Author: Davor Ljubenkov, Aalborg University
Supervisor: Sokol Kosta, Aalborg University

Diffie-Hellman key exchange

Diffie-Hellman algorithm is used to establish a shared secret between two parties which can be used for secret communication for exchanging data over a public network.

The algorithm in itself is very simple. Let's assume that Alice wants to establish a shared secret with Bob. Here is an example of the protocol with secret values (6 and 15).

1) Alice and Bob agree to use a prime number p = 23 and base g = 5. (These two values are chosen in this way to ensure that the resulting shared secret can take on any value from 1 to p–1).

2) Alice chooses a secret integer a = 6, then sends Bob A = g^a mod p (A = 5^6 mod 23 = 8)

3) Bob chooses a secret integer b = 15, then sends Alice B = g^b mod p (B = 5^{15} mod 23 = 19)

4) Alice computes s = B^a mod p (s = 19^6 mod 23 = 2)

5) Bob computes s = A^b mod p (s = 8^{15} mod 23 = 2)

6) Alice and Bob now share a secret (the number 2).

The number Alice get at step 4 is same as Bob got at step 5.

Bob computes:
A^b mod p = $(g^a$ mod $p)^b$ mod p = g^{ab} mod p

Alice computes:
B^a mod p = $(g^b$ mod $p)^a$ mod p = g^{ba} mod p

Diffie-Hellman algorithm is primarily used as a method of exchanging cryptography keys for use in symmetric encryption algorithms like AES. Please note that information is not shared during the key exchange. Here the two parties are creating a key together.

Fill in the missing gaps in order for this algorithm to work!

Sample output

```
Alice's Secret Key is 2
Bob's Secret Key is 2
```