PERTEMUAN 5
CRYPTOGRAPHY

A. TUJUAN PEMBELAJARAN

Pada Pertemuan ini akan dijelaskan mengenai kriptografi. Setelah mempelajari materi ini mahasiswa diharapkan mampu untuk:

1. Menjelaskan pengertian kriptografi
2. Memahami *symmetric chipers model*
3. Memahami Teknik Substitusi

B. URAIAN MATERI

1. Menjelaskan Pengertian Kriptografi

Kriptografi sebagai "seni menulis atau memecahkan kode." Ini secara historis akurat tetapi tidak menangkap luasnya bidang ini atau fondasi ilmiahnya saat ini. Definisi tersebut hanya berfokus pada kode-kode yang telah digunakan selama berabad-abad untuk memungkinkan komunikasi rahasia. Tetapi kriptografi saat ini mencakup lebih dari itu, berkaitan dengan mekanisme untuk memastikan integritas, teknik untuk bertukar kunci rahasia, protokol untuk mengautentikasi pengguna, lelang dan pemilihan elektronik, uang digital, dan banyak lagi. Tanpa mencoba memberikan karakterisasi yang lengkap, kami akan mengatakan bahwa kriptografi modern melibatkan studi teknik matematika untuk mengamankan informasi digital, sistem, dan komputasi terdistribusi terhadap serangan permusuhan.

Definisi kamus juga mengacu pada kriptografi sebagai seni. Sampai akhir abad ke-20, kriptografi memang sebagian besar merupakan seni. Membangun kode yang baik, atau memecahkan kode yang sudah ada, bergantung pada kreativitas dan pemahaman yang berkembang tentang cara kerja kode. Hanya ada sedikit teori yang dapat diandalkan dan, untuk waktu yang lama, tidak ada definisi yang berfungsi tentang apa yang merupakan kode yang baik. Dimulai pada 1970-an dan 1980-an, gambaran kriptografi ini berubah secara seluruhnya. Sebuah teori yang kaya mulai muncul, memungkinkan studi kriptografi yang ketat sebagai ilmu dan disiplin matematika. Perspektif ini, pada gilirannya,

memengaruhi cara para peneliti berpikir tentang bidang keamanan komputer yang lebih luas.

Perbedaan lain yang sangat penting antara kriptografi klasik (katakanlah, sebelum 1980-an) dan kriptografi modern berkaitan dengan pengadopsiannya. Secara historis, konsumen utama kriptografi adalah organisasi militer dan pemerintah. Hari ini, kriptografi ada dimana-mana, Jika anda pernah mengautentikasi diri dengan mengetik sandi, membeli sesuatu dengan kartu kredit melalui Internet, atau mengunduh pembaruan terverifikasi untuk sistem operasi Anda. Tidak diragukan lagi Anda telah menggunakan kriptografi. Dan, semakin banyak, programmer dengan pengalaman yang relatif sedikit diminta untuk "mengamankan" aplikasi yang mereka tulis dengan memasukkan mekanisme kriptografi.

Sistem kriptografi dicirikan oleh tiga dimensi independen, yaitu:

a. *The type of operations used for transforming plaintext to ciphertext,* Semua algoritma enkripsi didasarkan pada dua prinsip umum: substitusi, di mana setiap elemen dalam teks biasa (bit, huruf, kelompok bit atau huruf) dipetakan menjadi elemen lain, dan transposisi, di mana elemen dalam teks biasa disusun ulang. Persyaratan mendasar adalah tidak ada informasi yang hilang (yaitu, bahwa semua operasi dapat dibalik). Kebanyakan sistem, yang disebut sebagai sistem produk, melibatkan banyak tahapan substitusi dan transposisi.
b. *The number of keys used***,** Jika pengirim dan penerima menggunakan kunci yang sama, sistem ini disebut enkripsi simetris, kunci tunggal, kunci rahasia, atau konvensional. Jika pengirim dan penerima menggunakan kunci yang berbeda, sistem ini disebut sebagai enkripsi asimetris, dua kunci, atau kunci publik.
c. *The way in which the plaintext is processed***,** Sebuah block cipher memproses masukan satu blok elemen pada satu waktu, menghasilkan satu blok keluaran untuk setiap blok masukan. Stream cipher memproses elemen input secara terus menerus, menghasilkan output satu elemen pada satu waktu, seiring berjalannya waktu.

a. Cryptanalysis and Brute-Force Attack

Biasanya, tujuan menyerang sistem enkripsi adalah untuk memulihkan kunci yang digunakan daripada hanya untuk memulihkan teks biasa dari satu

teks sandi. Ada dua pendekatan umum untuk menyerang skema enkripsi konvensional:

1) Cryptanalysis

   Serangan cryptanalysis bergantung pada sifat dari algoritme ditambah mungkin beberapa pengetahuan tentang karakteristik umum dari teks biasa atau bahkan beberapa contoh pasangan teks-teks-teks. Jenis serangan ini memanfaatkan karakteristik algoritme untuk mencoba menyimpulkan teks biasa atau menyimpulkan kunci yang digunakan.

2) Brute-force attack

   Penyerang mencoba setiap kunci yang mungkin pada sepotong teks sandi sampai terjemahan yang jelas ke dalam teks biasa diperoleh. Rata-rata, setengah dari semua kunci yang mungkin harus dicoba untuk mencapai kesuksesan.

   Jika salah satu jenis serangan berhasil menyimpulkan kunci tersebut, efeknya adalah bencana besar: Semua pesan masa depan dan masa lalu yang dienkripsi dengan kunci tersebut akan disusupi.

Tabel 1. merangkum berbagai jenis cryptanalytic attacks berdasarkan jumlah informasi yang diketahui oleh kriptanalis. Masalah paling sulit disajikan ketika semua yang tersedia hanya ciphertext saja. Dalam beberapa kasus, bahkan algoritma enkripsi tidak diketahui, tetapi secara umum, kita dapat berasumsi bahwa lawan mengetahui algoritma yang digunakan untuk enkripsi. Satu kemungkinan serangan di bawah ini:

Tabel 2. Jenis Serangan pada Pesan Terenkripsi

Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext–ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

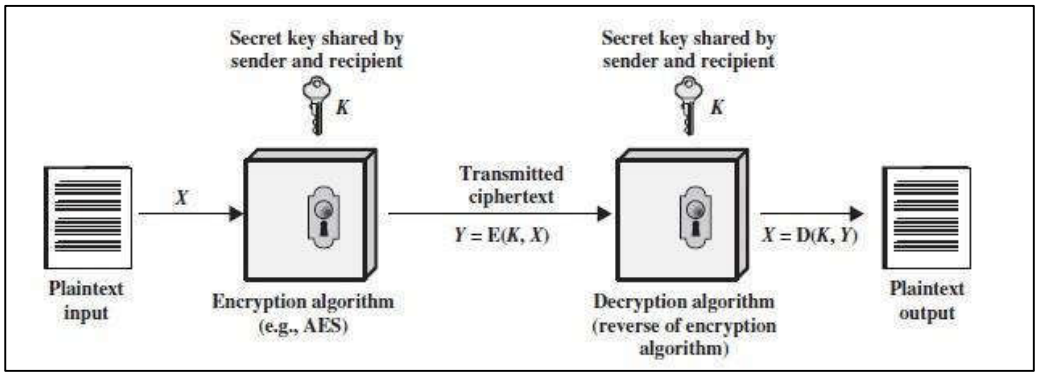
2. Memahami Symmetric Chipers Model

Symmetric Chiper Model atau skema enkripsi asimetris adalah algoritma untuk kriptografi yang menggunakan kunci kriptografi yang sama untuk enkripsi teks biasa dan dekripsi teks sandi . Kunci mungkin identik atau mungkin ada transformasi sederhana di antara dua kunci. Dalam praktiknya, kunci mewakili rahasia bersama antara dua pihak atau lebih yang dapat digunakan untuk memelihara tautan informasi pribadi. Persyaratan bahwa kedua belah pihak memiliki akses ke kunci rahasia adalah salah satu kelemahan utama enkripsi kunci simetris, dibandingkan dengan enkripsi kunci publik (juga dikenal sebagai enkripsi kunci asimetris). Lima bahan skema enkripsi simetris, diantaranya:

a. Plaintext: Ini adalah pesan atau data asli yang dapat dipahami yang dimasukkan ke dalam algoritme sebagai input.
b. Encryption algorithm: Algoritme enkripsi melakukan berbagai substitusi dan transformasi pada teks biasa.
c. Secret Key: Kunci rahasia juga dimasukkan ke dalam algoritma enkripsi. Kunci adalah nilai yang tidak bergantung pada teks biasa dan algoritme. Algoritme

akan menghasilkan keluaran yang berbeda tergantung pada kunci spesifik yang digunakan pada saat itu. Substitusi dan transformasi persis yang dilakukan oleh algoritme bergantung pada kunci.

d. Chipertext: Ini adalah pesan acak yang dihasilkan sebagai informasi. Itu tergantung pada teks biasa dan kunci rahasia. Untuk pesan tertentu, dua kunci berbeda akan menghasilkan dua teks sandi yang berbeda. Ciphertext adalah aliran data yang tampaknya acak dan, seperti berdiri, tidak dapat dipahami.
e. Decryption algorithm: pada dasarnya adalah algoritma enkripsi yang berjalan secara terbalik. Ini mengambil teks sandi dan kunci tersembunyi, kemudian mengbuahkan teks orisinil.



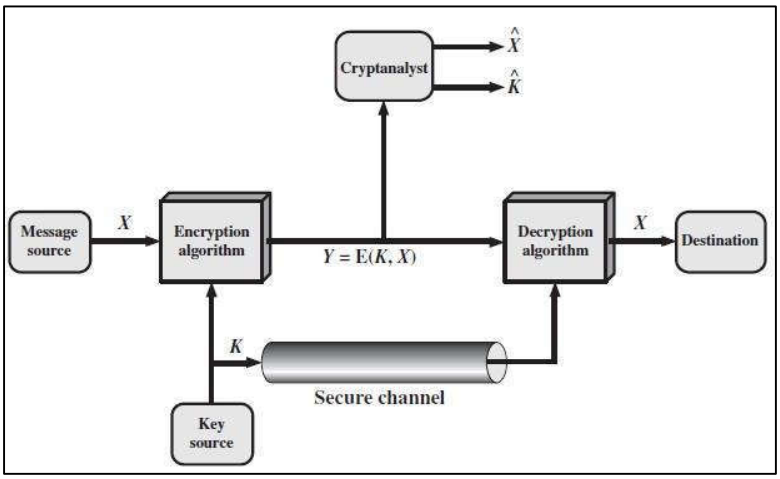
Gambar 6. Model Enkripsi Simetris yang Disederhanakan

Agar aman dari enkripsi konvensional, berikut dua syarat penggunaannya:

a. Kita membutuhkan algoritma enkripsi yang kuat. Paling tidak, kita ingin algoritme sedemikian rupa sehingga siapapun tidak akan dapat memecahkan ciphertext atau mengetahui kuncinya. Kondisi ini biasanya dinyatakan dalam bentuk yang lebih kuat: Lawan harus tidak dapat mendekripsi ciphertext atau menemukan kuncinya terlebih jika dia memiliki sejumlah ciphertext bersama dengan plaintext yang menghasilkan setiap ciphertext.
b. *Sender* dan *receiver* harus mendapatkan salinan dari kunci dengan cara yang aman juga mesti menyimpan kunci tersebut dengan aman. Apabila seseorang mampu menemukan dan mengetahui algoritma kunci tersebut, semua informasi/ komunikasi yang menggunakan kunci tersebut mampu untuk dibaca.

Tidak efektif untuk mendekripsi pesan berdasarkan ciphertext ditambah pengetahuan tentang algoritma enkripsi / dekripsi. Dengan kata lain, kita tidak

perlu merahasiakan algoritme; kita hanya perlu merahasiakan kuncinya. Fitur enkripsi simetris inilah yang membuatnya layak untuk digunakan secara luas. Fakta bahwa algoritme tidak perlu dirahasiakan.



Gambar 7. Model Sistem Kriptografi Simetris

Mengembangkan implementasi chip berbiaya rendah dari algoritma enkripsi data. chip ini banyak tersedia dan dapat digabungkan ke dalam sejumlah produk. Dengan penggunaan enkripsi simetris, masalah keamanan utama adalah menjaga kerahasiaan kunci.

Mari kita lihat lebih dekat pada elemen penting dari skema enkripsi simetris, menggunakan Gambar 2. Sumber menghasilkan pesan dalam teks biasa, X = [X1, X2, c, XM]. Unsur M dari X adalah huruf dalam beberapa alfabet terbatas. Secara tradisional, alfabet biasanya terdiri dari 26 huruf kapital. Saat ini, alfabet biner {0, 1} biasanya digunakan. Untuk enkripsi, kunci dalam bentuk K = [K1, K2, c, KJ] dibuat. Jika kunci dibuat di sumber pesan, maka kunci tersebut juga harus diberikan ke tujuan melalui beberapa saluran aman. Alternatifnya, pihak ketiga dapat membuat kunci dan mengirimkannya dengan aman ke sumber dan tujuan. Dengan pesan X dan kunci enkripsi K sebagai input, algoritma enkripsi membentuk ciphertext Y = [Y1, Y2, c, YN]. Kita bisa menulis ini sebagai

$$Y = E(K, X)$$

Notasi ini menunjukkan bahwa Y dihasilkan dengan menggunakan algoritma enkripsi E sebagai fungsi dari teks biasa X, dengan fungsi spesifik

ditentukan oleh nilai kunci K. Penerima yang dituju, yang memiliki kunci, mampu membalik:

$$X = D(K, Y)$$

Suatu yang berlawanan, mengamati Y tetapi tidak memiliki akses ke K atau X, dan dapat mencoba untuk memulihkan X atau K atau juga keduanya X dan K. Diasumsikan bahwa lawan mengetahui algoritma enkripsi (E) dan dekripsi (D). Jika lawan hanya tertarik pada pesan khusus ini, maka fokus dari usahanya adalah untuk memulihkan X dengan membuat perkiraan teks biasa X n. Seringkali, bagaimanapun, lawan tertarik untuk bisa membaca pesan masa depan juga, dalam hal ini upaya dilakukan untuk memulihkan K dengan membuat perkiraan K n.

3. Memahami Teknik Substitusi

Di bagian ini dan selanjutnya, kita memeriksa sampel dari apa yang mungkin disebut teknik enkripsi klasik. Sebuah studi tentang teknik ini memungkinkan kita untuk mengilustrasikan pendekatan dasar enkripsi simetris yang digunakan saat ini dan jenis serangan kriptanalitik yang harus diantisipasi.

Teknik substitusi adalah teknik dimana huruf-huruf dalam teks biasa diganti dengan huruf lain atau dengan angka atau simbol.1 Jika teks biasa dilihat sebagai urutan bit, maka substitusi melibatkan penggantian pola bit teks biasa dengan pola bit teks tersandi.

a. Caesar Cipher

Penggunaan sandi substitusi yang paling awal diketahui dan paling sederhana dilakukan oleh Julius Caesar. Sandi Caesar melibatkan penggantian setiap huruf alfabet dengan huruf berdiri tiga tempat lebih jauh di bawah alfabet. Sebagai contoh.

plain: temui aku setelah pesta toga

chiper: PHHW PH DIWHU WKH WRJD SDUWB

Perhatikan bahwa alfabet dililitkan sehingga huruf setelah Z adalah A. Kita dapat mendefinisikan transformasi dengan mendaftar semua kemungkinan, sebagai berikut:

plain: 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

cipher: 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

Mari kita tetapkan angka yang setara untuk setiap huruf:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Maka algoritmanya dapat diekspresikan sebagai berikut. Untuk setiap huruf p teks biasa, gantikan dengan huruf ciphertext C: 2

$$C = E(3, p) = (p + 3) \bmod 26$$

Pergeseran bisa berapapun jumlahnya sehingga algoritma Caesar umumnya adalah:

$$C = E(k, p) = (p + k) \bmod 26$$

di mana k mengambil nilai dalam rentang 1 hingga 25. Algoritme dekripsi sederhana:

$$p = D(k, C) = (C - k) \bmod 26$$

Jika diketahui bahwa ciphertext yang diberikan adalah sandi Caesar, maka kriptanalisis brute force mudah dilakukan: coba saja semua 25 kunci yang mungkin. Gambar 3 menunjukkan hasil penerapan strategi ini pada contoh ciphertext. Dalam kasus ini, teks biasa muncul sebagai menempati baris ketiga.

Tiga karakteristik penting dari masalah ini memungkinkan kami untuk menggunakan kriptanalisis brute force:

1) Algoritma enkripsi dan dekripsi diketahui.
2) Hanya ada 25 kunci untuk dicoba.
3) Bahasa teks biasa dikenal dan mudah dikenali.

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

Gambar 8. *Brute-Force Cryptanalysis of Caesar Chiper*

b. Monoalphabetic Ciphers

Dengan hanya 25 kemungkinan kunci, sandi Caesar jauh dari aman. Peningkatan dramatis dalam ruang kunci dapat dicapai dengan mengizinkan penggantian yang sewenang-wenang. Sebelum melanjutkan, kami mendefinisikan istilah permutasi. Permutasi dari himpunan hingga elemen S adalah urutan terurut dari semua elemen S, dengan setiap elemen muncul tepat satu kali. Misalnya, jika S = {a, b, c}, ada enam permutasi dari S:

abc, acb, bac, bca, cab, cba

Secara umum, terdapat n! permutasi himpunan n elemen, karena elemen pertama dapat dipilih dengan salah satu dari n cara, yang kedua dengan n - 1 cara, yang ketiga dengan n - 2 cara, dan seterusnya. Ingat tugas untuk sandi Caesar:

plain: 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

cipher: 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

Sebaliknya, jika baris "sandi" dapat berupa permutasi apa pun dari 26 karakter alfabet, maka ada 26! atau lebih besar dari 4 * 1026 kemungkinan kunci. Ini adalah 10 kali lipat lebih besar dari ruang kunci untuk DES dan tampaknya menghilangkan teknik brute force untuk kriptanalisis. Pendekatan semacam itu disebut sebagai sandi substitusi monoalphabetic, karena satu alfabet sandi (pemetaan dari alfabet biasa ke alfabet sandi) digunakan per pesan.

Namun, ada garis serangan lain. Jika kriptanalis mengetahui sifat dari teks biasa, maka analis dapat memanfaatkan keteraturan bahasa tersebut. Untuk melihat bagaimana kriptanalisis dapat berjalan, kami memberikan contoh parsial di sini yang diadaptasi dari salah satu di [SINK09]. Ciphertext yang harus dipecahkan adalah:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ

VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

Sebagai langkah pertama, frekuensi relatif huruf dapat ditentukan dan dibandingkan dengan distribusi frekuensi standar untuk bahasa Inggris, seperti yang ditunjukkan pada Gambar 4.

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

Gambar 9. Distribusi Frekuensi

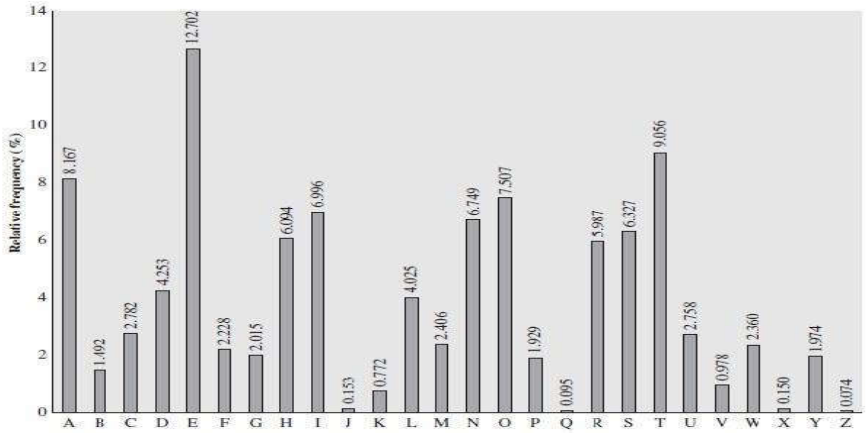
Membandingkan rincian ini dengan Gambar 3 nampaknya huruf sandi P dan Z setara dengan huruf biasa e dan t, tetapi tidak pasti yang mana. Huruf S, U, O, M, dan H semuanya memiliki frekuensi yang relatif tinggi dan mungkin

berhubungan dengan huruf biasa dari himpunan {a, h, i, n, o, r, s}. Huruf-huruf dengan frekuensi terendah (yaitu, A, B, G, Y, I, J) kemungkinan besar termasuk dalam himpunan {b, j, k, q, v, x, z}.

Ada beberapa cara untuk melanjutkan pada tahap ini. Kita dapat membuat beberapa tugas tentatif dan mulai mengisi teks biasa untuk melihat apakah itu tampak seperti "kerangka" pesan yang masuk akal. Pendekatan yang lebih sistematis adalah mencari keteraturan lainnya. Misalnya, kata-kata tertentu mungkin diketahui ada di dalam teks. Atau kita bisa mencari urutan huruf sandi yang berulang dan mencoba menyimpulkan padanan teks biasa mereka.

alat yang ampuh adalah dengan melihat frekuensi kombinasi dua huruf, yang dikenal sebagai digram. Tabel yang mirip dengan Gambar 3 dapat dibuat untuk menunjukkan frekuensi relatif dari digram. Digram seperti itu yang paling umum adalah th. Dalam ciphertext kami, diagram yang paling umum adalah ZW, yang muncul tiga kali. Jadi kita buat korespondensi Z dengan t dan W dengan h. Kemudian, dengan hipotesis sebelumnya, kita dapat menyamakan P dengan e. Sekarang perhatikan bahwa urutan ZWP muncul di ciphertext, dan kita dapat menerjemahkan urutan itu sebagai "the." Ini adalah trigram (kombinasi tiga huruf) yang paling sering digunakan dalam bahasa Inggris, yang sepertinya menunjukkan bahwa kita berada di jalur yang benar.

Selanjutnya, perhatikan urutan ZWSZ di baris pertama. Kita tidak tahu bahwa keempat huruf ini membentuk kata yang lengkap, tetapi jika demikian, bentuknya th_t. Jika demikian, S sama dengan a.



Gambar 10. Relative Frequency of Letters

c. Playfair Cipher

Sandi enkripsi banyak huruf yang paling terkenal adalah Playfair, yang memperlakukan diagram dalam teks biasa sebagai unit tunggal dan menerjemahkan unit-unit ini menjadi diagram ciphertext.

Algoritma Playfair didasarkan pada penggunaan matriks huruf 5 * 5 yang dibuat menggunakan kata kunci. Berikut adalah contoh yang dipecahkan oleh Lord Peter Wimsey dalam Dorothy Sayers's Have His Carcase.

Tabel 3. Contoh Matriks Huruf 5*5

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Dalam hal ini, kata kuncinya adalah monarki. Matriks dibuat dengan mengisi huruf-huruf dari kata kunci (minus duplikat) dari kiri ke kanan dan dari atas ke bawah, dan kemudian mengisi sisa matriks dengan huruf-huruf yang tersisa dalam urutan abjad. Huruf I dan J dihitung sebagai satu huruf. Plaintext dienkripsi dua huruf sekaligus, menurut aturan berikut:

1) Huruf teks biasa yang berulang dalam pasangan yang sama dipisahkan dengan huruf pengisi, seperti x, sehingga balon akan diperlakukan sebagai ba lx lo on.
2) Dua huruf teks biasa yang berada dalam baris matriks yang sama masing-masing diganti dengan huruf di sebelah kanan, dengan elemen pertama baris secara melingkar mengikuti yang terakhir. Misalnya, ar dienkripsi sebagai RM.
3) Dua huruf teks biasa yang berada di kolom yang sama masing-masing diganti dengan huruf di bawahnya, dengan elemen teratas kolom secara melingkar mengikuti yang terakhir. Misalnya, mu dienkripsi sebagai CM.
4) Jika tidak, setiap huruf teks biasa berpasangan diganti dengan huruf yang ada di barisnya sendiri dan kolom yang ditempati oleh huruf teks biasa lainnya. Jadi, hs menjadi BP dan ea menjadi IM (atau JM, sesuai keinginan pembuat enkrip).

C. SOAL LATIHAN/ TUGAS

1. Jelaskan definsi cryptography yang Anda ketahui!
2. Sebutkan dan jelaskan system cryptography!
3. Sebutkan persyaratan untuk penggunaan yang aman dari enkripsi konvensional!
4. Sebutkan dan jelaskan Skema enkripsi simetris!
5. Sebagai seorang kriptografer, keahlian apa yang paling utama selain kemampuan secara teknis mengenai persandian?

D. REFERENSI

Goodrich Stallings william (2014), Cryptography and Network Security Principles and Practice (6th Edition) Tersedia di : https://z-lib.org/

Katz Jonathan, Lindell Yehuda (2014), Introduction to Modern Cryptography, Second Edition Tersedia di: https://z-lib.org/

Goodrich Michael, Tamassia Roberto (2014), Introduction to Computer Security : Pearson New International Edition. Tersedia di : https://z-lib.org/

Paar Chirstof, Pelzl Jan (2009), Understanding Cryptography : A Textbook For Student and Practitioners. Tersedia di : https://z-lib.org/