Public Key Cryptosystems - Diffie Hellman
Public Key Cryptosystems - Diffie Hellman

Get two parties to share a secret number that no one else knows
Public Key Cryptosystems - Diffie Hellman

Get two parties to share a secret number that no one else knows
Public Key Cryptosystems - Diffie Hellman

Get two parties to share a secret number that no one else knows.
Can only use an insecure communications channel for exchange.
Public Key Cryptosystems - Diffie Hellman

Get two parties to share a secret number that no one else knows.
Can only use an insecure communications channel for exchange.

\[ p, g \]

- \( p \): prime & \((p-1)/2\) prime
- \( g \): less than \( p \)
  \[ n = g^k \mod p \]
  for all \( 0 < n < p \)
  and some \( k \)

(see http://gauss.ececs.uc.edu/Courses/c472/java/Generator/zstarn.html)
A strong prime \( p \):

- \( p \) is large
- \( p-1 \) has large prime factors (\( p = aq+1 \) for integer \( a \) and prime \( q \))
- \( q-1 \) has large prime factors (\( q = br+1 \) for integer \( b \), prime \( r \))
- \( p+1 \) has large prime factors.

A “large” safe prime is likely to be a strong prime.

It is shown by Stephen Pohlig and Martin Hellman in 1978 that if all the factors of \( p-1 \) are less than \( \log^c p \), then the problem of solving discrete logarithm modulo \( p \) is in P. Therefore, for cryptosystems based on discrete logarithm it is required that \( p-1 \) has at least one large prime factor.
Public Key Cryptosystems - Diffie Hellman

Important property:

\[(g^a \mod p)^b \mod p = (g^b \mod p)^a \mod p\]

\[p: \text{prime } \& \ (p-1)/2 \text{ prime}\]
\[g: \text{less than } p\]
\[n = g^k \mod p\]
\[\text{for all } 0 < n < p\]
\[\text{and some } k\]

(see http://gauss.ececs.uc.edu/Courses/c472/java/Generator/zstarn.html)
Public Key Cryptosystems - Diffie Hellman

Important property:

\[(g^a \mod p)^b \mod p = (g^b \mod p)^a \mod p\]

Example:

\[p = 563, \ g = 5, \ a = 9, \ b = 14\]

\[5^9 \mod 563 = 1953125 \mod 563 = 78\]

\[78^{14} = 308549209196654470906527744 \mod 563 = 117\]
Public Key Cryptosystems - Diffie Hellman

Important property:

\[(g^a \mod p)^b \mod p = (g^b \mod p)^a \mod p\]

Example:

\[p = 563, \ g = 5, \ a = 9, \ b = 14\]

\[5^9 \mod 563 = 1953125 \mod 563 = 78\]

\[78^{14} = 308549209196654470906527744 \mod 563 = 117\]

\[5^{14} \mod 563 = 6103515625 \mod 563 = 534\]

\[534^9 = 153312511596308814665178256828300148736 \mod 563 = 117\]
Public Key Cryptosystems - Diffie Hellman

Get two parties to share a secret number that no one else knows
Can only use an insecure communications channel for exchange
Public Key Cryptosystems - Diffie Hellman

Get two parties to share a secret number that no one else knows
Can only use an insecure communications channel for exchange
Public Key Cryptosystems - Diffie Hellman

Get two parties to share a secret number that no one else knows.
Can only use an insecure communications channel for exchange.

Receiver – 563, 5 – Sender

14 – 563, 5  – 9

Attacker
Public Key Cryptosystems - Diffie Hellman

Get two parties to share a secret number that no one else knows
Can only use an insecure communications channel for exchange

\[ 5^9 \mod 563 = 78 \]
Public Key Cryptosystems - Diffie Hellman

Get two parties to share a secret number that no one else knows.
Can only use an insecure communications channel for exchange.

\[ 78^{14} \mod 563 = 117 \]
Public Key Cryptosystems - Diffie Hellman

Get two parties to share a secret number that no one else knows
Can only use an insecure communications channel for exchange
Public Key Cryptosystems - Diffie Hellman

Get two parties to share a secret number that no one else knows
Can only use an insecure communications channel for exchange

$$5^{14} \mod 563 = 534$$

$$534^9 \mod 563 = 117$$
Public Key Cryptosystems - Diffie Hellman

Get two parties to share a secret number that no one else knows
Can only use an insecure communications channel for exchange
Public Key Cryptosystems - Diffie Hellman

Vulnerability to the "Man-in-the-middle" attack

Sender

Receiver

Attacker

563, 5

14

9

34
Public Key Cryptosystems - Diffie Hellman

Vulnerability to the "Man-in-the-middle" attack
Public Key Cryptosystems - Diffie Hellman

Vulnerability to the "Man-in-the-middle" attack

14 → Receiver → 563, 5 → Sender → 9

34 → Attacker → 250
Public Key Cryptosystems - Diffie Hellman

Vulnerability to the "Man-in-the-middle" attack

Diagram:
- Receiver
- Sender
- Attacker
- Numbers 14, 563, 5, 205, 34, 250
Public Key Cryptosystems - Diffie Hellman

Vulnerability to the "Man-in-the-middle" attack

14 -> Receiver -> Sender

563, 5

459

34 -> Attacker

250
Public Key Cryptosystems - Diffie Hellman

Vulnerability to the "Man-in-the-middle" attack

14  →  Receiver  ←  563, 5  →  Sender  →  9

459  ↓  34  ↓  250

534  ↓  563, 5  ↓  250

459  ↓  34  ↓  250
Public Key Cryptosystems - Diffie Hellman

Vulnerability to the "Man-in-the-middle" attack
Public Key Cryptosystems - Diffie Hellman

Vulnerability to the "Man-in-the-middle" attack

14
Receiver

563, 5

205
Sender

34
Attacker

459

9

459

250

459
Public Key Cryptosystems - Diffie Hellman

Vulnerability to the "Man-in-the-middle" attack
Public Key Cryptosystems - Diffie Hellman

Fixing the vulnerability to the "Man-in-the-middle" attack
Public Key Cryptosystems - Diffie Hellman

Where is the security?

Attacker sees $A=g^a \mod p$, $B=g^b \mod p$ but does not know $a,b$
Public Key Cryptosystems - Diffie Hellman

Where is the security?

Attacker sees $A = g^a \mod p$, $B = g^b \mod p$ but does not know $a, b$

Attacker needs to compute $K = g^{ab} \mod p$ from the above.

Can be done if it is feasible to take the $\log_p A$ and $\log_p B$

This is called the discrete logarithm problem.

Computing the discrete logarithm of a number modulo $p$ takes roughly the same amount of time as factoring the product of two primes the same size as $p$, which is what the security of the RSA cryptosystem relies on. Thus, the Diffie-Hellman protocol is roughly as secure as RSA.
Public Key Cryptosystems - Diffie Hellman

Signing a message:

Let $p$, $q$, $r$ be primes such that
\[ p = 2q + 1, \text{ and } q = 2r + 1 \]

Let $m$ be the message to be signed.

Let $x$ be a permanent secret key owned by the signer.

Let $g^x \mod q$ be the public key associated with $x$. 
Public Key Cryptosystems - Diffie Hellman

**Signing a message:**

Let \( p, q, r \) be primes such that
\[
p = 2q+1, \text{ and } q = 2r+1
\]
Let \( m \) be the message to be signed.
Let \( x \) be a permanent secret key owned by the signer
Let \( g^x \mod q \) be the public key associated with \( x \)

Generate a random secret \( y \) with public key \( g^y \mod p \)
Let \( Y = (g^y \mod p) \mod q; \) \( s \) be the signature
Find \( a, b, c \) s.t. \( ax + by = c \) with the following possibilities
\[
\begin{align*}
a &= m, \quad b = Y, \quad c = s; \\
a &= 1, \quad b = Ym, \quad c = s; \\
a &= 1, \quad b = Ym, \quad c = ms; \\
a &= 1, \quad b = Ym, \quad c = Ys; \\
a &= 1, \quad b = ms, \quad c = Ys
\end{align*}
\]
Public Key Cryptosystems - Diffie Hellman

Signing a message:

Let $p$, $q$, $r$ be primes such that

\[ p = 2q + 1, \text{ and } q = 2r + 1 \]

Let $m$ be the message to be signed.

Let $x$ be a permanent secret key owned by the signer.

Let $g^x \mod q$ be the public key associated with $x$.

Generate a random secret $y$ with public key $g^y \mod p$.

Let $Y = (g^y \mod p) \mod q$; $s$ be the signature.

Find $a$, $b$, $c$ s.t. $ax + by = c$ with the following possibilities:

\[ a=m, \quad b=Y, \quad c=s \]
\[ a=1, \quad b=YM, \quad c=s \]
\[ a=1, \quad b=YM, \quad c=ms \]
\[ a=1, \quad b=YM, \quad c=Ys \]
\[ a=1, \quad b=ms, \quad c=Ys \]

**Verify:**

\[ (g^x \mod q)^a \times (g^y \mod p)^b = g^c \mod p \]
Public Key Cryptosystems - Diffie Hellman

Signing a message:

Can't do this: $s = xm \mod q$ – to check the signature do this: $g^s \mod p = (g^x \mod p)^m \mod p$

But then $x = s/m \mod q$ revealing the secret $x$
Public Key Cryptosystems - Diffie Hellman

Signing a message:

Can't do this: \( s = xm \mod q \) – to check the signature do this: \( g^s \mod p = (g^x \mod p)^m \mod p \)

But then \( x = s/m \mod q \) revealing the secret \( x \)

A different \( y \) must be chosen for each signature -
If you have two sets of \( a, b, c \) for the same \( x, y \),
You can solve for the secrets \( x \) and \( y \).
Public Key Cryptosystems - Diffie Hellman

Signing a message:

Can't do this: $s = xm \mod q$ – to check the signature do this: $g^s \mod p = (g^x \mod p)^m \mod p$

But then $x = s/m \mod q$ revealing the secret $x$

A different $y$ must be chosen for each signature -

If you have two sets of $a, b, c$ for the same $x, y$,

You can solve for the secrets $x$ and $y$.

El Gamal and DSA have $a = 1, b = Ym, c = Ys$