- DIFFIE-HELLMAN

1) Alice e Bob si accordano per usare un numero primo $q = 23$ e la base $\alpha = 5$.

→ Primitive root

2) Alice sceglie un numero segreto $X_A = 6$ e manda a Bob $Y_A = \alpha^{X_A} \bmod q$

- $Y_A = 5^6 \bmod 23 = 8$

3) Bob sceglie l'intero segreto $X_B = 15$ e manda ad Alice $Y_B = \alpha^{X_B} \bmod q$

- $Y_B = 5^{15} \bmod 23 = 19$

4) Alice calcola $K_A = (\alpha^{X_B} \bmod q)^{X_A}$ od $q = Y_B^{X_A} \bmod q$

- $K_A = 19^6 \bmod 23 = 2$

5) Bob calcola $K_B = (\alpha^{X_A} \bmod q)^{X_B} \bmod q = Y_A^{X_B} \bmod q$

- $K_B = 8^{15} \bmod 23 = 2$