5025231116

Rafi Faheem Aziz

CH. 9

R.Q 9.4

1. Memungkinkan pembuatan pasangan key (publik-private) secara komputasional mudah & efisien.
2. Proses enkripsi harus dapat dilakukan dengan mudah oleh pengirim menggunakan public key dan pesan yang akan dienkripsi.
3. Proses dekripsi cipher text yang mudah menggunakan private key
4. Secara komputasi mustahil untuk menebak private key dan public key
5. Secara komputasi mustahil untuk recover pesan dari public key dan cipher text

P. 9.3

Diket : $C = 10$, $e = 5$, $n = 35$

a. Faktorkan $n \rightarrow 35 = 5 \times 7$

b. $\varphi(n) = \varphi(35) = (5-1)(7-1) = 4 \times 6 = 24$

c. d. sebagai invers dari e mod $\varphi(n) \rightarrow 5d = 1 \bmod 24$

$d = 5$

d. dekripsi $\rightarrow$ $M = C^d \bmod n = 10^5 \bmod 35$

$M = 5$

CH. 11

R.Q. 11.2

① Weak collision resistance : secara komputasi sulit untuk menemukan y yang menghasilkan hash yang sama dengan x yang sudah diberikan $H(x) = H(y)$

② Strong collision resistance : secara komputasi sulit untuk menemukan sembarang pasangan x dan y yang menghasilkan hash yang sama $H(x) = H(y)$

P. 11.8

$W_t = \sigma_1(W_{14}) + W_9 + \sigma_0(W_1) + W_0$

$\sigma_0(x) = ROTR^1(x) \oplus ROTR^8(x) \oplus SHR^7(x)$

$\sigma_1(x) = ROTR^{19}(x) \oplus ROTR^{61}(x) \oplus SHR^6(x)$

sehingga

$W_{16} = \sigma_1(W_{14}) + W_9 + \sigma_0(W_1) + W_0$

$W_{17} = \sigma_1(W_{15}) + W_{10} + \sigma_0(W_2) + W_1$

$W_{18} = \sigma_1(W_{16}) + W_{11} + \sigma_0(W_3) + W_2$

$W_{19} = \sigma_1(W_{17}) + W_{12} + \sigma_0(W_4) + W_3$

Chapter 13

P.Q. 13.5

Tanda tangan harus dibuat terlebih dahulu kemudian pesan baru dienkripsi. Hal ini memastikan bahwa dalam situasi sengketa. pihak ketiga dapat verifikasi TTD tanpa memerlukan kunci dekripsi penerima

P. 13.3

Dalam DSA, jika nilai k bocor maka private key user dapat dihitung dan dianggap bocor.

Chapter 14

R.Q. 14.9

1. Setiap pengguna memiliki pasangan kunci public-private yang valid
2. Ada certificate Authority terpercaya yang menerbitkan dan menandatangani sertifikat
3. Pihak yang menerima sertifikat harus dapat memverifikasi tanda tangan certificate authority
4. Sertifikat harus berisi identitas pemilik dan public key yg benar
5. Harus ada mekanisme untuk mengecek masa berlaku dan pencabutan sertifikat (CRL / OCSP)

P. 14.7

① Certificate Authority : menerbitkan & menandatangani sertifikat

② Registration Authority : memverifikasi identitas sebelum identitas sertifikat dibuat

③ Repository : menyimpan dan menyediakan sertifikat ~~dibuat~~ untuk public

④ Revocation system (CRL / OCSP) menyatakan apakah sertifikat sudah dicabut

⑤ End Users : pengguna yang memakai sertifikat untuk enkripsi/TTD

Chapter 16

P.Q. 16.5

IEEE 802.1X berfungsi sebagai mekanisme autentikasi akses jaringan. Ini memastikan hanya perangkat yang berhasil diautentikasi (melalui server seperti RADIUS) yang boleh mengakses jaringan, sehingga memberikan kontrol akses dan keamanan jaringan tingkat awal.