

Diffie Hellman:

$q$  is large prime.

$a$  is primitive root of  $q$

( $a$  is alpha)

$q=103$  (is modulus)

$a=5$

Private Key of A: (randomly chosen)

$X_A=19$

Public Key of A:

$Y_A=a^{X_A} \% q$

$Y_A=5^{19} \% 103$

$Y_A=86$

Private Key of B: (randomly chosen)

$X_B=21$

Public Key of B:

$Y_B=a^{X_B} \% q$

$Y_B=5^{21} \% 103$

$Y_B=90$

Public Key exchange

$Y_B$

$Key_A=Y_B^{X_A} \% q$

$Key_A=90^{19} \% 103$

$Key_A=37$

$Y_A$

$Key_B=Y_A^{X_B} \% q$

$Key_B=86^{21} \% 103$

$Key_B=37$