COMPUTER AND NETWORK SECURITY

SUPRIYATI, S.E., M.SI., AK., CA.

PENDAHULUAN

- Ciphers dan cryptosystems
- Secret-key cryptography
- Public-key cryptography
- Key agreement protocols
- Key management
- Digital signatures
- Public key infrastructures, certificates, dan certificates authorities
- Cryptanalysis
- Security Protocol
- Security attacks
- Network security

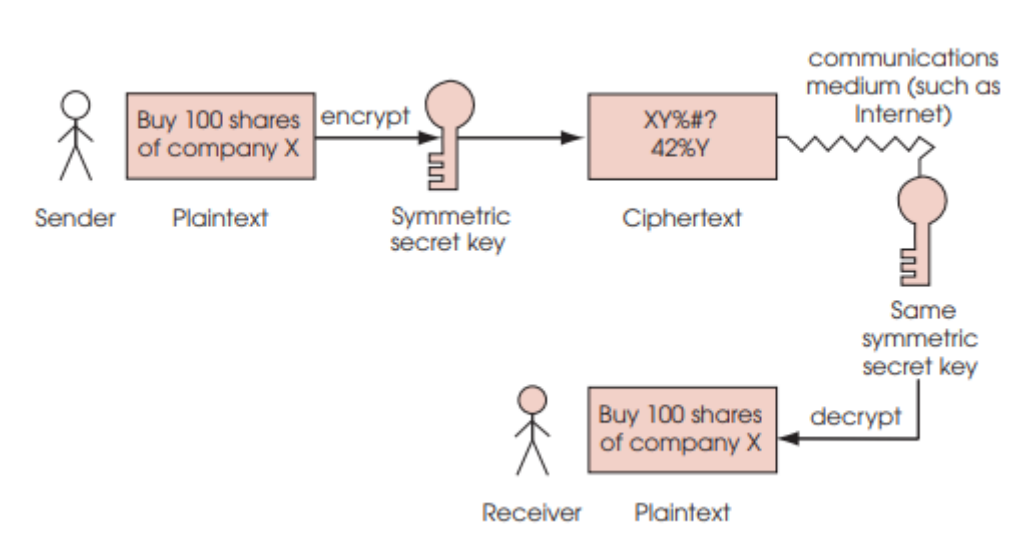
INTRODUCTION

- Ledakan e-business dan e-commerce memaksa bisnis dan konsumen untuk fokus pada keamanan Internet.
- Konsumen membeli produk, perdagangan saham, dan perbankan online. Mereka memberikan nomor kartu kredit, nomor jaminan sosial, dan informasi rahasia lainnya melalui situs Web.
- Bisnis mengirim informasi rahasia kepada klien dan vendor melalui Internet.
- Pada saat yang sama, terjadi peningkatan jumlah serangan keamanan. Individu dan organisasi rentan terhadap pencurian data dan serangan peretas yang dapat merusak file dan bahkan mematikan bisnis elektronik. Keamanan sangat penting bagi e-business.

CIPHER KUNO KE CRYPTOSYSTEM MODERN

- Cipher, atau cryptosystem, adalah teknik atau algoritma untuk mengenkripsi pesan.
- Cipher kriptografi digunakan sejauh zaman Mesir kuno. Dalam kriptografi kuno, pesan dienkripsi dengan tangan, biasanya dengan metode berdasarkan huruf abjad pesan.
- Cryptosystems modern adalah digital. Algoritma mereka didasarkan pada bit individual dari sebuah pesan daripada huruf-huruf alfabet.
- Komputer menyimpan data sebagai string biner, yang merupakan urutan satu dan nol. Setiap digit dalam urutan disebut bit.
- Kunci enkripsi dan dekripsi adalah string biner dengan panjang kunci yang diberikan. Sebagai contoh, sistem enkripsi 128-bit memiliki panjang kunci 128 bit. Kunci yang lebih panjang memiliki enkripsi yang lebih kuat; dibutuhkan lebih banyak waktu dan daya komputasi untuk "memecahkan kode."

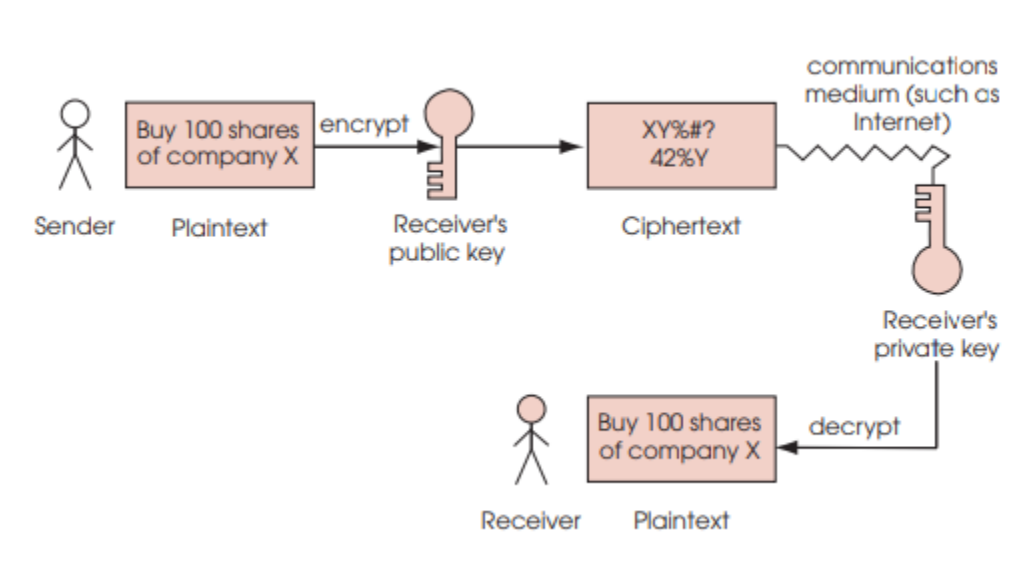
SECRET-KEY CRYPTOGRAPHY



Gambar Proses enkripsi dan dekripsi pesan menggunakan kunci rahasia simetris

- Secret-key cryptography menggunakan kunci rahasia simetris yang sama untuk mengenkripsi dan mendekripsi pesan. Dalam hal ini, pengirim mengenkripsi pesan menggunakan kunci rahasia simetris, kemudian mengirim pesan terenkripsi dan kunci rahasia simetris ke penerima yang dituju.
- Masalah mendasar dengan kriptografi kunci-rahasia adalah bahwa sebelum dua orang dapat berkomunikasi dengan aman, mereka harus menemukan cara untuk bertukar kunci rahasia simetris dan aman.

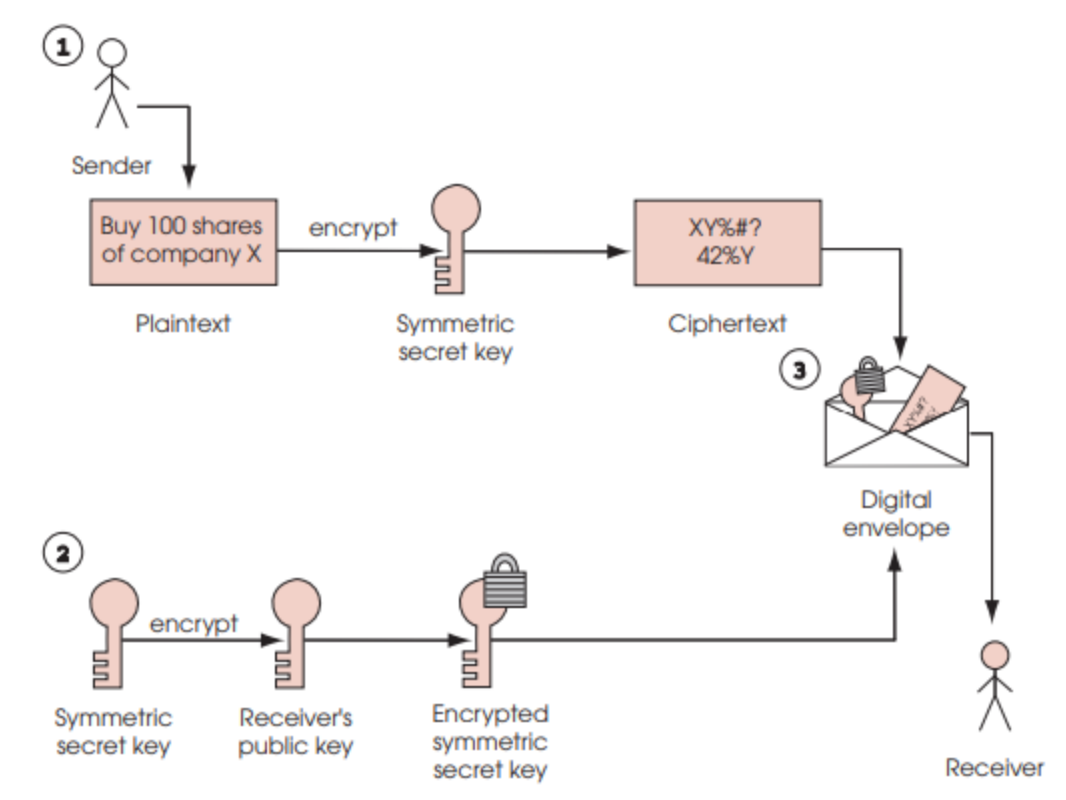
PUBLIC-KEY CRYPTOGRAPHY



Gambar Proses enkripsi dan dekripsi pesan menggunakan Public-key Cryptography

- Public-key Cryptography dikembangkan oleh Whitfield Diffie dan Martin Hellman, peneliti di Stanford University pada tahun 1976.
- Public-key Cryptography bersifat asimetris. menggunakan dua kunci terkait terbalik: kunci publik dan kunci pribadi.
- Kunci pribadi dirahasiakan oleh pemiliknya. Kunci publik didistribusikan secara bebas. Jika kunci publik digunakan untuk mengenkripsi pesan, hanya kunci pribadi yang sesuai yang dapat mendekripsi pesannya, dan sebaliknya.

KEY AGREEMENT PROTOCOLS



Gambar Proses Membuat amplop digital.

- Proses di mana dua pihak dapat bertukar kunci melalui media yang tidak aman disebut Key Agreement Protocols. Protokol mengatur aturan untuk komunikasi: Tepatnya algoritma enkripsi apa yang akan digunakan?
- Perjanjian kunci yang paling umum melindungi selubung digital. Menggunakan amplop digital, pesan dienkripsi menggunakan kunci rahasia simetris, dan kemudian kunci rahasia simetris dienkripsi menggunakan enkripsi kunci publik.

KEY MANAGEMENT

- Komponen utama manajemen kunci adalah pembuatan kunci — proses pembuatan kunci.
- Pihak ketiga dapat mencoba mendekripsi pesan dengan menggunakan setiap kunci dekripsi yang mungkin. Kunci dibuat aman dengan memilih panjang kunci yang sangat besar sehingga secara komputasi tidak layak untuk mencoba semua kombinasi tersebut.
- Algoritma pembangkitan-kunci terkadang dibuat secara tidak sengaja untuk memilih hanya dari sebagian kecil kunci yang mungkin.
- Jika subsetnya cukup kecil, maka mungkin pihak ketiga mencoba setiap kunci yang mungkin untuk memecahkan enkripsi. Karena itu, penting untuk memiliki program pembangkitan kunci yang benar-benar acak.

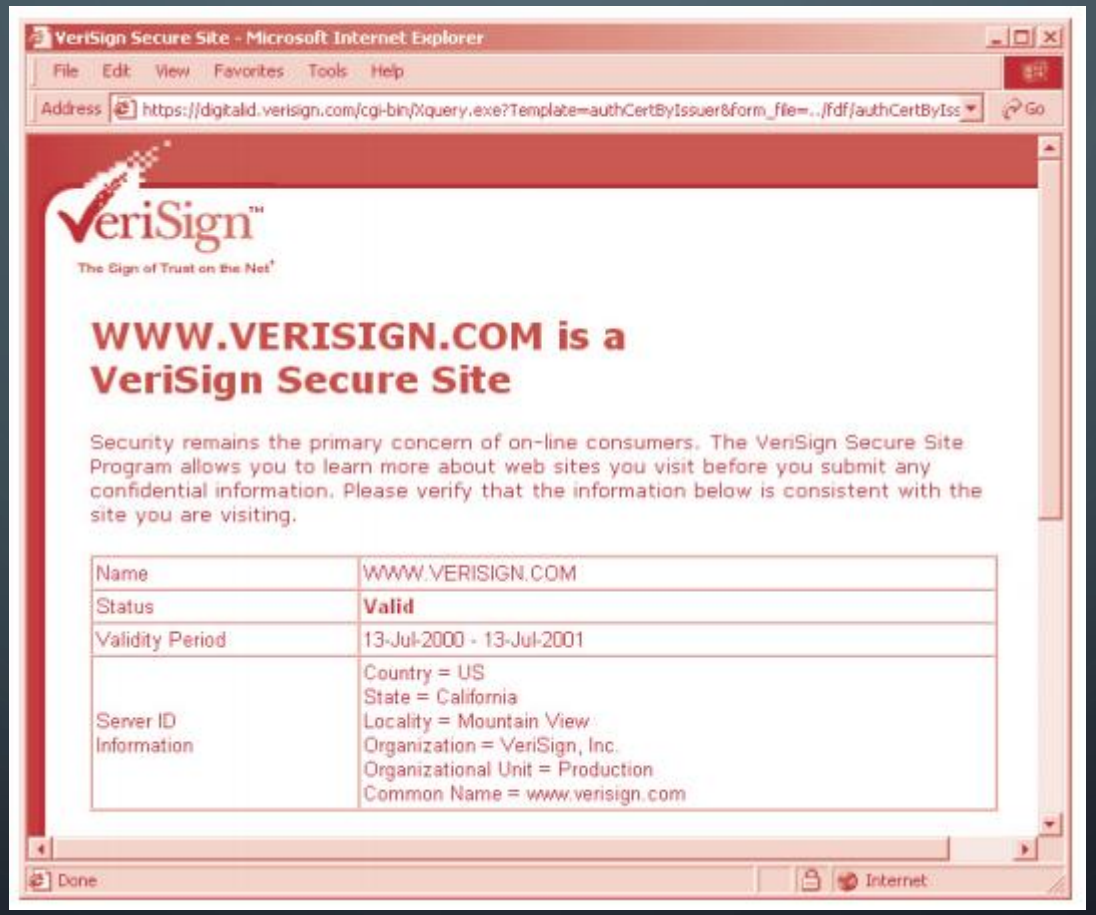
DIGITAL SIGNATURES

- Tanda tangan digital, setara elektronik dengan tanda tangan tertulis, dikembangkan untuk digunakan dalam kriptografi kunci publik untuk memecahkan masalah otentikasi dan integritas.
- Tanda tangan digital mengautentikasi identitas pengirim, dan, seperti tanda tangan tertulis, tanda tangan digital sulit dipalsukan.
- Untuk membuat tanda tangan digital, pengirim pertama-tama akan mengambil pesan teks asli dan menjalankannya melalui fungsi hash, yang merupakan perhitungan matematis yang memberikan nilai hash pada pesan tersebut.
- Ada perbedaan mendasar antara tanda tangan digital dan tanda tangan tulisan tangan. Tanda tangan tulisan tangan tidak tergantung pada dokumen yang ditandatangani. Jadi, jika seseorang dapat memalsukan tanda tangan tulisan tangan, mereka dapat menggunakan tanda tangan itu untuk memalsukan banyak dokumen. Tanda tangan digital dibuat menggunakan konten dokumen. Karenanya, tanda tangan digital Anda berbeda untuk setiap dokumen yang Anda tandatangani.

PUBLIC-KEY INFRASTRUCTURE, CERTIFICATES AND CERTIFICATION AUTHORITIES

- Public-key Infrastructure mengintegrasikan kriptografi kunci publik dengan digital certificates dan certification authorities untuk mengotentikasi pihak dalam suatu transaksi.
- Digital certificates adalah dokumen digital yang dikeluarkan oleh certification authorities (CA). Digital certificates mencakup nama subjek (perusahaan atau individu yang disertifikasi), kunci publik subjek, nomor seri, tanggal kedaluwarsa, tanda tangan otoritas sertifikasi tepercaya, dan informasi terkait lainnya. CA adalah lembaga keuangan atau pihak ketiga tepercaya lainnya, seperti VeriSign. CA bertanggung jawab untuk otentikasi, jadi CA harus hati-hati memeriksa informasi sebelum mengeluarkan digital certificates.

PUBLIC-KEY INFRASTRUCTURE, CERTIFICATES AND CERTIFICATION AUTHORITIES



Gambar contoh sertifikat digital VeriSign.

CRYPTANALYSIS

- Bahkan jika kunci dirahasiakan, adalah mungkin untuk kompromi keamanan suatu sistem. Mencoba mendekripsi ciphertext tanpa mengetahui kunci dekripsi dikenal sebagai cryptanalysis.
- Bentuk paling umum dari serangan cryptanalytic adalah serangan di mana algoritma enkripsi dianalisis untuk menemukan hubungan antara bit kunci enkripsi dan bit dari ciphertext.
- Seringkali, hubungan ini hanya bersifat statistik dan menggabungkan pengetahuan luar tentang plaintext. Tujuan dari serangan semacam itu adalah untuk menentukan kunci dari ciphertext.

SECURITY PROTOCOLS

Setiap orang yang menggunakan Web untuk e-bisnis dan e-commerce perlu memperhatikan keamanan informasi pribadi mereka. Ada beberapa protokol yang menyediakan keamanan transaksi, seperti:

- Secure Sockets Layer (SSL)
- Secure Electronic Transaction (SET)

SECURE SOCKETS LAYER (SSL)

- Protokol Secure Sockets Layer (SSL), yang dikembangkan oleh Netscape Communications, adalah protokol nonproprietary yang biasanya digunakan untuk mengamankan komunikasi di Internet dan Web.
- SSL dibangun ke banyak browser Web, termasuk Netscape Communicator, Microsoft Internet Explorer dan banyak produk perangkat lunak lainnya. Ini beroperasi antara protokol komunikasi TCP / IP Internet dan perangkat lunak aplikasi.
- SSL menggunakan teknologi kunci publik dan sertifikat digital untuk mengotentikasi server dalam transaksi dan untuk melindungi informasi pribadi saat berpindah dari satu pihak ke pihak lain melalui Internet. Transaksi SSL tidak memerlukan otentikasi klien.

SECURE ELECTRONIC TRANSACTION (SET)

- The Secure Electronic Transaction (SET) protocol, yang dikembangkan oleh Visa International dan MasterCard, dirancang khusus untuk melindungi transaksi pembayaran e-commerce. SET menggunakan sertifikat digital untuk mengautentikasi masing-masing pihak dalam transaksi e-commerce, termasuk pelanggan, pedagang dan bank pedagang. Kriptografi kunci publik digunakan untuk mengamankan informasi saat dikirimkan melalui Web.
- Pedagang harus memiliki sertifikat digital dan perangkat lunak SET khusus untuk memproses transaksi. Pelanggan harus memiliki sertifikat digital dan perangkat lunak dompet digital.

SECURITY ATTACKS

- Serangan cyber terbaru pada e-bisnis telah membuat halaman depan surat kabar di seluruh dunia. Serangan penolakan layanan, virus, dan worm menelan biaya miliaran dolar bagi perusahaan.
- Serangan penolakan layanan terjadi ketika sumber daya jaringan diambil oleh individu yang tidak berwenang, sehingga jaringan tidak tersedia untuk pengguna yang sah; biasanya, serangan dilakukan oleh server flooding dengan paket data. Tindakan ini sangat meningkatkan lalu lintas di jaringan, membanjiri server dan menjadikannya mustahil bagi pengguna yang sah untuk mengunduh informasi
- Virus dalam program komputer sering dikirim sebagai lampiran atau disembunyikan dalam klip audio, klip video, dan permainan yang dilampirkan, atau ditimpa, program lain untuk direplikasi sendiri. Virus dapat merusak file Anda atau bahkan menghapus hard drive.

NETWORK SECURITY: FIREWALLS

- Tool dasar dalam network security adalah firewall. Tujuan dari firewall adalah untuk melindungi jaringan area lokal (LAN) dari penyusup di luar jaringan.
- Ada dua jenis utama firewall: firewall packet-filtering dan application-level gateway.
- Firewall packet-filtering memeriksa semua data yang dikirim dari luar LAN dan secara otomatis menolak paket data yang memiliki alamat jaringan local
- Tujuan application-level gateway adalah untuk menyaring data aktual. Jika pesan dianggap aman, maka pesan dikirim ke penerima yang dituju.

NETWORK SECURITY: KERBEROS

- Kerberos adalah protokol open-source yang tersedia secara bebas yang dikembangkan di MIT. Ini menggunakan kriptografi kunci-rahasia simetris untuk mengotentikasi pengguna dalam jaringan dan untuk menjaga integritas dan privasi komunikasi jaringan.
- Otentikasi dalam sistem Kerberos ditangani oleh sistem Kerberos utama dan Ticket Granting Service (TGS) sekunder. Sistem Kerberos utama mengautentikasi identitas klien ke TGS; TGS mengotentikasi hak klien untuk mengakses layanan jaringan tertentu.

NETWORK SECURITY: BIOMETRICS

- Inovasi dalam keamanan kemungkinan besar adalah biometrik. Biometrik menggunakan informasi pribadi yang unik, seperti sidik jari, pemindaian iris mata atau pemindaian wajah, untuk mengidentifikasi pengguna. Sistem ini menghilangkan kebutuhan akan kata sandi, yang jauh lebih mudah untuk dicuri.
- Saat ini, kata sandi adalah cara utama otentikasi; namun, mulai terlihat adanya pergeseran ke kartu pintar dan Biometrik. Otentikasi dua faktor menggunakan dua cara untuk mengotentikasi pengguna, seperti biometrik atau kartu pintar yang digunakan bersama dengan kata sandi. Meskipun sistem ini berpotensi dikompromikan, menggunakan dua metode otentikasi lebih aman daripada hanya menggunakan kata sandi saja.

REFERENSI

https://bcomit.files.wordpress.com/2018/02/e-business-and-e-commerce-1.pdf