Algoritmo di Diffie-Hellman - 1

Nel 1976 due giovani ricercatori statunitensi, **Whitfield Diffie** e **Monte Hellman**, idearono un sistema per cui due individui scambiavano messaggi cifrati, senza per questo dover scambiare alcuna chiave.

Il protocollo **Diffie-Hellman** consente a due entità di **generare separatamente** una **chiave simmetrica comune** utilizzando un canale di comunicazione insicuro (**pubblico**) a partire da un valore di un **pre-master condiviso**.

Algoritmo di Diffie-Hellman - 2

Siano Alice e Bob i due interlocutori, entrambi a conoscenza di una **pre-master**che **consiste** in **due numeri**:

- una **base g** (**gruppo generatore**).
- un **numero primo p** utilizzato per il calcolo dei **moduli**.

Alice **genera** un **numero casuale a** che mantiene **segreto** ed esegue il calcolo $A = g^a \bmod p$ inviando in chiaro il valore di **A** a Bob.

Bob **genera** un **numero casuale b** che mantiene **segreto** ed esegue il calcolo $B = g^b \bmod p$ inviando in chiaro il valore di **B** a Alice.

Alice utilizza il numero ricevuto **B** per calcolare $K = B^a \bmod p$

Bob utilizza il numero ricevuto **A** per calcolare $K = A^b \bmod p$

I **due risultati coincidono** e rappresentano la **chiave simmetrica** che Alice e Bob utilizzeranno per comunicare.

Algoritmo di Diffie-Hellman - 3

Alice calcola:

$K = B^a \bmod p = (g^b \bmod p)^a \bmod p = (g^b)^a \bmod p = g^{ba} \bmod p$

Bob calcola:

$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = (g^a)^b \bmod p = g^{ab} \bmod p$

Alice e Bob trovano lo stesso risultato perché

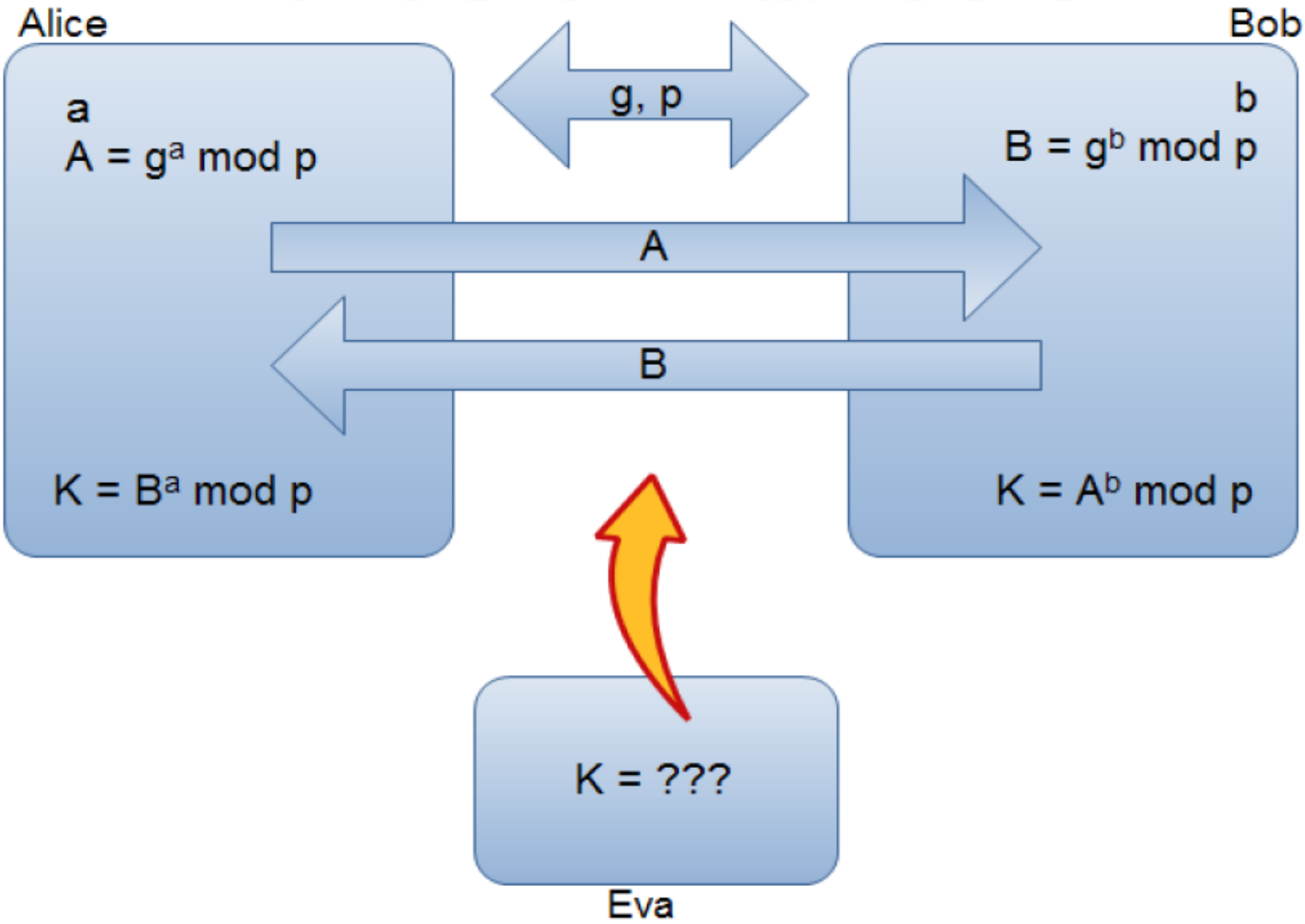
g^{ab} e g^{ba} sono uguali!

Si noti come solo a, b e $g^{ab} = g^{ba}$ sono segreti.

Tutti gli altri numeri sono mandati in chiaro, ossia pubblici.

Una volta che Alice e Bob calcolano la chiave segreta, essa può esser usata come chiave di cifratura simmetrica, conosciuta solo a loro, per mandare messaggi cifrati (3DES, IDEA, AES) tramite il canale di comunicazione in chiaro.

Algoritmo di Diffie-Hellman - 4



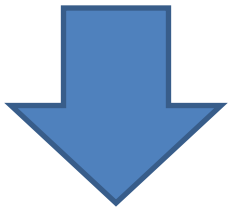
Algoritmo di Diffie-Hellman - 5

Alice e Bob hanno condiviso un **pre-master segreto** (il numero **K**) **senza comunicarlo esplicitamente**!

L'attaccante Eva può osservare **A**, **B**, **g**, **p** ma questa informazione non è sufficiente per ricavare **K**!

K è calcolabile solo conoscendo **a** o **b**, che tuttavia sono **segreti** e non vengono **mai trasmessi**.

Ricavare **a** da **A** (invertendo $A = g^a \bmod p$) o analogamente **b** da **B** (invertendo $B = g^b \bmod p$) significa risolvere un **logaritmo discreto**



computazionalmente difficile!

Per valori di **g** di oltre 300 cifre e di **a** di oltre 100, la soluzione e, quindi, il riconoscimento della chiave, risulta difficilissima.

Algoritmo di Diffie-Hellman - 6

• Molte funzioni normalmente invertibili, diventano **non invertibili** nella versione **modulare**.

• **Esempio**: il logaritmo

$$a^b = c$$

Trovare **b** dati **a** e **c** *è* computazionalmente semplice (**logaritmo**: $b = \log_a(c)$ "*logaritmo di **c** in base **a***" che è l'inverso dell'esponenziale, della potenza).

$$a^b \bmod m = c$$

Trovare **b** dati **a**, **c** ed **m** *è* computazionalmente molto difficile! (**logaritmo discreto** di un numero **c** in base **a** che è l'inverso della **potenza discreta**).

Algoritmo di Diffie-Hellman - 7

Esempio 1

g = 7, p = 11 (pubblici)

a = 3 (Alice) segreto

b = 6 (Bob) segreto

Alice calcola $A = 7^3 \bmod 11 = 2$ e lo comunica a Bob

Bob calcola $B = 7^6 \bmod 11 = 4$ e lo comunica ad Alice

Alice calcola **K** $= 4^3 \bmod 11 = 9$

Bob calcola **K** $= 2^6 \bmod 11 = 9$

Algoritmo di Diffie-Hellman - 8

Esempio 2

g = 5, p = 23 (pubblici)

a = 6 (Alice) segreto

b = 15 (Bob) segreto

Alice calcola A = 5^6 mod 23 = 8 e lo comunica a Bob

Bob calcola B = 5^{15} mod 23 = 19 e lo comunica ad Alice

Alice calcola **K** = 19^6 mod 23 = 2

Bob calcola **K** = 8^{15} mod 23 = 2

Algoritmo di Diffie-Hellman - 9

Esempio 2 - Come calcolare le potenze in modulo

$5^{15} \bmod 23 = 5^8 \times 5^4 \times 5^2 \times 5^1 \bmod 23 =$

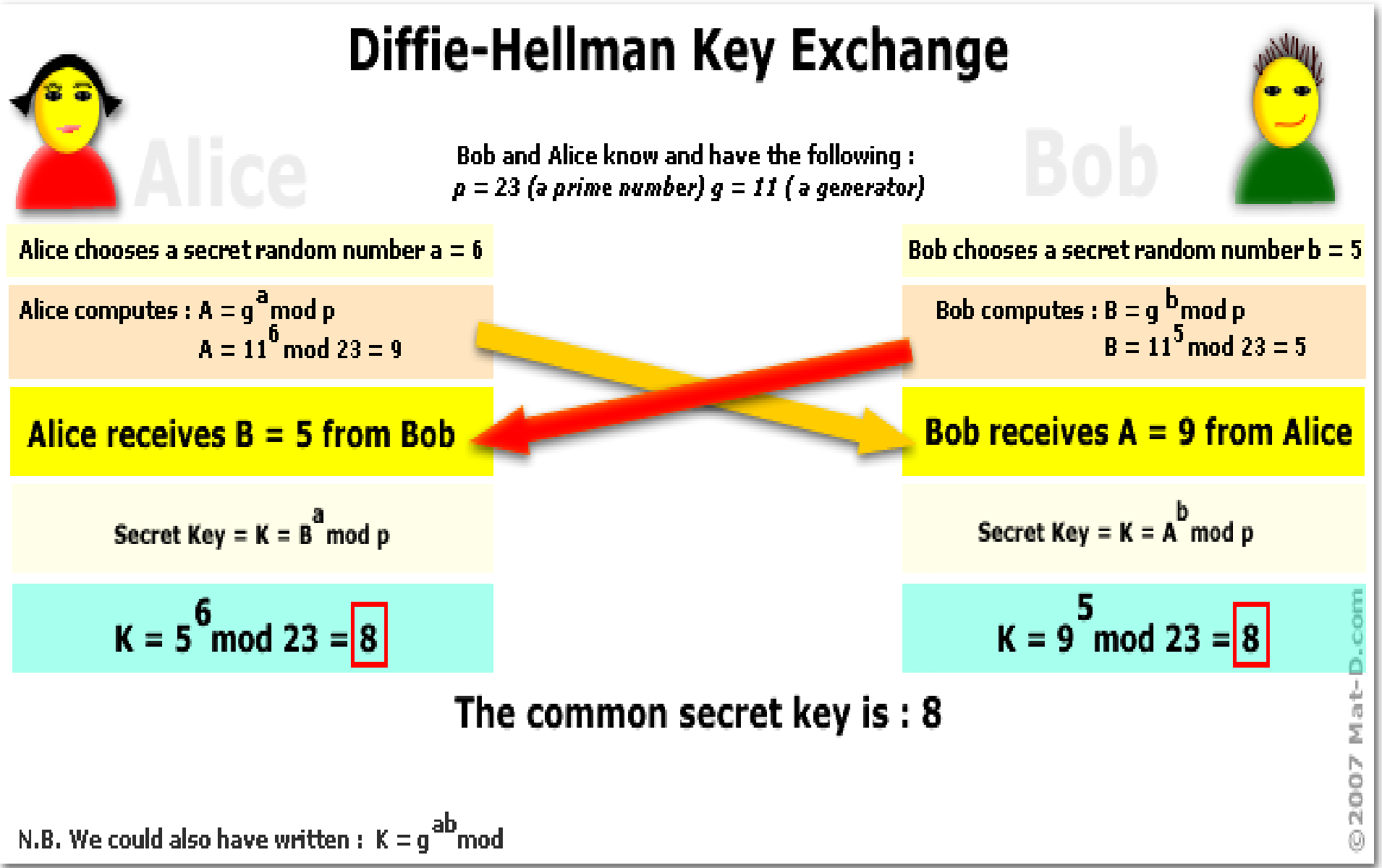
$[5^8 \bmod 23 \times 5^4 \bmod 23 \times 5^2 \bmod 23 \times 5^1 \bmod 23] \bmod 23$

- $5^1 \bmod 23 = 5$
- $5^2 \bmod 23 = 25 \bmod 23 = 2$
- $5^4 \bmod 23 = (5^2)^2 \bmod 23 = (5^2 \bmod 23)^2 \bmod 23$
  $= 2^2 \bmod 23 = 4 \bmod 23 = 4$
- $5^8 \bmod 23 = (5^4)^2 \bmod 23 = (5^4 \bmod 23)^2 \bmod 23$
  $= 4^2 \bmod 23 = 16 \bmod 23 = 16$

$5^{15} \bmod 23 = [16 \times 4 \times 2 \times 5] \bmod 23 = 640 \bmod 23 = 19$

Algoritmo di Diffie-Hellman - 10

Esempio 3



Algoritmo di Diffie-Hellman - 11

Nota: La **pre-master key** potrebbe anche essere resa **pubblica**, senza creare problemi alla crittografia.

A questo punto però l'algoritmo diventa ***anonimo*** (**non autenticato**). Se uno si mette in mezzo (**men in the middle**) e mi fa credere di essere il reale destinatario, io posso comunicare con lui credendo che sia il reale destinatario.

Nel caso invece di una **pre-master key** **riservata** e **nota a priori**, **solo chi conosce** la **pre-master key** può attivare una **sessione protetta**. Questa **tecnica è utilizzata** ad esempio nel **WiFi** dal **protocollo** **WPA-PSK** (Wi-Fi Protected Access - Pre Shared Key) , dove la **Pre Shared Key** viene utilizzata sia per l'**autenticazione** sia come **pre-master key** per generare la **chiave** di **sessione** con **Diffie-Hellman**.