IFCT0109. SEGURIDAD INFORMÁTICA

MF0489_3 SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

UD01

ANEXO.
PROTOCOLO DIFFIE-HELLMAN

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

PROTOCOLO DIFFIE-HELLMAN

PROTOCOLO DIFFIE-HELLMAN

Usuario A

$Elije\ \boldsymbol{P}\ y\ \boldsymbol{G}\ (raíz\ primitiva\ de\ P)$

$$G^{(P-1)} (\text{mod P}) = 1$$

Selecciona **a** < **P** (aleatorio)

$\boldsymbol{P} = 71$

$\mathbf{G} = 7$

$\mathbf{a} = 5$

PROTOCOLO DIFFIE-HELLMAN

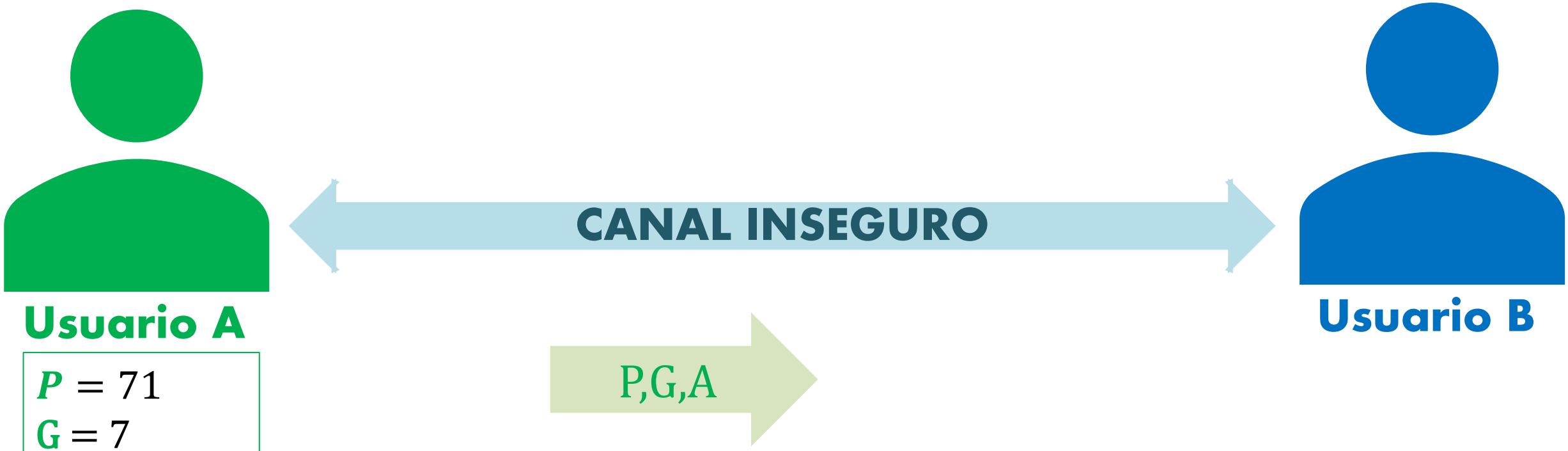
Usuario A

Calcula su clave pública A

$$A = G^a \bmod P$$

$$A = 7^5 \bmod 71 = 51$$

PROTOCOLO DIFFIE-HELLMAN



PROTOCOLO DIFFIE-HELLMAN

Usuario B

Recibe ***P*** *y* ***G***
y la clave pública de usuario A: ***A***
Selecciona b < P (aleatorio)

b =6

PROTOCOLO DIFFIE-HELLMAN

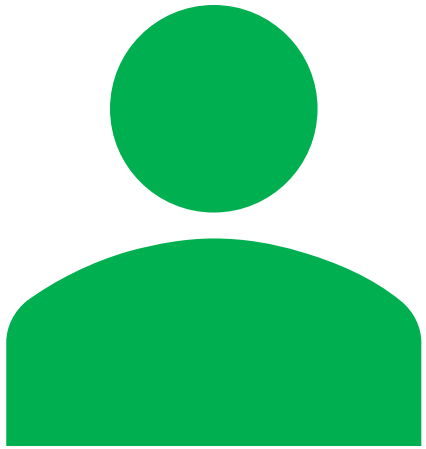
Usuario B

Calcula su clave pública B

$$B = G^b \bmod P$$

$$B = 7^6 \bmod 71 = 2$$

PROTOCOLO DIFFIE-HELLMAN

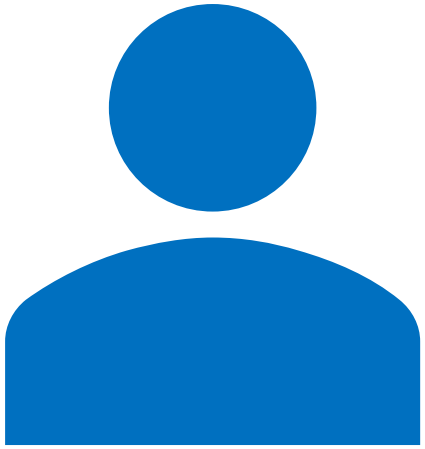


Usuario A

$P = 71$
$G = 7$
$a = 5$
$A = 51$

CANAL INSEGURO

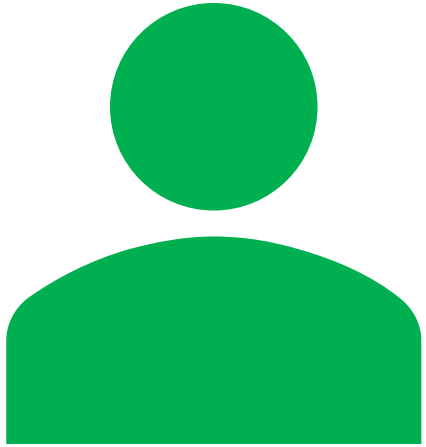
B



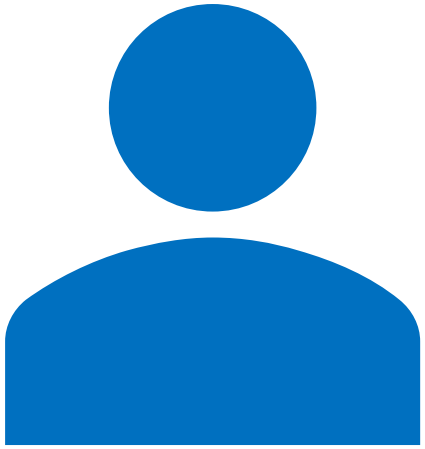
Usuario B

$P = 71$
$G = 7$
$b = 6$
$A = 51$
$B = 2$

PROTOCOLO DIFFIE-HELLMAN



P, G, A, B
han viajado por el canal inseguro



Usuario A

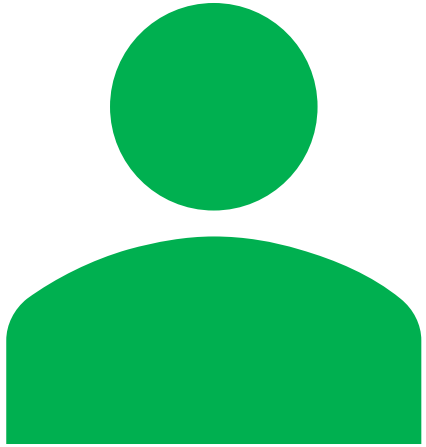
$\mathbf{P} = 71$
$\mathbf{G} = 7$
$\mathbf{a} = 5$
$\mathbf{A} = 51$
$\mathbf{B} = 4$

las claves privadas a y b no han viajado

Usuario B

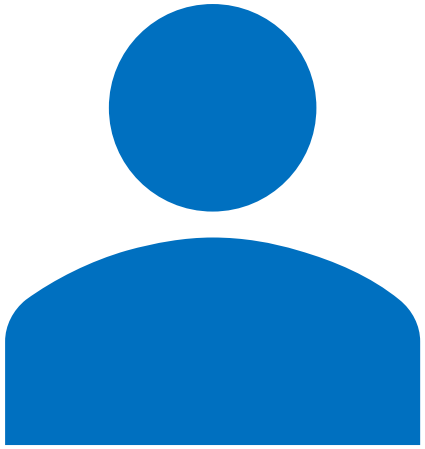
$\mathbf{P} = 71$
$\mathbf{G} = 7$
$\mathbf{b} = 6$
$\mathbf{A} = 51$
$\mathbf{B} = 2$

PROTOCOLO DIFFIE-HELLMAN



Usuario A

*Cada usuario (**A** y **B**),*
*con su clave privada (**a** y **b**)*
*Calcula la llave pública **K***
que van a usar en común



Usuario B

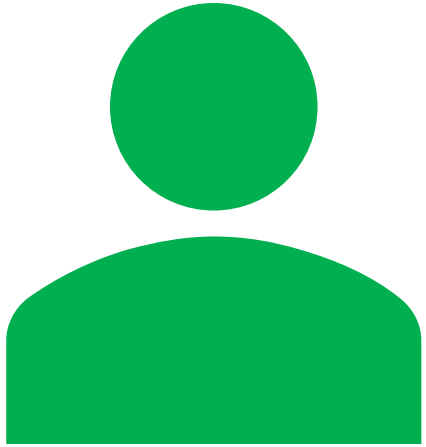
$K = B^a \bmod P$

$K = A^b \bmod P$

$$K = A^b \bmod P = (G^a \bmod P)^b \bmod P = G^{ab} \bmod P$$

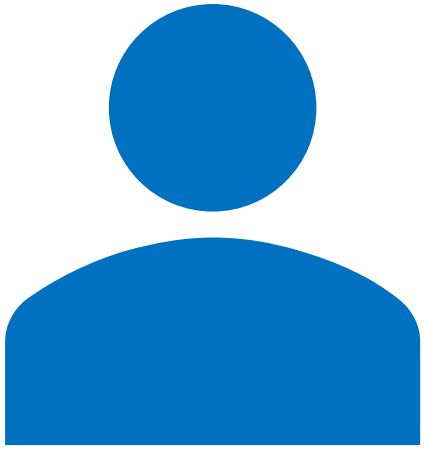
$$(G^b \bmod P)^a \bmod P = B^a \bmod P = K$$

PROTOCOLO DIFFIE-HELLMAN



Usuario A

Cada usuario,
con su clave privada (a y b)
Calculan la llave privada
que van a usar en común

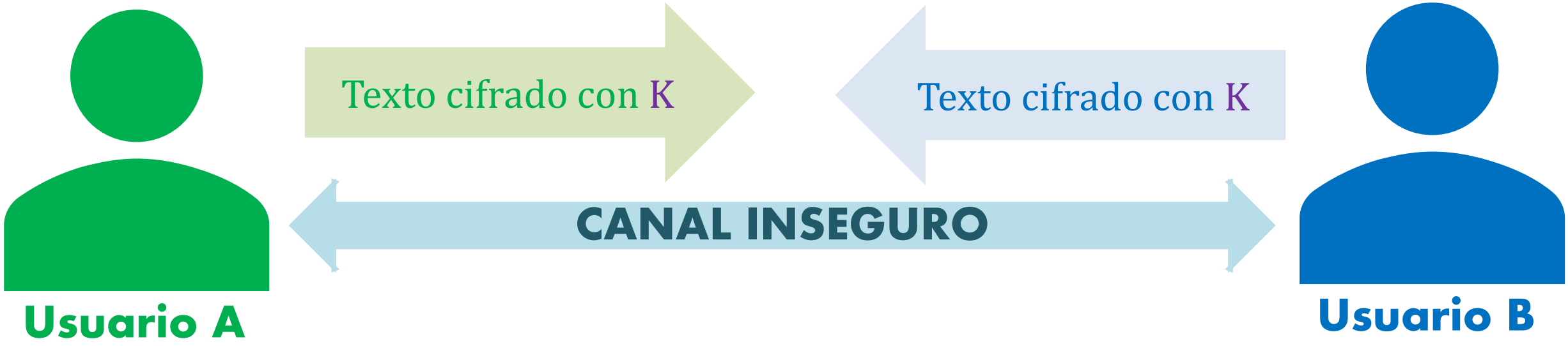


Usuario B

$$K = 2^5 \bmod 71 = 32$$

$$K = 51^6 \bmod 71 = 32$$

PROTOCOLO DIFFIE-HELLMAN



los datos ciajan cifrados con la clave pública comun de ***A*** *y* ***B***
pero no podrán ser descifrados por el atacante
ya que no conoce las claves privadas ***a*** *y* ***b***

PROTOCOLO DIFFIE-HELLMAN

El atacante puede conocer:

P, G, A y B

Tendría que calcular la clave secreta del Usuario A

$$A = G^{a} \bmod P$$

$$a = log_{G} A \bmod P$$

Es un cálculo computacionalmente complejo de calcular

ESTO ES TODO