TEKNIK CRYPTOGRAPHY (KRIPTOGRAFI) BAGIAN 1

PERTEMUAN 4

METODE KRIPTOGRAFI

Klasik

Modern

KRIPTOGRAFI KLASIK

- Teknik subsitusi: sebuah teknik enkripsi yang menggunakan metode pertikaran huruf pada plainteks dengan huruf lainnya atau dengan angka atau dengan simbol tertentu
- Contoh Teknik subsitusi:
  - monoalphabetic cipher
  - Caesar Cipher
  - Polyalphabetic cipher

MONOALPHABETIC CIPHER

- Satu karakter di plainteks diganti dengan satu karakter yang bersesuaian
- Fungsi penyandian adalah fungsi satu ke satu
- Jika plainteks terdiri dari huruf-huruf abjad, maka jumlah kemungkinan susunan huruf-huruf cipherteks yang dapat dibuat adalah 26! = 403.291.461.126.605.635.584.000.000
- Caesar cipher adalah kasus khusus dari monoalphabetic cipher, dimana susunan huruf cipherteks diperoleh dengan menggeser huruf-huruf abjad sejauh 3 karakter
- ROT13 adalah program enkripsi sederhana yang ditemukan pada Sistem UNIX dengan k = 13
    - Huruf A diganti dengan N, B diganti dengan O, dst

CAESAR CIPHER

- Teknik enkripsi subsitusi yang pertama kali dan paling sederhana ditemukan oleh Julius Caesar.
- Caesar cipher disebut juga Sandi Shift, Kode Caesar, atau Caesar's SHIFT
- Metode yang digunakan dalam Caesar cipher dengan mempertukarkan setiap huruf dari plainteks dengan huruf yang lain dengan interval 3 huruf dari huruf plainteks

CONTOH CAESAR CIPHER

- Plain: Belajar Mengamankan Informasi Penting
- Cipher: EHODMDU PHQJDPDQNDQ LQIRUPDVL SHQWLQJ
- Pergeseran dan kunci = 3

RUMUS CAESAR CIPHER

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

Untuk plainteks diberikan simbol P sedangkan untuk cipherteks C dan K untuk Kunci, sedangkan rumusan adalah sebagai berikut:

$C = E(P) = (P + K) \bmod 26$, untuk rumus enkripsi

$P = D(C) = (C - K) \bmod 26$, untuk rumus dekripsi

CONTOH PENGERJAAN RUMUS ENKRIPSI CAESAR CIPHER

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

Plainteks : Belajar Mengamankan Informasi Penting
Kunci = 3
Cipherteks ?

E(B) = (B + 3) mod 26
= (1 + 3) mod 26
= 4 ➔ E

E(L) = (L + 3) mod 26
= (11 + 3) mod 26
= 14 ➔ O

E(J) = (J + 3) mod 26
= (9 + 3) mod 26
= 12 ➔ M

E(E) = (E + 3) mod 26
= (4 + 3) mod 26
= 7 ➔ H

E(A) = (A + 3) mod 26
= (0 + 3) mod 26
= 3 ➔ D

E(R) = (R + 3) mod 26
= (17 + 3) mod 26
= 20 ➔ U

Dst…. Hasil Cipherteks = EHODMDU PHQJDPDQNDQ LQIRUPDVL SHQWLQJ

CATATAN

- Pergeseran 0 sama dengan pergeseran 26 (susunan huruf tidak berubah)
- Pergeseran lain untuk k > 25 dapat juga dilakukan namun hasilnya akan kongruen dengan bilangan bulat dalam 26. Misalkan k= 37 kongruen dengan 11 dalam modulo 26, atau 37 ° 11 (mod 26)
- Karena ada operasi penjumlahan, maka Caesar cipher kadang-kadang dinamakan Additive cipher

CONTOH CAESAR CIPHER

- Plainteks: LUMPUR LAPINDO
- K = 7
- Cipherteks: ?

PENGERJAAN DENGAN MODULO

- E(L) = (L + 7) mod 26 = (11 + 7) mod 26 = 18 mod 26 = 18 ➔ S
- E(U) = (U + 7) mod 26 = (20 + 7) mod 26 = 27 mod 26 = 1 ➔ B
- E(M) = (M + 7) mod 26 = (12 + 7) mod 26 = 19 ➔ T
- E(P) = (15 + 7) mod 26 = 22 ➔ W
- E(R) = (17 + 7) mod 26 = 24 ➔ Y
- E(A) = 7 mod 26 = 7 ➔H

Dst…….

Cipherteks = SBTWBY SHWPUKV

PENGERJAAN DENGAN URUTAN INTEGER

L	U	M	P	U	R		L	A	P	I	N	D	O
11	20	12	15	20	17		11	0	15	8	13	3	14
+7	+7	+7	+7	+7	+7		+7	+7	+7	+7	+7	+7	+7
18	27	19	22	27	24		18	7	22	15	20	10	21
	-26			-26									
	1			1									
S	B	T	W	B	Y		S	H	W	P	U	K	V

Ciphertext = SBTWBY SHWPUKV

DEKRIPSI?

S	B	T	W	B	Y		S	H	W	P	U	K	V
18	1	19	22	1	24		18	7	22	15	20	10	21
-7	-7	-7	-7	-7	-7		-7	-7	-7	-7	-7	-7	-7
11	-6	12	15	-6	17		11	0	15	8	13	3	14
	+26			+26									
	20			20									
L	U	M	P	U	R		L	A	P	I	N	D	O

Plainteks = LUMPUR LAPINDO