SISTEM ENKRIPSI SYMMETRIC DAN ASYMMETRIC

Symmetric:

- Memiliki satu kunci (disebut kunci rahasia) yang digunakan untuk proses enkripsi dan dekripsi
- Menyediakan " *two-way channel"* untuk pengguna-penggunanya (saling berbagi kunci antar pengguna)
- Menyediakan bukti *authentication* (keaslian) bahwa pesan yang diterima tidak dibuat oleh seorang yang bukan pengirimnya.
- Properti sistem ini membutuhkan pendistribusian kunci.
- Private Key Juga dikenal dengan sebutan kunci simetris, yakni penggunaan kunci yang sama untuk melakukan enkripsi dan dekripsi pada data yang diinginkan. Sebelum melakukan dekripsi, pengirim data harus terlebih dahulu membagikan kunci privatnya agar dapat didekripsi oleh penerima data. Biasanya digunakan dalam operasi resmi milik pemerintah.

Asymmetric:

- Disebut juga sebagai kunci publik (public key) yang memiliki dua jenis kunci yaitu public key untuk proses enkripsi dan private key untuk proses dekripsi
- Memiliki manajemen kunci yang dapat menyimpan, melindungi dan mengaktifasi kunci-kunci.
- Public Key Juga disebut dengan kriptografi asimetris, menggunakan dua kunci berbeda yang terkait secara matematis. Dua kunci ini adalah kunci privat yang harus dirahasiakan dan kunci publik yang dapat dibagi kebanyak orang sekaligus. Misalnya dalam mengirimkan data, si A melakukan enkripsi dengan kunci publik pada data yang dikirimkan, dan untuk membacanya si B harus menggunakan kunci privat yang diberikan si A.

Macam-Macam Enkripsi

Di samping cara kerja yang dibagi dalam dua jenis di atas, ada juga beberapa macam metode yang digunakan dalam melakukan enkripsi data.

Metode Enkripsi MD2

Dikembangkan oleh Ronal Rivest pada tahun 1989, yang merupakan kependekan dari *Massage-Digest Algorithm 2*. Banyak digunakan pada komputer 8 bit yang ditetapkan dalam RFC 1319. masih digunakan hingga tahun 2004 untuk infrastruktur kunci publik.

Metode Enkripsi MD4

Lanjutan dari metode pada poin pertama, dan diluncurkan pada tahun 1990. Memiliki panjang enkripsi mencapai 128 bit. Digunakan dalam menghitung NT-hash ringkasan *password* pada Microsoft Windows NT, XP dan juga seri Vista.

Metode Enkripsi MD5

Diluncurkan oleh orang yang sama, Ronald RIvest pada tahun 1994. Alasan pembaruan adalah metode sebelumnya, yakni MD4 dirasa tidak lagi aman untuk digunakan. Digunakan secara luas dengan *hash value* 128 bit.

Metode Enkripsi SHA

Adalah rangkaian *cryptographic hash* yang dirancang oleh NSA (National Security Agency) dan diterbitkan oleh NIST. Merupakan kependekan dari *Secure Hash Algorithm*. Tersedia dalam beberapa jenis, antara lain SHA-0, SHA-1 dan SHA-2.

Metode Enkripsi RC4

Merupakan satu jenis *stream chiper*, yakni dapat memproses unit atau masukan data pada satu saat. Penerapan metode ini memungkinkan enkripsi dan dekripsi dapat dilakukan pada berbagai ukuran *hash*. Algoritma yang digunakan berdasarkan permutasi acak.

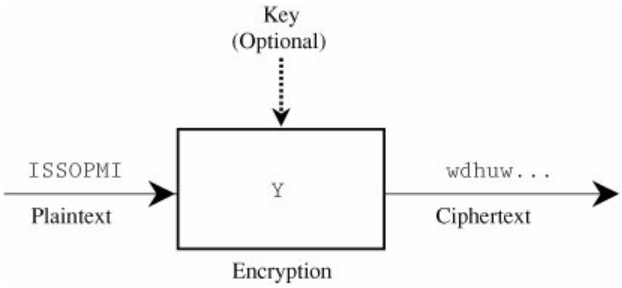
Metode Enkripsi Base64

Merupakan sistem untuk mewakili data mentah *byte* sebagai karakter ASCII. Tersedia dalam 6 bit *encoding* 8 bit ASCII karakter. Format yang dicetak menggunakan karakter, memungkinkan binari data yang akan dikirim dalam bentuk email dan akan disimpan dalam *database*.

CIPHER STREAM DAN BLOK

Stream:

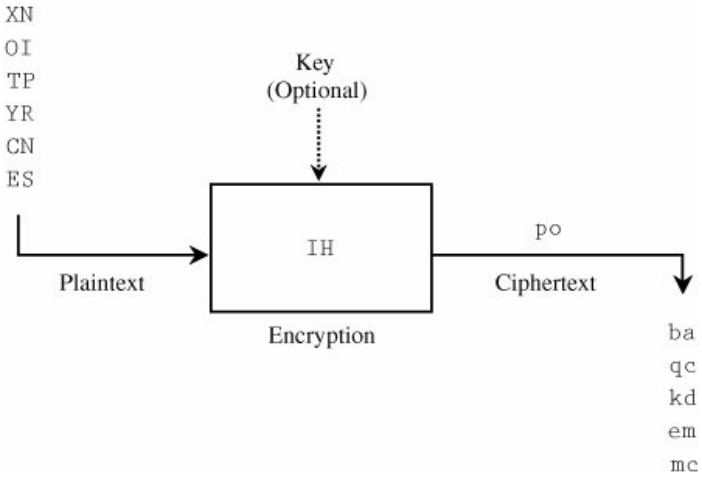
- Mengubah sebuah simbol dari plaintext secara langsung menjadi symbol ciphertext
- Ketergantungan transformasi hanya dalam simbol, kunci dan informasi control dari algoritma enkripsi.
- Beberapa kesalahan misalnya pelewatana karakter dalam dalam proses enkripsi, mempengaruhi enkripsi semua karakter-karakter berikutnya, namun kesalahan tersebut dapat dideteksi dan diperbaiki.



Gambar Diagram enkripsi *stream*

Blok:

- Cipher blok mengelompokkan symbol-simbol plaintext menjadi satu blok.
- Bekerja pada blok-blok plaintext dan menhasilkan blok-blok ciphertext



Gambar Diagram enkripsi blok

Perbandingan antara algoritma stream dan blok:

	Algoritma enkripsi stream	Algoritma enkripsi blok
Keuntungan	Kecepatan tranformasi Perambatan kesalahan yang rendah	Penyebaran yang tinggi (*high diffusion*) Kekebalan terhadap penyisipan suatu symbol
Kelemahan	Penyebaran ya ng rendah Dapat terjadi penyisipan symbol berbahaya dan modifikasi	Penenkripsian yang lambat Perambatan kesalahan

Karakteristik-karakteristik Algoritma enkripsi:
Confusion (membingungkan): sulit untuk memprediksi apa yang akan terjadi pada ciphertext dengan mengubah satu karakter dalam plaintext
Prinsip ***diffusion*** (menyebarkan): cipher seharusnya juga menyebarkan informasi dari plaintext di atas seluruh ciphertext sehingga perubahan dalam plaintext mempengaruhi banyak bagian dari ciphertext.

DES (DATA ENCRYPTION STANDARD)

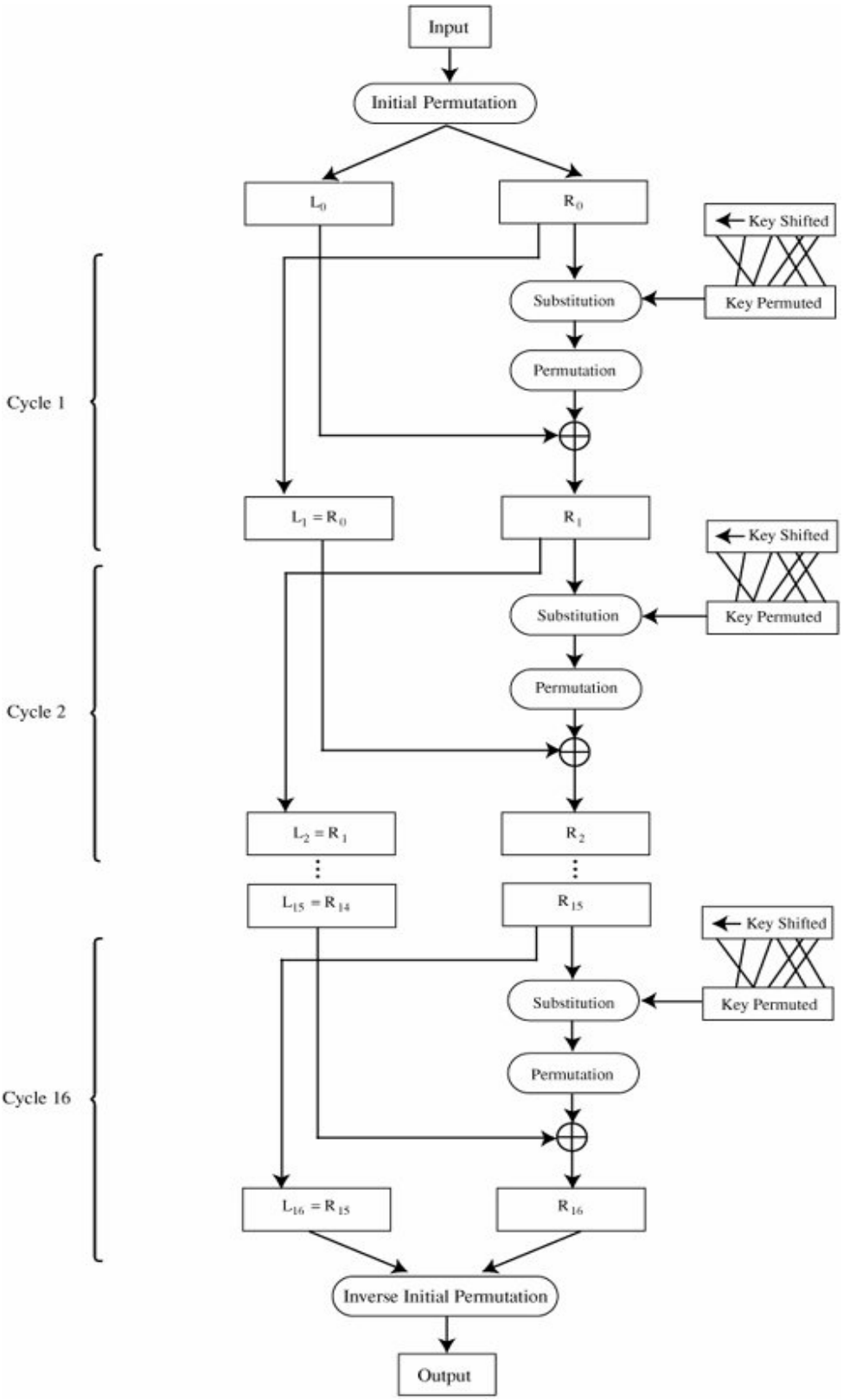
Data encryption algorithm dikembangkan oleh IBM untuk U.S. National Bureau od Standards (NBS) berdasarkan algoritma Lucifer yang dibuat pada tahun 1974.

Data Encryption Standard pada awalnya bernama DEA (Data Encryption Algorithm) di USA dan DEA-1 di negara lain. DES diadopsi oleh U.S. Federal standard pada bulan Novmeber 1976.

Overview DES:

- Kombinasi kompleks enkripsi blok dasar *substitution* dan *transposition*
- Memiliki pengulangan sebanyak 16 putaran
- Algoritma dimulai dari blok plaintext sebanyak 16-bit
- Key panjangnya 64-bit, tetapi faktanya hanya 56-bit (8-bit tambahan sering digunakan sebagai pemeriksaan digit dan tidak mempengaruhi enkripsi dalam implementasi normal)
- Pengguna dapat mengubah key setiap waktu

Rincian Algoritma DES:
Masukan plaintext dibagi menjadi blok-blok yang berukuran 64-bit yang kemudian dipermutasi (initial permutation)
Bit data ditransformasikan oleh 64-bit key (tetapi hanya 56-bit yang digunakan). Key dikurangi dari 64-bit menjadi 56-bit dengan menghilangkan bit 8, 16, 24, …64. Bit-bit tersebut diasumsikan sebagai bit paritas yang tidak membawa informasi dalam key.
Berikutnya rangkaian operasi dikenal sebagai ***cycle*** . 64 data bit yang dipermutasi dipecah menjadi dua bagian (32-bit) bagian kiri (*left*) dan kanan (*right*).
Key digeser kekiri (*shift left*) dengan sejumlah bit dan
dipermutasi. Key dikombinasikan



Gambar Diagram DES