MA-53G Intr. a la Criptografía	**Semestre Otoño, 1998**

Control No. 1 : 15 de Mayo

Profesor: Marcos Kiwi — *Auxiliar: Alejandro Hevia*

Tiempo: 4:00 horas

Problema 1:

(i).- Sea C un criptosistema de clave privada, cuyo conjunto de claves es $\mathcal{K} = \{k = (k_1, k_2) \mid k_1, k_2 \in \{0,1\}^l\}$ y donde la función de encripción está dada por: $E_k\colon \{0,1\}^l \to \{0,1\}^l$ tal que $E_k(M) = f(k_1, M \oplus k_2)$ donde $f\colon \{0,1\}^l \times \{0,1\}^l \to \{0,1\}^l$ es una función tal que cualquiera sea k_1 e y, $f(k_1, \cdot)$ y $f(\cdot, y)$ son permutaciones de $\{0,1\}^l$ que se pueden calcular, al igual que sus inversas, con $O(poly(l))$ operaciones.

Pruebe que se requiere $O(2^l poly(l))$ operaciones para descubrir la clave si se tienen $c = O(1)$ pares de texto puro/cifrado $(x_i, y_i)_{i=1,\ldots,c}$, y el sistema, en las variables k_1 y k_2, dado por $f(k_1, x_i \oplus k_2) = y_i$, $i = 1, \ldots, c$, tiene solución única.

(ii).- Se dice que $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ es un sistema de firmas si:

1. $\mathcal{P}$ es un conjunto de posibles mensajes.
2. $\mathcal{A}$ es un conjunto de posibles firmas.
3. $\mathcal{K}$ es un conjunto de posibles claves.
4. Para todo $K \in \mathcal{K}$, existe una función de firma $sig_K \in \mathcal{S}$ y una correspondiente función verificación $ver_K \in \mathcal{V}$. Además, $sig_K\colon \mathcal{P} \to \mathcal{A}$ y $ver_K\colon \mathcal{P} \times \mathcal{A} \to \{0,1\}$ son funciones tales que para todo $x \in \mathcal{P}$ y para todo $y \in \mathcal{A}$:

$$ver_K(x,y) = \begin{cases} 1 & \text{si } y = sig_K(x), \\ 0 & \text{si } y \neq sig_K(x). \end{cases}$$

La función sig_K debe permanecer secreta y la función ver_K es pública.

Proponga una implementación concreta de un sistema de firmas.

Problema 2:

(i).- Suponga que tenemos un conjunto de bloques encriptados por RSA y que no poseemos la clave privada d (aunque si conocemos la clave pública (n, e)). Suponga además que tenemos los textos cifrados $y_1, \ldots, y_k$ correspondientes a los textos puros $x_1, \ldots, x_k \in \mathbb{Z}_n$. Si alguien nos dice que uno de los x_i es tal que $x_i \neq 0$ y $(x_i, n) \neq 1$, ¿Puede recuperarse la clave privada d eficientemente? Justifique su respuesta.

(ii).- Suponga que tres individuos A, B, y C usan RSA y con claves públicas $(n_A, 3)$, $(n_B, 3)$, $(n_C, 3)$ respectivamente. Suponga además que D quiere enviar el *mismo* mensaje $m \in \{0, \ldots, n-1\}$, donde $n = \min\{n_A, n_B, n_C\}$, a los tres individuos A, B, C. Para ello D calcula

$$y_A = m^3 \bmod n_A \,, \qquad y_B = m^3 \bmod n_B \,, \qquad y_C = m^3 \bmod n_C \,,$$

y se los envía a A, B, y C según corresponda.

Pruebe que un adversario que intercepta los tres mensajes y_A, y_B, y_C puede determinar m aunque desconozca las claves secretas de A, B, C.

(iii).- Pruebe que RSA es una regla de encripción multiplicativa en el sentido que si la clave pública es $k = (n, e)$ entonces la función de encripción $f(x) = x^e \bmod n$, donde $x \in \mathbb{Z}_n$ satisface que

$$f(x)f(x') \;\equiv\; f(x \cdot x') \pmod{n}\,, \qquad \forall x, x' \in \mathbb{Z}_n \,.$$

Suponga que un adversario descubre un algoritmo determinístico a tiempo polinomial que dado un módulo n y un texto cifrado $y \in \mathbb{Z}_n$ retorna con una decripción de y (i.e. un $x \in \mathbb{Z}_n$ tal que $x^e \bmod n = y$) o retorna `nada`. Suponga además que, dado n, hay ϵn textos cifrados en $\mathbb{Z}_n$ para los cuales el algoritmo mencionado logra decriptar, donde $\epsilon \in (0, 1]$. Pruebe que dicho adversario puede diseñar un algoritmo probabilista eficiente, que decripta cada mensaje encriptado con f con probabilidad al menos ϵ.

<u>Indicación</u>: Primero estudie el caso en que el mensaje encriptado $x \in \mathbb{Z}_n$ es primo relativo con n.

Problema 3:

(i).- Pruebe el Terorema de Fermat para cuerpos finitos, i.e. pruebe que si $\mathbb{F}$ es un cuerpo finito, y $a \in \mathbb{F}$ entonces para todo $a \neq 0$, se tiene que

$$a^{q-1} = 1 \,, \qquad \text{donde} \;\; q = |\mathbb{F}| \,.$$

(ii).- Basandose en el resultado obtenido en la parte anterior, y asumiendo que puede realizar aritmética en $\mathbb{F}$ eficientemente, proponga un algoritmo para calcular a^{-1} cualquiera sea $a \in \mathbb{F} \setminus \{0\}$.

(iii).- Sea p primo y $q = p^k$. Sea $f \in \mathbb{Z}_p[X]$ un polinomio irreductible de grado n.[1] Considere el modelo $\mathbb{Z}_p[X]/(f)$ de $\mathbb{F}_q$ y describa la *idea* de un algoritmo eficiente, distinto al que encontró en la parte anterior, para calcular g^{-1} para cualquier $g \in \mathbb{F}_q \setminus \{0\}$. Asuma que puede calcular eficientement la suma, la resta, el producto, y el resto de dos elementos de $\mathbb{Z}_p[X]$. Fundamente su respuesta.

<u>Indicación</u>: Piense en el caso $k = 1$.

[1] Recuerde que un polinomio se dice irreductible si no se puede expresar como el producto de dos polinomios de menor grado.