Diffie-Hellman Key Exchange Algorithm

The **Diffie-Hellman key exchange** is a cryptographic protocol that allows two parties, traditionally referred to as Alice and Bob, to securely exchange a shared secret key over a public communication channel. This key can then be used to encrypt further communications between them. The security of this method is based on the difficulty of solving discrete logarithms in modular arithmetic.

Here's a step-by-step explanation of the process:

1. **Private Numbers**:

- Alice and Bob, each generate a **random number** (let's call them **a** and **b**, respectively) using a random number generator. These numbers are kept secret and not shared with anyone.

2. **Public Parameters**:

- Alice and Bob agree on two public integers, **N** and **g**, where **N** is a large prime number, and **g** is a primitive root modulo **N**. Both of these values are public and can be known to everyone, even potential attackers.

3. **Exchange of Values**:

- Alice computes $A = g^a \mod N$ and Bob computes $B = g^b \mod N$ using their private random numbers.
- They exchange their computed values A and B over the public communication channel.

4. **Shared Key Computation**:

- After receiving each other's value, Alice computes the **shared secret key** as:

$$ M = B^a \mod N = (g^b)^a \mod N = g^{ab} \mod N $$

- Bob computes the same shared secret key using Alice's value:

$$ M = A^b \mod N = (g^a)^b \mod N = g^{ab} \mod N $$

- Both end up with the **same value** for M, which becomes the **master key** that they use for their future encrypted communication.

Example: Diffie-Hellman in practice

Let's go through an example:

- Suppose Alice and Bob agree on the public parameters $N = 997$ and $g = 3$.
- Alice chooses her secret random number $a = 8$, and Bob chooses $b = 12$.
- Now, they proceed with the following steps:

1. **Alice calculates her value** A: $$ A = g^a \mod N = 3^8 \mod 997 = 6561 \mod 997 = 579 $$ So, Alice sends $A = 579$ to Bob.

2. **Bob calculates his value** B: $$ B = g^b \mod N = 3^{12} \mod 997 = 531441 \mod 997 = 40 $$ Bob sends $B = 40$ to Alice.

3. **Alice computes the shared key** M: $$M = B^a \mod N = 40^8 \mod 997 = 167772160000 \mod 997 = 887$$

4. **Bob computes the same shared key** M: $$M = A^b \mod N = 579^{12} \mod 997 = 887$$

Thus, both Alice and Bob have arrived at the same **shared master key**: **887**.

Why is the Diffie-Hellman Algorithm Secure?

The Diffie-Hellman key exchange is secure because, while **A** and **B** are exchanged openly, an attacker must solve the **discrete logarithm problem** to retrieve the original secret numbers **a** and **b**. The discrete logarithm problem is computationally infeasible to solve efficiently for large numbers, which is why the security of this method holds.

Usage in Real-World Applications

The Diffie-Hellman algorithm is foundational in various security protocols, such as TLS (used for secure communication on the Internet) and VPNs (Virtual Private Networks). It ensures that only two parties can generate a shared key that they can compute, even if an attacker monitors the communication channel.

From:
https://edu.iit.uni-miskolc.hu/ - **Institute of Information Science - University of Miskolc**

Permanent link:
https://edu.iit.uni-miskolc.hu/tanszek:oktatas:techcomm:diffie-hellman_key_exchange?rev=1728306392

Last update: **2024/10/07 13:06**