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

Examen : 13 de Diciembre

Profesor: Marcos Kiwi

Está estrictamente prohibido comentar el examen con cualquier persona excepto el profesor. Pueden consultar cualquier fuente bibliográfica pero sus soluciones pueden partir asumiendo sólo materia que se ha cubierto en el curso.

El examen se entrega en la oficina del profesor el viernes a las 12:00 hrs. No se aceptarán retrasos.

Problema 1:

1.- Pruebe que si m y n son dos enteros positivos impares entonces

$$\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right).$$

2.- Sean p y q números primos distintos, y sea $n = pq$. Suponga que g es un generador de $\mathcal{Z}_p^*$ y $\mathcal{Z}_q^*$ (i.e. las potencias de g módulo p corresponden a $\mathcal{Z}_p^*$ y las potencias de g módulo q corresponden a $\mathcal{Z}_q^*$). Sea x un entero relativamente primo a p y a q, y sean a y b tales que $g^a \equiv x \pmod{p}$ y $g^b \equiv x \pmod{q}$. De condiciones adicionales que garanticen la existencia de c tal que

$$g^c \equiv x \pmod{n}.$$

Asumiendo que sus condiciones se cumplen, muestre como calcular c eficientemente a partir de p, q, g, a, b.

Problema 2:

La intención de este problema es probar un famoso teorema obtenido en forma independiente por Sipser y Gács (1983). Tecnicamente el resultado dice que $BPP \subseteq \Sigma_2^P$. La anterior inclusión es una consecuencia directa del lema que se enuncia mas abajo.

1.- Sea L un lenguaje en BPP. Pruebe que existe un polinomio p y una máquina probabilista M que en entradas de largo n se detiene en a lo más $p(n)$ pasos (luego utiliza a lo más $p(n)$ bits aleatoreos), y tal que

$$\omega \in L \implies \Pr_{\rho\in\{0,1\}^{p(n)}}[\,M(\omega,\rho) = \mathit{acepta}\,] \geq 1 - \frac{1}{2^n}$$
$$\omega \notin L \implies \Pr_{\rho\in\{0,1\}^{p(n)}}[\,M(\omega,\rho) = \mathit{acepta}\,] \leq \frac{1}{2^n}.$$

<u>Nota 1</u>: Si X es una binomial de parámetros m y p entonces $\Pr[\,X \geq \alpha m\,] \leq 2^{mH(\alpha)}p^{\alpha m}$, donde $H(\alpha) = -\alpha\log_2(\alpha) - (1-\alpha)\log_2(1-\alpha)$.

2.- Dados $s, t \in \{0,1\}^{p(n)}$ denotaremos por $s \oplus t$ el XOR de s y t. Si $S = \{s_1, \ldots, s_{p(n)}\} \subset \{0,1\}^{p(n)}$ denotaremos por $S \oplus t$ al conjunto $\{s_1 \oplus t, \ldots, s_{p(n)} \oplus t\}$. Pruebe el siguiente

Lema 1 *Para n suficientemente grande, $\omega \in L$ si y sólo si $\exists S = \{s_1, \ldots, s_{p(n)}\} \subset \{0,1\}^{p(n)}$ tales que $\forall t \in \{0,1\}^{p(n)}$, $S \oplus t$ contiene un elemento ρ tal que $M(\omega, \rho) = acepta$.*

Nota: La demostración más simple conocida del lemma enunciado consiste en primero probar que si $\omega \in L$ entonces

$$\Pr_{S \subset \{0,1\}^{p(n)} \text{ t.q. } |S| = p(n)} \left[\exists t \in \{0,1\}^{p(n)} \text{ t.q. } \forall \rho \in S \oplus t, M(\omega, \rho) \neq \mathit{acepta} \right] \quad < \quad 1\,,$$

y que si $\omega \notin L$ entonces cualquiera sea $S \subset \{0,1\}^{p(n)}$, $|S| = p(n)$,

$$\Pr_{t \in \{0,1\}^{p(n)}} \left[\exists \rho \in S \oplus t, M(\omega, \rho) = \mathit{acepta} \right] \quad < \quad 1\,.$$

Problema 3: Suponga que dos paises A y B quieren llegar a un acuerdo para prohibir tests nucleares. Ninguno de los paises confía en el otro, en ambos casos por buenas razones. Sin embargo, estan dispuestos a establecer un sistema de verificación a ser implantado en varias localidades del territorio de ambos paises. Cada sistema de verificación consiste de un sofisticado sismografo, un pequeño computador para interpretar las lecturas del sismografo y generar mensajes, y un radio-transmisor. Explique como se puede utilizar criptografía de clave pública de forma de lograr las siguientes condiciones:

- Cada país insiste en conocer el texto plano de todos los mensajes que emanan de su territorio para asegurarse que el sistema no es utilizado por el otro país para llevar adelante actividades de espionaje.
- Cada país insiste que el otro país no debe poder fabricar un mensaje de los sistemas que transmiten desde su territorio (i.e. un mensaje diciendo que todo esta bien, cuando de hecho el sismografo a detectado una violación del tratado).
- Cada país insiste que si el otro país falsamente afirma haber recibido notificación del sistema de una violación al tratado nuclear, entonces cualquier tercer país podrá determinar que, de hecho nunca se envió tal notificación.
- Los sistemas de verificación en ambos paises deben ser idénticos y deben ser construidos e instalados en forma conjunta por científicos de ambos paises.

Discuta la seguirdad del sistema que proponga, y muestre que se satisfacen las condiciones pedidas.

Nota: Puede asumir que el sistema construido por los científicos no puede ser alterado una vez instalado.

Problema 4: Asuma que A ha elegido dos primos impares distintos p y q y que desea comunicarselos a B utilizando un canal inseguro. A no desea que un adversario que se encuentre monitoreando el canal de comunicación obtenga información alguna con respecto a p y q.

A puede implementar el siguiente protocolo:

1. A le envía a B el entero $n = pq$
2. B elige y al azar en $\mathcal{Z}_n^*$ y le envía a A el entero $x = y^2 \bmod n$
3. A calcula las cuatro raices cuadradas módulo n de x, i.e. $y_0, n - y_0, y_1, n - y_1$, elige y' al azar entre ellas, y envía y' a B.
4. Si $y \neq y'$ e $y \neq n - y'$ entonces B calcula $\mathrm{mcd}(y + y', n)$ y obtiene la factorización de n.

1.- Pruebe que con probabilidad $1/2$ al final del protocolo B conoce p y q.

2.- Sea X un adversario que se encuentra monitoreando el canal de comunicación. Pruebe que después del primer paso del protocolo descrito, X puede impersonar tanto a A como a B (sin conocer p y q) de forma de generar mensajes (en el segundo y tercer paso del protocolo) cuya distribución de probabilidad conjunta es idéntica a aquella distribución que se observa cuando A y B llevan a cabo el protocolo. Luego, en la factorización de n, X no gana nada monitoreando el canal de comunicación.

3.- Si se repite l veces el protocolo de manera independiente, la probabilidad que B no obtenga la factorización de n es a lo más $1/2^l$. En el caso que $p \equiv q \equiv 3 \pmod 4$, muestre como se puede modificar el protocolo de forma que B obtenga la factorización de n con una sola ejecución del protocolo pero X nuevamente no gane nada monitoreando el canal de comunicación. (Explique porque su protocolo no funcionaría en el caso que $p \equiv 3 \pmod 4$ y $q \equiv 1 \pmod 4$.)

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 oir 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.

1. 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. A y B no comparten ninguna clave secreta de antemano. Asuma que C es un adversario pasivo, i.e. no puede alterar los mensajes transmitidos.

   Nota 1: Suponga que A y B poseen relojes sincronizados.

2. 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.

   Asumiendo que A y B saben que C esta interceptando sus comunicaciones pero que su mecanismo de intercepción tiene una probabilidad de error de 0.01, 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.

<u>Nota 2</u>: 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). Su solución debe ser incondicionalmente segura.