CRIPTOGRAFÍA Y COMPUTACIÓN

EXAMEN FINAL - JUNIO 2014

Cuestión 1. Sea $n = 10961$ y $f : \mathbb{Z}_n \to \mathbb{Z}_n$, $f(x) = x^2$, la función de Rabin. ¿Se puede factorizar n teniendo en cuenta que $f(12) = f(5323)$? (sin usar fuerza bruta).

Cuestión 2. ¿Podemos deducir a partir de que $\left(\frac{2}{143}\right) = 1$, que 2 tiene raíz cuadrada módulo 143?

Cuestión 3. Los cifrados polialfabéticos deben su nombre a que utilizan más de un alfabeto para cifrar.

Cuestión 4. Todo polinomio en $\mathbb{Z}_2[X]$ de grado 7 que sea irreducible es primitivo.

Cuestión 5. Realiza en el cuerpo AES la operación $B5 \cdot 19 + AA^{-1}$.

Cuestión 6. Tenemos un sistema de firma digital DSS con parámatros

$$(p, q, \alpha, y) = (67, 11, 59, 15)$$

y un mensaje cuyo resumen es $h = 5$. ¿Es válido $(7, 2)$ como firma de este mensaje?

Ejercicio 1. Demuestra que el polinomio $a(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$ es primitivo. Sea l el LFSR asociado a $a(x)$. Utiliza l con semilla 1011 para generar una secuencia pseudo-aleatoria. Demuestra que cumple los postulados de Golomb.

Ejercicio 2. Pedro quiere enviar a Jesús los cuatro últimos dígitos de su tarjeta de crédito. Jesús dispone de un criptosistema ElGamal con clave pública $(p, \alpha, y) = (6547, 8, 4565)$. Pedro hace uso de ese sistema de cifrado para enviar el mensaje, y lo que Jesús recibe es es $(5777, 5686)$. ¿Cuáles son los cuatro últimos dígitos de la tarjeta de Pedro?

Cuando Jesús recibió su clave privada, lo que recibió fue el mensaje 100101000100110. La clave venía cifrada por un sistema de cifrado en bloque que operaba en modo CFB en el que el parámetro s era igual al tamaño del bloque, que vale 3 y el bloque inicial es el bloque 000.

La función de cifrado trabaja entonces con bloques de 3 bits, lo que equivale a trabajar con números módulo 8. Dicha función es $f(x) = 5x + 5 \pmod 8$.

Una vez descifrado el mensaje, lo que obtiene Jesús es un número en binario a partir del cual obtiene su clave privada.

Calcula la clave privada y comprueba que efectivamente es la clave privada asociada a la clave pública $(6547, 8, 4565)$.

Cada cuestión vale un máximo de 0.75 puntos. El primer ejercicio 2 y el segundo 3.5.