 \equiv 25 \pmod{26}, \quad 0 \leq C_2 < 26$

Dengan cara yang sama diperoleh:

6 25 18 2 23 13 21 2 3 9 25 23 4 14 21 2

17 2 11 18 17 2

Angka tersebut di ubah ke huruf dengan menggunakan tabel 8.1

GZ SC XN VC DJ ZX EO VC RC LS RC

Langkah – langkah untuk mengdeskripsikan pesan dari cipher hill sebagai berikut:

a. Huruf-huruf ini diterjemahkan ke dalam setara numerik (Tabel 8.1),
b. Menggunakan transformasi yang ditentukan,
c. Ubah angka tersebut menjadi huruf.

Untuk mendeskripsikan :

GZ SC XN VC DJ ZX EO VC RC LS RC

Diterjemahkan dengan tabel 8.1

6 25 18 2 23 13 21 2 3 9 25 23 4 14 21 2 17 2 11 18 17 2

Bentuk:

$C_1 \equiv 5P_1 + 17P_2 \pmod{26}$

$C_2 \equiv 4P_1 + 15P_2 \pmod{26}$

Diubah, dengan menggunakan matrik dan mencari inversnya.

$$\begin{pmatrix} 5 & 17 \\ 4 & 15 \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} \equiv \begin{pmatrix} C_1 \\ C_2 \end{pmatrix}$$

Mencari $\begin{pmatrix} P_1 \\ P_2 \end{pmatrix}$ dengan mencari invers dari $\begin{pmatrix} 5 & 17 \\ 4 & 15 \end{pmatrix}$, diperoleh

$P_1 \equiv 17C_1 + 5C_2 \pmod{26}$

$P_2 \equiv 18C_1 + 23C_2 \pmod{26}$

Untuk 6 dan 25

$P_1 \equiv 17.\ 6 + 5\ .\ 25 \equiv 19 \pmod{26}$

$P_2 \equiv 18\ .\ 6 + 23.\ 25 \equiv 7 \pmod{26}$

Dengan cara yang sama diperoleh

19 7 4 6 14 11 3 8 18 1 20 17 8 4 3 8 13 14 17 14 13 14

Angka tersebut diterjemahkan dengan tabel 8. 1

TH EG OL DI SB UR IE DI NO RO NO

Dengan menggabungkan huruf-huruf yang sesuai dengan kata-kata, kita menemukan bahwa pesan tersebut

THE GOLD IS BURIED IN ORONO.

Contoh:

(Rosen, K.H. 2011. *Elementary Number Theory and Its Application Sixth Edition. Monmouth University*. Hal. 307)

Dengan menggunakan n = 3, enkripsikan pesan STOP PAYMENT dengan menggunakan matrik $A = \begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{pmatrix}$

Untuk mengenkripsi blok plaintext panjang tiga, kita menggunakan hubungan

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv A \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} (mod\ 26)$$

Untuk mengenkripsi pesan STOP PAYMENT, pertama kita membagi pesan menjadi tiga huruf (menambahkan huruf boneka X, pada akhir pesan, jika perlu, sehingga blok akhir memiliki tiga huruf), menjadi

STO PPA YME NTX.

Terjemahkan huruf menjadi angka dengan tabel 8.1

18	19	14	15	15	0	24	12	4	13	19	23
p_1	p_2	p_3	p_1	p_2	p_3	p_1	p_2	p_3	p_1	p_2	p_3

Blok pertama $\begin{pmatrix} 18 \\ 19 \\ 14 \end{pmatrix}$

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv A \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} (mod\ 26)$$

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv \begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{pmatrix} \begin{pmatrix} 18 \\ 19 \\ 14 \end{pmatrix} \equiv \begin{pmatrix} 8 \\ 19 \\ 13 \end{pmatrix} (mod\ 26)$$

Dengan cara yang sama lakukan untuk $P_1\ P_2\ P_3$ yang lain, diperoleh

8 19 13 13 4 15 0 2 22 20 11 0

Angka tersebut diterjemahkan ke huruf dengan menggunakan tabel 8.1,

ITN NEP ACW ULA

Untuk mendeskripsikan:

ITN NEP ACW ULA

Langkah pertama menerjemahkan ke dalam angka

8 19 13 13 4 15 0 2 22 20 11 0

Bentuk $\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv A \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} (mod\ 26)$ diubah menjadi $\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \equiv \overline{A} \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} (mod\ 26)$.

Di mana :

$$\overline{A} = \begin{pmatrix} 6 & -5 & 11 \\ -5 & -1 & -10 \\ -7 & 3 & 7 \end{pmatrix}$$

Untuk $\begin{pmatrix} 8 \\ 19 \\ 13 \end{pmatrix}$

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \equiv \begin{pmatrix} 6 & -5 & 11 \\ -5 & -1 & -10 \\ -7 & 3 & 7 \end{pmatrix} \begin{pmatrix} 8 \\ 19 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} 18 \\ 19 \\ 14 \end{pmatrix} (mod\ 26)$$

Dengan cara yang sama diperoleh

18 19 14 15 15 0 24 12 4 13 19 23

Terjemahkan ke dalam huruf,

STOP PAYMENT

5. Cipher Stream

Chiper autokey ditemukan oleh vigenere pada abad keenam belas. Chiper autokey menggunakan kunci awal, yang merupakan karakter tunggal, kunci berikutnya adalah karakter plaintext. Secara khusus, chiper autokey bergeser setiap

karakter plaintext, selain karakter pertama, setara numerik dari karakter sebelumnya modulo 26, itu menggeser karakter pertama setara numerik dari karakter modulo 26. Artinya, cipher mengenkripsi autokey p_i karakter sesuai dengan transformasi

$$c_i \equiv p_i + k_i \ (mod\ 26),$$

dimana p_i adalah setara numerik dari karakter ke *i* plaintext, c_i adalah setara numerik dari karakter ke *i* ciphertext, dan k_i setara numerik *i* karakter kunci stream, diberikan oleh $k_1 = s$, dimana *s* adalah setara numerik dari karakter awal dan $k_i = p_{i-1}$ untuk $i \geq 2$.

Untuk mendekripsi pesan dengan cipher autokey, kita perlu mengetahui kunci. Kita kurangi kunci dari karakter ciphertext Modulo pertama untuk menentukan karakter plaintext pertama, dan kemudian kita kurangi setara numerik dari masing-masing karakter plaintext modulo 26 dari karakter ciphertext berikutnya untuk mendapatkan karakter plaintext berikutnya.

Secara singkat, langkah – langkah untuk mengenkripsikan pesan dari cipher stream sebagai berikut:

a. Terjemahkan huruf menjadi angka,
b. Kunci diperoleh dengan k_1= cipher kunci sedangkan kunci yang lain diambil dari angka pesan dengan ketentuan $k_i = p_{i-1,}$
c. Menggunakan transformasi $c_i \equiv p_i + k_i \ (mod\ 26),$
d. Angka diubah kembali ke huruf.

Contoh:

(Rosen, K.H. 2011. *Elementary Number Theory and Its Application Sixth Edition. Monmouth University*. Hal. 312)

Untuk mengenkripsi pesan plaintext HERMIT menggunakan cipher kunci X (dengan setara numerik 23), pertama-tama kita menerjemahkan huruf HERMIT menjadi setara numerik didapat 7 4 17 12 8 19. Kunci terdiri dari nomor 23 7 4 17 12 8.

$p_1 + k_1 = 7 + 23 \equiv 4 \pmod{26}$

$p_2 + k_2 = 4 + 7 \equiv 11 \pmod{26}$

$p_3 + k_3 = 17 + 4 \equiv 21 \pmod{26}$

$p_4 + k_4 = 12 + 17 \equiv 3 \pmod{26}$

$p_5 + k_5 = 8 + 12 \equiv 20 \pmod{26}$

$p_6 + k_6 -= 19 + 8 \equiv 1 \pmod{26}$.

Menerjemahkan angka di atas ke dalam huruf di peroleh ELVDUB.

Secara singkat, langkah – langkah untuk mengdeskripsikan pesan dari cipher stream sebagai berikut:

a. Ubah huruf pesan menjadi angka (lihat tabel 8.1),
b. Kunci diperoleh dengan $k_1 = s$, dimana s adalah setara numerik dari karakter awal,
c. Kita kurangi kunci dari karakter ciphertext Modulo pertama untuk menentukan karakter plaintext pertama, dan kemudian kita kurangi setara numerik dari masing-masing karakter plaintext modulo 26 dari karakter ciphertext berikutnya untuk mendapatkan karakter plaintext berikutnya,
d. Ubah angka menjadi huruf.

Contoh:

(Rosen, K.H. 2011. *Elementary Number Theory and Its Application Sixth Edition. Monmouth University*. Hal. 312)

Deskripskani pesan ciphertext RMNTU menggunakan kunci F (dengan setara numerik 5) . Pertama kita menerjemahkan karakter ciphertext menjadi setara numerik, didapat 17 12 13 19 20. Setara numerik dari karakter plaintext pertama, diperoleh dengan komputasi dengan $k_1 = s$, sehingga

$$p_1 = c_1 - s \equiv 17 - 5 \equiv 12 \pmod{26}.$$

Kita memperoleh setara numerik dari karakter plaintext berturut-turut sebagai berikut:

$$p_2 = c_2 - k_1 = 12 - 12 = 0 \pmod{26}$$
$$p_3 = c_3 - k_2 = 13 - 0 = 13 \pmod{26}$$
$$p_4 = c_4 - k_3 = 19 - 13 = 6 \pmod{26}$$
$$p_5 = c_5 - k_4 = 20 - 6 = 14 \pmod{26}.$$

Artikan angka tersebut dengan huruf,
MANGO.

Latihan:

1. Menggunakan Cipher Vigenere, enkripsikan pesan DO NOT OPEN THIS ENVELOPE dengan kunci SECRET.

(Rosen, K.H. 2011. *Elementary Number Theory and Its Application Sixth Edition. Monmouth University*. Hal. 313, No 1).

Jawab:

Pertama, artikan pesan dan kunci ke dalam angka (tabel 8.1)

D	O	N	O	T	O	P	E	N	T	H	I	S	E	N	V	E	L	O	P	E
3	14	13	14	19	14	15	4	13	19	7	8	18	4	13	21	4	11	14	15	4
p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}	p_{12}	p_{13}	p_{14}	p_{15}	p_{16}	p_{17}	p_{18}	p_{19}	p_{20}	p_{21}

dan,

S	E	C	R	E	T
18	4	2	17	4	19
k_1	k_2	k_3	k_4	k_5	k_6

Menggunakan Cipher Vigenere:

$c_i \equiv p_i + k_i \pmod{26}$

di peroleh:

$c_1 = p_1 + k_1 = 3 + 18 \equiv 21 \pmod{26}$

$c_2 = p_2 + k_2 = 14 + 4 \equiv 18 \pmod{26}$

$c_3 = p_3 + k_3 = 13 + 2 \equiv 15 \pmod{26}$

$c_4 = p_4 + k_4 = 14 + 17 \equiv 5 \pmod{26}$

$c_5 = p_5 + k_5 = 19 + 4 \equiv 23 \pmod{26}$

$c_6 = p_6 + k_6 = 14 + 19 \equiv 7 \pmod{26}$

$c_7 = p_7 + k_7 = 15 + 18 \equiv 7 \pmod{26}$

$c_8 = p_8 + k_8 = 4 + 4 \equiv 8 \pmod{26}$

$c_9 = p_9 + k_9 = 13 + 2 \equiv 15 \pmod{26}$

$c_{10} = p_{10} + k_{10} = 19 + 17 \equiv 10 \pmod{26}$

.

.

dst

Angka tersebut diartikan ke dalam huruf menggunakan tabel 8.1, kita peroleh

VSPFX HHIPK LBKIP MIEGT I.

2. Menggunakan Cipher Vigenere, deskripsikan pesan WBRCS LAZGJ MGKMF V dengan kunci SECRET.

   (Rosen, K.H. 2011. *Elementary Number Theory and Its Application Sixth Edition. Monmouth University*. Hal. 313, No 2).

   Jawab:

   Artikan pesan dan kunci tersebut dengan angka (lihat tabel 8.1).

W	B	R	C	S	L	A	Z	G	J	M	G	K	M	F	V
22	1	17	2	18	11	0	25	6	9	12	6	10	12	5	21
c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	c_{13}	c_{14}	c_{15}	c_{16}

   dan,

S	E	C	R	E	T
18	4	2	17	4	19
k_1	k_2	k_3	k_4	k_5	k_6

   Menggunakan Cipher Vigenere:

   $c_i \equiv p_i + k_i \pmod{26}$

   $p_i \equiv c_i - k_i \pmod{26}$

   di peroleh:

   $p_1 = c_1 - k_1 = 22 - 18 \equiv 4 \pmod{26}$

   $p_2 = c_2 - k_2 = 1 - 4 \equiv 23 \pmod{26}$

   $p_3 = c_3 - k_3 = 17 - 2 \equiv 15 \pmod{26}$

   $p_4 = c_4 - k_4 = 2 - 17 \equiv 11 \pmod{26}$

   $p_5 = c_5 - k_5 = 18 - 4 \equiv 14 \pmod{26}$

   $p_6 = c_6 - k_6 = 11 - 19 \equiv 18 \pmod{26}$

   $p_7 = c_7 - k_7 = 0 - 18 \equiv 8 \pmod{26}$

   $p_8 = c_8 - k_8 = 25 - 4 \equiv 21 \pmod{26}$

   $p_9 = c_9 - k_9 = 6 - 2 \equiv 4 \pmod{26}$

   .

   .

dst.

Angka tersebut diartikan ke dalam huruf menggunakan tabel 8.1, kita peroleh EXPLOSIVES INSIDE.

C. Penutup

Kesimpulan:

Disipin ilmu yang membahas sistem kerahasiaan disebut kriptologi. Kriptografi merupakan bagian dari kriptologi. Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi. Enkripsi adalah proses mengubah suatu pesan, data, atau informasi asli (plaintext) menjadi suatu pesan, data, atau informasi dalam bahasa sandi (ciphertext). Sedangkan dekripsi adalah proses mengubah pesan, data, atau informasi dalam suatu bahasa sandi (ciphertext) kembali menjadi pesan, data, atau informasi asli (plaintext).

Referensi

Rosen, K.H. 2011. *Elementary Number Theory and Its Application Sixth Edition. Monmouth University*.