ERWIEN TJIPTA WIJAYA, ST.,M.KOM

KEAMANAN INFORMASI

TEKNIK - TEKNIK PENYANDIAN ENKRIPSI DAN DESKRIPSI DATA (PART - II)

PENGGUNAAN KUNCI

- Salah satu cara untuk menambah tingkat keamanan sebuah algoritma enkripsi dan deskripsi adalah dengan menggunakan sebuah kunci (***Key***) yang biasa disebut **K**
- Sehingga persamaan matematisnya menjadi:

  EK (M) = C

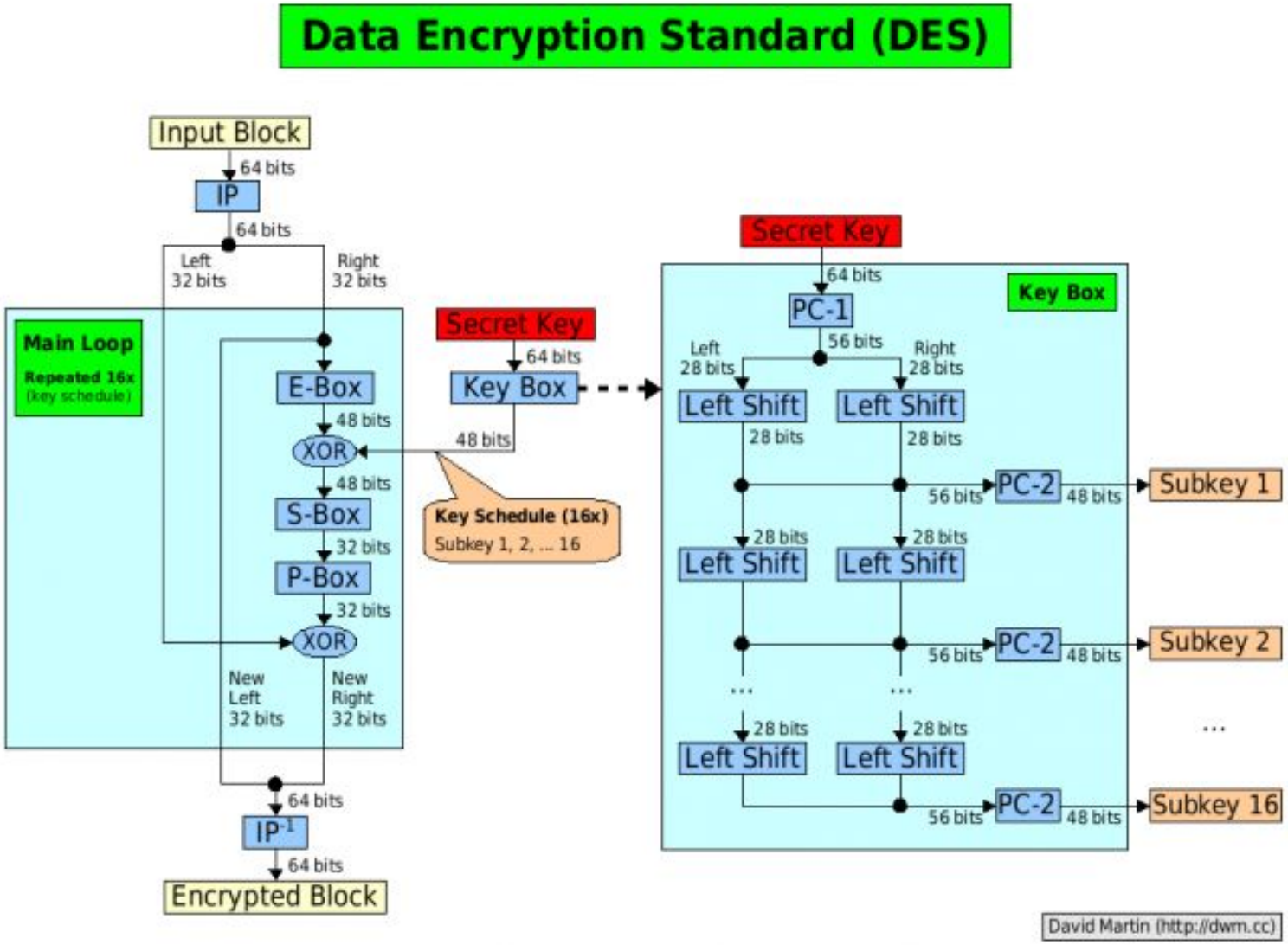
  DK (M) = M
- Terdapat 2 macam kunci :

1. Algoritma Simetris
2. Algoritma Asimetris

ALGORITMA SIMETRIS

- Suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci deskripsi sehingga algoritma ini disebut juga sebagai single-key algorithm
- Sebelum melakukan pengiriman pesan, pengirim dan penerima harus memilih suatu kunci tertentu yang sama untuk dipakai bersama, dan kunci ini haruslah rahasia bagi pihak yang tidak berkepentingan sehingga algoritma ini disebut juga algoritma kunci rahasia (secret-key algorithm).
- Metode : DES (Data Encryption Standard)

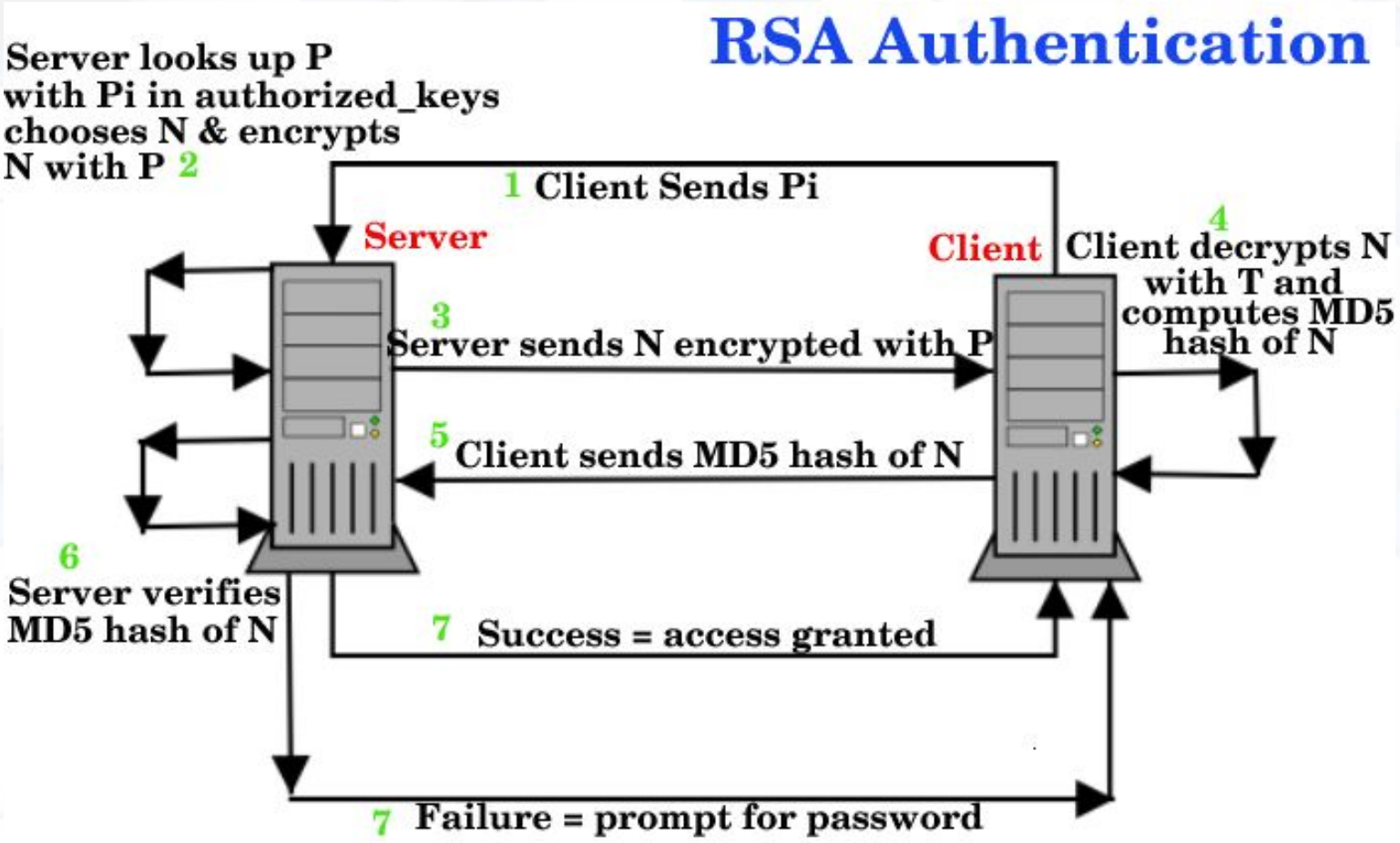
ALGORITMA SIMETRIS : DES



ALGORITMA ASIMETRIS

- Suatu algoritma dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi.
- Pada algoritma ini menggunakan dua kunci yakni kunci publik (public key) dan kunci privat (private key).
- Kunci publik disebarkan secara umum sedangkan kunci privat disimpan secara rahasia oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci privat yang digunakan.
- Metode : RSA (Rivest, Shamir, Adleman)

ALGORITMA ASIMETRIS : RSA



SOLUSI ENKRIPSI MODERN

- Data Encryption Standard (DES) :

1. Standar bagi USA Government
2. Popular untuk metode secret key
3. Terdiri dari : 40-bit, 56-bit dan 3x56-bit (Triple DES)
4. Didukung ANSI dan IETF

- Advanced Encryption Standard (AES)

1. Untuk menggantikan DES (2001)
2. Menggunakan variable length block cipher
3. Key length : 128-bit, 192-bit, 256-bit

SOLUSI ENKRIPSI MODERN

- Digital Certificate Server (DCS)

1. Verfikasi untuk digital signature
2. Authentikasi user
3. Menggunakan Public dan Private Key
4. Contoh : Netscape Certificate Server

- IP Security (IPSec)

1. Enkripsi public/private key
2. Dirancang oleh CISCO System
3. Menggunakan DES 40-bit dan authentication
4. Built-in pada produk CISCO
5. Solusi tepat untuk Virtual Private Network (VPN) dan Remote Network Access

SOLUSI ENKRIPSI MODERN

- Karberos

1. Solusi untuk user authentication
2. Dapat menangani multiple platform/system
3. Free charge (open source)
4. IBM menyediakan versi komersial : Global Sign On (GSO)

- Point-to-point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol (L2TP)

1. Dirancang oleh Microsoft
2. Autentication berdasarkan PPP(Point to point protocol)
3. Enkripsi berdasarkan algoritm Microsoft (tidak terbuka)
4. Terintegrasi dengan NOS Microsoft (NT, 2000, XP)

SOLUSI ENKRIPSI MODERN

- Remote Access Dial-in User Service (RADIUS)

1. Multiple remote access device menggunakan 1 database untuk authentication
2. Didukung oleh 3com, CISCO, Ascend
3. Tidak menggunakan encryption

- RSA Encryption

1. Dirancang oleh Rivest, Shamir, Adleman tahun 1977
2. Standard de facto dalam enkripsi public/private key
3. Didukung oleh Microsoft, apple, novell, sun, lotus
4. Mendukung proses authentication
5. Multi platform

SOLUSI ENKRIPSI MODERN

- Secure Hash Algorithm

1. dirancang oleh National Institute of Standard and Technology (NIST) USA.
2. bagian dari standar DSS(Decision Support System) USA dan bekerja sama dengan DES untuk digital signature.
3. SHA-1 menyediakan 160-bit message digest
4. Versi : SHA-256, SHA-384, SHA-512 (terintegrasi dengan AES)

- MD5

1. dirancang oleh Prof. Robert Rivest (RSA, MIT) tahun 1991
2. menghasilkan 128-bit digest.
3. cepat tapi kurang aman

SOLUSI ENKRIPSI MODERN

- Secure Shell (SSH)

1. Digunakan untuk client side authentication antara 2 sistem
2. Mendukung UNIX, windows, OS/2
3. Melindungi telnet dan ftp (file transfer protocol)

- Secure Socket Layer (SSL)

1. Dirancang oleh Netscape, menyediakan enkripsi RSA pada layes session dari model OSI.
2. Independen terhadap servise yang digunakan.
3. Melindungi system secure web e-commerce
4. Metode public/private key dan dapat melakukan authentication
5. Terintegrasi dalam produk browser dan web server Netscape.

SOLUSI ENKRIPSI MODERN

- Security Token

1. Aplikasi penyimpanan password dan data user di smart card

- Simple Key Management For Internet Protocol

1. Seperti SSL bekerja pada level session model OSI.
2. Menghasilkan key yang static, mudah bobol.

APLIKASI ENKRIPSI

- Beberapa aplikasi yang memerlukan enkripsi untuk pengamanan data atau komunikasi diantaranya adalah :

1. Jasa Telekomunikasi :
    - Enkripsi untuk mengamankan informasi konfidensial baik berupa suara, data, maupun gambar yang akan dikirimkan ke lawan bicaranya.
    - Enkripsi pada transfer data untuk keperluan manajemen jaringan dan transfer on-line data billing.
    - Enkripsi untuk menjaga copyright dari informasi yang diberikan.

2. Militer dan Pemerintah :
    - Enkripsi diantaranya digunakan dalam pengiriman pesan.
    - Menyimpan data-data rahasia militer dan kenegaraan dalam media penyimpanannya selalu dalam keaadan terenkripsi.

APLIKASI ENKRIPSI

- Data Perbankan

1. Informasi transfer uang antar bank harus selalu dalam keadaan terenkripsi

- Data Konfidensial Perusahaan

1. Rencana strategis, formula-formula produk, database pelanggan/karyawan dan database operasional
2. pusat penyimpanan data perusahaan dapat diakses secara on-line.
3. Teknik enkripsi juga harus diterapkan untuk data konfidensial untuk melindungi data dari pembacaan maupun perubahan secara tidak sah.

APLIKASI ENKRIPSI

- Pengamanan Electronic Mail :

1. Mengamankan pada saat ditransmisikan maupun dalam media penyimpanan.
2. Aplikasi enkripsi telah dibuat khusus untuk mengamankan e-mail, diantaranya PEM (Privacy Enhanced Mail) dan PGP (Pretty Good Privacy), keduanya berbasis DES dan RSA.

- Kartu Plastik :

1. Enkripsi pada SIM Card, kartu telepon umum, kartu langganan TV kabel, kartu kontrol akses ruangan dan komputer, kartu kredit, kartu ATM, kartu pemeriksaan medis, dan lain - lain.
2. Enkripsi teknologi penyimpanan data secara magnetic, optik, maupun chip.

KEAMANAN DARI DEVIL PROGRAM

- Taksonomi ancaman perangkat lunak / klasifikasi program jahat (malicious program)

1. Program-program yang memerlukan program inang (host program). Fragmen program tidak dapat mandiri secara independen dari suatu program aplikasi, program utilitas atau program sistem.

2. Program-program yang tidak memerlukan program inang. Program sendiri yang dapat dijadwalkan dan dijalankan oleh sistem operasi.

KEAMANAN DARI DEVIL PROGRAM

- Tipe - tipe program jahat :

1. Bacteria
2. Logic bomb
3. Trapdoor
4. Trojan Horse
5. Virus
6. Worm

TUGAS:

- Buat presentasi untuk 3 orang :
- Jelaskan perbedaan dan berikan contoh - contoh cara mendiagnosa dan penanganannya dari jenis mailcious dibawah ini:

1. Bacteria
2. Logic bomb
3. Trapdoor
4. Trojan Horse
5. Virus
6. Worm

- Dipresentasikan minggu depan!
- Presentasi wajib hadir karena untuk nilai tugas.

Terima Kasih