Diffie–Hellman Key Exchange

Paolo Bettelini

Contents

1 Diffie Hellman

Diffie–Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel.

Scenario: a *client* and a *server* want to establish a shared secret.

- The *client* generates a random private key k_c
- The *server* generates a random private key k_s
- The two parts publicly establish a common G (generator)

We define a function

$$y = f(G, k)$$

such that given y and G it is very hard to get k.
The function must also satisfy the following identity

$$f(f(G, k_1), k_2) = f(f(G, k_2), k_1)$$

For instance the function G^k would satisfy this identity since $\left(G^{k_1}\right)^{k_2} = \left(G^{k_2}\right)^{k_1}$, but not the first property.

Given the function $f(G, k)$

- The *client* computes $y_c = f(G, k_c)$
- The *server* computes $y_s = f(G, k_s)$
- The two parts publicly exchange y_c and y_s
- The *client* computes $y = f(y_s, k_c)$
- The *server* computes $y = f(y_c, k_s)$

Now the *client* and *server* share the same value of y since $f(y_s, k_c) = f(y_c, k_s)$.
The value of y is unknown to anyone who has traced the communication between the *client* and the server.