# Diffie-Hellman Key Exchange -

www.ruxandraolimid.weebly.com/pagesonsecurity

## DLP

- $\mathcal{A}$ is given: (G,q,g,A) with *G* cyclic group of order *q, g* generator and $A = g^a$ , $a \leftarrow^R Z_q$
- $\mathcal{A}$ returns: a’ in $Z_q$

The experiment outputs:

1 if $A = g^{a'}$ , 0 otherwise

$\forall\mathcal{A}$ PPT, ∃ $\varepsilon(n)$ negligible such that:

$\Pr[DLP_{\mathcal{A}}(n)=1] \le \varepsilon(n)$

## CDH

- $\mathcal{A}$ is given: (G,q,g,A,B) with *G* cyclic group of order *q, g* generator, $A = g^a, B = g^b$ , $a,b \leftarrow^R Z_q$
- $\mathcal{A}$ returns: K in $Z_q$

The experiment outputs:

1 if $K = g^{ab}$ , 0 otherwise

$\forall\mathcal{A}$ PPT, ∃ $\varepsilon(n)$ negligible such that:

$\Pr[CDH_{\mathcal{A}}(n)=1] \le \varepsilon(n)$

## DDH

$\forall\mathcal{A}$ PPT, ∃ $\varepsilon(n)$ negligible such that:

$\Pr[\mathcal{A}(G,q,g,g^a,g^b,g^c)=1]$ -

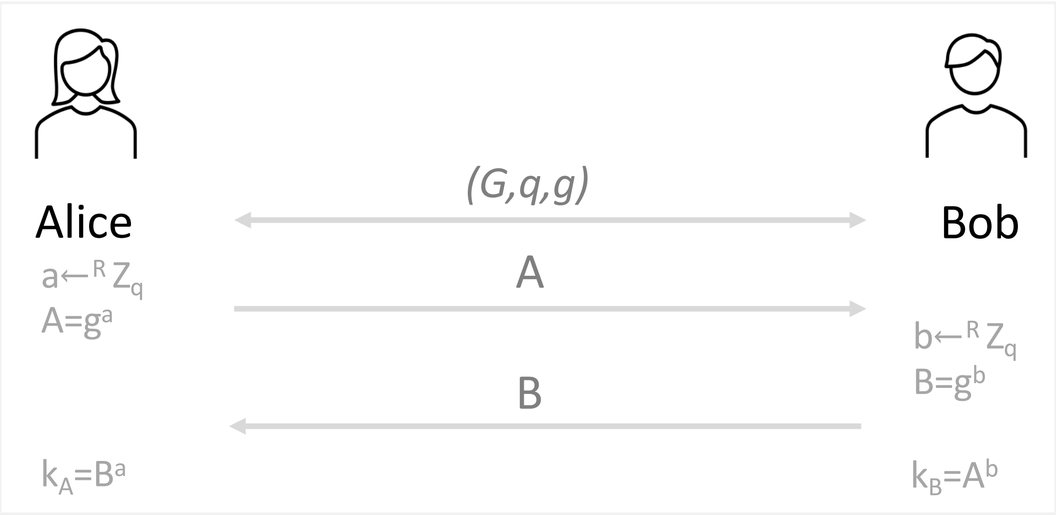
$\Pr[\mathcal{A}(G,q,g,g^a,g^{b,}g^{ab})=1] \le \varepsilon(n)$

for $a,b,c \leftarrow^R Z_q$

Stronger security

DLP: Discrete Logarithm Problem
DDH: Decisional Diffie-Hellman Problem
CDH: Computational Diffie-Hellman Problem

## Diffie-Hellman Key Exchange



Alice

$a \leftarrow^R Z_q$
$A=g^a$

(G,q,g)

A

B

Bob

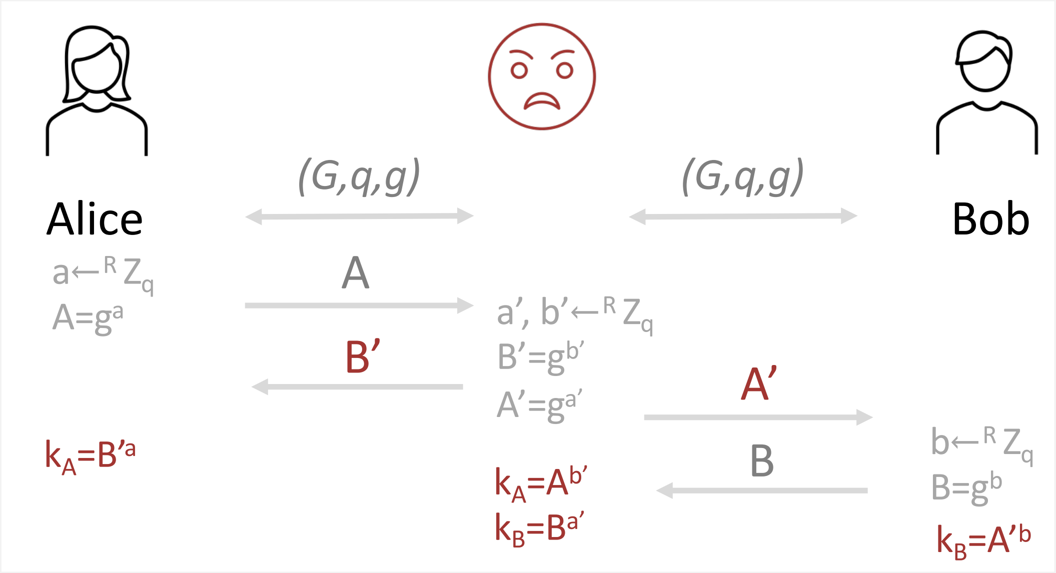
$b \leftarrow^R Z_q$
$B=g^b$

$k_A=B^a$

$k_B=A^b$

*Attacks:* no authentication of parties, Man-in-the-Middle

## Man-in-the-Middle



Alice

$a \leftarrow^R Z_q$
$A=g^a$

(G,q,g)

A

B’

$k_A=B'^a$

$a', b' \leftarrow^R Z_q$
$B'=g^{b'}$
$A'=g^{a'}$

$k_A=A^{b'}$
$k_B=B^{a'}$

(G,q,g)

A’

B

Bob

$b \leftarrow^R Z_q$
$B=g^b$
$k_B=A'^b$

Pages on SecuRity
by Ruxandra F. Olimid