Attacks on Diffie-Hellman Protocol

Network Security - IT653

Deepti Agrawal
KReSIT, IIT Bombay
Diffie-Hellman Protocol

Alice

Choose $a$

$A = g^a \mod P$

Send

Bob

Choose $b$

$B = g^b \mod P$

Send

Compute

$K_{ab} = B^a \mod P$

$K_{ba} = A^b \mod P$

$3^5 \mod 13 = 9 = 10^8 \mod 13$
Diffie-Hellman Conjecture

- Discrete Logarithm Problem (DLP)
  - To find $z$ given $g^z$

- DH problem (DHP)
  - Problem of solving the shared key

- DH conjecture (DHC)
  - Solving DLP amounts to solving DHP
Basics

- **Group**
  
  (G, +) satisfying the properties of closure, associativity, identity and inverse.

- **Cyclic Group**
  
  A group that can be generated by a single element g (the group generator).

- **Subgroup**
  
  Subset H of group elements of a group G that satisfies the four group requirements.
Trivial attacks on Diffie-Hellman Protocol

- **Simple Exponent**
  1. \( a = 1 \) or \( b = 1 \)
  2. \( a = p-1 \) or \( b = p-1 \)

- **Simple Substitution Attacks**
  \( g^a = 1 \) or \( g^b = 1 \)
Mathematical attacks on Diffie-Hellman Protocol

- **Subgroup Confinement Attack**

  Example: \( p = 19, \ g = 2 \)

  Generated group
  \[
  \{2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10, 1\}
  \]

  \( a = 2, \ A = 2^2 = 4 \)

  Subgroup generated by \( A = S_A = \{4, 16, 7, 9, 17, 11, 6, 5, 1\} \)

  \( b = 3, \ B = 2^3 = 8 \)

  Sub-group generated by \( B = S_B = \{8, 7, 18, 11, 12, 1\} \)

  \( K_{ab} = 2^6 = 7 \)

  **Note**: \( K_{ab} \) belongs to \( S_A \) intersection \( S_B \)

  **Solution**: Use Safe primes (\( p = 2q + 1 \))
Mathematical attacks on Diffie-Hellman Protocol (Cont..)

- Attacks based on composite order subgroup

The shared secret key $g^{(abq)} = (g^{(ab)})^{((p-1)/2)}$ can take only one of 2 possible values:
- $g^{((p-1)/2)}$ or 1
  according as whether $(g^{(ab)})$ is odd or even!

Think : How is this different from the conventional man in the middle attack?)
Conclusion

- Diffie-Hellman Conjecture does not hold for some keys in DHP.