

1. Considera una generación RSA de claves anómala donde

- a) N es un número primo
- b) N es producto de tres números primos, p, q, r .

Comenta qué problemas de seguridad o ventajas puede tener la generación en el caso a), y estudia la corrección del esquema resultante con la generación b).

2. Considera el cifrado de Rabin (RSA con exponente de cifrado igual a 2). Si el módulo público es N , supón que conoces un valor $\epsilon \neq -1, 1$ tal que $\epsilon^2 = 1 \pmod N$. Analiza la seguridad del esquema en el sentido:

- a) NM-CPA
- b) IND-CCA2
- b) IND-CPA
- c) OW-CPA

3. Vamos ahora a considerar un esquema de cifrado que utiliza polinomios (cuyos coeficientes estarían en un cuerpo finito). Supongamos que la clave pública es una pareja de polinomios del mismo grado n ,

$$p(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \text{ y } q(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n.$$

La clave secreta es una raíz r de p , es decir, $p(r) = 0$. Para cifrar mensajes, contemplamos las siguientes opciones:

- a) $c = p(x)q(x) + m$
- b) $p(x)q(x) + q(x) + m$
- c) $t(p(x)q(x)) + m$, con t elegido uniformemente al azar.

Describe en cada caso como se realizaría el descifrado. Analiza la seguridad de esas opciones, al menos en el sentido IND-CPA, IND-CCA2, NM-CPA, NM-CCA2.

4. Un esquema de Zeng-Seberry. Sea G un grupo de orden primo q generado por un elemento g . Supongamos que V es una función que coge un elemento h del grupo y construye $V(h)$, una cadena de bits aleatoria. Considera H una función hash. La clave pública del esquema será

**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