# Diffie-Hellman Key Exchange

Common Prime q
Primitive root $\alpha$

| Sender - A | Receiver - B |
| --- | --- |
| Public key - $Y_A$<br>Private key - $X_A$ | Public key - $Y_B$<br>Private key - $X_B$ |

$Y_A = \alpha^{XA} \bmod q$

$Y_B = \alpha^{XB} \bmod q$

$K_A = Y_B^{XA} \bmod q$

$K_B = Y_A^{XB} \bmod q$

q=71, $\alpha = 7$

| Sender - A | Receiver - B |
|---|---|
| Public key - $Y_A$<br>Private key - 5 | Public key - $Y_B$<br>Private key - 12 |

1) A's Public key?

$Y_A = \alpha^{XA} \bmod q$

$Y_A = 7^5 \bmod 71$

$= 51$

5 => 101

$7 \bmod 71 = 7$

$7^2 \bmod 71 = 49$

$49^2 \bmod 71 = 58$

$58 \times 7 \bmod 71 = 51$

$Y_B = 7^{12} \bmod 71$

$= 4$

12 => 1100

0: $7 \bmod 71 = 7$

0: $7^2 \bmod 71 = 49$

1: $49^2 \bmod 71 = 58$

1: $58^2 \bmod 71 = 27$

$27 \times 58 \bmod 71 = 4$

$K_A = Y_B^{XA} \bmod q$

$K_A = 4^5 \bmod 71$

$= 30$

$K_B = 51^{12} \bmod 71$

$= 30$

$K_A = K_B$

Sample mod

$42^{5} \bmod 1073$

5 => 101

1: 42 mod 1073= 42

0: $42^2$ mod 1073= 691

1: $691^2$ mod 1073= 1069

1069 x 42 mod 1073= 905

$691^2 = 477481$

477481 / 1073 =444.9

444 x 1073 = 476412

477481-476412 = 1069

$13^6 \bmod 17$

6 => 110

13 mod 17 => 13

$13^2 \bmod 17$ => 16

$16^2 \bmod 17$ => 1

1x16 mod 17 => 16