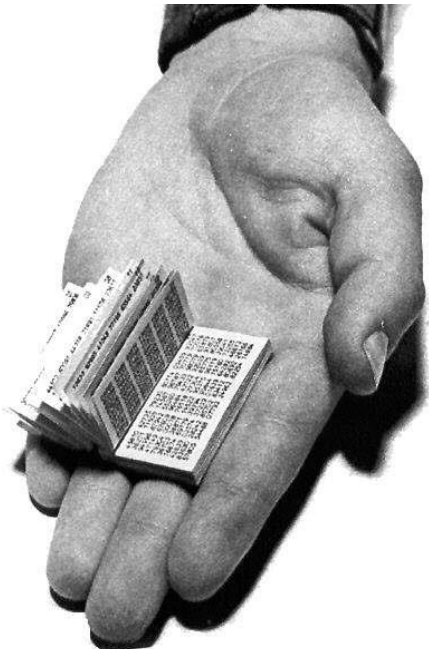


Bahan kuliah IF4020 Kriptografi

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



Oleh: Rinaldi M

**Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
2026**

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 acak sejati (*truly random*).
 2. Panjang kunci = panjang plainteks
 3. Kunci hanya boleh digunakan sekali, tidak boleh digunakan ulang untuk mengenkripsi pesan yang lain
- Acak sejati artinya tidak dapat diprediksi nilainya dan tidak dapat diulang kembali pembangkitannya. Ini berbeda dengan *pseudo random* yang bisa diulang kembali pembangkitan nilai acak asalkan umpan (*seed*) nya sama.
 - 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 oleh Gilbert Vernam pada tahun 1917 dan kemudian secara matematis dibuktikan memiliki *perfect secrecy* oleh Claude Shannon tahun 1949.
- OTP mengatasi kelemahan pada *Vigenere Cipher*. *Vigenere Cipher* mengulang penggunaan kunci secara periodik → mudah ditemukan dengan metode Kasiski.
- Pada OTP, panjang kunci = panjang plainteks, seluruh karakternya acak sejati

Plainteks: otpadalahcipheryangtidakbisadipecahkan

Kunci: trjkdndkdwerylgrgdkopcegyhbdwjbtrfhgvk

Gilbert Vernam

🌐 10 languages ▾

Article [Talk](#)

Read [Edit](#) [View history](#)

From Wikipedia, the free encyclopedia

Gilbert Sandford Vernam (April 3, 1890 – February 7, 1960) was a [Worcester Polytechnic Institute](#) 1914 graduate and [AT&T Bell Labs](#) engineer who, in 1917, invented an additive [polyalphabetic stream cipher](#) and later co-invented an automated [one-time pad cipher](#).

Vernam proposed a teleprinter cipher in which a previously prepared [key](#), kept on [paper tape](#), is combined character by character with the [plaintext](#) message to produce the [ciphertext](#). To decipher the ciphertext, the same key would be again combined character by character, producing the [plaintext](#). Vernam later worked for the [Postal Telegraph Company](#), and became an employee of [Western Union](#) when that company acquired Postal in 1943. His later work was largely with automatic switching systems for [telegraph](#) networks.

Gilbert Vernam

Born	April 3, 1890
Died	February 7, 1960 (aged 69)
Alma mater	Worcester Polytechnic Institute
Occupation	Cryptographer



- *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
MMQHL	OHQQD	SMHNP	HHOHQ	GXRFP	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

Letter	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
Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plainteks: otpadalahcipheryangtidakbisadipecahkan

Kunci: trjkdndkdwerylgrgdkopcegyhbdwjbtrfhgvk

Cipherteks: HKYKGNOKKYMGPXPGQQHXFEQZPTDZRQXTFOQVX

- Aturan enkripsi dan dekripsi yang digunakan persis sama seperti pada *Vigenere Cipher*, bedanya tidak ada perulangan kunci secara periodik.
- Enkripsi: $C = (P + K) \bmod 26$
Contoh ($P = \text{'o'}$, $K = \text{'t'}$): $C = (\text{'o'} + \text{'t'}) \bmod 26 = (14 + 19) \bmod 26 = 33 \bmod 26 = 7 = \text{'H'}$
- Dekripsi: $P = (C - K) \bmod 26$
Contoh ($C = \text{'H'}$, $K = \text{'t'}$): $P = (\text{'H'} - \text{'t'}) \bmod 26 = (7 - 19) \bmod 26 = -12 \bmod 26 = 14 = \text{'o'}$

- **Contoh 1:**

Plainteks: onetimepad

Kunci: tbfrgfarfm

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:**

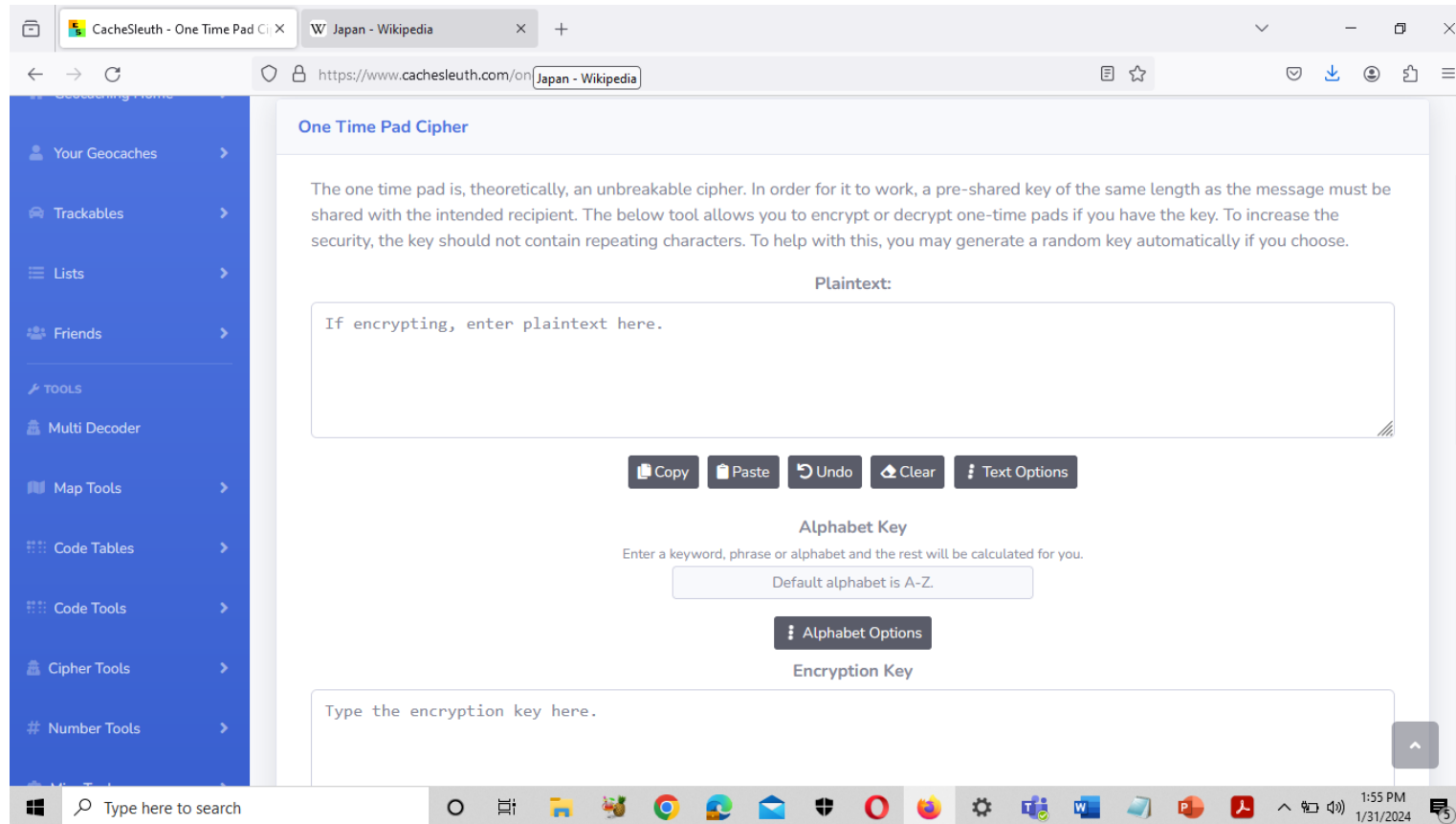
Plainteks: nantimalamsayatunggukamudidepanwarungkopi

Kunci: gtrskncvbrwpoatqljfmxtrpjsrzolfhtbmaedpvy

Cipherteks: TTELSZCGBDOPMAMKYPLGHTDJMAUDDLSDTSGNKNDKG

Demo One Time Pad Onlie

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



- Kunci untuk OTP harus seluruhnya acak sejati 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 OTP (acak) + plainteks (tidak acak) = cipherteks (acak)

Enkripsi: $C = (P + K) \bmod 26$

Dekripsi: $P = (C - K) \bmod 26$

2. Hanya terdapat satu kunci yang memetakan plainteks ke cipherteks, begitu juga sebaliknya

→ fungsi $C = (P + K) \bmod 26$ adalah pemetaan satu-ke-satu (*one-to-one*).

→ artinya, untuk sembarang plainteks dan cipherteks hanya ada satu kunci yang memetakannya satu sama lain

→ Akibatnya, jika kriptanalisis mencoba mendekripsi cipherteks dengan beberapa kunci berbeda ada kemungkinan menghasilkan beberapa plainteks yang bermakna, sehingga kriptanalisis kesulitan menentukan plainteks mana yang benar.

- **Contoh 3:** Misalkan kriptanalisis mencoba kunci LMCCAWAAZD untuk mendekripsi cipherteks HOJKOREGHP
Plainteks yang dihasilkan: SALMONEGGS (telur ikan Salmon)

Bila ia mencoba kunci: ZDVUZOYEYO

Plainteks yang dihasilkan: GREENFIELD (lapangan hijau)

Kriptanalisis: ???????? Kunci mana yang benar? (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

- Pembuktian

“kunci OTP (acak) + plainteks (tidak acak) = cipherteks (acak)”

sebagai berikut:

Misalkan:

$$C = (P + K) \bmod 26$$

dengan K dipilih secara uniform:

$$P(K = k) = \frac{1}{26}, \quad k = 0, 1, \dots, 25.$$

Untuk setiap nilai plainteks tertentu $P = p$, pemetaan

$$C = (P + K) \bmod 26$$

merupakan pemetaan satu-ke-satu dari semua kemungkinan K ke semua kemungkinan C .

Akibatnya:

$$P(C = c \mid P = p) = \frac{1}{26}$$

untuk setiap c (yaitu: $P(C = 'a') = P(C = 'b') = \dots = P(C = 'z') = \frac{1}{26}$)

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*. Ia menulis pembuktian tsb di dalam makalahnya:
“Shannon, C. E. (1949). *Communication theory of secrecy systems*. Bell System Technical Journal, 28(4), 656–715.”
- Menurut Shannon, suatu sistem memiliki *perfect secrecy* apabila setelah penyerang memperoleh cipherteks, informasi mengenai plainteks tidak bertambah. Secara matematis, kondisi tersebut dinyatakan sebagai:

$$P(P = p \mid C = c) = P(P = p)$$

Artinya, probabilitas suatu plainteks tertentu tetap sama sebelum maupun setelah cipherteks diamati

Communication Theory of Secrecy Systems^{*}

By C. E. SHANNON

1 INTRODUCTION AND SUMMARY

The problems of cryptography and secrecy systems furnish an interesting application of communication theory¹. In this paper a theory of secrecy systems is developed. The approach is on a theoretical level and is intended to complement the treatment found in standard works on cryptography². There, a detailed study is made of the many standard types of codes and ciphers, and of the ways of breaking them. We will be more concerned with the general mathematical structure and properties of secrecy systems.

The treatment is limited in certain ways. First, there are three general types of secrecy system: (1) concealment systems, including such methods as invisible ink, concealing a message in an innocent text, or in a fake covering cryptogram, or other methods in which the existence of the message is concealed from the enemy; (2) privacy systems, for example speech inversion, in which special equipment is required to recover the message; (3) "true" secrecy systems where the meaning of the message is concealed by cipher, code, etc., although its existence is not hidden, and the enemy is assumed to have any special equipment necessary to intercept and record the transmitted signal. We consider only the third type—concealment system are primarily a psychological problem, and privacy systems a technological one.

Secondly, the treatment is limited to the case of discrete information where the message to be enciphered consists of a sequence of discrete sym-

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. Untuk pesan yang sangat panjang atau komunikasi yang berlangsung terus-menerus, kebutuhan kuncinya menjadi sangat besar.
 2. Karena kunci dibangkitkan harus benar-benar acak (*truly random*), maka 'tidak mungkin' pengirim dan penerima membangkitkan kunci acak yang sama secara simultan (bersamaan).

- Untuk menggunakan OTP, pengirim dan penerima harus menyepakati kunci yang digunakan, kunci harus sepanjang pesan, dan hanya boleh digunakan sekali.
- 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 Tidak cocok untuk komunikasi dinamis. Bayangkan untuk komunikasi modern seperti:
 - *WhatsApp*
 - *HTTPS*
 - *VPN*
 - *cloud storage*
 - *email*
 - komunikasi IoT, dll

data yang dikirim terus berubah, perangkat bisa berganti, pengguna bisa *offline*, dan pesan memiliki ukuran yang berbeda-beda.

- Dengan OTP, setiap tambahan data membutuhkan tambahan kunci yang benar-benar acak dan belum pernah digunakan. Ini membuat manajemen kunci menjadi sangat berat.

- OTP pernah 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**