Caesar Chipper

Subianto | AMIK JTC SEMARANG

Pengertian

Caesar Cipher merupakan salah satu algoritma cipher tertua dan paling diketahui dalam perkembangan ilmu kriptografi.

Caesar cipher merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan penukaran karakter pada plainteks menjadi tepat satu karakter pada chiperteks.

Teknik seperti ini disebut juga sebagai chiper abjad tunggal

- Inti dari algoritma kriptografi ini adalah melakukan pergeseran

Langka-langkah

- Menentukan besarnya pergeseran karakter yang digunakan dalam membentuk cipherteks ke plainteks.
- Menukarkan karakter pada plainteks menjadi cipherteks dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya.

Contoh

- Caesar Chiper dengan kunci pergeseran 4

pi : 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
ci : 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

Plaintext :
S U B I A N T O

Chipertext
W Y F M R X S

ALGORITMA

Algoritma dar Caesar cipher adalah jika (a=1.b=2, dan seterusnya).

Plaintex diberi simbol "P" dan cipher text adalah "C" dan kunci adalah "K".

- **Rumus untuk enskripsi :**

  C = E(P) = (P+K) mod (26)

- **Rumus untuk deskripsi :**

  P = D(C) = (C–K) mod (26)

- Dari contoh di atas, maka enskripsi dapat dilakukan dengan rumus :

  C= E(P) =(P+4) mod (26)

- Sedangkan untuk deskripsinya adalah :

  P = D(C) = (C–4) mod (26)

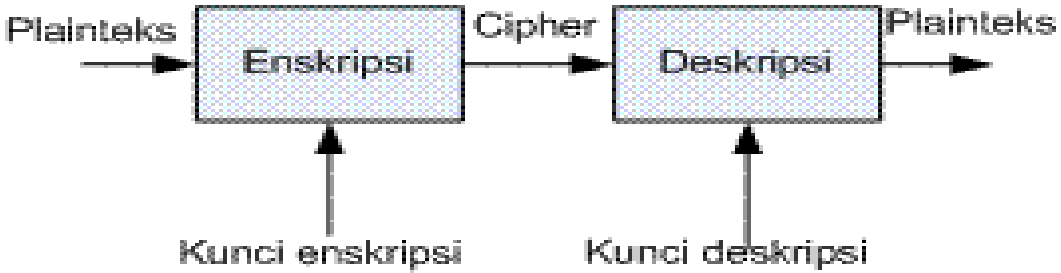
Kelemahan

- Tingkat keamanannya rendah, jumlah kuncinya hanya 26 kunci saja.
- Teknik pemecahan kata kunci dapat dilakukan dengan cara melakukan pengecekan terhadap semua kunci yang ada yang berjumlah 26 tersebut.

AFFINE Chipper

Subianto | AMIK JTC SEMARANG

GAMBARAN



Secara matematis, proses enkripsi merupakan pengoperasian fungsi E (enkripsi) menggunakan e (kunci enkripsi) pada M *(plaintext)* sehingga dihasilkan C *(ciphertext)*, notasinya :

$$\mathbf{E_e(M) = C}$$

Sedangkan untuk proses dekripsi, merupakan pengoperasian fungsi D (*desciption*) menggunakan d (kunci dekripsi) pada C *(ciphertext)* sehingga dihasilkan M *(plaintext)*, notasinya :

$$\mathbf{D_d(C) = M}$$

Sehingga dari dua hubungan diatas berlaku :

$$\mathbf{D_d(E_e(M)) = M}$$

Affine chipper

- *Affine cipher* pada metode *affine* adalah perluasan dari metode *Caesar Cipher*, yang mengalihkan plainteks dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran *P* menghasilkan cipherteks *C* dinyatakan dengan fungsi kongruen:

$$C \equiv m\,P + b \pmod{n}$$

n adalah ukuran alphabet, *m* adalah bilangan bulat yang harus relatif prima dengan *n* (jika tidak relatif prima, maka dekripsi tidak bisa dilakukan) dan b adalah jumlah pergeseran (*Caesar cipher* adalah khusus dari *affine cipher* dengan *m*=1).

- Untuk melakukan deskripsi, persamaan di atas harus dipecahkan untuk memperoleh *P*. Solusi kekongruenan tersebut hanya ada jika inver m (mod n), dinyatakan dengan m^{-1}. Jika m^{-1} ada maka dekripsi dilakukan dengan persamaan sebagai berikut:

$$\mathbf{P \equiv m^{-1}(C - b) \pmod{n}}$$

Gambaran Umum Sistem

Pengisian Huruf dan Angka

Huruf	A	B	C	…	…	X	Y	Z
Angka	0	1	2	…	…	23	24	25

Pengujian Plaintext

D	A	N	I
3	0	13	8

Plainteks:

D A N I

Ekivalen:

3 0 13 8

N = 26

K = Relatif Prima (1,3,**5**,**7**,9,11,15,17,19,21,23,25)

Kunci pertama = 5

Kunci kedua = 7

- *affine cipher* dengan mengambil m = 5 (karena 5 relatif prima dengan 26) dan b= 7. Karena alphabet yang digunakan 26 huruf, maka n = 26.
- Enkripsi plainteks dihitung dengan kekongruenan:

$$C \equiv 5P + 7 \pmod{26}$$

  - P1= 3 –> c1 ≡ 5.3 + 7 ≡ 22 (mod 26) ≡ 22 = W
  - P2= 0–> c2 ≡ 5.0 + 7 ≡ 7(mod 26) ≡ 7 = H
  - P3= 13 –> c3 ≡ 5.13 + 7 ≡ 72 (mod 26) ≡ 20 = U
  - P4= 8–> c4 ≡ 5.8 + 7 ≡ 47 (mod 26) ≡ 21 = V

W H U V

Pengujian Cippertext

W	H	U	V
22	7	20	21

Cipherteks:
W H U V W V Y H

Ekivalen:
22 7 20 21 22 21 24 7

N = 26
K = RelatifPrima (1,3,**5**,**7**,9,11,15,17,19,21,23,25)
Kunci pertama = 5
Kunci kedua = 7

- Untuk mengembalikan teks yang telah dienskripsi menjadi pesan rahasia dapat dilakukan pendekripsian, pertama-tama dapat dihitung 5^{-1} (mod 26), yang dapat dihitung dengan memecahkan kekongruenan lanjar.

$$\mathbf{5x \equiv 1 \pmod{26}}$$

- Untuk deskripsi dengan hasil 1 maka solusinya adalah

$$x = 21 \pmod{26}$$

dikarenakan

$$5.21 = 105 \bmod 26$$

menghasilkan = 1.

$P \equiv 21\ (C - 7) \pmod{26}$

- P1=22–> c1 ≡ 21.(22 – 7) ≡ 315(mod 26) ≡ 3 = D
- P2= 7 –> c2 ≡ 21.(7 – 7) ≡ 0 (mod 26) ≡ 0 = A
- P3=20 –> c3 ≡ 21.(20 – 7) ≡ 273(mod 26) ≡ 13 = N
- P4=21–> c4 ≡ 21.(21 – 7) ≡ 294(mod 26) ≡ 8 = I