BAB III
KONSEP DASAR KRIPTOGRAFI

3.1 Kriprografi

3.1.1 Sejarah Kriptografi

Kata kriptografi berasal dari bahasa Yunani, “kryptós” yang berarti tersembunyi dan “gráphein” yang berarti tulisan. Kriptografi telah digunakan oleh Julius Caesar sejak zaman Romawi Kuno. Teknik ini dijuluki Caesar cipher untuk mengirim pesan secara rahasia, meskipun teknik yang digunakannya sangat tidak memadai untuk ukuran kini. (Kriptografi 2020) Casanova menggunakan pengetahuan mengenai kriptografi untuk mengelabui Madame d’Urfe (ia mengatakan kepada Madame d’Urfe bahwa sesosok jin memberi tahu kunci rahasia Madame d’Urfe kepadanya, padahal ia berhasil memecahkan kunci rahasia berdasarkan pengetahuannya mengenai kriptografi), sehingga ia mampu mengontrol kehidupan Madame d’Urfe secara total. (Kromodimoeljo, 2010).

3.1.2 Pengertian Kriptografi

Kriptografi adalah ilmu mengenai teknik enkripsi dimana “naskah asli” (plaintext) diacak menggunakan suatu kunci enkripsi menjadi “naskah acak yang sulit dibaca” (ciphertext) oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi bisa mendapatkan kembali data asli. Probabilitas mendapat kembali naskah asli oleh seseorang yang tidak mempunyai kunci dekripsi dalam waktu yang tidak terlalu lama adalah sangat kecil.

Teknik enkripsi yang digunakan dalam kriptografi klasik adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. Untuk public key cryptography, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan - bilangan yang sangat besar. (Kromodimoeljo, 2010).

3.1.3 Aspek Keamanan Kriptografi

Kriptografi memiliki beberapa aspek keamanan antara lain :

a. **Kerahasiaan (confidentiality)**, menjamin bahwa data-data tersebut hanya bisa diakses oleh pihak-pihak tertentu saja. Kerahasiaan bertujuan untuk melindungi suatu informasi dari semua pihak yang tidak berhak atas informasi tersebut.
b. **Otentikasi (authentication)**, merupakan identifikasi yang dilakukan oleh masing – masing pihak yang saling berkomunikasi, maksudnya beberapa pihak yang berkomunikasi harus mengidentifikasi satu sama lainnya. Informasi yang didapat oleh suatu pihak dari pihak lain harus diidentifikasi untuk memastikan keaslian dari informasi yang diterima.
c. **Integritas (integrity)**, menjamin setiap pesan yang dikirim pasti sampai pada penerimanya tanpa ada bagian dari pesan tersebut yang diganti, diduplikasi, dirusak, diubah urutannya, dan ditambahkan. Integritas data

bertujuan untuk mencegah terjadinya pengubahan informasi oleh pihak-pihak yang tidak berhak atas informasi tersebut. Untuk menjamin integritas data ini pengguna harus mempunyai kemampuan untuk mendeteksi terjadinya manipulasi data oleh pihak-pihak yang tidak berkepentingan. Manipulasi data yang dimaksud di sini meliputi penyisipan, penghapusan, maupun penggantian data.

d. **Nirpenyangkalan (Nonrepudiation)**, mencegah pengirim maupun penerima mengingkari bahwa mereka telah mengirimkan atau menerima suatu pesan. Jika sebuah pesan dikirim, penerima dapat membuktikan bahwa pesan tersebut memang dikirim oleh pengirim yang tertera. Sebaliknya, jika sebuah pesan diterima, pengirim dapat membuktikan bahwa pesannya telah diterima oleh pihak yang ditujunya. (Ariyus, 2008).

3.2 Cryptosystem

Cryptographic system (kriptografi sistem) atau *cryptosystem (kriptosistem)* adalah suatu fasilitas untuk mengkonversikan plaintext ke ciphertext dan sebaliknya. Dalam sistem ini, seperangkat parameter yang menentukan transformasi pencipheran tertentu disebut suatu set kunci. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci kriptografi.

3.3 Karakteristik Cryptosystem

Karakteristik Cryptosystem yang baik:

a. Keamanan sistem terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.
b. Cryptosystem yang baik memiliki ruang kunci (keyspace) yang besar.
c. Cryptosystem yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh tes statistik yang dilakukan terhadapnya.
d. Cryptosystem yang baik mampu menahan seluruh serangan yang telah dikenal sebelumnya.

3.4 Macam – Macam Cryptosystem

1. Symmetric Cryptosystem

Dalam symmetric cryptosystem ini, kunci yang digunakan untuk proses enkripsi dan dekripsi pada prinsipnya identik, tetapi satu buah kunci dapat pula diturunkan dari kunci yang lainnya. Kunci-kunci ini harus dirahasiakan. Oleh karena itulah sistem ini sering disebut sebagai secret-key ciphersystem. Jumlah kunci yang dibutuhkan umumnya adalah :

$$\frac{\mathrm{n}C_2}{2} = n.(n-1)$$

dengan n menyatakan banyaknya pengguna.Contoh dari sistem ini adalah Data Encryption Standard (DES), Blowfish, IDEA.

2. Assymmetric Cryptosystem

Dalam assymmetric cryptosystem ini digunakan dua buah kunci. Satu kunci yang disebut kunci publik (public key) dapat dipublikasikan, sedang kunci yang lain yang disebut kunci privat (private key) harus dirahasiakan. Proses menggunakan sistem ini dapat diterangkan secara sederhana sebagai berikut : bila A ingin mengirimkan pesan kepada B, A dapat menyandikan pesannya dengan menggunakan kunci publik B, dan bila B ingin membaca

surat tersebut, ia perlu mendekripsikan surat itu dengan kunci privatnya. Dengan demikian kedua belah pihak dapat menjamin asal surat serta keaslian surat tersebut, karena adanya mekanisme ini. Contoh sistem ini antara lain RSA Scheme dan Merkle-Hellman Scheme.

3.5 Protokol Criptosystem

Cryptographic protocol adalah suatu protokol yang menggunakan kriptografi. Protokol ini melibatkan sejumlah algoritma kriptografi, namun secara umum tujuan protokol lebih dari sekedar kerahasiaan. Pihak-pihak yang berpartisipasi mungkin saja ingin membagi sebagian rahasianya untuk menghitung sebuah nilai, menghasilkan urutan random, atau pun menandatangani kontrak secara bersamaan.
Penggunaan kriptografi dalam sebuah protokol terutama ditujukan untuk mencegah atau pun mendeteksi adanya eavesdropping dan cheating.[11]

3.6 Jenis Penyerangan Pada Protokol

Jenis – jenis penyerangan pada protocol, yaitu :

a. Ciphertext-only attack. Dalam penyerangan ini, seorang cryptanalyst memiliki ciphertext dari sejumlah pesan yang seluruhnya telah dienkripsi menggunakan algoritma yang sama.
b. Known-plaintext attack. Dalam tipe penyerangan ini, cryptanalyst memiliki akses tidak hanya ke ciphertext sejumlah pesan, namun ia juga memiliki plaintext pesan-pesan tersebut.
c. Chosen-plaintext attack. Pada penyerangan ini, cryptanalyst tidak hanya memiliki akses atas ciphertext dan plaintext untuk beberapa pesan, tetapi ia juga dapat memilih plaintext yang dienkripsi.
d. Adaptive-chosen-plaintext attack. Penyerangan tipe ini merupakan suatu kasus khusus chosen- plaintext attack. Cryptanalyst tidak hanya dapat memilih plaintext yang dienkripsi, ia pun memiliki kemampuan untuk memodifikasi pilihan berdasarkan hasil enkripsi sebelumnya. Dalam chosen- plaintext attack, cryptanalyst mungkin hanya dapat memiliki plaintext dalam suatu blok besar untuk dienkripsi; dalam adaptive-chosen-plaintext attack ini ia dapat memilih blok plaintext yang lebih kecil dan kemudian memilih yang lain berdasarkan hasil yang pertama, proses ini dapat dilakukannya terus menerus hingga ia dapat memperoleh seluruh informasi.
e. Chosen-ciphertext attack. Pada tipe ini, cryptanalyst dapat memilih ciphertext yang berbeda untuk didekripsi dan memiliki akses atas plaintext yang didekripsi.
f. Chosen-key attack. Cryptanalyst pada tipe penyerangan ini memiliki pengetahuan tentang hubungan antara kunci-kunci yang berbeda.
g. Rubber-hose cryptanalysis. Pada tipe penyerangan ini, cryptanalyst mengancam, memeras, atau bahkan memaksa seseorang hingga mereka memberikan kuncinya.

3.7 Jenis Penyerangan Pada Jalur Komunikasi

Penyerangan pada jalur komunikasi, yaitu :

a. Sniffing: secara harafiah berarti mengendus, tentunya dalam hal ini yang diendus adalah pesan (baik yang belum ataupun sudah dienkripsi) dalam

suatu saluran komunikasi. Hal ini umum terjadi pada saluran publik yang tidak aman. Sang pengendus dapat merekam pembicaraan yang terjadi.

b. Replay attack: Jika seseorang bisa merekam pesan-pesan handshake (persiapan komunikasi), ia mungkin dapat mengulang pesan-pesan yang telah direkamnya untuk menipu salah satu pihak.

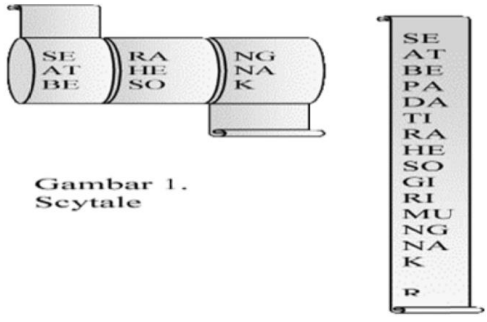
c. Spoofing: Penyerang – misalnya Maman – bisa menyamar menjadi Anto. Semua orang dibuat percaya bahwa Maman adalah Anto. Penyerang berusaha meyakinkan pihak-pihak lain bahwa tak ada salah dengan komunikasi yang dilakukan, padahal komunikasi itu dilakukan dengan sang penipu/penyerang. Contohnya jika orang memasukkan PIN ke dalam mesin ATM palsu – yang benar-benar dibuat seperti ATM asli – tentu sang penipu bisa mendapatkan PIN-nya dan copy pita magentik kartu ATM milik sang nasabah. Pihak bank tidak tahu bahwa telah terjadi kejahatan.

d. Man-in-the-middle: Jika spoofing terkadang hanya menipu satu pihak, maka dalam skenario ini, saat Anto hendak berkomunikasi dengan Badu, Maman di mata Anto seolah-olah adalah Badu, dan Maman dapat pula menipu Badu sehingga Maman seolah-olah adalah Anto. Maman dapat berkuasa penuh atas jalur komunikas ini, dan bisa membuat berita fitnah.

3.8 Metode Kriptografi

3.8.1 Metode kuno

a. 475 S.M. bangsa Sparta, suatu bangsa militer pada jaman Yunani kuno, menggunakan teknik kriptografi yang disebut scytale, untuk kepentingan perang. Scytale terbuat dari tongkat dengan papyrus yang mengelilinginya secara spiral. Kunci dari scytale adalah diameter tongkat yang digunakan oleh pengirim harus sama dengan diameter tongkat yang dimiliki oleh penerima pesan, sehingga pesan yang disembunyikan dalam papyrus dapat dibaca dan dimengerti oleh penerima.



Gambar 1.
Scytale

Gambar 3.1 Scytale

b. Julius Caesar, seorang kaisar terkenal Romawi yang menaklukkan banyak bangsa di Eropa dan Timur Tengah juga menggunakan suatu teknik kriptografi yang sekarang disebut Caesar cipher untuk berkorespondensi sekitar tahun 60 S.M. Teknik yang digunakan oleh Sang Caesar adalah mensubstitusikan alfabet secara beraturan, yaitu

oleh alfabet ketiga yang mengikutinya, misalnya, alfabet ‘’A" digantikan oleh "D", "B" oleh "E", dan seterusnya.

Gambar 3.2 Julius Caesar

3.8.2 Metode Modern

a. Digital Certificate Server (DCS)
   1) verifikasi untuk digital signature
   2) autentikasi user
   3) menggunakan public dan private key

   contoh : Netscape Certificate Server
b. 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
c. 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)
d. Secure Socket Layer (SSL)
   1) dirancang oleh Netscape
   2) menyediakan enkripsi RSA pada layes session dari model OSI.
   3) independen terhadap servise yang digunakan.
   4) melindungi system secure web e-commerce
   5) metode public/private key dan dapat melakukan authentication
   6) terintegrasi dalam produk browser dan web server Netscape.
e. Security Token

   aplikasi penyimpanan password dan data user di smart card
f. Simple Key Management for Internet Protocol
   1) seperti SSL bekerja pada level session model OSI.
   2) menghasilkan key yang static, mudah bobol.
g. MD5
   1) dirancang oleh Prof. Robert Rivest (RSA, MIT) tahun 1991
   2) menghasilkan 128-bit digest.
   3) cepat tapi kurang aman
h. Secure Hash Algoritm (SHA)
   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)
i. RSA Encryption

1) dirancang oleh Rivest, Shamir, Adleman tahun 1977
2) standar de facto dalam enkripsi public/private key
3) didukung oleh Microsoft, apple, novell, sun, lotus
4) mendukung proses authentication
5) multi platform

j. 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

k. 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)

l. Kerberos
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)

m. Advanced Encryption Standard (AES)
1) untuk menggantikan DES (launching akhir 2001)
2) menggunakan variable length block chipper
3) key length : 128-bit, 192-bit, 256-bit
4) dapat diterapkan untuk smart card.[11]

Soal

1. Jelaskan apa itu yang dimaksud dengan kriptografi?
2. Sebutkan bagian aspek keamanan kriptografi!