One-Time Pad (OTP

Bahan Kuliah Keamanan Data

Sevi **Nurafni**

Fakultas Sains dan Teknologi
Universitas Koperasi Indonesia 2025

Cipher yang Tidak Dapat Dipecahkan

- *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 lewat masanya karena breakable cipher

- Apakah *unbreakable cipher* memang ada?

- Apa syarat sebuah cipher disebut unbreakable cipher?
  1. Kunci harus benar-benar acak (*trully random*)
  2. Penjang kunci = panjangteks

- Acak: tidak dapat diprediksi nilainya dan tidak dapat diulang
- Akibat 1 dan 2: plainteks yang sama tidak selalu menghasilkan cipherteks yang sama

One-Time Pad (OTP)

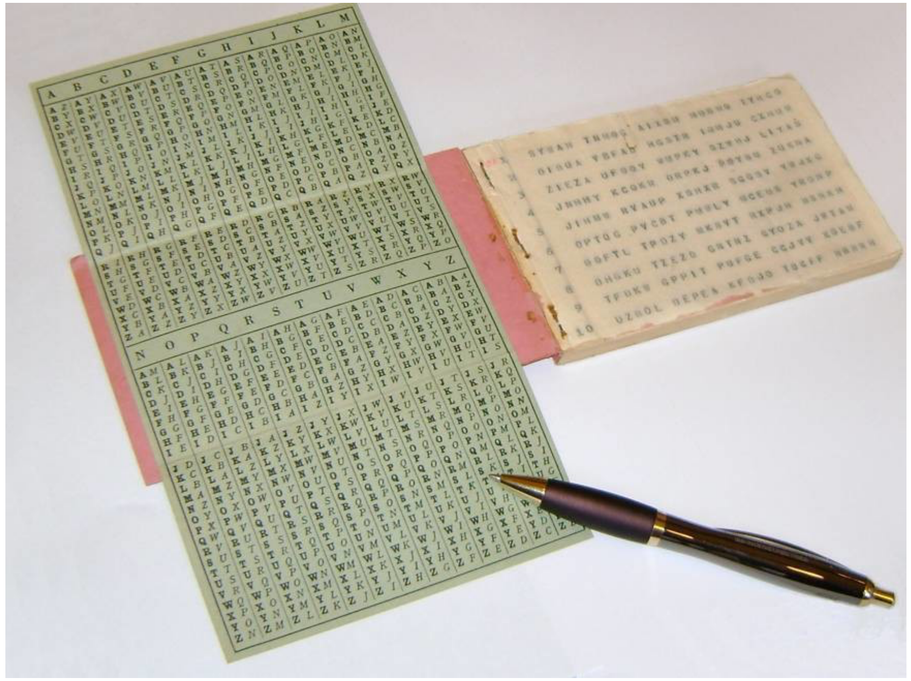
- Satu-satunya algoritma kriptografi sempurna aman (*perfect secrecy*) hingga tidak dapat dipecahkan adalah one-time pad (OTP)

- 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: `otpadalahcipheryangtidakbisadipecahkan`
- Kunci: `qwertyuiopasdfghjklzxcvbnmsdfghjklcvbd`

One-Time Pad (OTP)

- OTP (pad = kertas bloknot) berisi deretan huruf-huruf 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

One-Time Pad (OTP)

- Pengirim dan penerima pesan memiliki salinan 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 lain

One-Time Pad (OTP)

- Plainteks: `otpadalahcipheryangtidakbisadipecahkan`
- Kunci: `qwertyuiopasdfghjklzxcvbnmsdfghjklcvbd`
- Aturan enkripsi dan dekripsi yang digunakan persis sama seperti Vigenere Cipher, bedanya tidak ada perulangan kunci secara periodik.
- Enkripsi: $c_i = (p_i + k_i) \bmod 26$
- Dekripsi: $p_i = (c_i - k_i) \bmod 26$

Contoh-1

- Plainteks: `onetimepad`
- Kunci: `tbfrgfarfm`

- Misalkan `A = 0,B = 1,… ,Z = 25`
- Cipherteks: `HOJKOREGHP`
- Yang dalam hal ini diperoleh sebagai berikut:

  `(o + T) mod 26 = H`

  `(n + B) mod 26 = O`

  `(e + F) mod 26 = J,` dst

Contoh-2

- Plainteks: `selamatliburlebaran`
- Kunci: `sdfghjksadfghjkbrdv`

- Cipherteks:?

One-Time Pad (OTP)

- Kunci untuk OTP harus seluruhnya acak dan sepanjang pesan
- Bagaimana jika kunci diambil dari teks yang panjang? (Misalnya tulsian di dalam novel, buku, berita, dan sebagainya)?
  - Ini bukan lagi OTP
  - 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?
  - Bukan lagi one-time pad
  - Tidak aman

One-Time Pad (OTP)

- OTP tidak dapat dipecahkan karena:
  1. kunci acak + plainteks yang tidak acak = cipherteks yang seluruhnya acak.
     - Hanya terdapat satu kunci yang memetakan plainteks ke cipherteks, begitu juga sebaliknya.
  2. Mendeskripsikan cipherteks dengan beberapa kunci berbeda dapat menghasilkan plainteks yang bermakna, sehingga kriptanalis kesulitan menentukan plainteks mana yang benar

Contoh-3

- Misalkan kriptanalis mencoba kunci `LMCCAWAAZD`
- Untuk mendeskripsi cipherteks `HOJKOREGHP`
- Plainteks yang dihasilkan: `SALMONEGGS`

- Jika yang dicoba dalah kunci `ZDVUZOEYEO`
- Plainteks yang dihasilkan: `GREENFIELD`

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

Kelemahan OTP

- Meskipun OTP menawarkan keamanan yang sempurna, tetapi tidak umum digunakan dalam aplikasi praktis.
- Alasan:
  1. Tidak efektif, 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

Kelemahan OTP

- OTP hanya dapat digunakan jika tersedia saluran komunikasi kedua yang cukup 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)

Contoh Penggunaan OTP

- Perang dingin antara AS dan Uni Soviet (tahun 1940):
- Agen spionase Uni Soviet membaca kunci one-time pad ke AS
- Pesan-pesan rahasia dienkripsi dengan OTP dan dikirim dari AS
- Di Uni Soviet, kunci OTP yang sma digunakan untuk mendeskripsi cipherteks

SELAMAT BELAJAR