Public Key Encryption/Authentification

CS6025 Data Encoding

Yizong Cheng

3-10-15

Diffie-Hellman Key Exchange (1976)

- Global parameters: q, a large prime number, and α, a primitive root of q.
- A and B generate random private keys Xa and Xb, and public keys Ya = α^{Xa} mod q and Yb = α^{Xb} mod q, respectively and exchange the public keys over an insecure channel.
- The shared secret is $Ya^{Xb}=Yb^{Xa}$ mod q

Secrecy of the Shared Secret

- Knowing q, α, and Ya=α^{Xa} mod q, it is infeasible to compute Xa, the discrete logarithm base α of Ya mod q.
- Man-in-the-middle attack is possible.

ElGamal Public Key Encryption (1984)

- Given Diffie-Hellman keys, encrypt plaintext $m<q$.
- A chooses random $k<q$ and compute $K=(Yb)^k$, $C_1=\alpha^k$, $C_2 = Km$, all mod q and sends (C_1 , C_2) to B. ($Yb=\alpha^{Xb}$)
  - K is called the one-time key, used to encrypt and decrypt the message as in
  - C2 = Km mod q and m = C2/K mod q
- B computes $K=C_1^{Xb}$ and $m=C_2K^{-1}$, all mod q.
- All we need is the receiver's public key for the sender to do encryption.
  - Only the receiver is able to decrypt using its private key.

ElGamal Digital Signature Scheme (1985)

- Given Diffie-Hellman keys, sign (message digest) $m<q$.
- A chooses random $K < q$ and computes $S1=\alpha^K$.
- A computes $S2 = K^{-1} (m – Xa\ S1) \bmod (q – 1)$.
- The signature is (S1, S2), sent along with m.
- B compute $V1 = \alpha^m \bmod q$ and $V2 = Ya^{S1}\ S1^{S2} \bmod q$.
- The signature is valid if V1 = V2.
- $V2 = \alpha^{XaS1}\alpha^{KS2} \bmod q = V1 = \alpha^m \bmod q$ is the same as
- $\alpha^{m-XaS1} \bmod q = \alpha^{KS2} \bmod q$, or $m – XaS1 \bmod (q-1) = K\ S2 \bmod (q-1)$, a property for α to be a primitive root of q.

Schnorr Digital Signature Scheme (1991)

- Chooses primes p, a 1024-bit number, and q, a 160-bit number, such that q is a factor of p – 1.
- Choose α such that $\alpha^q = 1 \bmod p$.
- A chooses random $0 < s < q$ as the private key and $v = \alpha^{-s} \bmod q$ as the public key.
- A chooses random $0 < r < q$ and computes $x = \alpha^r \bmod q$.
- A has message m and computes using SHA-1 $e = H(m || x)$.
- A computes $y = (r + se) \bmod q$ and the signature is (e, y).
- B computes $x' = \alpha^y v^e \bmod p$ and verifies $e = H(m||x')$.

Digital Signature Algorithm (DSA, 1996)

- Global parameters: primes p and q such that q divides p-1 and $g=h^{(p-1)/q} \bmod p$ for some $h<p-1$.
- private key $x<q$, a random number
- public key $y = g^x \bmod p$
- per-message secret number $k<q$
- (r,s) as signature to message $m<q$.

DSA Signing and Verification

- Signing: $r=(g^k \bmod p) \bmod q$
- $s = [k^{-1}(m+xr)] \bmod q$
- Verifying: $w=s^{-1} \bmod q$
- $u1 = mw \bmod q$
- $u2 = rw \bmod q$
- $v=(g^{u1}y^{u2} \bmod p) \bmod q$
- Test: $v=r$?

Homework 15: due 3-23-15

- Complete H15.java to implement ElGamal and DSA
- Print out hexadecimal values for comparison and verification.
-