SACHIN DUHAN (21117/MC/087)

Qn:1 PGP packets → pretty good privacy.

↳ is used for providing confidentiality in email and file Storage literal packets

following are the packets that provide confidentiality are as :-

1. Compressed data packet
2. Public-key encrypted packet
3. public-key packet
4. User ID packet
5. Signature packet
6. Literal data packet
7. Conventional-key-encrypted data packet

Qn: 2 Digital Signature Algorithm (DSA) :- is based on the modular exponentiation and discrete logarithmic problems.

Verifying a signature :-

~~1. Verify hash~~

let a Signature (r, s) be a valid signature for a given message m when :-

| q = prime

1. $0 < r < q$ and $0 < s < q$

when q is the range i.e. $x \in \{1, q-1\}$

(2) Compute $w : s^{-1} \bmod q$

(3) Compute $u_1 : H(m) \cdot w \bmod q$

(4) Compute $u_2 : r \cdot w \bmod q$

(5) Compute $v : (g^{u_1} \cdot y^{u_2} \bmod p) \bmod q$

The signature can be verified iff $\boxed{v = r}$

Correctness of algorithm :- we know that

$$g = h^{(p-1)/q} \bmod p,$$

it follow, $g^p \equiv h^{p-1} \equiv 1 \bmod p$ $g > 0$ & q is prime

and g must have order q

the signer computes

$$s = k^{-1} (H(m) + xr) \bmod q$$

Then

$$k = H(m) s^{-1} + xrs^{-1}$$

$$\Rightarrow H(m)w + xrw \pmod q$$

Since g has a order $q \pmod p$, we can say that,

$$g^k = g^{H(m)w} \; g^{xrw} \quad \text{or}$$

$$= g^{H(m)w} \; g^{xrw} \Rightarrow g^{H(m)w} \; g^{rw}$$

$\rightarrow g^{u_1} y^{u_2} \pmod p$

$u_1 = H(m) \cdot w \bmod q$

$u_2 = r \cdot w \bmod q$

finally the correctness of the DSA follows from

$r = (g^k \bmod p) \bmod q$

$\rightarrow (g^{u_1} y^{u_2} \bmod p) \bmod q$

$r \Rightarrow v$

Hence Verified

SACHIN DUHAN

2K17/MC/087

Q.no 3

challange - response entity authentication

↳ is a method where claimant elucidates that she is aware of the secret without sending it. The challange comes when a time varying number or time stamp is being sent by the verifier, who checks stuff.

The claimant also applies a function to the challange and fowards the result also known as the response. The response is replied to the verfier. when the verfier recieves the response i.e. sent by claimant proves that claimant knows the secret.