



Actividad 14 Diffie-Hellman

En equipos (1,2 o 3 personas) resolver los siguientes ejercicios

- Considera que Alicia y Betito comparten $g=5$, $n=49$, $K_a=37$ y $K_b=19$. Encuentra los valores de a , b y K . (Incluye el diagrama en tu respuesta)
- Describe en un diagrama el proceso de intercambio de llaves para 3 entidades: Alicia, Betito y Carlitos.

Nota: Los procedimientos deben realizarse a mano, debes escanear tus notas y juntarlas con este documento o tomar una foto e incluirla como imagen al final de este archivo.

Trabajos sin procedimientos a mano valen 0 puntos.

Al finalizar guarda un sólo archivo como PDF. Un integrante debe subirlo a classroom, el resto solo debe marcar su tarea como entregada y poner en comentarios el nombre de quien sube el archivo.



M. en C. Nidia A. Cortez Duarte



Actividad 14 Diffie-Hellman

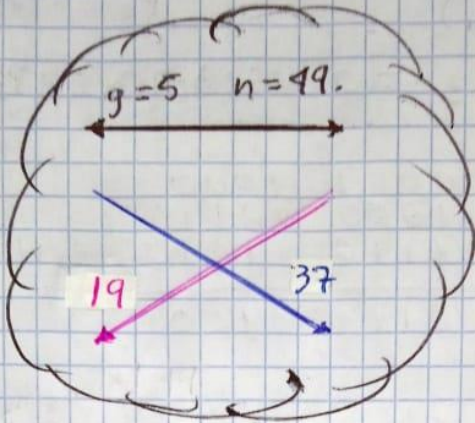
Actividad 14

Alicia

$a = 4$ ~~\times~~
 $K_A = 37$
 $K_A = g^a \mod n$
 $37 = 5^4 \mod 49$?
Así $\mod 49$
 $5^1 = 5$
 $5^2 = 25$
 $5^3 = 27$
 $5^4 = 37$ ✓
Por lo que
 $a = 4$ ~~\times~~
tenemos que:
 $K = (K_B)^a \mod n$
 $K = (19)^4 \mod 49$
 $K = 30$ ~~\times~~

Betito

$b = 7$ ~~\times~~
 $K_B = 19$
 $K_B = g^b \mod n$
 $19 = 5^7 \mod 49$?
Así $\mod 49$
 $5^1 = 5$
 $5^2 = 25$
 $5^3 = 27$
 $5^4 = 37$
 $5^5 = 38$
 $5^6 = 43$
 $5^7 = 19$ ✓
Por lo que
 $b = 7$ ~~\times~~
Tenemos que:
 $K = (K_A)^b \mod n$
 $K = (37)^7 \mod 49$
 $K = 30$ ~~\times~~





Actividad 14 Diffie-Hellman

Diffie-Hellman

Alicia.
a

$K_A = g^a \mod n$

$K'_A = (K_C)^a \mod n$

$K'_A = g^{ca} \mod n$

$K = (K'_C)^a \mod n$

$K = g^{bca} \mod n$

Betito
b

$K_B = g^b \mod n$

$K'_B = (K_A)^b \mod n$

$K'_B = g^{ab} \mod n$

$K = (K'_A)^b \mod n$

$K = g^{cab} \mod n$

Carlitos.
c

$K_C = g^c \mod n$

$K'_C = (K_B)^c \mod n$

$K'_C = g^{bc} \mod n$

$K = (K'_B)^c \mod n$

$K = g^{abc} \mod n$

Diagrama de flujo:

El diagrama muestra la comunicación entre Alicia, Betito y Carlitos. Se indica la generación de claves públicas K_A, K_B, K_C y la recepción de claves privadas K'_A, K'_B, K'_C por parte de Carlitos. Finalmente, se muestra la generación de la clave compartida K por cada uno de ellos.

M. en C. Nidia A. Cortez Duarte

