GUIÓN DE CRIPTOGRAFÍA

FUNCIONES DE UN SOLO SENTIDO

Ejercicio 1. Sea $(a_1, \ldots, a_k)$ una secuencia super-creciente de números positivos (la suma de los términos que preceden a a_i es menor que a_i, para todo i). Elige $n > \sum a_i$, y u un entero positivo tal que $\gcd(n, u) = 1$. Define $a_i^* = u a_i \bmod n$. La función mochila (knapsack) asociada a $(a_1^*, \ldots, a_k^*)$ es

$$f : \mathbf{Z}_2^k \to \mathbf{N},\ f(x_1, \ldots, x_k) = \sum_{i=1}^{k} x_i a_i^*.$$

Implementa esta función y su inversa, tal y como se explica en [2, §4.5]. La llave pública es $(a_1^*, \ldots, a_k^*)$, mientras que la privada (y puerta de atrás) es $((a_1, \ldots, a_k), n, u)$.

Ejercicio 2. Sea p un (pseudo-)primo mayor o igual que vuestro número de identidad. Encuentra un elemento primitivo, α, de $\mathbb{Z}_p^*$ (se puede usar [3, 2.132 (iv)]; para facilitar el criterio, es bueno escoger p de forma que $(p-1)/2$ sea también primo, y para ello usamos Miller-Rabin). Definimos

$$f : \mathbf{Z}_p \to \mathbf{Z}_p,\ x \mapsto \alpha^x.$$

Calcula el inverso de tu fecha de nacimiento con el formato AAAAMMDD.

En lo que sigue, p y q son enteros primos, y $n = pq$.

Ejercicio 3. Sea $f : \mathbf{Z}_n \to \mathbf{Z}_n$ la función de Rabin: $f(x) = x^2$. Sea $n = 48478872564493742276963$. Sabemos que $f(12) = 144 = f(37659670402359614687722)$. Usando esta información, calcula p y q (mira la demostración de [1, Lemma 2.43]).

Ejercicio 4. Elige a_0 y a_1 dos cuadrados arbitrarios módulo n (n como en el Ejercicio 3). Sea

$$h : \mathbf{Z}_2 \times (\mathbf{Z}_n)^* \to (\mathbf{Z}_n)^*,\ h(b, x) = x^2 a_0^b a_1^{1-b}.$$

Usa la construcción de Merkle-Damgård para implementar una función resumen tomando h como función de compresión (esta h fue definida por Goldwasser, Micali y Rivest). Los parámetros a_0, a_1 y n se hacen públicos (la función debería admitir un parámetro en el que venga especificado el vector inicial).

Ejercicio 5. Sea p el menor primo entero mayor o igual que tu número de identidad, y sea q el primer primo mayor o igual que tu fecha de nacimiento (AAAAMMDD). Selecciona e tal que $\gcd(e, (p-1)(q-1)) = 1$. Define la función RSA

$$f : \mathbf{Z}_n \to \mathbf{Z}_n,\ x \mapsto x^e.$$

Calcula el inverso de 1234567890.

Ejercicio 6. Sea $n = 50000000385000000551$, y que sabemos que una inversa de $\mathbb{Z}_n \to \mathbb{Z}_n$, $x \mapsto x^5$ es $x \mapsto x^{10000000074000000101}$ (esto es, conoces tanto la llave pública como la privada de la función RSA). Encuentra p y q usando el método explicado en [2, Page 92]. Compara este procedimiento con el algoritmo de Miller-Rabin y el Ejercicio 3.

Ejercicio 7. En este ejercicio se pide implementar un sistema de firma digital y verificación de la firma. Se puede elegir entre firma RSA o DSS.

Al igual que antes, debe realizar tres tareas: generación de claves (ejercicios anteriores), generación de firma y verificación de firma.

Para la generación de la firma, se le introducirá un mensaje a cifrar (fichero) y el fichero con la clave (privada), y deberá generar una firma, que se guardará en un fichero de texto.

Puesto que lo que realmente se firma no es el mensaje, sino un resumen del mensaje, hay que generar un resumen de dicho mensaje. Para esto emplearemos la función SHA1 (se pueden añadir otras funciones resumen). Cualquiera de las implementaciones de esta función que hay en la red puede ser usada.

Para la verificación de la firma, se introduce el mensaje (fichero) que se ha firmado, un fichero con la firma (con el mismo formato que el generado en el apartado anterior) y un fichero con la clave (pública). Deberá responder si la firma es o no válida.

REFERENCIAS

[1] S. Goldwasser, M. Bellare, Lecture Notes on Cryptography
[2] P. J. Cameron, Notes on cryptography.
[3] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.