Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

CC BY NC SA

"Criptosistemas asimétricos"

Test de autoevaluación

Seleccione la respuesta correcta.

1. En los criptosistemas de clave pública o asimétricos:
   - Ambos interlocutores conocen una misma clave simétrica que usan tanto para cifrar como para descifrar.
   - **Cada interlocutor conoce su clave privada, y todos conocen las claves públicas de todos.**
   - Cada interlocutor conoce su clave pública y todos conocen las claves privadas de todos.
   - Ambos interlocutores conocen una misma clave asimétrica que usan tanto para cifrar como para descifrar.

2. En los criptosistemas de clave pública o asimétricos, cuando A envia un mensaje cifrado para B:
   - Utiliza la clave privada de B para cifrar el mensaje.
   - Utiliza la clave privada de A para cifrar el mensaje
   - **Utiliza la clave pública de B para cifrar el mensaje**
   - Utiliza la clave pública de A para cifrar el mensaje.

3. La seguridad de los sistemas de clave pública o asimétricos se basa:
   - En problemas complejos resolubles con algoritmos polinomiales.
   - En problemas difíciles basados en funciones biyectivas sin trampa
   - Se basan en el problema difícil de resolver el logaritmo discreto
   - **Algunos sistemas se basan en la dificultad de factorizar los números enteros**

4. En comparación con los criptosistemas simétricos:
   - Para un tamaño de clave equivalente, los asimétricos son más rápidos.
   - Para un tamaño de clave equivalente, los simétricos son más rápidos.
   - **El tamaño de clave recomendado para los asimétricos es de mayor longitud que la recomendada para los simétricos.**
   - El tamaño de clave recomendado para los asimétricos es de menor longitud que la recomendada para los simétricos.

5. Si A ha elegido e=23 con n=143, elija el valor correcto de su clave d en el sistema RSA:
   - 49
   - **47**
   - 23
   - 1

6. Las claves RSA de B son e=(13,33), d=(17,33). Si A desea cifrar para B el mensaje M=2, elija cuál es el valor correcto del mensaje cifrado:
   - **8**
   - 4
   - 29
   - 12

7. Si A ha elegido p=13 para generar sus claves de El Gamal (cifrado), seleccione qué valor de entre los siguientes puede utilizar como generador g:
   - **2**
   - 3
   - 4
   - 5

8. B ha elegido las siguientes claves y parámetros de El Gamal (cifrado): p=17, g=7, x=5, y=11. Si A cifra para B el mensaje M=6, utilizando la clave efímera k_e=9, elija cuál es el valor correcto del mensaje cifrado:
   - (15,2)
   - (3,12)
   - **(10,5)**
   - (12,11)