Algoritma Kriptografi Klasik (bag 1)

IF5054 Kriptografi

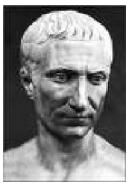
Pendahuluan

- Algoritma kriptografi klasik berbasis karakter
- Menggunakan pena dan kertas saja, belum ada komputer
- Termasuk ke dalam kriptografi kunci-simetri
- Tiga alasan mempelajari algoritma klasik:
  1. Memahami konsep dasar kriptografi.
  2. Dasar algoritma kriptografi modern.
  3. Memahami kelemahan sistem *cipher*.

Algoritma kriptografi klasik:

1. *Cipher* Substitusi (*Substitution Ciphers*)
2. *Cipher* Transposisi (*Transposition Ciphers*)

Cipher Substitusi



- Contoh: *Caesar Cipher*
- Tiap huruf alfabet digeser 3 huruf ke kanan

p_i : 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
c_i : **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**

- Contoh:
  Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX
  Cipherteks: **DZDVL DVWHULA GDQ WHPDQQBA REHOLA**

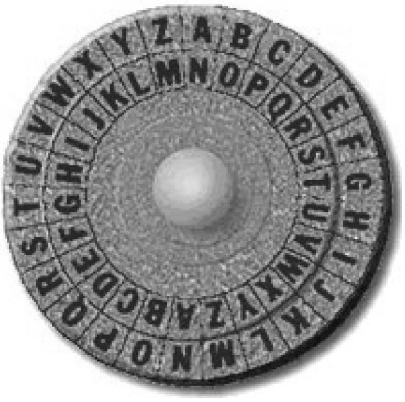
- Dalam praktek, cipherteks dikelompokkan ke dalam kelompok n-huruf, misalnya kelompok 4-huruf:

DZDV LDVW HULA GDQW HPDQ QBAR EHOL A

- Atau membuang semua spasi:

DZDVLDVWHULAGDQWHPDQQBAREHOLA

- Tujuannya agar kriptanalisis menjadi lebih sulit



- *Caesar wheel*

- Misalkan $A = 0$, $B = 1$, …, $Z = 25$, maka secara matematis caesar *cipher* dirumuskan sebagai berikut:

  Enkripsi: $c_i = E(p_i) = (p_i + 3) \bmod 26$
  Dekripsi: $p_i = D(c_i) = (c_i - 3) \bmod 26$

- Jika pergeseran huruf sejauh k, maka:

  Enkripsi: $c_i = E(p_i) = (p_i + k) \bmod 26$
  Dekripsi: $p_i = D(c_i) = (c_i - k) \bmod 26$
  k = kunci rahasia

- Untuk 256 karakter ASCII, maka:

  Enkripsi: $c_i = E(p_i) = (p_i + k) \bmod 256$
  Dekripsi: $p_i = D(c_i) = (c_i - k) \bmod 256$
  k = kunci rahasia

Kelemahan:

Caesar cipher mudah dipecahkan dengan *exhaustive key search* karena jumlah kuncinya sangat sedikit (hanya ada 26 kunci).

Contoh: kriptogram XMZVH

Tabel 1. Contoh *exhaustive key search* terhadap cipherteks XMZVH

Kunci (k) *ciphering*	'Pesan' hasil dekripsi	Kunci (k) *ciphering*	'Pesan' hasil dekripsi	Kunci (k) *ciphering*	'Pesan' hasil dekripsi
0	**XMZVH**	17	**GVIEQ**	8	**PERNZ**
25	**YNAWI**	16	**HWJFR**	7	**QFSOA**
24	**ZOBXJ**	15	**IXKGS**	6	**RGTPB**
23	**APCYK**	14	**JYLHT**	5	**SHUQC**
22	**BQDZL**	13	**KZMIU**	4	**TIVRD**
21	**CREAM**	12	**LANJV**	3	**UJWSE**
20	**DSFBN**	11	**MBOKW**	2	**VKXTF**
19	**ETGCO**	10	**NCPLX**	1	**WLYUG**
18	**FUHDP**	9	**ODQMY**		

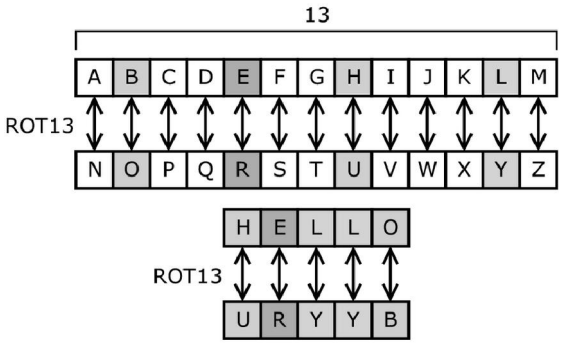
Plainteks yang potensial adalah CREAM dengan $k = 21$.
Kunci ini digunakan untuk mendekripsikan cipherteks lainnya.

```
   PHHW PH DIWHU WKH WRJD SDUWB
KEY
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   …
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
```


Contoh: Kriptogram **HSPPW** menghasilkan dua kemungkinan kunci yang potensial, yaitu k = 4 menghasilkan pesan DOLLS dan k = 11 menghasilkan WHEEL.

Jika kasusnya demikian, maka lakukan dekripsi terhadap potongan cipherteks lain tetapi cukup menggunakan k = 4 dan k = 11 agar dapat disimpulkan kunci yang benar.

- Di dalam sistem operasi Unix, `ROT13` adalah fungsi menggunakan *Caesar cipher* dengan pergeseran $k = 13$



- Contoh: `ROT13(ROTATE) = EBGNGR`
- Nama "ROT13" berasal dari *net.jokes* (*hhtp://groups.google.com/group/net.jokes*) (tahun 1980)
- ROT13 biasanya digunakan di dalam forum *online* untuk menyandikan jawaban teka-teki, kuis, canda, dsb
- Enkripsi arsip dua kali dengan `ROT13` menghasilkan pesan semula:

  `P = ROT13(ROT13(P))`

  sebab $ROT_{13}(ROT_{13}(x)) = ROT_{26}(x) = x$
- Jadi dekripsi cukup dilakukan dengan mengenkripsi cipherteks kembali dengan `ROT13`

- CIPHER : USVFMPWFOFWFSEJF
- Coba cari dekripsinya dengan exhaustive key search
- USVF MPWF OFWFS EJF