MA-53G Intr. a la Criptografía	**Semestre Primavera, 1996**

Control No. 1 : 26 de Octubre

Profesor: Marcos Kiwi — *Tiempo: 3.5 hrs.*

Problema 1: El proposito de este problema es construir un protocolo que le permita a dos individuos a gran distancia uno del otro convenir en el resultado del lanzamiento de una moneda.

Un sistema de *funciones dos a uno de puerta secreta* consta de cuatro algoritmos:

- Un algoritmo el cual genera un par de claves K_e y K_d, y otro algoritmo que dadas dos entradas K'_e y K'_d permite decidir si estas son claves como las generadas por el algoritmo anterior.
- Un algoritmo el cual dado una clave K_e del tipo adecuado, construye una función $f\colon \mathcal{P} \to \mathcal{C}$ tal que cualquier elemento c en la imagen de f tiene exactamente dos preimagenes p_1, $p_2 \in \mathcal{P}$ tal que $f(p_j) = c$.
- Otro el cual dada una clave K_d que "invierte" K_e puede encontrar ambas preimágenes de cualquier c en la imagen de f.

Aquí suponemos que es computacionalmente muy costoso encontrar K_d conocido sólo K_e. Observar, que dado un elemento $p_1 \in \mathcal{P}$ es posible calcular, si uno conoce K_e y K_d, el otro elemento p_2 tal que que tiene la misma imagen que p_1 a través de f; aquí suponemos que conociendo sólo K_e, *cualquiera* sea p_1 es computacionalmente muy costoso calcular el elemento p_2 que lo acompaña.

(i).- (2.5 pts.) Describa el protocolo de un juego basado en un sistema de funciones dos a uno de puerta secreta, en el que participan dos jugadores y en el cual cada jugador tiene una probabilidad de "ganar" (de una definición adecuada de "ganar") de un 50%.

(ii).- (1.0 pto.) Sea $n = p \cdot q$, donde p y q son primos impares. Se define sobre $\mathcal{Z}_n^*$ la siguiente relación de equivalencia: $x\mathcal{R}y \Leftrightarrow x = -y$. Sea $\mathcal{P} = \mathcal{C} = \mathcal{Z}_n^*/\mathcal{R}$ (i.e. el conjunto de residuos módulo n primos a n donde los opuestos aditivos se han identificado). Muestre que la función $f\colon \mathcal{P} \to \mathcal{C}$ tal que $f(x) = x^2 \bmod n$ es tal que todo elemento en la imagen de f tiene dos preimágenes.

(iii).- (2.5 pts.) Basandose en la parte anterior proponga un sistema de funciones dos a uno de puerta secreta. Explicite la forma de elegir K_e y K_d. Justifique que su propuesta puede implementarse eficientemente.

Problema 2:

(i).- (3.0 pts.) 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 $\forall x \in \mathcal{P}$ y $\forall y \in \mathcal{A}$:

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

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

Proponga un sistema de firmas basado en RSA.

(ii).- (1.5 pts.) Sea p un número primo impar, y sean α, β generadores de $\mathcal{Z}_p^*$. Pruebe que en $\mathcal{Z}_p$ existe un algoritmo eficiente para calcular $\log_\alpha : \mathcal{Z}_p^* \to \mathcal{Z}_{p-1}$ si y solo si existe un algoritmo eficiente para calcular $\log_\beta : \mathcal{Z}_p^* \to \mathcal{Z}_{p-1}$.

(iii).- (1.5 pts.) Sea p un número primo, y sea g un generador de $\mathcal{Z}_p^*$. Se define la función $LD_1 \colon \mathcal{Z}_p^* \to \{0,1\}$ por $LD_1(g^i) = i \bmod 2$, $i \in \mathcal{Z}_{p-1}$. De un algoritmo eficiente para calcular $LD_1(\cdot)$.

Problema 3: El análisis probabílistico del test de primalidad de Solovay-Strassen requiere el siguiente resultado:

Lema 1 *Sea n un entero positivo impar. Si n es compuesto, y*

$$G(n) = \left\{ a \in \mathcal{Z}_n^* : \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod n \right\},$$

entonces

$$|G(n)| \leq \frac{n-1}{2}.$$

El objetivo de este problema es probar el anterior resultado.

(i).- (1.5 pts.) Pruebe que $G(n)$ es subgrupo de $\mathcal{Z}_n^*$ y que si $G(n) \neq \mathcal{Z}_n^*$ entonces $|G(n)| \leq \frac{n-1}{2}$.

(ii).- (1.5 pts.) Suponga que $n = p^k q$ donde p y q son impares, p es primo, $k \geq 2$ y $\mathrm{mcd}(p,q) = 1$. Sea $a = 1 + p^{k-1}q$. Pruebe que

$$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod n.$$

Indicación: Use el Teorema del Binomio para calcular $a^{\frac{n-1}{2}}$.

(iii).- (1.5 pts.) Sea $n = p_1 \ldots p_s$ donde los p_i son primos impares distintos. Sean a, u enteros tales que u no es residuo cuadrático módulo p_1, $a \equiv u \pmod{p_1}$, y $a \equiv 1 \pmod{p_2 \ldots p_s}$.[1] Pruebe que

$$\left(\frac{a}{n}\right) \equiv -1 \pmod n,$$

y concluya que

$$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod n.$$

(iv).- (1.5 pts.) Pruebe el Lema 1.

[1] Observar que el Teorema Chino del Resto garantiza la existencia de a.