Diffie-Hellman Key Exchange Method

Well-Known One-Way Functions

- **Discrete Logarithm**:
  Given p, g, and x, computing y in $y = g^x \pmod{p}$ is EASY
  Given p, g, y, computing x in $y = g^x \pmod{p}$ is HARD
- Factoring:
  Given p and q, computing n in $n = p \cdot q$ is EASY
  Given n, computing p or q in $n = p \cdot q$ is HARD
- Discrete Square Root:
  Given x and y, computing y in $y = x^2 \pmod{n}$ is EASY
  Given y and n, computing x in $y = x^2 \pmod{n}$ is HARD
- Discrete eth Root:
  Given x, n and e, computing y in $y = x^e \pmod{n}$ is EASY
  Given y, n and e, computing x in $y = x^e \pmod{n}$ is HARD

Diffie-Hellman Key Exchange Method

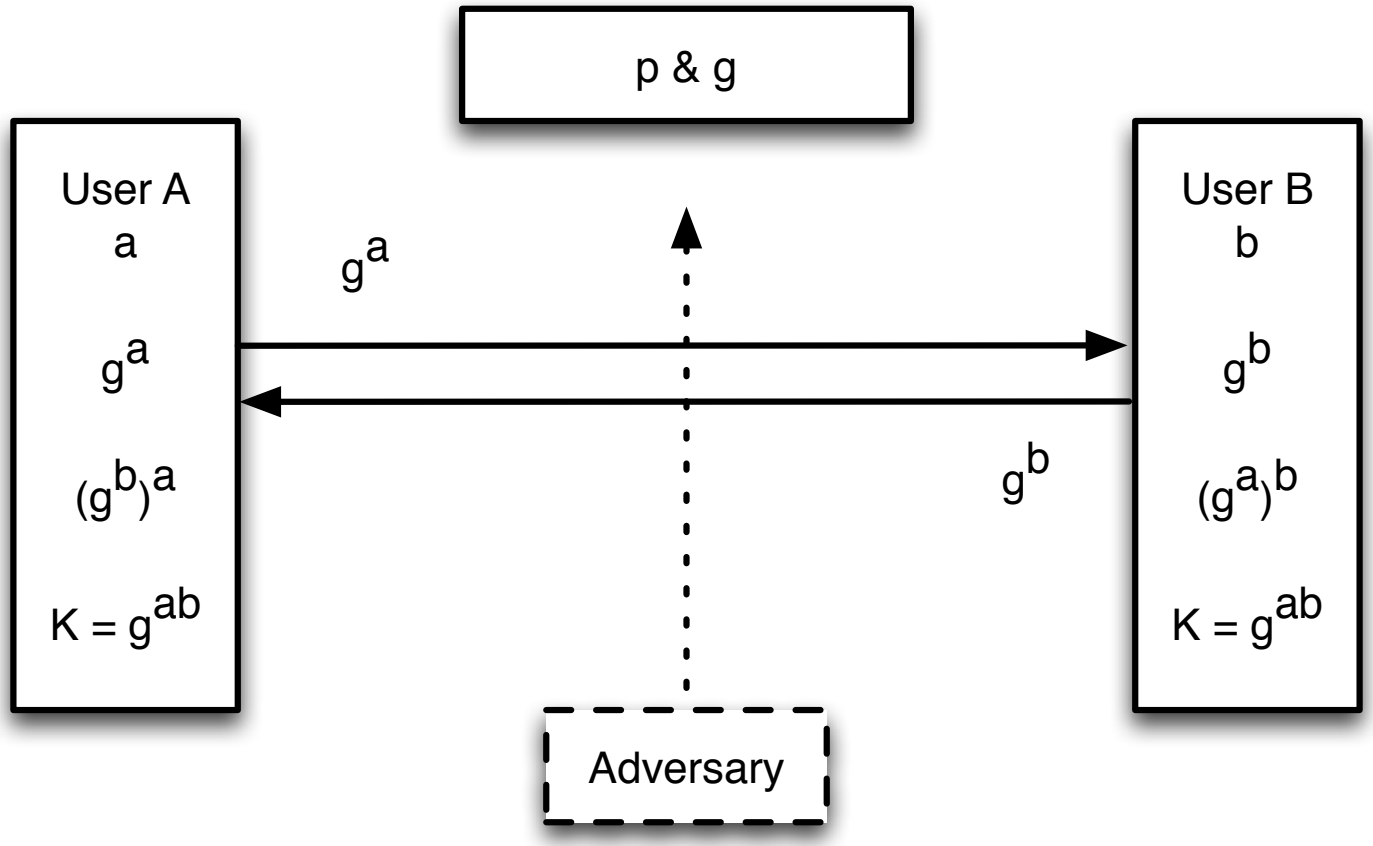
- Martin Hellman (1945): American cryptologist and co-inventor of public key cryptography in cooperation with Whitfield Diffie and Ralph Merkle at Stanford
- Bailey Whitfield Diffie (1944) is an American cryptographer and co-inventor of public key cryptography
- Diffie and Hellman's paper "New Directions in Cryptography" was published *IEEE Tran. Information Theory* in Nov 1976
- It introduced a radically new method of distributing cryptographic keys, that went far toward solving one of the fundamental problems of cryptography, key distribution
- It has become known as Diffie-Hellman key exchange.

Diffie-Hellman Key Exchange Method

- A and B agree on a prime p and a primitive element g of $\mathcal{Z}_p^*$
- This is accomplished in public: p and g are known to the adversary
- A selects $a \in \mathcal{Z}_p^*$, computes $s = g^a \pmod p$, and sends s to B
- B selects $b \in \mathcal{Z}_p^*$, computes $r = g^b \pmod p$, and sends r to A
- A computes $K = r^a \pmod p$
- B computes $K = s^b \pmod p$

$$K = r^a = (g^b)^a = g^{ab} \pmod p$$
$$K = s^b = (g^a)^b = g^{ab} \pmod p$$

Diffie-Hellman Key Exchange Method



Discrete Logarithm Problem

- The adversary knows the group: p and g
- The adversary also sees (obtains copies of) $s = g^a$ and $r = g^b$
- The **discrete logarithm problem** (DLP): the computation of $x \in \mathcal{Z}_p^*$ in

$$y = g^x \pmod{p}$$

given p, g, and y

- Example: Given $p = 23$ and $g = 5$, find x such that

$$10 = 5^x \pmod{23}$$

Answer: $x = 3$

Discrete Logarithm Problem

- Given $p = 158(2^{800} + 25) + 1 =$

  $$1053546280395016975304616582933958731948871814925913489342$$
  $$6087342587178835751858673003862877377055779373829258737624$$
  $$5199045043066135085968269741025626827114728303489756321430$$
  $$0237166369174066615907176472549470083113107138189921280884$$
  $$003892629359$$

  and $g = 17$, find $x \in \mathcal{Z}_p^*$ such that

  $$2 = 17^x \pmod{p}$$

  Answer: ?

- How difficult is it to find x?

Diffie-Hellman Key Exchange Method

- The Diffie-Hellman algorithm allows two parties to agree on a key that is known only to them, except that the adversary can solve the DLP
- Once the secret key (shared key) is established, the parties can use a secret-key cryptographic algorithm to encrypt and decrypt
- However, we still have the problem of establishing $n(n-1)/2$ keys between n parties, and other difficulties of the secret-key cryptography also remain
- But, we no longer need a (secret-key type) secure channel — the Diffie-Hellman algorithm gave us a secure channel, whose security depends on computational difficulty of the DLP
- The Diffie-Hellman algorithm is not a public-key encryption method
- However, there are public-key encryption methods based on the DLP