**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)

YA = axa mod q => YA = 513 mod 7

=> YA = 513 (1220703125) mod 7 => YA = 5(public)

YB = axb mod q => YB = 517 mod 7

=> YB = 517 (762939453125) mod 7 => YB = 3 (public)

YA is Alices’s public key which she sends to Bob

YB is Bob’s public key which he sends to Alice.

They now calculate the shared symmetric key.

KAB=YB xa mod q => YB13 mod 7 => 313 mod 7 => 1594323 mod 7 = 3

KAB=YA xb mod q => YA17 mod 7 => 517 mod 7 => 762939453125 mod 7 = 3

Their Shared Secret Key is 3.