MODUL KRIPTOGRAFI

(CTI 312)

MODUL 2

TEKNIK ALGORITMA KRIPTOGRAFI

DISUSUN OLEH

IR. NIZIRWAN ANWAR, M.T

UNIVERSITAS ESA UNGGUL

2020

MODUL 2
TEKNIK ALGORITMA KRIPTOGRAFI

1. PENDAHULUAN

Dalam teknik Dasar Kriptografi terbagi 5 (lima) kelompok yaitu :

1) SUBSTITUSI

2) BLOCKING

3) PERMUTASI

4) EKSPANSI

5) **PEMAMPATAN**

1.1 TEKNIK SUBSTITUSI

Dalam kriptografi, sandi substitusi adalah jenis metode enkripsi dimana setiap satuan pada teks terang digantikan oleh teks tersandi dengan tabel yang teratur. Metode penyandian substitusi telah dipakai dari kriptografi klasik hingga kriptografi modern. Langkah pertama adalah membuat suatu tabel substitusi. Tabel substitusi dapat dibuat sesuka hati, dengan catatan bahwa penerima pesan memiliki tabel yang sama untuk keperluan decrypt. Bila tabel substitusi dibuat secara acak, akan semakin sulit pemecahan ciphertext oleh orang yang tidak berhak.

Metode ini dilakukan dengan mengganti setiap huruf dari teks asli dengan huruf lain sebagai huruf sandi yang telah didefinisikan sebelumnya oleh algoritma kunci.

1.2 TEKNIK BLOCKING

Sistem enkripsi ini terkadang membagi plaintext menjadi beberapa blok yang terdiri dari beberapa karakter, kemudian di enkripsikan secara independen.

Caranya : Plaintext dituliskan secara vertikal ke bawah berurutan pada lajur, dan dilanjutkan pada kolom berikutnya sampai seluruhnya tertulis. ciphertext-nya adalah hasil proses plaintext secara horizontal berurutan sesuai dengan blok-nya.

1.3 TEKNIK PERMUTASI

Salah satu teknik enkripsi yang terpenting adalah permutasi atau sering juga disebut transposisi. Teknik ini memindahkan atau merotasikan karakter dengan aturan tertentu. Prinsipnya adalah berlawanan dengan teknik substitusi. Dalam teknik substitusi, karakter berada pada posisi yang tetap tapi identitasnya yang diacak. Pada teknik permutasi, identitas karakternya tetap, namun posisinya yang diacak.

Caranya sebelum dilakukan permutasi, umumnya plaintext terlebih dahulu dibagi menjadi blok-blok dengan panjang yang sama. Plaintext akan dibagi menjadi blok-blok yang terdiri dari 6 karakter, untuk mencari chipertext pada teknik ini.

1.4 TEKNIK EKSPANSI

Suatu metode sederhana untuk mengacak pesan adalah dengan memelarkan pesan itu dengan aturan tertentu. Salah satu contoh penggunaan teknik ini adalah dengan meletakkan huruf konsonan atau bilangan ganjil yang menjadi awal dari suatu kata di akhir kata itu dan menambahkan akhiran “an”. Jika suatu kata dimulai dengan huruf vokal atau bilangan genap, ditambahkan akhiran “i”.

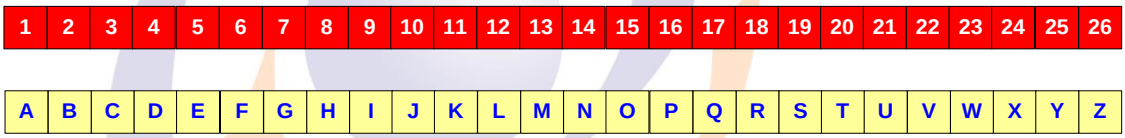
1.5 TEKNIK PEMAMPATAN

Mengurangi panjang pesan atau jumlah bloknya dengan cara lain untuk menyembunyikan isi pesan.

Contoh sederhana ini menggunakan cara menghilangkan setiap karakter ke-tiga secara berurutan. Karakter-karakter yang dihilangkan disatukan kembali dan disusulkan sebagai “lampiran” dari pesan utama, dengan diawali oleh suatu karakter khusus, dalam contoh ini menggunakan ” * “.

2. TUTORIAL TEKNIK KRIPTOGRAFI

Contoh tutorial pembuatan enkripsi dalam teknik kriptografi dengan sebuah plaintext (diketahui), di bawah ini

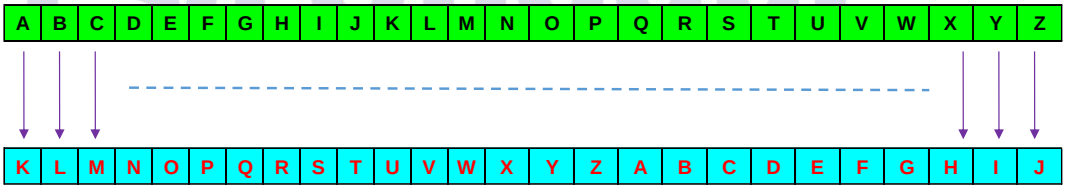


Gambar 2.1 Urutan Abjad Alfabet Fonetik ICAO

2.1 TEKNIK SUBSTITUSI

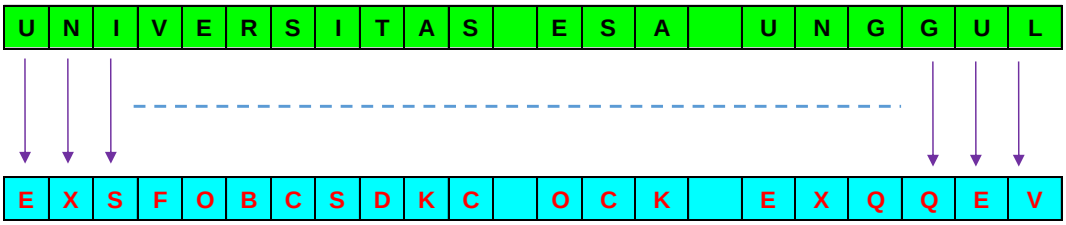
Contoh 1 : Substitusi (ROT10)

Dalam susunan alphabet dengan teknik subsitusi ROT10, akan terjadi pergeseran abjad A → K, B → L, C → M …dst (gambar 2.2)



Gambar 2.2 Subsitusi (ROT10)

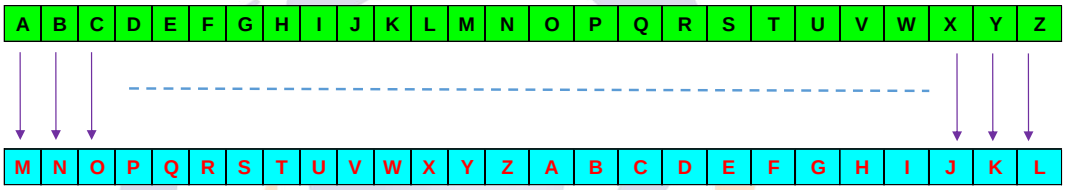
Bila plaintext “UNIVERSITAS ESA UNGGUL”, maka akan menghasilkan chipertext dengan menggunakan gambar 2.2 diatas



Gambar 2.3 Chipertext Teknik Subsitusi (ROT10)

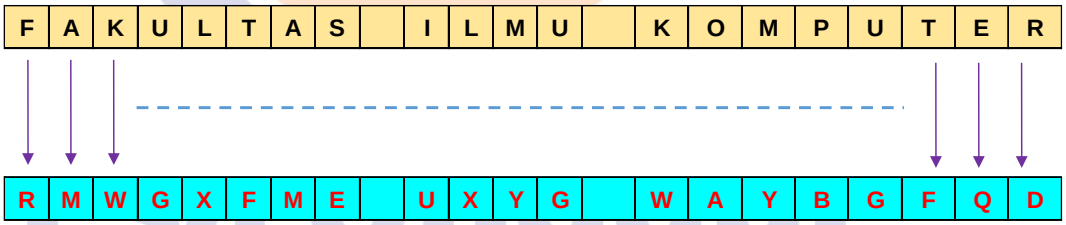
Plaintext	Chipertext
UNIVERSITAS ESA UNGGUL	EXSFOBCSDKC OCK EXQQEV

Contoh 2 : Substitusi (ROT12)



Gambar 2.4 Subsitusi (ROT12)

Bila plaintext “FAKULTAS ILMU KOMPUTER”, maka akan menghasilkan chipertext dengan menggunakan gambar 2.4 diatas

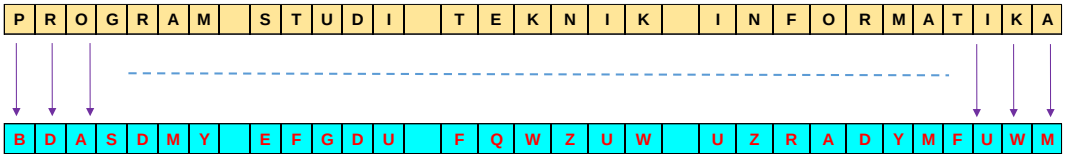


Gambar 2.5 Chipertext Teknik Subsitusi (ROT12)

Plaintext	Chipertext
FAKULTAS ILMU KOMPUTER	RMWGXFME UXYG WAYBGFQD

Contoh 3 : Substitusi (ROT12)

Dengan cara yang sama pada contoh 2 dan 3, pada contoh 3 dengan plaintext “PROGRAM STUDI TEKNIK INFORMATIKA” menghasilkan chipertext pada gambar 2.6



Gambar 2.6 Chipertext Teknik Subsitusi (ROT12)

Plaintext	Chipertext
PROGRAM STUDI TEKNIK INFORMATIKA	BDASDMY EFGDU FQWZUW UZRADYMFUWM

2.2 TEKNIK BLOCKING

Contoh 1 ; Plaintext

Gambar 2.7 Plaintext Teknik Blocking (contoh 1)

Tabel 2.1 Blocking K = 5 dan 5 Kolom

	1	2	3	4	5
Block 1	U	R	S		U
Block 2	N	S		U	L
Block 3	I	I	E	N	
Block 4	V	T	S	G	
Block 5	E	A	A	G	

Tabel 2.2 Blocking K = 7 dan 4 Kolom

	1	2	3	4
Block 1	U	I	A	L
Block 2	N	T		
Block 3	I	A	U	
Block 4	V	S	N	
Block 5	E		G	
Block 6	R	E	G	
Block 7	S	S	U	

Tabel 2.3 Blocking K = 9 dan 3 Kolom

	1	2	3
Block 1	U	A	G
Block 2	N	S	G
Block 3	I		U
Block 4	V	E	L
Block 5	E	S	
Block 6	R	A	
Block 7	S		
Block 8	I	U	
Block 9	T	N	

Tabel 2.4 Blocking K = 11 dan 2 Kolom

	1	2
Block 1	U	
Block 2	N	E
Block 3	I	S
Block 4	V	A
Block 5	E	
Block 6	R	U
Block 7	S	N
Block 8	I	G
Block 9	T	G
Block 10	A	U
Block 11	S	L

Dari hasil blocking dari yang disajikan 4 (empat) tabel contoh 1 diatas, menghasilkan chipertext

Tabel 2.5 Chipertext untuk Blocking K = 5, 7, 9 dan 11

	PlainText = " UNIVERSITAS ESA UNGGUL"										
	Chipertext										
5	U RSU	N SUL	I IEN	V TSG	E AAG						
7	U IAL	N T	I AU	V SN	E G	R EG	S SU				
9	U AG	N SG	I U	V EL	E S	R A	S	I U	T N		
11	U	N E	I S	V A	E	R U	S N	I G	T G	A U	S L

Contoh 2 ; Plaintext

F	A	K	U	L	T	A	S		I	L	M	U		K	O	M	P	U	T	E	R

Gambar 2.8 Plaintext Teknik Blocking (contoh 2)

Tabel 2.6 Blocking K = 5 dan 5 Kolom

	1	2	3	4	5
Block 1	F	T	L	O	E
Block 2	A	A	M	M	R
Block 3	K	S	U	P	
Block 4	U			U	
Block 5	L	I	K		

Tabel 2.7 Blocking K = 7 dan 4 Kolom

	1	2	3	4
Block 1	F	S	K	R
Block 2	A		O	
Block 3	K	I	M	
Block 4	U	L	P	
Block 5	L	M	U	
Block 6	T	U	T	
Block 7	A		E	

Tabel 2.8 Blocking K = 9 dan 3 Kolom

	1	2	3
Block 1	F	I	U
Block 2	A	L	T
Block 3	K	M	E
Block 4	U	U	R
Block 5	L		
Block 6	T	K	
Block 7	A	O	
Block 8	S	M	
Block 9		P	

Tabel 2.9 Blocking K = 11 dan 2 Kolom

	1	2
Block 1	F	L
Block 2	A	M
Block 3	K	U
Block 4	U	
Block 5	L	K
Block 6	T	O
Block 7	A	M
Block 8	S	P
Block 9	T	T
Block 10		E
Block 11	I	R

Dari hasil blocking dari yang disajikan 4 (empat) tabel contoh 2 diatas, menghasilkan chipertext

Tabel 2.10 Chipertext untuk Blocking K = 5, 7, 9 dan 11

PlainText = " FAKULTAS ILMU KOMPUTER"

Chipertext

5	F TLOE	A AMMR	K SUP	U U	L IK					
7	F SKR	A O	K IM	U LP	L MU	T UT	A E			
9	F IU	A LT	K ME	U UR	L	T K	A O	S M	P	
11	F L	A M	K U	U	L K	T O	A M	S P	T T	E	I R

2.3 TEKNIK PERMUTASI

Plaintext diketahui (contoh),

UNIVERSITAS ESA UNGGUL FAKULTAS ILMU KOMPUTER PROGRAM STUDI TEKNIK INFORMATIKA

Dengan menggunakan asumsi permutasi yang terdiri 6 karakter dimana karakter pertama bertukar tempat dengan karakter terakhir,

karakter kedua menjadi karakter kelima dan sebaliknya kemudia karakter ketiga menjadi ke-empat.

Tabel 2.11 Plaintext Teknik Permutasi

U	N	I	V	E	R	S	I	T	A	S		E	S	A		U	N
G	G	U	L		F	A	K	U	L	T	A	S		I	L	M	U
	K	O	M	P	U	T	E	R		P	R	O	G	R	A	M	
S	T	U	D	I		T	E	K	N	I	K	I	N	F	O	R	M
A	T	I	K	A													

Dengan teknik permutasi (6 karakter) akan menghasilkan ciphertext

Tabel 2.12 Chipertext Teknik Permutasi

R	E	V	I	N	U		S	A	T	I	S	N	U		A	S	E
F		L	U	G	G	A	T	L	U	K	A	U	M	L	I		S
U	P	M	O	K		R	P		R	E	T		M	A	R	G	O
	I	D	U	T	S	K	I	N	K	E	T	M	R	O	F	N	I
	A	K	I	T	A												

Chipertext

REVINU SATISNU ASEF LUGGATLUKAUMLI SUPMOK RP RET MARGO IDUTSKINKETMROFNI AKITA

Plaintext	Chipertext
UNIVERSITAS ESA UNGGUL FAKULTAS ILMU KOMPUTER PROGRAM STUDI TEKNIK INFORMATIKA	REVINU SATISNU ASEF LUGGATLUKAUMLI SUPMOK RP RET MARGO IDUTSKINKETMROFNI AKITA

2.4 TEKNIK EKSPANSI

Pada teknik ini dengan menggunakan dimana aturan tiap kata dengan huruf vocal akan ditambahkan dengan imbuhan “-i” pada akhir kalimatnya, dan untuk awal huruf konsonan depan dipindahkan ke belakang kata serta ditambahkan dengan imbuhan “-an” di akhir kata.

Bila plaintext

UNIVERSITAS ESA UNGGUL FAKULTAS ILMU KOMPUTER PROGRAM STUDI TEKNIK INFORMATIKA

Sehingga chipertext menjadi

UNIVERSITASI ESAI UNGGULI AKULTASFAN ILMUI OMPUTERKAN ROGRAMPAN TUDISAN EKNIKTAN NFORMATIKAI

Plaintext	Chipertext
UNIVERSITAS ESA UNGGUL FAKULTAS ILMU KOMPUTER PROGRAM STUDI TEKNIK INFORMATIKA	UNIVERSITASI ESAI UNGGULI AKULTASFAN ILMUI OMPUTERKAN ROGRAMPAN TUDISAN EKNIKTAN NFORMATIKAI

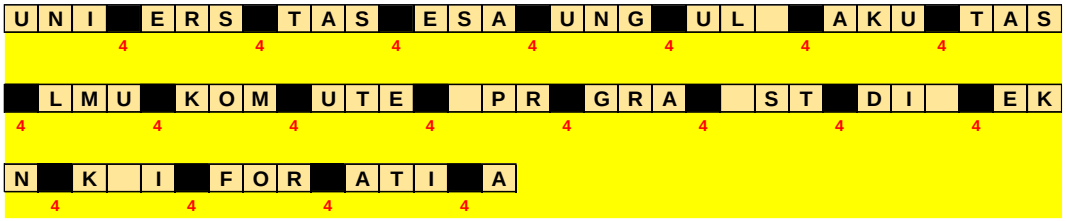
2.5 TEKNIK PEMAMPATAN

Tabel 2.13 Plaintext Teknik Pemampatan

U	N	I	V	E	R	S	I	T	A	S		E	S	A		U	N	G	G	U	L		F	A	K	U	L	T	A	S		
I	L	M	U		K	O	M	P	U	T	E	R		P	R	O	G	R	A	M		S	T	U	D	I		T	E	K			
N	I	K		I	N	F	O	R	M	A	T	I	K	A																				

Kemudian dari plaintext yang telah disusun dalam tabel 2.13 kita block (warna hitam) per 4 karakter (gambar 2.14).

Tabel 2.14 Blocking Plaintext 4 karakter



Pesan yang dimampatkan yang dihasilkan pem-blockan dari tabel 2.14

Tabel 2.15 Pemampatan Plaintext 4 karakter

Sehingga chipertext dari teknik pemampatan adalah

UNIERSTASESAUNGUL AKUTASLMUKOMUTE PRGRA STDI EKNK IFORATI A &VI G FLI PROM U TI NMK

Plaintext	Chipertext
UNIVERSITAS ESA UNGGUL FAKULTAS ILMU KOMPUTER PROGRAM STUDI TEKNIK INFORMATIKA	UNIERSTASESAUNGUL AKUTASLMUKOMUTE PRGRA STDI EKNK IFORATI A &VI G FLI PROM U TI NMK

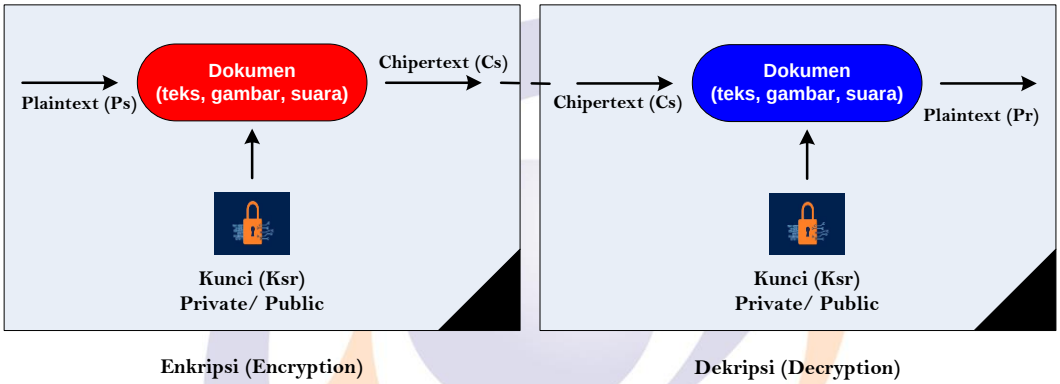
3. PERKEMBANGAN TEKNIK KRIPTOGRAFI

Dalam teknik kriptografi berdasarkan perkembangan terbagi menjadi 2 (dua), antara lain

1) Kriptografi klasik

2) Kriptografi modern

Baik klasik maupun modern dalam memproses data yang akan diamankan ‘secure’ kita harus menentukan bentuk algoritma yang berkaitan dengan enkripsi (***encryption***) dan dekripsi (***decryption***), plaintext menjadi chipertext dan agar utuh kembali maka harus satu proses lagi chipertext menjadi plaintext



Gambar 2.8 Konsep Umum Kriptografi

3.1 KLASIK

Bentuk awal dari penulisan rahasia membutuhkan lebih sedikit dari implementasi penulisan sejak banyak orang tidak dapat membaca. lawan yang lebih terpelajar, membutuhkan kriptografi yang nyata. Tipe sandi klasik utama ialah **sandi transposisi**, di mana mengatur aturan huruf pada dan **sandi subtitusi,** di mana secara sistematis metode **mono-alphabet** dan atau **poly-alphabet**.

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

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

Gambar 2.8 Susunan Alfabet

Enkripsi digunakan untuk menyakinkan kerahasiaan di komunikasi, termasuk teknik untuk pemeriksaan integritas pesan, autentikasi identitas pengirim/penerima, tanda-tangan digital, bukti interaktif dan komputasi keamanan, serta banyak lagi yang lain.

3.1.1 Mono-Alphabet (contoh)

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
Jika penggeseran yang dilakukan sebanyak 3 kali																									
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

Langkah proses enkripsi untuk mendapatkan chipertext ;

[1] Plaintext

TEKNIK KRIPTOGRAFI																
T	E	K	N	I	K		K	R	I	P	T	O	G	R	A	F	I

[2] Chipertext

WHNQLN NULSWRJUDIL																
W	H	N	Q	L	N		N	U	L	S	W	R	J	U	D	I	L

3.1.2 Poly-Alphabet (contoh)

1) Satu Kunci

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
Jika penggeseran yang dilakukan sebanyak 3 kali																									
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

Langkah proses enkripsi untuk mendapatkan chipertext ;

[1] Plaintext

TEKNIK KRIPTOGRAFI																
T	E	K	N	I	K	K	R	I	P	T	O	G	R	A	F	I

[2] Kunci Tunggal

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

[3] Chipertext

QBHKFH HOFMQLDOACF																
Q	B	H	K	F	H		H	O	F	M	Q	L	D	O	A	C	F

2) Dua Kunci

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
Jika penggeseran yang dilakukan sebanyak 3 kali																									
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

Langkah proses enkripsi mendapatkan chipertext ;

[1] Plaintext

TEKNIK KRIPTOGRAFI																
T	E	K	N	I	K	K	R	I	P	T	O	G	R	A	F	I

[2] Kunci K1 dan K2

K1

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

K2

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

[3] Posisi Chiper, K1 dan K2

Chipertext	K1	K2	K1	K2	K1	K2		K1	K2	K1	K2	K1	K2	K1	K2	K1	K2	K1
Posisi K1	K1		K1		K1			K1		K1		K1		K1		K1		K1
Posisi K2		K2		K2		K2			K2		K2		K2		K2		K2	

[4] Enkripsi dengan K1 dan K2

QIHGFG HQFOQMDQAAF																	
Q	I	H	G	F	G		H	Q	F	O	Q	M	D	Q	A	A	F

[5] Chipertext

QIHGFG HQFOQMDQAAF

3) Tiga Kunci

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
Jika penggeseran yang dilakukan sebanyak 3 kali																									
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

Langkah proses enkripsi mendapatkan chipertext

[1] Plaintext

TEKNIK KRIPTOGRAFI																	
T	E	K	N	I	K		K	R	I	P	T	O	G	R	A	F	I

[2] Kunci K1 K2 dan K3

K1

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

K2

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

K3

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

[3] Posisi Chiper, K1, K2 dan K3

Chipertext	K1	K2	K3	K1	K2	K3		K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2
Posisi K1	K1			K1				K1			K1			K1			K1	
Posisi K2		K2			K2				K2			K2			K2			K2
Posisi K3			K3			K3				K3			K3			K3		

[4] Enkripsi dengan K1, K2 dan K3

VBCKFI HODMSHDQICD

V	B	C	K	F	I		H	O	D	M	S	H	D	Q	I	C	D

[5] Chipertext

VBCKFI HODMSHDQICD

3.2 MODERN

Kriptografi modern merupakan hasil dari suatu pengembangan kriptografi klasik dan berbasis bit dalam rangka mendukung era computer berbasis digital. Dan pada konsep ini menggunakan algoritma beroperasi dalam mode bit dibandingkan dengan kriptografi konvensional pada mode karakter. Teknik kriptografi modern secara detail akan dibahas lebih lanjut pada modul-modul berikutnya