Universidad Rey Juan Carlos

Grado en Ingeniería de la Ciberseguridad

Criptografía

Sesión 5. Clave Pública (II).

---

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 $\epsilon^2 = 1 \bmod N$. 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,

   $$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots, + a_n x^n \text{ y } q(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n.$$

   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 G, g, y donde $y = g^x$ y $x \in \{1, \ldots, q-1\}$ es la clave secreta. Para cifrar un mensaje m se siguen los siguientes pasos:

   a) Se elige $k \in \{0, ..., q-1\}$ al azar

   b) se define $z := V(y^k)$

   c) se define $t := H(m)$

   d) se construye el texto cifrado $c = (c_1, c_1) = (g^k, z \oplus (m \| t))$

   Piensa en los rangos y dominios de V y H para que la descripción anterior sea correcta. Describe el algoritmo de descifrado. Analiza la seguridad CCA2 del esquema anterior.