Diffie Hellman Example

COMP830

Diffie Hellman is a Key exchange protocol designed to allow the sharing of a calculated symmetric key.

There are 2 people who do not know each other who wish to calculate the same secret (shared / symmetric) key. They must do this publicly where anyone listening can hear what they are communicating.

Alice tells Bob publicly her chosen prime number (q=7). (public)

Bob Tells Alice publicly his chosen prime number (a=5). (public)

They then choose secret keys that only they will know. They do not tell each other what this key is.

Alice selects: xa = 13 (private)

Bob selects: xb = 17 (private)

$Y_A = a^{xa} \bmod q \Rightarrow Y_A = 5^{13} \bmod 7$

$\Rightarrow Y_A = 5^{13} (1220703125) \bmod 7 \Rightarrow Y_A = 5$ (public)

$Y_B = a^{xb} \bmod q \Rightarrow Y_B = 5^{17} \bmod 7$

$\Rightarrow Y_B = 5^{17} (762939453125) \bmod 7 \Rightarrow Y_B = 3$ (public)

Y_A is Alices's public key which she sends to Bob

Y_B is Bob's public key which he sends to Alice.

They now calculate the shared symmetric key.

$K_{AB} = Y_B{}^{xa} \bmod q \Rightarrow Y_B{}^{13} \bmod 7 \Rightarrow 3^{13} \bmod 7 \Rightarrow 1594323 \bmod 7 = 3$

$K_{AB} = Y_A{}^{xb} \bmod q \Rightarrow Y_A{}^{17} \bmod 7 \Rightarrow 5^{17} \bmod 7 \Rightarrow 762939453125 \bmod 7 = 3$

Their Shared Secret Key is 3.