Algoritma Kriptografi Klasik

Oleh : Tim Dosen Kriptografi

Vigènere Cipher

Termasuk ke dalam *cipher* abjad-majemuk (*polyalpabetic substitution cipher*).

- Dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigènere pada abad 16 (tahun 1586).
- Tetapi sebenarnya Giovan Batista Belaso telah menggambarkannya pertama kali pada tahun 1553 seperti ditulis di dalam bukunya *La Cifra del Sig. Giovan Batista Belaso*
- Algoritma tersebut baru dikenal luas 200 tahun kemudian yang oleh penemunya *cipher* tersebut kemudian dinamakan *Vigènere Cipher*

- *Cipher* ini berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan Abad 19 (akan dijelaskan pada bahan kuliah selanjutnya).

- *Vigènere Cipher* digunakan oleh Tentara Konfiderasi (*Confederate Army*) pada Perang Sipil Amerika (*American Civil war*).

- Perang Sipil terjadi setelah *Vigènere Cipher* berhasil dipecahkan.

- *Vigènere Cipher* menggunakan Bujursangkar *Vigènere* untuk melakukan enkripsi.

- Setiap baris di dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan *Caesar Cipher.*

- Kunci: $K = k_1 k_2 \ldots k_m$

  k_i untuk $1 \leq i \leq m$ menyatakan jumlah pergeseran pada huruf ke-i.

  Karakter cipherteks: $c_i(p) = (p + k_i) \bmod 26$ *(*)*

Plainteks

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
a	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
b	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
c	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
d	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
e	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
f	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
g	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
h	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
i	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
j	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
K	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
l	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
m	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
n	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
o	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
p	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
q	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
r	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
s	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
t	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
u	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
v	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
w	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
x	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
y	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
z	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

Bujursangkar *Vigènere*

- Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang secara periodik.

- Misalkan panjang kunci = 20, maka 20 karakter pertama dienkripsi dengan persamaan (*), setiap karakter ke-*i* menggunakan kunci k_i.

  Untuk 20 karakter berikutnya, kembali menggunakan pola enkripsi yang sama.

- Contoh: kunci = `sony`

  Plainteks: `THIS PLAINTEXT`

  Kunci: `sony sonysonys`

- Contoh enkripsi:

KUNCI \ Plainteks	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	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
b	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
c	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
d	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
e	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
f	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
g	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
h	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
i	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
j	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
K	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
l	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
m	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
n	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
o	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
p	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
q	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
r	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
s	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
t	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
u	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
v	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
w	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
x	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
y	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
z	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

Enkripsi huruf T dengan kunci s

- Hasil enkripsi seluruhnya adalah sebagai berikut:

Plainteks : `THIS PLAINTEXT`
Kunci : `sony sonysonys`
Cipherteks : **`LVVQ HZNGFHRVL`**

- Pada dasarnya, setiap enkripsi huruf adalah *Caesar cipher* dengan kunci yang berbeda-beda.

$(T + S) \bmod 26 = L$
$(H + O) \bmod 26 = V$
dst

- Huruf yang sama tidak selalu dienkripsi menjadi huruf cipherteks yang sama pula.

  Contoh: huruf plainteks `T` dapat dienkripsi menjadi **`L`** atau **`H`**, dan huruf cipherteks **`V`** dapat merepresentasikan huruf plainteks `H`, `I`, dan `X`

- Hal di atas merupakan karakteristik dari *cipher* abjad-majemuk: setiap huruf cipherteks dapat memiliki kemungkinan banyak huruf plainteks.

- Pada *cipher* substitusi sederhana, setiap huruf cipherteks selalu menggantikan huruf plainteks tertentu.

- Plainteks:

Jawa Timur Bakal Tenggelam

Semburan lumpur panas di desa Porong, Sidoarjo, Jawa Timur belum juga berakhir. Sudah beberapa desa tenggelam. Entah sudah berapa rumah, bangunan, pabrik, dan sawah yang tenggelam.

Sampai kapan semburan lumpur berhenti, tiada yang tahu. Teknologi manusia tidak berhasil menutupi lubang semburan. Jika semburan lumpur tidak berhenti juga, mungkin Jawa Timur akan tenggelam

- Kunci: `langitbiru`

- Cipherteks:

```
Uajg Bbnci Vlknr Bxooxywaz

Ymfcciuy lhsxns xrhls qo lxti Gicoam, Abewrluo,
Wget Uqdoc brrcf kcxu meegsajz. Jooau hmufzrjl
dryi mfvxaplns. Mguiy mfdnn jxsigu cuzgp,
ubvxoyaa, viusqb, xln fgeti grhr trtozftrg.

Dazvib liguy srsjnsie ffmcaz ufzyyytv, zqtei
puyg ggpn. Umbhzlbmq fbvlmta goltl jvlsafot
ffvlnfpv rcubvx mpmoazto. Rzel srsjnsie ffmcaz
mjlre meenmguq aora, zavzlqe Dlwn Zqfvz reln
kvzhmcux
```

- *Vigènere Cipher* dapat mencegah frekuensi huruf-huruf di dalam cipherteks yang mempunyai pola tertentu yang sama seperti pada *cipher* abjad-tunggal.

- Jika periode kunci diketahui dan tidak terlalu panjang, maka kunci dapat ditentukan dengan menulis program komputer untuk melakukan *exhaustive key search*.

- Contoh: Diberikan cipherteks sbb:

TGCSZ GEUAA EFWGQ AHQMC

dan diperoleh informasi bahwa panjang kunci adalah *p* huruf dan plainteks ditulis dalam Bahasa Inggris, maka *running* program dengan mencoba semua kemungkinan kunci yang panjangnya tiga huruf, lalu periksa apakah hasil dekripsi dengan kunci tersebut menyatakan kata yang berarti.

Cara ini membutuhkan usaha percobaan sebanyak 26^p kali.

Varian *Vigenere Cipher*

1. *Full Vigènere cipher*

- Setiap baris di dalam tabel tidak menyatakan pergeseran huruf, tetapi merupakan permutasi huruf-huruf alfabet.
- Misalnya pada baris a susunan huruf-huruf alfabet adalah acak seperti di bawah ini:

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

2. *Auto-Key Vigènere cipher*

- Jika panjang kunci lebih kecil dari panjang plainteks, maka kunci disambung dengan plainteks tersebut.

- Misalnya,

  Pesan: NEGARA PENGHASIL MINYAK

  Kunci: INDO

maka kunci tersebut disambung dengan plainteks semula sehingga panjang kunci menjadi sama dengan panjang plainteks:

- Plainteks : NEGARAPENGHASILMINYAK
- Kunci : INDONEGARAPENGHASILMI

3. Running-Key Vigènere cipher

- Kunci adalah string yang sangat panjang yang diambil dari teks bermakna (misalnya naskah proklamasi, naskah Pembukaan UUD 1945, terjemahan ayat di dalam kitab suci, dan lain-lain).

- Misalnya,

  Pesan: NEGARA PENGHASIL MINYAK

  Kunci: KEMANUSIAN YANG ADIL DAN BERADAB

- Selanjutnya enkripsi dan dekripsi dilakukan seperti biasa.

Playfair Cipher

- Termasuk ke dalam *polygram cipher*.

- Ditemukan oleh Sir Charles Wheatstone namun dipromosikan oleh Baron Lyon Playfair pada tahun 1854.

Sir Charles Wheatstone

Baron Lyon Playfair

- *Cipher* ini mengenkripsi pasangan huruf (digram atau digraf), bukan huruf tunggal seperti pada *cipher* klasik lainnya.

- Tujuannya adalah untuk membuat analisis frekuensi menjadi sangat sulit sebab frekuensi kemunculan huruf-huruf di dalam cipherteks menjadi datar (*flat*).

- Kunci kriptografinya 25 buah huruf yang disusun di dalam bujursangkar 5x5 dengan menghilangkan huruf J dari abjad.

Contoh kunci:

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

Jumlah kemungkinan kunci:
25!=15.511.210.043.330.985.984.000.000

- Susunan kunci di dalam bujursangkar diperluas dengan menambahkan kolom keenam dan baris keenam.

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

Baris ke-6 = baris ke-1
Kolom ke-6 = kolom ke-1

- Pesan yang akan dienkripsi diatur terlebih dahulu sebagai berikut:

1. Ganti huruf J (bila ada) dengan I
2. Tulis pesan dalam pasangan huruf (*bigram*).
3. Jangan sampai ada pasangan huruf yang sama. Jika ada, sisipkan Z ditengahnya
4. Jika jumlah huruf ganjil, tambahkan huruf Z di akhir

Contoh:

Plainteks: GOOD BROOMS SWEEP CLEAN

→ Tidak ada huruf J, maka langsung tulis pesan dalam pasangan huruf:

GO OD BR OZ OM SZ SW EZ EP CL EA NZ

Algoritma enkripsi:

1. Jika dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kanannya.

2. Jika dua huruf terdapat pada kolom kunci yang sama maka tiap huruf diganti dengan huruf di bawahnya.

3. Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf yang digunakan sampai sejauh ini.

Contoh: Kunci (yang sudah diperluas) ditulis kembali sebagai berikut:

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

Plainteks (dalam pasangan huruf):

GO OD BR OZ OM SZ SW EZ EP CL EA NZ

Cipherteks:

FP UT EC UW PO DV TV BV CM BG CS DY

Enkripsi OD menjadi **UT** ditunjukkan pada bujursangkar di bawah ini:

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

titik sudut ke-4 ↓

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

Kunci dapat dipilih dari sebuah kalimat yang mudah diingat, misalnya:

JALAN GANESHA SEPULUH

Buang huruf yang berulang dan huruf J jika ada:

ALNGESHPU

Lalu tambahkan huruf-huruf yang belum ada (kecuali J):

ALNGESHPUBCDFIKMOQRTVWXYZ

Masukkan ke dalam bujursangkar:

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

- Karena ada 26 huruf abjad, maka terdapat 26 x 26 = 677 bigram, sehingga identifikasi bigram individual lebih sukar.

- Sayangnya ukuran poligram di dalam *Playfair cipher* tidak cukup besar, hanya dua huruf sehingga *Playfair cipher* tidak aman.

- Meskipun *Playfair cipher* sulit dipecahkan dengan analisis frekuensi relatif huruf-huruf, namun ia dapat dipecahkan dengan analisis frekuensi pasangan huruf.

- Dalam Bahasa Inggris kita bisa mempunyai frekuensi kemunculan pasangan huruf, misalnya pasangan huruf TH dan HE paling sering muncul.

- Dengan menggunakan tabel frekuensi kemunculan pasangan huruf di dalam Bahasa Inggris dan cipherteks yang cukup banyak, *Playfair cipher* dapat dipecahkan.

Affine Cipher

- Perluasan dari Caesar cipher
- Enkripsi: $C \equiv mP + b \pmod{n}$
- Dekripsi: $P \equiv m^{-1}(C - b) \pmod{n}$
- Kunci: m dan b

Keterangan:

1. n adalah ukuran alfabet
2. m bilangan bulat yang relatif prima dengan n
3. b adalah jumlah pergeseran
4. *Caesar cipher* adalah khusus dari *affine cipher* dengan $m = 1$
5. m^{-1} adalah inversi $m \pmod{n}$, yaitu $m \cdot m^{-1} \equiv 1 \pmod{n}$

- Dua buah bilangan bulat *a* dan *b* dikatakan *relatif prima* jika

  PBB (*a*, *b*) = 1.

- Contoh:

  Plainteks: KRIPTO (10 17 8 15 19 14)

  n = 26, ambil m = 7 (7 relatif prima dengan 26)

  b = 10

  Enkripsi: $C \equiv 7P + 10 \pmod{26}$

  $p_1 = 10 \rightarrow c_1 \equiv 7 \cdot 10 + 10 \equiv 80 \equiv 2 \pmod{26}$ (huruf 'C')

  $p_2 = 17 \rightarrow c_2 \equiv 7 \cdot 17 + 10 \equiv 129 \equiv 25 \pmod{26}$ (huruf 'Z')

  $p_3 = 8 \rightarrow c_3 \equiv 7 \cdot 8 + 10 \equiv 66 \equiv 14 \pmod{26}$ (huruf 'O')

  $p_4 = 15 \rightarrow c_4 \equiv 7 \cdot 15 + 10 \equiv 115 \equiv 11 \pmod{26}$ (huruf 'L')

  $p_5 = 19 \rightarrow c_5 \equiv 7 \cdot 19 + 10 \equiv 143 \equiv 13 \pmod{26}$ (huruf 'N')

  $p_6 = 14 \rightarrow c_6 \equiv 7 \cdot 14 + 10 \equiv 108 \equiv 4 \pmod{26}$ (huruf 'E')

  Cipherteks: **CZOLNE**

- Dekripsi:
  - Mula-mula hitung m^{-1} yaitu $7^{-1} \pmod{26}$
    dengan memecahkan $7x \equiv 1 \pmod{26}$
    Solusinya: $x \equiv 15 \pmod{26}$
    sebab $7 \cdot 15 = 105 \equiv 1 \pmod{26}$
  - Jadi, $P \equiv 15\,(C - 10) \pmod{26}$

$c_1 = 2 \quad \square\ p_1 \equiv 15 \cdot (2 - 10) = -120 \equiv 10 \pmod{26}$ (huruf 'K')
$c_2 = 25 \quad \square\ p_2 \equiv 15 \cdot (25 - 10) = 225 \equiv 17 \pmod{26}$ (huruf 'R')
$c_3 = 14 \quad \square\ p_3 \equiv 15 \cdot (14 - 10) = 60 \equiv 8 \pmod{26}$ (huruf 'I')
$c_4 = 11 \quad \square\ p_4 \equiv 15 \cdot (11 - 10) = 15 \equiv 15 \pmod{26}$ (huruf 'P')
$c_5 = 13 \quad \square\ p_5 \equiv 15 \cdot (13 - 10) = 45 \equiv 19 \pmod{26}$ (huruf 'T')
$c_6 = 4 \quad \square\ p_6 \equiv 15 \cdot (4 - 10) = -90 \equiv 14 \pmod{26}$ (huruf 'O')

Plainteks yang diungkap kembali: **KRIPTO**

- Salah satu cara memperbesar faktor kerja untuk *exhaustive key search:* enkripsi tidak dilakukan terhadap huruf individual, tetapi dalam blok huruf.

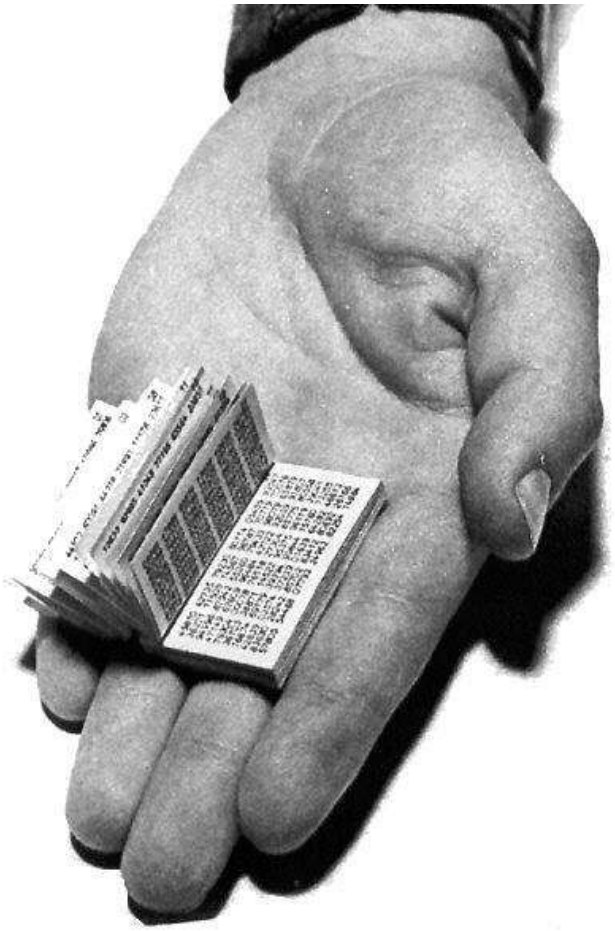
- Misal, pesan `KRIPTOGRAFI` dipecah menjadi kelompok 4-huruf:

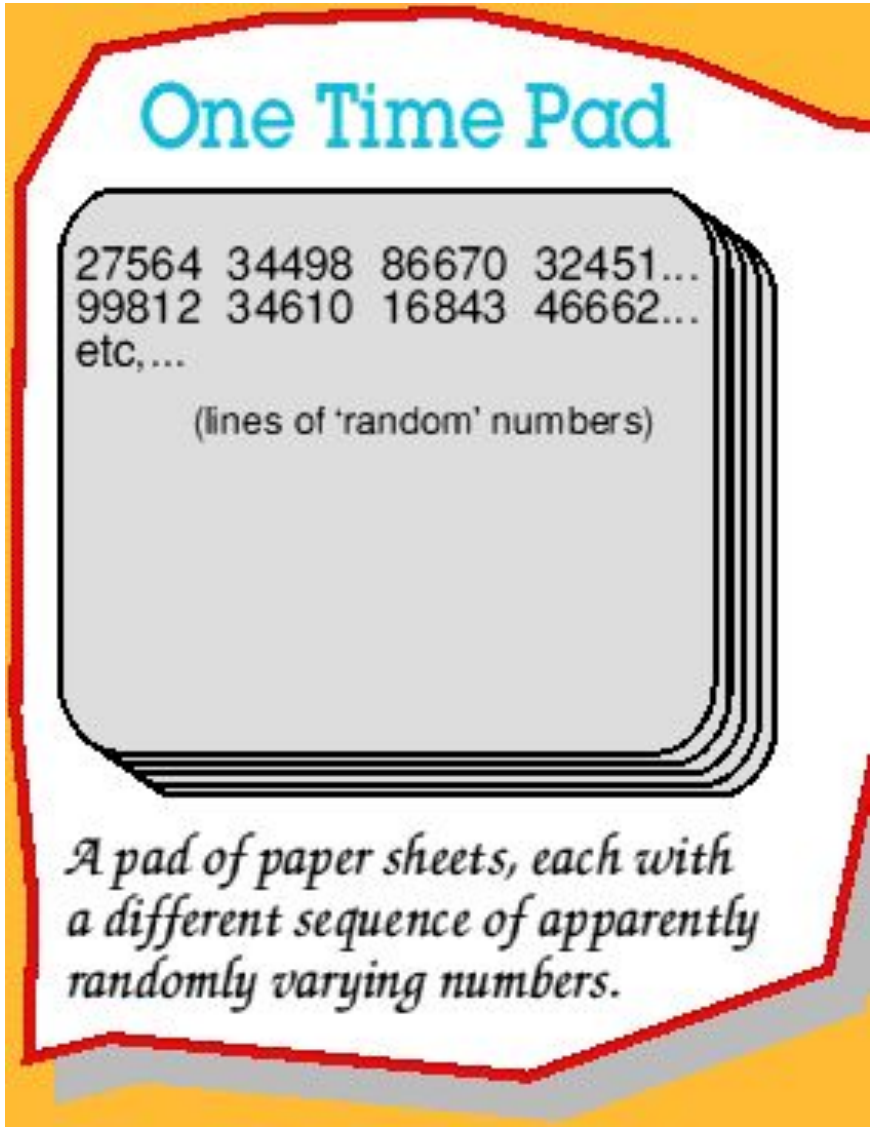
```
KRIP TOGR AFI
```

(ekivalen dengan 10170815 19140617 000508, dengan memisalkan ‘A’ = 0, ‘B’ = 1, …, ‘Z’ = 25)

One-Time Pad (OTP)

- *OTP* ditemukan pada tahun 1917 oleh Major Joseph Mauborgne.
- OTP termasuk ke dalam kelompok algoritma kriptografi simetri.
- *One-time pad* (*pad* = kertas bloknot) berisi deretan karakter-karakter kunci yang dibangkitkan secara acak.




One Time Pad
27564 34498 86670 32451...
99812 34610 16843 46662...
etc,...
(lines of 'random' numbers)
A pad of paper sheets, each with a different sequence of apparently randomly varying numbers.

- Penerima pesan memiliki salinan (*copy*) *pad* yang sama.
- Satu *pad* hanya digunakan sekali (*one-time*) saja untuk mengenkripsi pesan.
- Sekali *pad* telah digunakan, ia dihancurkan supaya tidak dipakai kembali untuk mengenkripsi pesan yang lain.

- Panjang kunci OTP = panjang plainteks, sehingga tidak ada kebutuhan mengulang penggunaan kunci selama proses enkripsi.

- Aturan enkripsi yang digunakan persis sama seperti pada *Vigenere Cipher*.

- Enkripsi: $c_i = (p_i + k_i) \bmod 26$

- Dekripsi: $c_i = (p_i - k_i) \bmod 26$

- **Contoh 1**:
  plainteks: ONETIMEPAD
  kunci: TBFRGFARFM

Misalkan A = 0, B = 1, …, Z = 25.

cipherteks: HOJKOREGHP

yang mana diperoleh sebagai berikut:

(O + T) mod 26 = H
(N + B) mod 26 = O
(E + F) mod 26 = J, dst

- **Sistem *OTP* sulit dipecahkan karena:**
  1. Barisan kunci acak + plainteks yang tidak acak = cipherteks yang seluruhnya acak.

  2. Mendekripsi cipherteks dengan beberapa kunci berbeda dapat menghasilkan plainteks yang bermakna, sehingga kriptanalis tidak punya cara untuk menentukan plainteks mana yang benar.

- **Contoh**:

  Misalkan kriptanalis mencoba kunci LMCCAWAAZD

  *untuk mendekripsi cipherteks **HOJKOREGHP**

  Plainteks yang dihasilkan: **SALMONEGGS**

Bila ia mencoba kunci: ZDVUZOEYEO

Plainteks yang dihasilkan: **GREENFIELD**

Kriptanalis: ???????

Kelemahan OTP

- Meskipun OTP adalah algoritma yang sempurna aman, tetapi ia tidak banyak digunakan dalam praktek.

- Alasan:

1. Karena panjang kunci = panjang pesan, maka OTP hanya cocok untuk pesan berukuran kecil

   Masalah yang timbul: - penyimpanan kunci

   - pendistribusian kunci

2. Karena kunci dibangkitkan secara acak, maka ‘tidak mungkin’ pengirim dan penerima membangkitkan kunci yang sama secara simultan.

- *OTP* hanya dapat digunakan jika tersedia saluran komunikasi kedua yang cukup aman untuk mengirim kunci.

- Saluran kedua ini umumnya lambat dan mahal.

- Misalnya pada perang dingin antara AS dan Uni Soviet (dahulu), kunci dibangkitkan, disimpan, lalu dikirim dengan menggunakan jasa kurir yang aman

Tugas :

1. Tugas dienkripsi dengan Vigenere chiper dengan plain text
   BELAJAR KRIPTOGRAFI UNTUK INDONESIA MERDEKA
   - Kunci : INFORMATIKA
2. Dekrip chipper text berikut menggunakan algoritma super enkripsi (Caesar chipper dan scytale chipper) dengan kunci 5:
   - **NJNSXYINFTFESPE**
3. Upload jawaban dengan format Tugas3_Kriptografi_kelas_nim_nama.pdf