

Pregunta 1

Enunciado de la pregunta

Supongamos que Alice y Bob se comunican utilizando el esquema de ElGamal, y Bob publica su clave pública El Gamal $(g, h) = (2, 6)$; suponiendo además que trabajamos módulo 23.

Alice va a enviarle a Bob el mensaje $M = 12$. Si el algoritmo de cifrado necesita generar algún número aleatorio, escoge $Y = 8$.

¿Cuál es el cifrado de ese mensaje? Da la solución con números menores que 23, y explica brevemente cómo la has obtenido.

Si lo necesitas, usa esta notación: a^b denota "a elevado a b", $a*b$ denota "a por b"

Pregunta 2

Enunciado de la pregunta

Considera una función hash H con salida de 256 bits, y que cumple la propiedad PR. Responde razonadamente a las siguientes preguntas:

a) ¿Cumple también la propiedad CR?

b) Sin otra información adicional, ¿puedes decir un número de mensajes el los que habrás de evaluar H para estar seguro de encontrar una colisión?

Pregunta 3

Enunciado de la pregunta

Para este ejercicio usamos la notación "_" para indicar subíndices, es decir " C_i " denotaría "C sub i".

Alice y Bob van a usar un cifrador en DES en modo CTR para enviarse mensajes, con longitud de bloque y clave de 64 bits. Para no tener que pasarse siempre un bloque adicional, introducen una variante; si Alice envía un mensaje a Bob, el contador se inicializa siempre con una cadena de ceros (es decir, $C_0 := \text{Ctr} := 0||0||\dots||0$), y si Bob envía un mensaje a Alice, el contador se inicializa siempre con una cadena de unos (es decir, $C_0 := \text{Ctr} := 1||1||\dots||1$).

¿Qué puedes comentar acerca de este sistema?

**CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70**

**ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70**

Cartagena99

Pregunta 4

Enunciado de la pregunta

Recuerda que a^b denota "a elevado a b"

Menciona herramientas criptográficas que se ajusten a la descripción en cada caso.

Explica **muy brevemente, con una frase**, tu elección:

- a) Función hash muy insegura y con 160 bits de salida
- b) Función en la variable n que tenga complejidad no lineal, no sea un polinomio, y esté en la clase $O(n^2)$ // "O grande" de n al cuadrado.
- c) Esquema de firma basada en el problema de factorización y más seguro que la firma RSA de libro de texto
- d) Esquema de cifrado asimétrico basado en el problema de la mochila

Pregunta 5

Enunciado de la pregunta

Razona si estas dos afirmaciones son verdaderas o falsas.

- a) Todo esquema de cifrado de clave pública NM-CPA es también IND-CPA
- b) Todo esquema de cifrado de clave pública NM-CPA es también NM-CCA2.

The logo for Cartagena99 features the text 'Cartagena99' in a stylized, blue, serif font. The '99' is significantly larger and more prominent than the word 'Cartagena'. The text is set against a light blue background with a subtle gradient and a soft shadow effect.

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70