KRIPTOGRAFI SIMETRIS

KULIAH KRIPTOGRAFI DAN KEAMANAN JARINGAN

DIMENSI KRIPTOGRAFI

- **Tipe operasi untuk transformasi plaintext menjadi ciphertext**
  - Substitusi: elemen pada plaintext dipetakan ke elemen lain.
  - Transposisi: elemen pada plaintext disusun ulang.
- **Jumlah key:**
  - Simetris
  - Asimetris
- **Cara pemrosesan plaintext**
  - Block cipher: memproses 1 blok dalam satu waktu.
  - Stream cipher: memproses elemen input secara kontinyu.

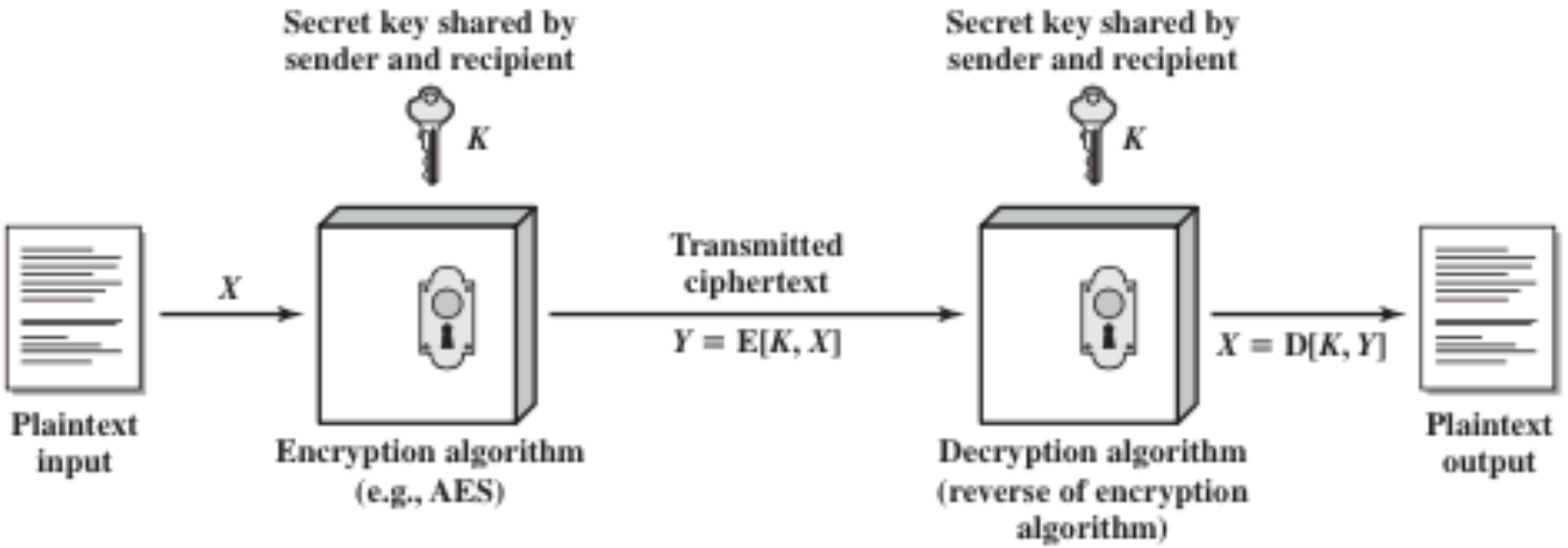
PENYANDIAN SIMETRIS

- **Disebut juga penyandian konvensional atau kunci rahasia atau kunci tunggal.**
- **Pengirim dan penerima berbagi kunci yang sama**
- **Paling banyak digunakan**
  - Semua algoritma enkripsi klasik merupakan penyandian simetris
  - Merupakan satu-satunya model penyandian yang digunakan sebelum penemuan penyandian asimetris pada sekitar tahun 1970an

KOMPONEN PENYANDIAN SIMETRIS

- **Lima komponen:**
  - Plaintext
  - Algoritma enkripsi: substitusi dan transformasi terhadap plaintext.
  - Secret key: input untuk algoritma enkripsi.
  - Ciphertext
  - Algoritma dekripsi.
- **Dua kebutuhan untuk keamanan dengan enkripsi konvensional:**
  - Algoritma enkripsi yang kuat.
    - Intruder tidak bisa mendekripsi ciphertext atau mengetahui key meskipun dia mempunyai beberapa pasangan ciphertext dan plaintext.
  - Pengirim dan penerima mendapatkan secret key dengan cara yang aman dan tetap mengamankannya.

SKEMA KRIPTOGRAFI SIMETRIS



- **Simbol-simbol:**
  - Plaintext: $X = [X_1, X_2, \ldots, X_M\}$
  - Key: $K = [K_1, K_2, \ldots, K_J\}$
  - Ciphertext: $Y = [Y_1, Y_2, \ldots, Y_N\}$
  - Algoritma enkripsi: E
  - Algoritma dekripsi: D
  - $Y = E(K, X)$
  - $X = D(K, Y)$

PEMECAHAN KODE

- **Dua pendekatan:**
  - Cryptanalisis/kriptoanalisis: mencari karakteristik algoritma
  - Brute-force attack: intruder mencoba setiap key pada ciphertext sampai didapatkan pesan yang dapat dibaca/dimengerti.

BRUTE-FORCE ATTACK

- **Mencoba semua kunci yang mungkin sampai didapatkan text yang dapat dibaca.**
- **Secara rata-rata, setengah dari semua key yang mungkin harus dicoba.**

Ukuran key (bit)	Jumlah alternatif key	Waktu (1 dekripsi/ mikro dtk)	Waktu (10^6 dekripsi/ mikro dtk)
32	$2^{32} = 4.3 \times 10^9$	35.8 menit	2.15 mili dtk
56	7.2×10^{16}	1142 tahun	10.01 dtk
128	3.4×10^{38}	5.4×10^{24} tahun	5.4×10^{18} tahun
168	$3.7x\ 10^{50}$	5.9×10^{36} tahun	5.9×10^{30} tahun
26 karakter (permutasi)	$26! = 4 \times 10^{26}$	6.4×10^{12} tahun	6.4×10^6 tahun

KRIPTOANALISIS

- **Terdiri dari beberapa level.**
- **Kerkhoff's principle: intruder mengetahui semua detil cryptosystem kecuali kunci rahasia.**
- **Paling sulit: hanya ciphertext yang diketahui.**
- **Paling mudah: algoritma, ciphertext, plaintext dan ciphertext pasangannya, ciphertext dan hasil dekripsinya.**

- **Beberapa tipe serangan kriptoanalisis**

Type of Attack	Known to Cryptanalyst
Ciphertext only	• Encryption algorithm • Ciphertext to be decoded
Known plaintext	• Encryption algorithm • Ciphertext to be decoded • One or more plaintext–ciphertext pairs formed with the secret key
Chosen plaintext	• Encryption algorithm • Ciphertext to be decoded • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	• Encryption algorithm • Ciphertext to be decoded • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	• Encryption algorithm • Ciphertext to be decoded • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

SERANGAN CIPHERTEXT-ONLY

- **Diberikan: suatu ciphertext c**
- **Q: apakah plaintext m?**
- **Suatu skema enkripsi betul-betul tidak aman jika skema tersebut tidak aman terhadap serangan ciphertext-only.**

SERANGAN KNOWN-PLAINTEXT

- **Diberikan: (m_1,c_1), (m_2,c_2), …, (m_k,c_k) dan suatu ciphertext lain c.**
- **Q: apakah plaintext dari c?**
- **Q: apakah kunci yang digunakan?**

CHOSEN-PLAINTEXT ATTACK

- **Diberikan: (m_1,c_1), (m_2,c_2), …, (m_k,c_k), di mana m_1, m_2, …, m_k dipilih oleh attacker; dan suatu ciphertext lain c.**
- **Q: apakah plaintext dari c, atau apakah kunci rahasianya?**

CHOSEN-CIPHERTEXT ATTACK

- **Diberikan: (m_1,c_1), (m_2,c_2), …, (m_k,c_k), di mana c_1, c_2, …, c_k dipilih oleh attacker; dan ciphertext lain c.**
- **Q: apakah plaintext dari c, atau apakah kunci rahasianya?**

KRITERIA ALGORITMA ENKRIPSI

- **Skema enkripsi yang 'unconditionally secure': ciphertext yang diperoleh dari algoritma enkripsi tidak memiliki cukup informasi yang dapat digunakan untuk menentukan plaintext-nya secara unik, meski terdapat jumlah ciphertext yang tidak terbatas dan sumber daya tidak terbatas.**
- **Algoritma enkripsi harus memenuhi salah satu di antara 2 syarat:**
  - Biaya untuk memecahkan kode melebihi nilai informasi.
  - Waktu untuk memecahkan kode melebihi masa pemanfaatan informasi.
- **Skema enkripsi yang 'computationally secure': memenuhi 1 di antara 2 kriteria di atas.**