One-Time Pad, Cipher yang Tidak Dapat Dipecahkan (*Unbreakable Cipher*)

Bahan kuliah

IF4020 Kriptografi

Pendahuluan

- *Unbreakable cipher* merupakan klaim yang dibuat oleh kriptografer terhadap algoritma kriptografi yang dirancangnya.

- Namun, kebanyakan algoritma yang sudah pernah dibuat orang adalah *breakable cipher*.

- *Caesar Cipher*, *Vigenere Cipher* , *Playfair Cipher*, *Enigma Cipher*, *Hill Cipher*, dll sudah *obselete* karena *breakable cipher*.

- Apakah *unbreakable cipher* memang ada?

  Jawaban: ada

- Apa syarat *unbreakable cipher*?

  Jawaban:

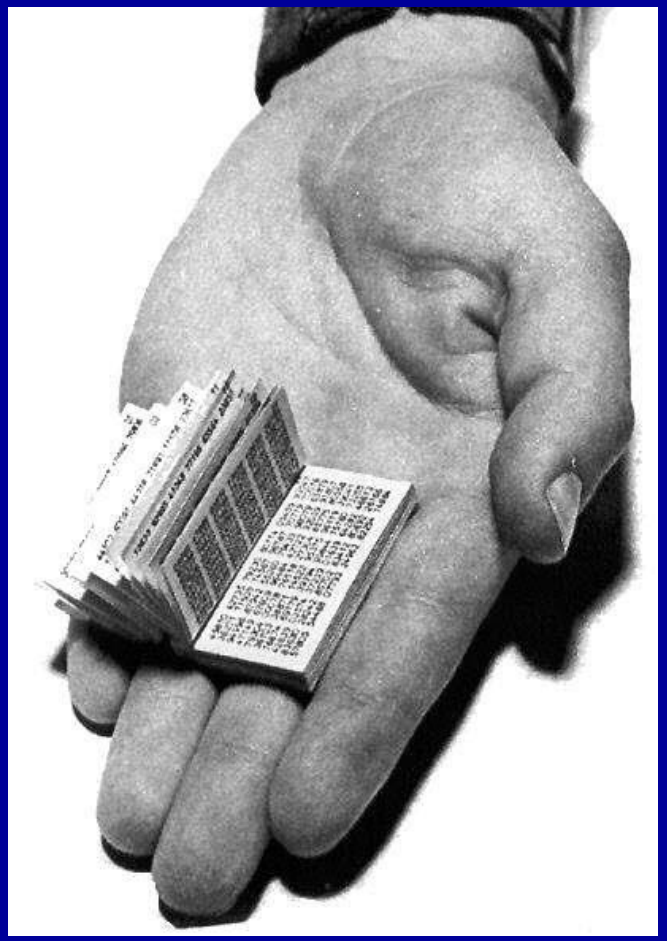
  1. Kunci harus benar-benar acak.
  2. Panjang kunci = panjang plainteks

  Akibatnya: plainteks yang sama tidak selalu menghasilkan cipherteks yang sama

One-Time Pad (OTP)

- Satu-satunya algoritma kriptografi sempurna sehingga tidak dapat dipecahkan adalah *one-time pad*.
- *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.



```
CIHJT UUHML FRUGC ZIBGD BQPNI PDNJG LPLLP YJYXM
DCXAC JSJUK BIOYT MWQPX DLIRC BEXYK VKIMB TYIPE
UOLYQ OKOXH PIJKY DRDBC GEFZG UACKD RARCD HBYRI
DZJYO YKAIE LIUYW DFOHU IOHZV SRNDD KPSSO JMPQT
MHQHL OHQQD SMHNP HHOHQ GXRPJ XBXIP LLZAA VCMOG
AWSSZ YMFNI ATMON IXPBY FOZLE CVYSJ XZGPU CTFQY
HOVHU OCJGU QMWQV OIGOR BFHIZ TYFDB VBRMN XNLZC
```

- 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

- Contoh lainnya untuk pesan yang lebih panjang:

Plainteks:
`nantimalamsayatunggukamudidepanwarungkopi`

Kunci:
`gtrskncvbrwpoatqljfmxtrpjsrzolfhtbmaedpvy`

Cipherteks :
`TTELSZCGBDOPMAMKYPLGHTDJMAUDDLSDTSGNKNDKG`

- **Sistem *OTP* ini tidak dapat 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: ???????

- Sebagai latihan, misalkan alfabet yang digunakan adalah 27 karakter (26 huruf plus sebuah spasi) dan diberikan sebuah cipherteks:

  `TLCYKUMGDFAWTZVOYKLENSZZHYZRW`

  temukan kunci yang menghasilkan plainteks:

  `mr johnson left his house last night`

  lalu temukan kunci lain yang menghasilkan plainteks

  `i saw the mysterious plane behind me`

Kelemahan OTP

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

- Alasan:

  1. Tidak mangkus, karena panjang kunci = panjang pesan.

     Msalah 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.

- *As a practical person, I've observed that one-time pads are theoretically unbreakable, but practically very weak. By contrast, conventional ciphers are theoretically breakable, but practically strong." -* ***Steve Bellovin***