MA-53g Intr. a la Criptografía	20 de Enero, 2002
Examen	
	Hasta las 12:00 hrs. del 22/01

Elija 2 de los siguientes 4 problemas.

PROBLEMA 1: [**Encripción con un mazo de cartas**]

Alicia baraja un mazo de cartas y las reparte entre ella y Roberto (cada quien recibe 26 cartas). Alicia desea ahora enviar un mensaje M a Roberto diciendo algo en voz alta. Eva escucha todo lo que dice Alicia (pero no puede ver sus cartas).

(i).- Suponiendo que $M \in \{0,1\}^{48}$, describa como puede Alicia comunicar M a Roberto de forma que Eva no obtenga nada de información acerca de M.

(ii).- Suponiendo ahora que $M \in \{0,1\}^{49}$, pruebe que no existe ningún protocolo que le permite a Alicia comunicar M a Roberto de forma que Eva no obtenga información acerca de M

Indicación: El que Eva no obtenga información acerca de M significa que cualquiera sea la secuencia de bits B la probabilidad que Alicia diga K es independiente de M, i.e., cualquiera sean M_0 y M_1, se tiene que

$$\mathbb{P}\left(\text{Alicia dice } B | M = M_0\right) = \mathbb{P}\left(\text{Alicia dice } B | M = M_1\right) ,$$

donde la probabilidad es sobre las distintas formas de barajar el mazo.

PROBLEMA 2:

(i).- Sean $\{E_k\}_{k \in \mathcal{K}}$ una familia de funciones de encripción donde cada E_k es una permutación de $\{0,1\}^{|k|}$. Para cada $k \in \mathcal{K}$ se define la función de encripción probabilista que a cada $M \in \{0,1\}^{|k|}$ le asocia

$$F_k(M) \stackrel{\text{def}}{=} (E_k(R), R \oplus M) ,$$

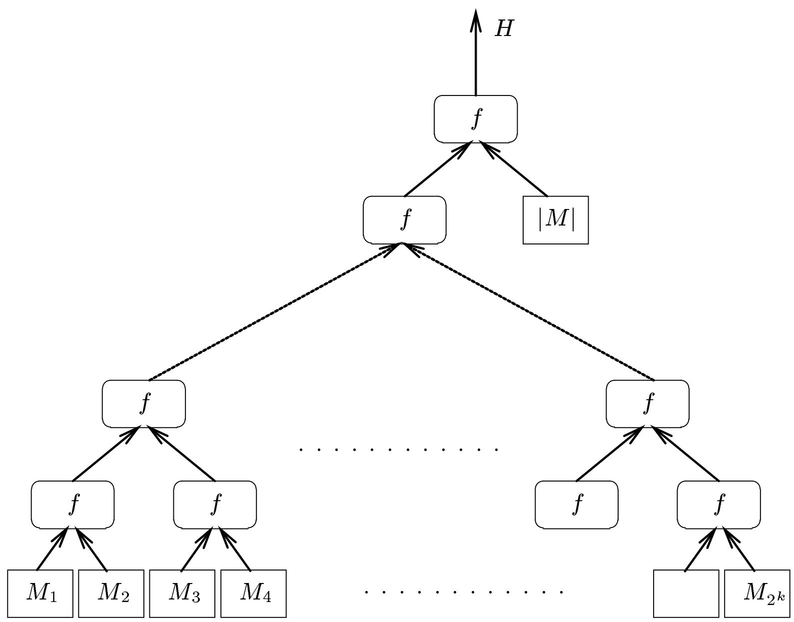
donde R es una secuencia de bits aleatorios del mismo tamaño del mensaje M. Para cada nueva encripción de un mensaje se elije una nueva secuencia R de bits aleatorios.

Se dice que un ataque es *de reconstrucción de clave a texto puro elegido* si al adversario le es permitido fijar un $n \in \mathbb{N}$, generar una secuencia de mensajes $M_1, M_2, \ldots, M_n$, y para cada M_i obtener el correspondiente texto cifrado.

Se dice dice que un ataque es *de reconstrucción de clave a texto puro aleatorio* si al adversario le es permitido fijar un $n \in \mathbb{N}$, y obtener pares de texto puro/cifrado donde el texto puro es elegido al azar.

Pruebe que si el criptosistema basado en las funciones de encripción probabilista $\{F_k\}_{k\in\mathcal{K}}$ es vulnerable ante un ataque de reconstrucción de clave a texto puro elegido entonces también lo es ante un ataque de reconstrucción de clave a texto puro aleatorio.

(ii).- Se a f una función de compresión que toma como entradas dos bloques de L bits y retorna un bloque de L bits. Sea H la función hash definida sobre los $M = M_1||\ldots||M_{2^k}$ donde $M_i \in \{0,1\}^L$ y $L2^k < 2^L$, dada por la construcción de la siguiente figura:



Pruebe que si se puede encontrar una colisión para H, entonces se puede encontrar una colisión para f.

Problema 3:

(i).- Suponga que dado p se puede encontrar un divisor q de $p-1$ tal que $q > \sqrt{p}$. Pruebe que entonces el siguiente algoritmo puede usarse para establecer la primalidad de p.

- Determinar un primo q divisor de $p-1$ tal que $q > \sqrt{p}$
- Escoger a al azar en $\mathbb{Z}_p^*$
- Si $1 < \mathrm{mcd}(a-1, p) < p$ entonces p es compuesto.
- Verificar que $a^q \equiv_p 1$.
- Recursivamente probar que q es primo.

Observe que basta probar el siguiente

Lemma 1 *Si* $q > \sqrt{p}$ *es un primo y para algún* $a \in \mathbb{Z}_p^*$, $\mathrm{mcd}(a-1, p) = 1$ *y* $a^q \equiv_p 1$, *entonces* p *es primo.*

<u>Indicación</u>: Asuma que existe un $d \leq \sqrt{p}$ divisor de p y estudie el orden de a en $\mathbb{Z}_d^*$.

(ii).- Sea $\mathcal{A}$ un algoritmo eficiente cuyas entradas son de la forma (N, e, y, p), donde $N \in \{0,1\}^k$ es el producto de dos primos distintos y $e \in \mathbb{Z}_{\varphi(n)}^*$. Suponga que cualquiera sean N y e, para el 51% de los valores de $(y, p) \in \mathbb{Z}_N^* \times \{0,1\}^k$ el algoritmo $\mathcal{A}$ en la entrada (N, e, y, p) retorna $\langle y, p \rangle \stackrel{\text{def}}{=} \sum_{i=1}^n y_i p_i$ (aritmética en $\mathbb{Z}_2$) donde $y = x^e \bmod N$.

Explique como usar $\mathcal{A}$ para construir un algoritmo eficiente $\mathcal{A}'$ tal que cualquiera sean N y e con las características antes mencionadas, para el 99% de los valores de $y \in \mathbb{Z}_N^*$ retorna $x \in \mathbb{Z}_N^*$ tal que $y = x^e \bmod N$. Especifique el número de veces que $\mathcal{A}'$ invoca $\mathcal{A}$.

PROBLEMA 4: **[Test de primalidad de Solovay–Strassen]**

El objetivo de este problema es probar el siguiente

Lemma 2 *Sea n un entero positivo impar. Si n es compuesto, y*

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

entonces $|G(n)| \leq |\mathbb{Z}_n^*|/2$.

(i).- Pruebe que $G(n)$ es subgrupo de $\mathbb{Z}_n^*$ y que si $G(n) \neq \mathbb{Z}_n^*$ entonces $|G(n)| \leq |\mathbb{Z}_n^*|/2$.

(ii).- 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

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

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

(iii).- 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, $a \equiv u \bmod p_1$, y $a \equiv 1 \bmod p_2 \ldots p_s$.[1] Pruebe que

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

y concluya que $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \bmod n$.

(iv).- Pruebe el Lemma 2.

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