Date

Nama: Montana Gunning

NIM : 11619017

1) DSA specifies that if the signature generation process results in a value of $s=0$, a new value of k should be generated and the signature should be recalculated. Why?

=> Karena saat pengguna menghasilkan signature dengan nilai $s=0$, maka secara tidak sengaja telah mengungkapkan kunci private x ke persamaan:

$$s = (k^{-1}(H(M) + xr)) \bmod q \mid x = \frac{-H(M)}{r} \bmod q.$$

Dimana M dan r dapat diperoleh dari pesan melalui jaringan. Dan q adalah komponen yang bersifat public global yang mana dapat diketahui semua orang. Shingga, nilai baru k akan digenerate dan dihitung ulang signaturenya. Ditarenakan tidak mungkin nilai dari $r=0$ atau $s=0$ jika signaturenya benar.

2) what happens if a k value use in creating a DSA signature is compromised?

=> Kunci private dari user di kompromikan jika nilai k ditemukan:

$$s = (k^{-1}(H(M) + xr)) \bmod q \Rightarrow x = \frac{sk - HM}{r} \bmod q$$

Nilai H(M), r, s, dapat diperoleh dari pesan melalui jaringan dan q merupakan komponen bersifat public global. Maka jika nilai k diketahui, akan mudah mengetahui kunci private x

3) In an RSA digital signature scheme, Bob signs message x_i and sends them together with the signatures s_i and her public key to Alice. Bob's public key is the pair (n, e); her private key is d; Oscar can perform man-in-the-middle attacks, i.e., he can replace Bob's public key by his own on the channel. His goal is to alter messages and provide these with a digital signature which will check out correctly on Alice's side, Show everything that oscar must do for a successful attack.

=> Yang harus dilakukan oleh oscar:

a) Oscar menerima pesan antara Bob and Alice

b) Pesan yang diterima, akan diubah oleh oscar. dan menandatangani pesan tersebut dengan private key yang milik oscar

c) Kemudian, oscar akan mengirim pesan baru yang telah diubah dan yang telah ditambah dengan signature dan public key sesuai (e', n') dari sini Alice (yang salah satunya dari oscar)

4] Given an RSA signature scheme with the public key (n = 9797, e = 131), which of the foreowing signatures are valid?

a). (x = 123, sig(x) = 6292)

↳ sig(x) = $x^d \bmod n$

signature valid given $sign(x)^e \equiv x \pmod n$

(n, e) => public key => (9797, 131)

↳ x = 123, sig(x) = 6292

$sig(x)^e \equiv x \pmod n$

$(6292)^{131} \equiv 123 \pmod{9797}$

$123 \equiv 123$ (valid)

b) (x = 4333, sig(x) = 4768)

↳ $sig(x)^e \equiv x \pmod n$

$(4768)^{131} \equiv 4333 \pmod{9797}$

$9644 \not\equiv 4333$ (trdath valid)

c) (x = 4333, sig(x) = 1424)

↳ $sig(x)^e \equiv x \pmod n$

$(1424)^{131} \equiv 4333 \pmod{9797}$

$4333 \equiv 4333$ (valid)

5] Problem 13.7 from william stallings "Cryptography & network security"

↳ it is tempting to try to develop a variation on Diffie-Hellman that could be used as a digital signature. Here is one that is simpler that DSA and that does not require. A secret random number in addition to the private key

public element = q prime number.

α $\alpha < q$ and α is a primitive root of q

private key = x $x < q$

public key = $y = a^x \bmod q$

To sign a message M, compute H = H(M), which is the hash code of the message. We require that gcd [(H, q-1) = 1. If not, append the hash to the message and calculate a new hash. Continue this process until a hash code is produced that is relatively prime to (q-1). Then calculate z to satisfy $z \times H = x \pmod{q-1}$.

Date

The signature of the message is α^z. To verify the signature, a user verifies that $y = (\alpha^z)^h \equiv a^x \bmod q$.

a) Show that this scheme works. That is show that the verification process produces an equality if the signature is valid
↳ Untuk memverifikasi signature, user memverifikasi bahwa $(g^z)^h = g^x \bmod p$.

b) Show that the scheme is unacceptable by describing a simple technique for forging a user's signature on an arbitrary message
↳ Untuk memalsukan signature pada pesan dengan hashnya h - lalu, dihitung y untuk memenuhi $yh = 1 \bmod (p-1)$. Kemudian, $g^{yh} = g$. Jadi $g^{xyh} = g^x \bmod p$.
Sehingga, (h, g^h) adalah signature yang valid dan lawan dapat menghitung g^{xy} sebagai $(g^x)^y$.