Diffie-Hellman-Merkle

Ramki Thurimella
Key Exchange Protocol

- Establishing secret keys for N people
  - Requires $N(N-1)/2$ separate keys
  - This is a quadratic function that grows rapidly
  - For e.g., when $N=30$, you need 435 keys

- DH protocol was invented to reduce this complexity
  - Two people communication over an insecure line
  - Can agree on the same key
  - Eavesdropper cannot figure out the key
Groups

- $p$ is a large prime (2000 – 4000 bits long)
- DH protocol uses $\mathbb{Z}_p^*$, multiplicative group mod $p$
- For an element $g$ from the group, let $q$ be the smallest positive integer value such that $g^q = 1 \mod p$
  - $q$ is the order of $g$
- Example: Consider $\mathbb{Z}_7^*$ and let $g$ be 4. Then the powers of 4 are $4^1 \mod 7 = 4$, $4^2 \mod 7 = 2$, $4^3 \mod 7 = 64 \mod 7 = 1$. So, $q = 3$.
- Example: Let $g$ be 3. $3^1 \mod 7 = 3$, $3^2 \mod 7 = 2$, $3^3 \mod 7 = 27 \mod 7 = 6$, $3^4 \mod 7 = 81 \mod 7 = 4$, $3^5 \mod 7 = 243 \mod 7 = 5$, $3^6 \mod 7 = (((3^3 \mod 7) \times (3^3 \mod 7)) \mod 7 = 36 \mod 7 = 1$.
  So, $q = 6$. 
Groups (cont.)

- An element whose order is \( p-1 \) is a \textit{primitive element} of the group, i.e. it generates the whole group.
- In the previous example, \( 3 \) is primitive but not \( 4 \).
- Some mathematical facts
  - For any \( g \), the order of \( g \) is a divisor of \( p-1 \).
  - For any \( a \) of the group, \( a^{p-1} = 1 \).
  - Proof:
    - Let \( g \) be a generator of \( \mathbb{Z}_p^* \).
    - Let \( x \) be such that \( g^x = a \) (\( \therefore g \) is a generator, such an \( x \) must exist).
    - \[ a^{p-1} = g^{x(p-1)} = (g^{p-1})^x = (1)^x = 1 \] \( \Box \)
Fact: \((g^a \mod p)^b \mod p = (g^b \mod p)^a \mod p\)

All computations over a group of integers modulo \(p\) for some large prime \(p\)

Easy to compute powers mod a prime but hard to reverse, for large integers (*discrete log* problem)

- \(p\) a prime > 300 digits, \(a\) and \(b\) > 100 digits, even the best algorithms could not find \(a\) given \(g\), \(p\), and \(g^a \mod p\), even using all of mankind's computing power. \(g = 2\) or 5
Diffie-Hellman (DH) cont.

- Alice and Bob agree on a large prime $p$ and a generator $g$
- Alice picks a random number $a$, $0 < a < p$
- sends $g^a$ to Bob, and keeps $a$ secret
- Bob picks a random number $b$, $0 < b < p$, sends $g^b$ to Alice, and keeps $b$ secret
- Alice computes $(g^b)^a$
- Bob computes $(g^a)^b$
(g^b)^a and (g^a)^b are equal because multiplication in groups is associative.

Only a, b and g^{ab} = g^{ba} \mod p are kept secret.

All the other values—p, g, g^a \mod p, and g^b \mod p—are sent in the clear.
Man-In-The-Middle (MITM)

\[ x \in \mathbb{Z}_p^* \]
\[ g^x \]
\[ v \in \mathbb{Z}_p^* \]
\[ g^v \]
\[ y \in \mathbb{Z}_p^* \]
\[ g^v \]
\[ w \in \mathbb{Z}_p^* \]
\[ g^w \]
\[ k = (g^w)^x \]
\[ k = (g^x)^w \]
\[ k = (g^y)^v \]

Random member \( \in \mathcal{R} \)
MITM defense for a special case

- If the key \( k \) is being used to encrypt voice or video link
- Have Bob read the first few bits of \( h(k) \)
- Have Alice read the next few bits of \( h(k) \)
- Assume Alice and Bob can recognize each other, they can verify that they have the same key
- Eve cannot compute the preimage of \( h(k) \)
Pitfalls

- What if Eve replaces $g^x$ and $g^y$ with $1$ while they are in transit?
  - The key would be $1$!
  - Check that these values are not $1$

- What if order $q$ of $g$ is much smaller than $p-1$?
  - The key $k$ would come from a small set
    $\{1, g^1, \ldots, g^q\}$
  - Check that $p$ is prime and that order of $g$ is $p-1$
Safe Primes

- To avoid problems with subgroups, pick a *safe prime*
- A *safe prime* is a large prime $p$ of the form $2q+1$ where $q$ is also prime
- Such $\mathbb{Z}_p^*$ has 4 subgroups, one corresponding to each of the divisors of $p-1$ or $2q$
  - $\{1\}$
  - $\{1,p-1\}$
  - $\{1,2,...,q\}$
  - $\{1,2,...,2q\}$
Safe Primes Example

- Let $p = 23$, then $q = 11$
- Such $\mathbb{Z}_{23}^*$ has 4 subgroups, one corresponding to each of the divisors of $p-1$ or 22
  - $\{1\}$
  - $\{1,22\}$ note: $222 \% 23 = 1$
  - $\{1,2,3,4,6,8,9,12,13,16,18\}$
    - Order of this subgroup is 11
    - Verify that this subgroup is closed under $*$ (i.e. for any $x,y$ from this subgroup $(x*y)\%23$ should also be in the subgroup)
  - $\{1,2,\ldots,22\}$