MA53G Intr. a la Criptografía	**Semestre Primavera, 2001**

Tarea No. 2

Profesor: Marcos Kiwi	*Fecha de entrega: Control 1*

Elija 4 de los siguientes 5 problemas

Problema 1:

(i).- Sean $e, d \in \mathbb{Z}^*_{\varphi(n)}$ tales que $ed \equiv_{\varphi(n)} 1$. Sabemos que $RSA_{n,e} : \mathbb{Z}^*_n \to \mathbb{Z}^*_n$ tiene inversa $RSA_{n,d}$. Use el Teorema Chino del Resto para establecer que $RSA'_{n,e} : \mathbb{Z}_n \to \mathbb{Z}_n$ tal que $RSA'_{n,e}(x) = x^e \bmod n$ tiene inversa $RSA'_{n,d}$.

Suponga ahora que para $i = 1, \ldots, k$ tenemos que $y_i = RSA'_{n,e}(x_i)$, donde $x_1, \ldots, x_k \in \mathbb{Z}_n$. Sabiendo que para algún $i \in \{1, \ldots, k\}$ se tiene que $x_i \in \mathbb{Z}_n \setminus \mathbb{Z}^*_n$, pruebe que puede calcularse $\varphi(n)$ y por lo tanto determinarse d.

(ii).- Suponga que tres individuos A, B y C usan RSA 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 y C. Para ello D calcula

$$\begin{aligned} y_A &= RSA_{n_A,3}(m) = m^3 \bmod n_A\,, \\ y_B &= RSA_{n_B,3}(m) = m^3 \bmod n_B\,, \\ y_C &= RSA_{n_C,3}(m) = m^3 \bmod n_C\,, \end{aligned}$$

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

Use el Teorema Chino del Resto para probar que un adversario que intercepta los tres mensajes y_A, y_B, y_C puede determinar m. (Observe que un adversario siempre tiene acceso a las claves públicas.)

Problema 2: Suponga que un adversario descubre un algoritmo determinista a tiempo polinomial que dado un módulo n y un texto cifrado $y \in \mathbb{Z}^*_n$ retorna un texto plano $x \in \mathbb{Z}^*_n$ tal que $RSA_{n,e}(x) = x^e \bmod n = y$ o retorna `nada`. Suponga además que para $\epsilon \in (0, 1]$, dado n, hay ϵn textos cifrados en $y \in \mathbb{Z}_n$ para los cuales el algoritmo mencionado logra encontrar el correspondiente x. Pruebe que dicho adversario puede diseñar un algoritmo probabilista eficiente que dado $y = RSA_{n,e}(x)$ encuentra el correspondiente $x \in \mathbb{Z}^*_n$ con probabilidad al menos $1 - \chi$, cualquiera sea $\chi \in (0, 1]$.

Indicación: Recuerde que $RSA_{n,e}$ es un homomorfismo de grupos, i.e., para todo $x, \rho \in \mathbb{Z}^*_n$,

$$RSA_{n,e}(\rho) \cdot RSA_{n,e}(x) \equiv_n RSA_{n,e}(\rho \cdot x)\,.$$

Problema 3:

(i).- Pruebe el Teorema 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).- Basándose 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 $a \in \mathbb{F} \setminus \{0\}$.

PROBLEMA 4: Demuestre que es una mala idea elegir primos de la forma $p = 2^k + 1$ para protocolos basados en la conjetura de intractabilidad del problema del logaritmo discreto, en particular, pruebe que para dicho tipo de primos, el problema del logaritmo discreto puede ser resuelto eficientemente.

Indicación: Sea g un generador de $\mathbb{Z}_p^*$. Pruebe que conocido $y = g^x \bmod p$ se puede calcular el bit menos significativo de $x \in \mathbb{Z}_{p-1}$ y que conocido dicho bit es posible calcular eficientemente el siguiente bit menos significativo de x. Generalice.

PROBLEMA 5: A y B utilizan una red de broadcast para comunicarse (imagine que utilizan una ethernet o radiotransmisores). Un adversario computacional todopoderoso, C, escucha las transmisiones. La red de broadcast tiene la propiedad que C puede oír todo lo que A y B transmiten, pero no puede determinar QUIEN (A o B) transmite. Obviamente, si A o B transmiten un mensaje, cada uno puede determinar quien lo envió.

(i) Diseñe un protocolo mediante el cual A y B pueden establecer una clave secreta común de tal forma que C no tenga ninguna información acerca de cual es la clave secreta establecida, inclusive si A y B no comparten ninguna clave secreta de antemano. Asuma que C no puede alterar los mensajes transmitidos.

    Indicación: Suponga que A y B poseen relojes sincronizados y estudie primero como como pueden A y B establecer un bit en común sin que C obtenga información sobre dicho bit.

(ii) Asuma ahora que C puede determinar quien transmite pero que su mecanismo de intercepción tiene una probabilidad de error de 0.01 (i.e., cuando C recibe un bit hay una probabilidad de 0.01 de que este bit sea distinto del que originalmente se envío). A y B no tienen este problema de recepción. Diseñe un protocolo que les permita a A y B establecer una clave secreta de n bits de largo sin que C logre obtener información alguna concerniente a la clave (su solución debe funcionar con alta probabilidad). Pruebe sus afirmaciones.

    Indicación: Estudie la distribución inducida en $\{0,1\}$ por $x_1 + \ldots + x_n \bmod 2$ cuando existe un $i \in \{1,\ldots,n\}$ tal que $x_i \in_R \{0,1\}$ es independiente de x_j, para todo $j \neq i$.

Nota: Observe que C es computacionalmente todopoderoso. Esto significa que su protocolo no se puede basar en el hecho que C no puede resolver un problema (e.g., no puede esperar que C no pueda factorizar o calcular logaritmos discretos).