Anish Sachdeva

Class Fun
Date
Page No.

ENS class Test - III

Q1) ~~Digital signature verifying process~~ (DSS)

Digital Signature Standard (DSS) is the digital signature algorithm DSA developed by the U.S National Security Agency (NSA) to generate a digital signature for the authentication of electronic documents.

Verification Process (Operation)

The DSA Algorithm involves 4 operations:-

I) Key Generation

Key Generation has 2 phases. The first phase is choice of algorithm parameter, while second phase computes a single key pair for one user.

Parameter Generation

- Choose an approved cryptographic hash function H with output length |H| bits. In the original DSS, H always has SHA-1 but the stronger SHA-2 algorithm are approved for use in current DSS.

- Choose length L (key length) multiple of 64 between 512 and 1024 inclusive.

- Choose modulus length N such that $N < L$ and $N \leq |H|$

- Choose N-bit prime q

- Choose integer h randomly from $\{2, \ldots p-2\}$

- Compute $g = h^{(p-1)/q} \bmod p$. In the rare case that $g=1$ try again with different h.

Per User key

Given set of parameters, the second phase computes key-pair for single user.

- Choose an integer x randomly from $\{1 \ldots q-1\}$
- Compute $y = g^{x} \bmod p$

x is private key and y is public key.

Key Distribution

The signer should publish the public key y
The signer should keep the private key x secret.

Signing

A message m is signed as follows:-

- Choose integer k randomly from $\{1 \ldots q-1\}$
- Compute $r = (g^{k} \bmod p) \bmod q$ if $r=0$, choose k again

- compute $s = (k^{-1}(H(m) + x(r))) \bmod q$
  If $s=0$ start again with different k.

The signature is (r, s)

The calculation of k and r amount to creating a new per-message key.

Verifying A Signature

One can verify a signature (r,s) is a valid signature for a message m as follows:-

- Verify that $0 < r < q$ and $0 < s < q$
- Compute $w = s^{-1} \bmod q$
- Compute $u_1 = H(m) \cdot w \bmod q$
- Compute $u_2 = r \cdot w \bmod q$
- Compute $v = (g^{u_1} y^{u_2} \bmod p) \bmod q$
- The signature is valid iff $v = r$

Correctness of Algorithm

The signature scheme is correct in the sense that the verifier will always accept genuine signatures. This can be shown as follows:-

Since $g = h^{(p-1)/q} \bmod p$ it follows that $g^q \equiv h^{p-1} \equiv 1 \bmod p$

by Fermatt's little theorem. Since $g > 0$ and q is prime, g must have order q.

The signer computes

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

Thus

$$k \equiv H(m)s^{-1} + xrs^{-1}$$
$$\equiv H(m)w + xrw \pmod q$$

Since g has order $q \bmod p$ we have

$$g^k \equiv g^{H(m)w} g^{xrw}$$
$$\equiv g^{H(m)w} g^{xrw}$$
$$\equiv g^{u_1} y^{u_2} \bmod p$$

Finally, the correctness of DSA follows from

$$r = (g^k \bmod p) \bmod q$$
$$= (g^{u_1} g^{u_2} \bmod p) \bmod q$$
$$= v$$