

Cryptography and Network Security

Key Management

Xiang-Yang Li

Key Exchange

- ❑ Public key systems are much slower than private key system
 - Public key system is then often for short data
 - Signature, key distribution
- ❑ Key distribution
 - One party chooses the key and transmits it to other user
- ❑ Key agreement
 - Protocol such two parties jointly establish secret key over public communication channel
 - Key is the function of inputs of two users

Possible Attacks

- ❑ Observes all messages over the channel
- ❑ Save messages for reuse later
- ❑ Masquerade various users in the network

Key Predistribution

- ❑ Trusted Authority (TA) generates keys for all pair of users and transmits to them
 - Large overhead (for TA and user)
- ❑ Blom Scheme
 - Keys are chosen from a finite field Z_p
 - P is public prime number
 - TA transmits $k+1$ elements of Z_p to each user over secure channel
 - Secure condition: any set of at most k users (not U, V) can not determine any information about $K_{u,v}$

Blom Scheme

□ Scheme (when $k=1$)

- Each user u has distinct element r_u from Z_p
- TA choose a, b, c and defines
 - $f(x, y) = a + b(x + y) + cxy \pmod p$
- For each u , TA computes
 - $g_u(x) = f(x, r_u) \pmod p$
- TA transmits $g_u(x)$ to user u
- Two users u and v compute the common key
 - $f(r_u, r_v) = a + b(r_u + r_v) + c r_u r_v \pmod p$
 - Here $f(r_u, r_v) = g_v(r_u) = g_u(r_v)$

Security of Blom Scheme

- ❑ Less than k users can not determine keys
- ❑ However, more than k users can compute any keys
 - Solving equations to get a, b, c for $k=1$
- ❑ Generally
 - Function $f(x, y) = a_{i,j} x^i y^j \pmod p$
 - Here $a_{i,j} = a_{j,i}$

Diffie-Hellman Key Predist.

- ❑ Computationally secure
 - if discrete logarithm is intractable
- ❑ Scheme
 - Assume prime number p public and an integer c public
 - Each user u has secret component a_u
 - User u computes $b_u = c^{a_u} \bmod p$
 - TA certifies it by computing
 - $(\text{ID}(u), b_u, \text{sig}_{\text{TA}}(\text{ID}(u), b_u))$
 - The common key of two users u and v is
 - $K = c^{a_u a_v} \bmod p$

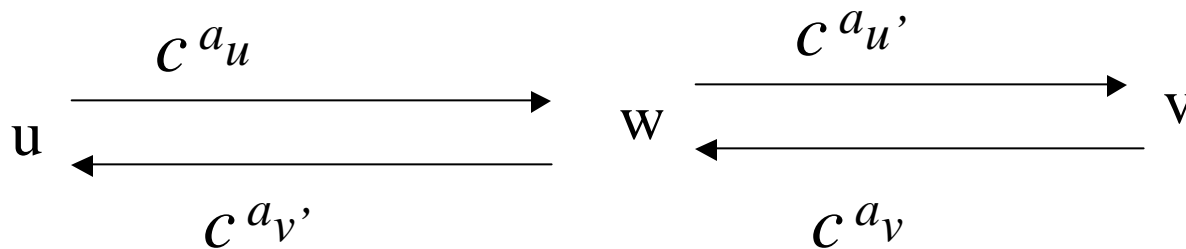
Diffie-Hellman Key Exchange

- ❑ Computationally secure
 - if discrete logarithm is intractable
- ❑ Scheme
 - Assume prime number p public and an integer c public
 - Each user u chooses a secret component a_u (new!)
 - User u computes $b_u = c^{a_u} \bmod p$
 - User v computes $b_v = c^{a_v} \bmod p$
 - The common key of two users u and v is
 - $K = c^{a_u a_v} \bmod p$

Middle Attack

□ Intruder w intercept the communications

- Intruder w communications with u
- Intruder w communications with v



- The key computed by u is
 - $K = c^{a_u a_{v'}} \text{ mod } p$

Authenticated Key Agreement

- ❑ Public-key distribution of secret keys
- ❑ Diffie-Hellman key exchange