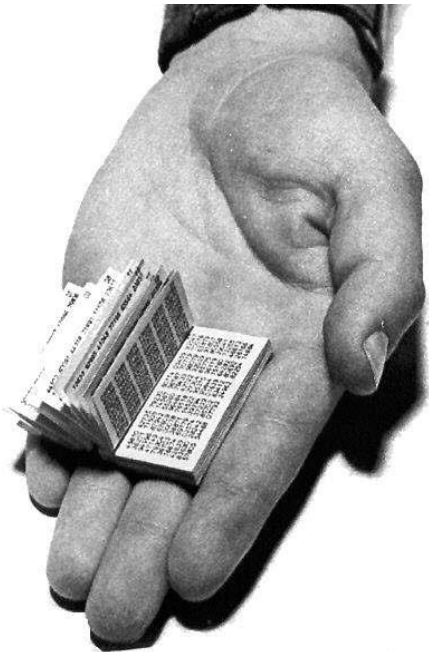


Bahan kuliah IF4020 Kriptografi

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



**Oleh: Rinaldi Munir**


**Program Studi Teknik Informatika  
Sekolah Teknik Elektro dan Informatika  
Institut Teknologi Bandung  
2024**

# 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, Affine Cipher, Enigma Cipher, Hill Cipher*, dll sudah kadaluarsa karena *breakable cipher*.

- Apakah *unbreakable cipher* memang benar-benar ada?  
Jawaban: ada!
- Apa syarat sebuah *cipher* disebut *unbreakable cipher*?  
Jawaban:
  1. Kunci harus benar-benar acak (*trully random*).
  2. Panjang kunci = panjang plainteks
  3. Kunci hanya boleh digunakan sekali, tidak boleh digunakan ulang untuk mengenkripsi pesan yanglain
- Acak artinya tidak dapat diprediksi nilainya dan tidak dapat diulang pembangkitannya
- Akibat 1 dan 2: plainteks yang sama tidak selalu menghasilkan cipherteks yang sama

# *One-Time Pad (OTP)*

- Satu-satunya algoritma kriptografi sempurna aman (*perfect secrecy*) sehingga tidak dapat dipecahkan adalah *one-time pad (OTP)*.
- OTP ditemukan pada tahun 1917 oleh Major Joseph Mauborgne → 
- OTP mengatasi kelemahan pada *Vigenere Cipher*. *Vigenere Cipher* mengulang penggunaan kunci secara periodik → mudah ditemukan dengan metode Kasiski.
- Pada OTP, panjang kunci = panjang plainteks

**Plainteks:** otp adalah cipher yang tidak bisa dipecahkan

**Kunci:** trjkdndkdwerylgrgdkopcegyhbdwjbtrfhgvk

- *One-time pad* (*pad* = kertas bloknote) berisi deretan huruf-huruf kunci yang dibangkitkan secara acak.



Sumber: <https://www.cryptomuseum.com/crypto/otp/index.htm>

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

- Pengirim dan penerima pesan memiliki salinan (*copy*) *pad* yang sama.
- Satu *pad* hanya digunakan sekali (*one-time*) saja untuk mengenkripsi pesan
  - itulah mengapa dinamakan *one-time pad*.
- Sekali *pad* telah digunakan, ia dihancurkan supaya tidak dipakai kembali untuk mengenkripsi pesan yang lain
  - menyulitkan kriptanalisis

**Plainteks:** otpadalahcipheryangtidakbisadipecahkan

**Kunci:** trjkdndkdwerylgrgdkopcegyhbdwjbtrfhgvk

**Cipherteks:** HKYKGNOKKYMFGFPXPGQQHXFEQZPTDZRQXTFOQVX

- Aturan enkripsi dan dekripsi yang digunakan persis sama seperti pada *Vigenere Cipher*, bedanya tidak ada perulangan kunci secara periodik.

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

Contoh:  $c_2 = (t + r) \bmod 26 = (19 + 17) \bmod 26 = 36 \bmod 26 = 10 = \text{'K'}$

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

Contoh:  $p_2 = (K - t) \bmod 26 = (10 - 17) \bmod 26 = -7 \bmod 26 = 19 = \text{'t'}$



- **Contoh 1:**

Plainteks: onetimepad

Kunci: t b f r g f a r f m

Misalkan  $A = 0, B = 1, \dots, Z = 25$ .

cipherteks: HOJKOREGHP

yang dalam hal ini diperoleh sebagai berikut:

$$(o + T) \bmod 26 = H$$

$$(n + B) \bmod 26 = O$$

$$(e + F) \bmod 26 = J, \text{ dst}$$

- **Contoh 2:**

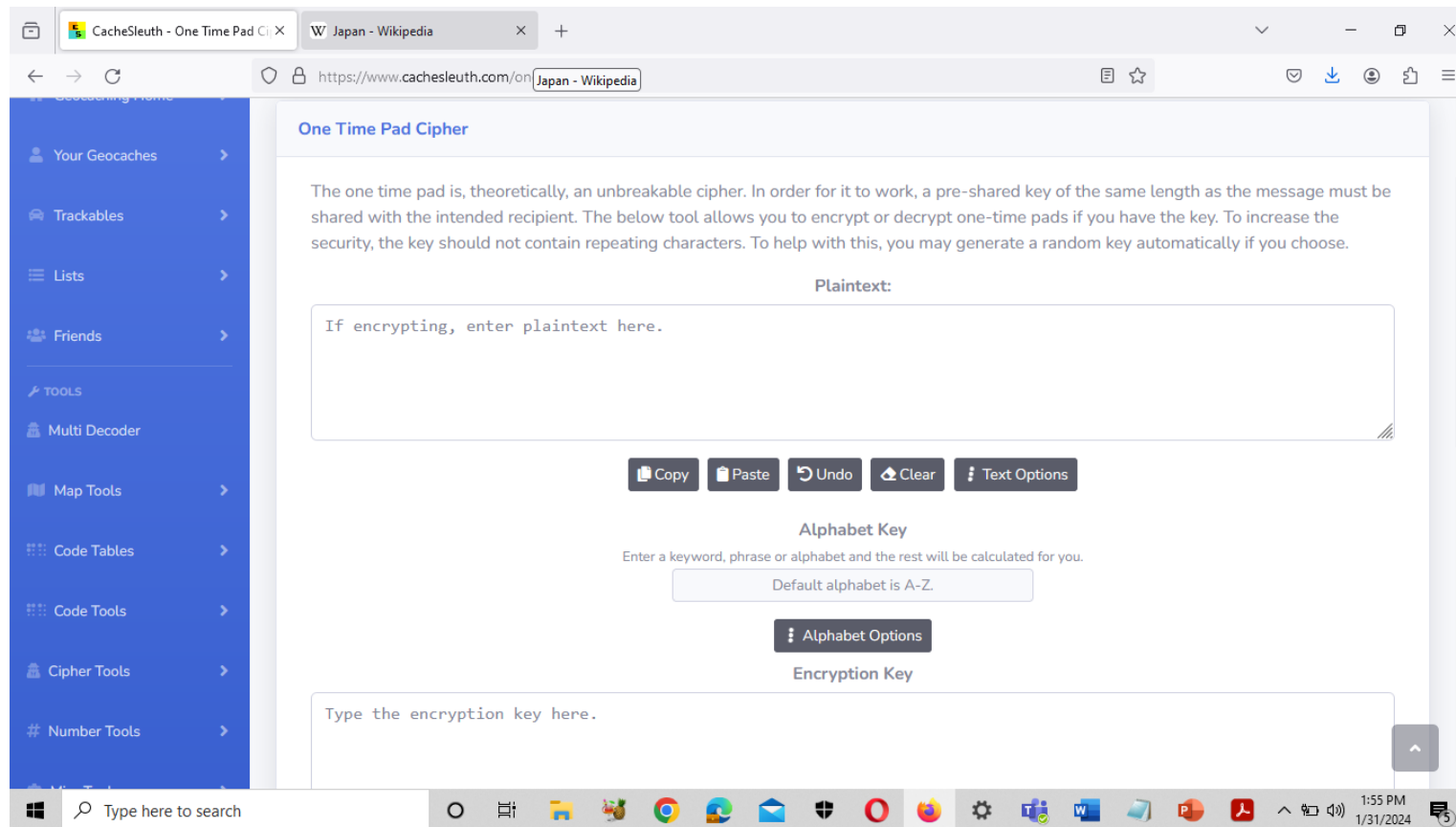
Plainteks:    nantimalamsayatunggukamudidepanwarungkopi

Kunci:        gtrskncvbrwpoatqljfmxtrpjsrzolfhtbmaedpvy

Cipherteks: TTELSZCGBDOPMAMKYPLGHTDJMAUDDLSDTSGNKNDKG

# Demo One Time Pad Onlie

- <https://www.cachesleuth.com/onetimepad.html>



The screenshot shows a web browser window with two tabs: "CacheSleuth - One Time Pad Cipher" and "Japan - Wikipedia". The address bar shows the URL "https://www.cachesleuth.com/onetimepad.html". The main content area is titled "One Time Pad Cipher" and contains the following text: "The one time pad is, theoretically, an unbreakable cipher. In order for it to work, a pre-shared key of the same length as the message must be shared with the intended recipient. The below tool allows you to encrypt or decrypt one-time pads if you have the key. To increase the security, the key should not contain repeating characters. To help with this, you may generate a random key automatically if you choose."

Below the text, there are two main sections:

- Plaintext:** A text input field with the placeholder text "If encrypting, enter plaintext here." Below the field are buttons for "Copy", "Paste", "Undo", "Clear", and "Text Options".
- Alphabet Key:** A section with the instruction "Enter a keyword, phrase or alphabet and the rest will be calculated for you." Below this is a text input field containing "Default alphabet is A-Z." and a button for "Alphabet Options".

At the bottom, there is an "Encryption Key" section with a text input field containing the placeholder text "Type the encryption key here." The browser's taskbar at the bottom shows the Windows search bar, system tray icons, and the time "1:55 PM 1/31/2024".

- Kunci untuk OTP harus seluruhnya acak dan sepanjang pesan.
- Bagaimana jika kunci diambil dari teks yang panjang (misalnya tulisan di dalam novel, buku, berita, dan sebagainya)?
  - ini bukan lagi OTP (sebab tulisan di buku/novel/berita bukan acak)
  - tidak menghasilkan *perfect secrecy*
  - dapat dipecahkan
- Kunci di dalam OTP hanya dipakai sekali dan tidak pernah digunakan kembali. Bagaimana jika kunci dipakai untuk kedua kalinya?
  - ia bukan lagi *one-time pad*, tetapi *two-time pad*
  - tidak aman

- **OTP ini tidak dapat dipecahkan karena:**
  1. Kunci acak + plainteks yang tidak acak = cipherteks yang seluruhnya acak.  
$$\text{Enkripsi: } c_i = (p_i + k_i) \bmod 26$$
$$\text{Dekripsi: } p_i = (c_i - k_i) \bmod 26$$
  2. Hanya terdapat satu kunci yang memetakan plainteks ke cipherteks, begitu juga sebaliknya.
- Mendekripsi cipherteks dengan beberapa kunci berbeda dapat menghasilkan plainteks yang bermakna, sehingga kriptanalis kesulitan menentukan plainteks mana yang benar.

- **Contoh 3:** Misalkan kriptanalisis mencoba kunci LMCCAWAAZD untuk mendekripsi cipherteks HOJKOREGHP  
Plainteks yang dihasilkan: SALMONEGGS

Bila ia mencoba kunci: ZDVUZOYEYO  
Plainteks yang dihasilkan: GREENFIELD

Kriptanalisis: ??????? (bingung sendiri 😊 )

- Contoh ini menunjukkan bahwa untuk sembarang plainteks dan cipherteks hanya ada satu kunci yang memetakannya satu sama lain.

- Sebagai latihan, misalkan 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

# Perfect Secrecy



Claude Shannon

- *Perfect secrecy*: Cipherteks tidak menyediakan informasi apapun tentang plainteks maupun kunci.

- Pada tahun 1949, Claude Shannon dari Laboratorium Bell membuktikan bahwa OTP memiliki *perfect secrecy*.

Pembuktian dari Shannon adalah sebagai berikut:

- Tiap karakter pada kunci yang *trully random* diasumsikan dipilih secara independen (independen dari plainteks atau cipherteks)
- Misalkan  $x$  adalah plainteks, dan misalkan  $r$  adalah karakter yang berkoresponden dengan karakter kunci.
- Cipherteks  $y = (x + r) \bmod 26$  adalah karakter yang acak, sehingga  $x$  tidak dapat diprediksi dari  $y$ . **qed**



# Kelemahan OTP

- Meskipun OTP menawarkan keamanan yang sempurna, tetapi ia tidak umum digunakan dalam aplikasi praktis (aplikasi komersil maupun aplikasi lainnya).
- Alasan:
  1. Tidak sangkil, karena panjang kunci = panjang pesan.  
Makin panjang pesan, makin besar ukuran kuncinya. Butuh komputasi yang berat untuk membangkitkan milyaran karakter-karakter yang benar-benar acak.
  2. Karena kunci dibangkitkan secara acak, maka 'tidak mungkin' pengirim dan penerima membangkitkan kunci yang sama secara bersamaan.

- Untuk menggunakan OTP, pengirim dan penerima harus menyepakati kunci yang digunakan, kunci harus sepanjang pesan.
- Hal ini sulit dilakukan secara praktek.
- *OTP* hanya dapat digunakan jika tersedia saluran komunikasi kedua yang sangat aman untuk mengirim kunci.
- Saluran kedua ini tidak boleh sama dengan saluran untuk mengirim pesan.
- Saluran kedua ini umumnya lambat dan mahal (misalnya lewat jalur darat, memakai kurir terpercaya dan tidak bisa dikenali).
- Atau, kunci dikirim pada saluran yang sama dengan saluran pengiriman pesan tetapi pada waktu yang berbeda dengan pengiriman pesan.

OTP digunakan oleh mata-mata (*spy*) selama Perang Dunia II



**Pejabat eksekutif operasi khusus dari Inggris memperlihatkan syal yang bertuliskan kunci OTP selama PD II**

Sumber: John H Reif, History of Computing, Duke University

# Penggunaan OTP pada perang dingin antara AS dan Uni Soviet

## The Moscow–Washington hotline [1963]:

- Komunikasi antara AS dan Uni Soviet menggunakan hotline komunikasi langsung antara pemimpin AS dan Uni Soviet.
- Hotline difasilitasi dengan peralatan OTP yang bernama ITT Intelex Teletype L015
- ITT Intelex Teletype dikembangkan setelah krisis rudal Cuba untuk menghindari perang nuklir
- **ITT Intelex Teletype mengenkripsi pesan menggunakan OTP**
  - Kunci *one-time pad* disimpan di dalam pita magnetic yang diterbangkan antara Washington DC dan Moscow.



**ITT Intelex Teletype L015 used for original Moscow–Washington hotline**  
(Lyndon Baines Johnson Library and Museum)



**The Pentagon in Arlington County, Virginia, U.S.**



**Kremlin in Moscow, Russia**

- *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***