Enkripsi dan Kriptografi

EDP Audit

Enkripsi adalah sarana utama perlindungan aset informasi. Jika diterapkan dengan benar, enkripsi akan menggagalkan hampir setiap serangan singkat dari upaya yang disponsori secara nasional. Enkripsi dapat digunakan untuk melindungi aset informasi, baik yang disimpan pada tape atau disk, maupun saat transit pada link komunikasi.

Evolusi Penggunaan Enkripsi

Sebelum 1990-an

Pengguna utama teknologi enkripsi adalah pemerintah nasional, kontraktor pemerintah, dan sistem perbankan swasta.

Era Internet

Dengan perkembangan internet dan perdagangan elektronik, kebutuhan untuk pertukaran aman informasi elektronik menjadi sangat penting bagi entitas komersial dan konsumen.

Kriptografi adalah cara terkuat untuk mengamankan informasi elektronik terhadap pencurian atau kompromi. Namun, kriptografi dapat menjadi sekutu dan musuh dari amannya pertukaran informasi elektronik.

Ancaman Keamanan Sistem Komputer

Serangan Hacker

Sistem komputer Departemen Pertahanan AS mengalami sekitar 250.000 serangan hacker pada tahun 1995, dengan jumlah yang berlipat ganda setiap tahun.

Pencurian Rahasia Militer

Hacker Belanda mencuri rahasia militer AS selama Perang Teluk Persia dan menawarkannya ke Irak, yang bisa mengubah jalannya perang.

Kerentanan Infrastruktur

Tim keamanan nasional AS berhasil memperoleh akses ke sistem jaringan tenaga listrik yang dapat menyabotase dan menenggelamkan negara ke dalam kegelapan.

Kekuatan Komputasi dalam Memecahkan Enkripsi

Internet telah membuat kemungkinan untuk mengumpulkan sumber komputasi besar dalam memecahkan sebuah kunci enkripsi.

1994

Kunci RSA 129-digit rusak melalui usaha gabungan 1.600 komputer di seluruh dunia, menghabiskan 5.000 MIPS dalam sebulan.

1

1997

Ian Goldberg menghubungkan 250 komputer untuk menguji 100 miliar kemungkinan kunci per jam, memecahkan algoritma enkripsi RSA 40-bit dalam 3,5 jam.

2

1999

Tim ilmuwan internasional di Belanda menentukan faktor prima RSA-155 menggunakan 300 komputer selama 7 bulan.

3

Pentingnya Enkripsi dalam Keamanan Informasi

Enkripsi adalah aspek yang paling penting dari keamanan informasi dan komponen utama dalam infrastruktur keamanan informasi secara keseluruhan dari setiap proses elektronik.

Keamanan Nasional

Melindungi informasi yang berkaitan dengan masalah keamanan nasional.

Transaksi Keuangan

Mengamankan transaksi keuangan elektronik dalam semua sistem perbankan besar.

Perdagangan Elektronik

Melindungi perdagangan elektronik di kalangan pedagang dan konsumen.

Pertukaran Data

Mengamankan pertukaran data elektronik (EDI) antara perusahaan dan pelanggan.

Empat Pilar Kontrol Kriptografi

Kerahasiaan

Memastikan hanya penerima yang dituju dapat membaca informasi yang dikirimkan.

Integritas

Menjamin informasi tidak diubah, ditambahkan, atau dihapus selama transmisi.

Keaslian

Memverifikasi bahwa pesan berasal dari sumber yang sah dan bukan entitas tidak dikenal.

Tanpa Penolakan

Mencegah pengirim menyangkal fakta bahwa ia mengirimkan pesan.

Terminologi Kriptografi

Enkripsi

Tindakan atau proses menerjemahkan pesan ke dalam bentuk tersembunyi dengan menggunakan formula rahasia atau algoritma.

Dekripsi

Tindakan atau proses menerjemahkan pesan tersembunyi ke dalam bentuk aslinya yang dapat dibaca.

Algoritma

Prosedur langkah demi langkah untuk memecahkan masalah dalam jumlah terbatas. Formula rahasia yang digunakan untuk mengenkripsi dan mendekripsi pesan.

Kriptografi

Seni atau ilmu mengenkripsi dan mengartikan pesan dengan menggunakan kunci rahasia atau kode.

Kriptoanalisis

Seni atau ilmu mengartikan pesan terenkripsi tanpa manfaat kunci atau kode rahasia.

Kriptologi

Studi ilmiah baik dari kriptografi maupun kriptanalisis.

Tiga Kaki Pesan Elektronik yang Aman

Enkripsi

Membantu menjamin kerahasiaan informasi yang sedang dikirim dan melindungi data yang tersimpan pada media elektronik.

Hashing

Membantu memastikan integritas pesan dengan memverifikasi bahwa informasi tidak diubah selama transmisi.

Tanda Tangan Digital

Membantu memastikan keaslian transmisi elektronik dan tanpa penolakan dari transmisi oleh pembuatnya.

Jika salah satu kaki gagal, pesan tersebut tidak lagi sepenuhnya aman.

Algoritma Enkripsi: Simetris vs Asimetris

Algoritma Simetris

Menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi pesan.

- Contoh: DES (Data Encryption Standard)
- Panjang kunci: 56-bit
- Digunakan oleh lembaga keuangan dan ATM
- Lebih cepat dalam pemrosesan

Algoritma Asimetris

Memerlukan kunci yang berbeda tetapi secara matematis terkait untuk mengenkripsi dan mendekripsi.

- Menggunakan kunci publik dan pribadi
- Contoh: RSA
- Panjang kunci lebih panjang (1024-2048 bit)
- Lebih lambat tetapi lebih aman

Sejarah Data Encryption Standard (DES)

1

1977

DES diadopsi sebagai Standar Pengolahan Informasi Federal (FIPS) oleh pemerintah AS untuk informasi sensitif tapi tidak rahasia.

2

Pengembangan

DES dikembangkan oleh IBM di bawah kontrak dengan National Institute of Standards and Technology (NIST), menggunakan panjang kunci 56-bit.

3

Adopsi Komersial

Penggunaan DES oleh instansi pemerintah menyebabkan penerimaan umum untuk enkripsi komersial, termasuk oleh lembaga keuangan dan sistem ATM.

4

Kelemahan

Kemajuan teknologi mengikis kekuatan dan efektivitas DES, membuatnya rentan terhadap serangan kekuatan brutal.

Peretakan DES: Tantangan RSA

Pada 17 Juni 1997, algoritma enkripsi DES dirusak oleh Rocke Verser, seorang programmer dari Loveland, Colorado, sebagai tanggapan atas "RSA Secret-Key Challenge".

72Q

Kemungkinan Kunci

Lebih dari 72 kuadriliun kemungkinan kunci (72,057,594,037,972,936) dalam kunci 56-bit.

7B

Kecepatan Pengujian

Tim Verser menguji hampir 7 miliar kunci per detik dan 601 triliyun kunci per hari.

25%

Kunci Diidentifikasi

Kunci ditemukan setelah pengujian sekitar 18 kuadriliun kunci, atau 25% dari kemungkinan kunci.

> "Kami telah menunjukkan bahwa DES dapat retak, dan itu tidak sulit untuk melakukannya. Berarti kita perlu membuat tampilan yang sangat serius dalam bagaimana data dienkripsi dan disimpan serta disahkan." - Rocke Verser

Tantangan DES II dan Deep Crack

Tantangan DES II (1998)

Tim Distributed.Net memecahkan tantangan dalam 39 hari dengan mengkoordinasikan 22.000 peserta di seluruh dunia dan lebih dari 50.000 CPU.

- Mencari lebih dari 61 kuadriliun kunci
- Tingkat puncak: 26 triliun kunci per detik
- Kunci ditemukan setelah mencari 85% solusi

Deep Crack (Juli 1998)

Electronic Frontier Foundation (EFF) melaporkan satu komputer bernama "Deep Crack" memecahkan pesan enkripsi DES dalam 56 jam.

- Biaya proyek: $220.000
- 36.864 mikroprosesor
- Masing-masing menguji 2,5 juta kunci per detik

Hubungan Panjang Kunci, Kecepatan Komputer, dan Biaya

Kemudahan algoritma simetris yang dapat dikalahkan pada dasarnya fungsi dari kecepatan komputer, panjang kunci, dan sumber daya keuangan yang tersedia untuk hacker.

Panjang Kunci	Waktu Pemecahan	Biaya Hardware
26 bit	Sebentar/sekali	$50.000-$75.000
38 bit	Sekitar 1 jam	$50.000-$75.000
40 bit	Sekitar 4 jam	$50.000-$75.000
48 bit	Sekitar 1 bulan	$50.000-$75.000
56 bit (DES)	30 tahun / 10 hari	$75.000 / $1 juta
128 bit	Sangat aman (30+ tahun)	-

Setiap bit tambahan yang ditambahkan pada panjang kunci akan menggandakan jumlah kemungkinan kombinasi.

Advanced Encryption Standard (AES)

Pada tahun 1996, NIST memulai proses pemilihan penggantian algoritma DES, yang dikenal dengan Standar Enkripsi Tambahan (AES).

01

Juni 1998: Babak 1

15 kandidat diserahkan ke NIST untuk ditinjau oleh komunitas kriptografi mengenai keamanan, efisiensi, dan keacakan.

02

Agustus 1999: Lima Finalis

NIST menyebutkan lima finalis AES: MARS, RC6, Rijndael, Serpent, dan Twofish.

03

Oktober 2000: Pemilihan

NIST mengumumkan Rijndael sebagai AES baru yang diusulkan karena kombinasi terbaik dari keamanan, kinerja, dan fleksibilitas.

04

26 Mei 2002: Efektif

Rijndael diumumkan sebagai FIPS 197 (AES) dan menjadi efektif sebagai standar enkripsi baru.

Lima Finalis AES

1. **MARS (IBM)**
   Kunci bersama blok sandi simetrik dengan blok 128 bit dan ukuran kunci variabel. Menawarkan keamanan tiga kali lipat dari DES dengan kecepatan lebih tinggi.

2. **RC6 (RSA Labs)**
   Perbaikan evolusioner dari RC5 dengan rotasi data yang bergantung. Menawarkan keamanan yang baik dan kinerja yang baik.

3. **Rijndael (Belgia)**
   Blok variabel dan panjang kunci 128, 192, atau 256 bit. Dapat diimplementasikan dengan sangat efisien pada berbagai prosesor dan hardware.

4. **Serpent (UK/Israel/Norwegia)**
   Sandi blok 128 bit yang lebih cepat dari DES dan mendukung implementasi potongan bit yang sangat efisien.

5. **Twofish (Bruce Schneier dkk)**
   Blok 128 bit dan panjang variabel kunci 128, 192, atau 256 bit dengan fitur pengaturan kunci yang efisien.

Keamanan Algoritma Asimetris

Algoritma asimetris menggunakan panjang kunci yang lebih panjang dari algoritma simetris. Untuk mengalahkan algoritma asimetris, seseorang harus menentukan kesesuaian kunci rahasia dari kunci publik.

256 bit

Mudah diperhitungkan oleh pengguna komputer dengan rata-rata pengalaman dan sumber daya.

384 bit

Dapat dipecah oleh kelompok riset universitas atau perusahaan.

512 bit

Berada dalam jangkauan pemerintah utama.

768 bit

Mungkin tidak aman dalam jangka panjang.

1024 bit

Harus aman untuk beberapa tahun kecuali kemajuan algoritmik besar dibuat.

2048 bit

Dianggap aman selama beberapa dekade.

Cara Mengalahkan Algoritma Enkripsi

Kelemahan Algoritma

Algoritma itu sendiri mungkin lemah atau secara matematis dapat diprediksi.

Contoh: Pada 1995, dua mahasiswa UC Berkeley menemukan metode untuk memecahkan skema enkripsi kunci publik Netscape Navigator dalam waktu kurang dari satu menit.

Paul Kocher mengidentifikasi bahwa kunci untuk beberapa sistem enkripsi dapat diprediksi dengan mencatat waktu yang diperlukan algoritma untuk mendekripsi pesan.

Serangan Kekuatan Brutal

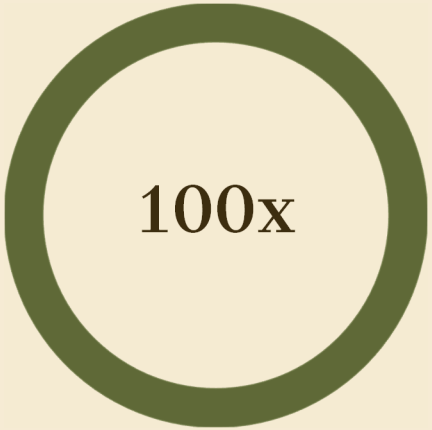
Menerapkan penggunaan satu atau lebih komputer untuk menguji semua kemungkinan kunci secara matematis sampai yang benar teridentifikasi.

Kelemahan: Semakin panjang kunci, semakin sulit untuk mengalahkan algoritma dalam hal waktu dan uang.

Trade-off: Kunci yang lebih panjang memakan waktu dan biaya lebih banyak bagi penerima untuk mendekripsi informasi.

Perbandingan Kecepatan: Simetris vs Asimetris

Kriptografi asimetris memiliki kunci yang lebih panjang dari kriptografi simetris, sehingga bisa jauh lebih lambat dalam pemrosesan.



Perbedaan Kecepatan

Beberapa kriptografi kunci pribadi (simetris) sekitar 100 kali lebih cepat daripada kriptografi kunci publik (asimetris).

Akibatnya, kriptografi asimetris kurang praktis untuk mengenkripsi transmisi bervolume tinggi, real-time, atau informasi yang besar. Sebagian besar jaringan ATM menggunakan sistem enkripsi simetris seperti DES karena kecepatan pemrosesan yang diperlukan.

Enkripsi Asimetris untuk Kerahasiaan

Enkripsi asimetris adalah metode yang diterima secara umum dalam menjamin kerahasiaan sebagian besar transaksi perdagangan elektronik.

Pengirim

Mengenkripsi pesan menggunakan kunci publik penerima dan mengirimkan pesan terenkripsi.

Transmisi

Pesan terenkripsi dikirim melalui jaringan atau internet.

Penerima

Mendekripsi pesan menggunakan kunci pribadinya yang hanya diketahui olehnya.

Kerahasiaan tercapai karena hanya penerima yang mengetahui kunci pribadinya dan satu-satunya yang dapat mendekripsi pesan pengirim.

Fungsi Hash Satu Arah

Tujuan utama dari hashing adalah membantu memastikan bahwa informasi elektronik yang dikirim ke penerima belum diubah, informasi lain belum ditambahkan, dan informasi belum dihapus dari transmisi.

Fungsi Hash

Rumus matematika yang menggunakan pesan elektronik sebagai masukan dan membuat blok data yang disebut inti pesan.

MD-5 dan SHA-1

Dua fungsi hashing satu arah yang umum. SHA-1 adalah standar FIPS pemerintah AS dan standar ANSI.

Satu Arah

Hanya dapat digunakan untuk menghitung inti pesan dalam satu arah. Tidak dapat menentukan informasi asli dari inti pesan.

Tanpa Bentrokan

Tidak menghasilkan inti pesan yang sama untuk set data yang berbeda. Semakin panjang inti pesan, semakin kecil risiko bentrokan hash.

Enkripsi dengan Hashing untuk Integritas

Hashing dapat diterapkan dalam hubungannya dengan enkripsi asimetris untuk mencapai kerahasiaan dan integritas pesan.

01

Pengirim: Membuat Inti Pesan

Merujuk pesan ke fungsi hashing satu arah untuk membuat inti pesan.

02

Pengirim: Mengenkripsi

Pesan dan inti pesan dienkripsi menggunakan kunci publik penerima, kemudian ditransmisikan.

03

Penerima: Mendekripsi

Mendekripsi pesan dan inti pesan menggunakan kunci pribadinya.

04

Penerima: Memverifikasi

Merujuk pesan yang didekripsi ke algoritma hashing yang sama dan membandingkan inti pesan yang dihasilkan dengan yang diterima.

Jika integritas pesan utuh, inti pesan pengirim akan setuju dengan inti yang dikomputasi oleh penerima.

Tanda Tangan Digital dan Sertifikat Digital

Tanda tangan digital dan sertifikat digital digunakan untuk memberikan jaminan kepada penerima pesan bahwa pesan tersebut asli dan tidak dapat ditolak oleh pengirimnya.

Tanda Tangan Digital

Untuk menandatangani pesan secara digital, pengirim menunjukkan pesan ke fungsi hashing satu arah. Inti pesan yang dihasilkan dienkripsi menggunakan kunci pribadi pengirim, sehingga menghasilkan tanda tangan digital.

Sertifikat Digital

Diterbitkan oleh otoritas sertifikat (CA) terpercaya. Mengidentifikasikan pengirim dan berisi kunci publik pengirim serta tanda tangan digital dari CA terpercaya.

Penerima harus memperoleh sertifikat digital secara independen dari CA terpercaya sebelum menerima pesan dari pengirim.

Proses Lengkap: Enkripsi, Hashing, dan Tanda Tangan Digital

1

Pengirim: Hash Pesan

Hash pesan menggunakan fungsi hash satu arah untuk menghasilkan inti.

2

Pengirim: Buat Tanda Tangan

Enkripsi inti dengan kunci pribadi pengirim untuk membuat tanda tangan digital.

3

Pengirim: Enkripsi Pesan

Enkripsi pesan menggunakan kunci publik penerima.

4

Pengirim: Kirim

Kirim pesan terenkripsi dan tanda tangan digital ke penerima.

5

Penerima: Dekripsi Pesan

Dekripsi pesan menggunakan kunci pribadi penerima.

6

Penerima: Hash Pesan

Hash pesan menggunakan fungsi hash satu arah yang sama seperti pengirim.

7

Penerima: Verifikasi Tanda Tangan

Dekripsi tanda tangan digital menggunakan kunci publik pengirim dari sertifikat digital.

8

Penerima: Bandingkan

Bandingkan inti pesan untuk memverifikasi integritas dan keaslian. Jika sama, pesan asli; jika berbeda, tolak.

Peran Otoritas Sertifikat (CA)

Otoritas sertifikat dibentuk untuk membantu memastikan bahwa pemegang kunci publik tahu siapa yang membuat pesan menggunakan kunci pribadinya.

Menyatakan Keaslian

Menyatakan keaslian kunci publik dan mengidentifikasi pembuat kunci publik/pribadi.

Mendistribusikan Kunci

Mendistribusikan kunci publik kepada pihak-pihak yang memerlukan untuk komunikasi yang aman.

Jenis CA

Lembaga keuangan, penjual keamanan produk, dan lembaga pemerintah dapat menjadi otoritas sertifikat.

Beberapa negara bagian AS, seperti Utah dan Washington, telah menyusun undang-undang untuk memastikan bahwa otoritas sertifikat memenuhi standar tertentu sebelum mereka berlisensi dan secara hukum "dipercaya".

Manajemen Kunci dan Aspek Politik Kriptografi

Tantangan Manajemen Kunci

Dengan perdagangan elektronik, manajemen kunci menjadi tantangan besar. Rumus untuk menentukan jumlah kunci unik yang diperlukan:

$$K = \frac{n(n-1)}{2}$$

Dimana K adalah jumlah kunci unik dan n adalah jumlah entitas yang berkomunikasi.

Entitas (n)	Kunci (K)
10	45
100	4.950
1.000	499.500
10.000	49.999.500

Aspek Politik

Pemerintah AS membatasi ekspor perangkat lunak enkripsi untuk kepentingan keamanan nasional dan penegakan hukum.

- Sebelumnya dibatasi hingga 40-56 bit
- Tahun 2000: Pelonggaran kontrol ekspor ke 15 negara
- Perdebatan antara privasi vs keamanan nasional
- Negara lain juga membatasi impor dan penggunaan

Kriptografi memainkan peran penting dalam keamanan nasional, privasi pribadi, dan aktivitas kompetitif bisnis.