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

Tarea No. 4

Profesor: Marcos Kiwi *Fecha de entrega: Control 2*

Elija 4 de los siguientes 5 problemas

PROBLEMA 1: Suponga que se divide un mensaje $M \in \{0,1\}^*$ en bloques (agregando 0's a M si fuese necesario) de m bits $M_1, M_2, \ldots, M_N \in \{0,1\}^m$ y se tiene un criptosistema convencional (por ejemplo DES) con función de encripción E_k. Asumiendo que E_k es una función bien definida para toda clave $k \in \{0,1\}^m$ cuyo dominio y recorrido son $\{0,1\}^n$, $n < 2m$, se sugiere calcular el valor hash G del mensaje M de la siguiente forma:

1. $H_0 \in \{0,1\}^n$ valor inicial fijo y conocido.
2. $H_i = E_{M_i}(H_{i-1})$, $i = 1, \ldots, N$.
3. $G = H_N$.

Pruebe que dada una constante $\epsilon > 0$ y bloques $Q_1, Q_2, \ldots, Q_{N-2} \in \{0,1\}^m$ se pueden encontrar, con probabilidad al menos $1-\epsilon$ y realizando a lo más $O(2^{n/2})$ evaluaciones de la función de encripción, dos bloques $X, Y \in \{0,1\}^m$ tales que la concatenación de los bloques $Q_1, Q_2, \ldots, Q_{N-2}, X, Y$ forman un mensaje con valor hash G.

En caso de necesitarlo, especifique que supuestos razonables debe satisfacer el criptosistema utilizado para que su argumento sea válido.

Indicación: Recuerde que $(1+x)^n \leq e^{nx}$, para todo $x \geq 0$.

PROBLEMA 2: Estudiaremos el concepto de *sistemas públicos de firmas digitales de grupos.*

Suponga que una corporación requiere que para que un documento sea firmado en nombre de la corporación sus n vice-presidentes deben firmar el documento. Una posible forma de lograr lo anterior es que cada vice-presidente cree su propia firma digital utilizando un sistema de firmas digitales público. Sólo los documentos que contengan las firmas de los n vice-presidentes se considerarán firmados por la corporación. Este sistema es ineficiente pues requiere agregar n firmas a un documento para que este quede validado.

Los sistemas de firmas digitales de grupos solucionan el problema mencionado en el párrafo anterior. Esto se logra compartiendo una clave secreta entre los vice-presidentes. Sea k una clave secreta, y k_i la parte de la clave de propiedad del i-ésimo vice-presidente. En el momento de la firma el i-ésimo vice-presidente produce una firma parcial $sig_{k_i}(M)$ las cuales luego son combinadas para formar la firma $sig_k(M)$ del documento M.

Por ejemplo, consideremos RSA con clave pública (N, e) y clave secreta d. Una forma de implementar un sistema de firmas digitales de grupo como el discutido más arriba es que un cierto árbitro de confianza de todos genere una clave (p, q, e, d) (donde p y q son primos tales que $N = pq$, y $ed = 1 \bmod \varphi(N)$) haga público (N, e), le entregue al i-ésimo vice-presidente el valor d_i donde

$$d \;=\; d_1 + d_2 + \cdots + d_n \bmod \varphi(n)\,,$$

y luego el árbitro se auto-destruya.

Más tarde cuando los vice-presidentes quieran firmar un mensaje M el i-ésimo vice-presidente puede producir $\sigma_i = M^{d_i} \bmod N$ y luego en forma conjunta pueden calcular

$$\sigma \;=\; \prod_{i=1}^{n} \sigma_i \bmod N \;=\; \prod_{i=1}^{n} M^{d_i} \bmod N \;=\; M^d \bmod N\,,$$

que es la firma correcta de la corporación para el documento M.

Considere ahora el siguiente sistema de firmas: sea p primo y g un generador de $\mathbb{Z}_p^*$, $a \in \mathbb{Z}_{p-1}$ la clave secreta y $\beta = g^a \bmod p$ la clave pública. Para firmar un mensaje x se elije un número $k \in \mathbb{Z}_{p-1}$ y se calcula $\gamma = g^k \bmod p$ y $\delta = a\gamma + k - x \bmod (p-1)$. El par (γ, δ) es la firma. Para verificar la firma uno debe comprobar que $g^{x+\delta} \equiv_p \gamma\beta^\gamma$.

(i).- Describa un sistema de firmas digitales de grupo similar al basado en RSA pero basado en el sistema de firmas digitales recién descrito.

(ii).- Basándose en la parte anterior, y asumiendo que todos los vice–presidentes tienen acceso a una misma fuente de aleatoriedad, proponga un sistema de firmas digitales de grupo pero que no requiera un árbitro de confianza de todas las partes involucradas.

Problema 3: Sea $F : \{0,1\}^k \times \{0,1\}^l \to \{0,1\}^l$ una familia de funciones. Considere CBC MAC basado en F y definido sobre el espacio de mensajes M tal que $|M|$ es múltiplo de l. Pruebe que el sistema es inseguro (utilice que M puede tener distintos largos).

Problema 4: Recuerde que en el sistema de firmas de ElGamal la clave pública de un usuario consiste en un primo p, un generador $g \in \mathbb{Z}_p^*$, otro elemento $y \in \mathbb{Z}_p^*$ y la clave secreta es un entero $x \in \{1, \ldots, p{-}1\}$ tal que $g^x \equiv_p y$.

Para firmar un mensaje $m \in \mathbb{Z}_{p-1}$, el usuario elije al azar $k \in \mathbb{Z}_{p-1}^*$, calcula $r = g^k \bmod p$ y $s = k^{-1}(m - xr) \bmod (p{-}1)$ (aritmética en $\mathbb{Z}_{p-1}$). La firma de m es $\langle r, s\rangle$. Para validar la firma se verifica si $g^m \equiv_p y^r r^s$.

(i).- Pruebe que el sistema de firmas de ElGamal es inseguro cuando el mismo k se elije para calcular las firmas de dos mensajes m_0 y m_1 distintos.

(ii).- Pruebe que el sistema de firmas de ElGamal es inseguro cuando se usa $k, k{+}1, k{+}2, \ldots$ para firmar una secuencia de mensajes distintos $m_0, m_1, m_2, \ldots$ (donde k es elegido en $\mathbb{Z}_{p-1}^*$ y la aritmética es módulo p)

Problema 5: Sea p un primo fijo y g un generador de $\mathbb{Z}_p^*$, ambos públicamente conocidos. Sea ω una clave privada compartida por Alicia y Roberto quienes quieren establecer otra clave secreta común usando ω para autenticarse mutuamente. A ambos les preocupa ser víctima de un ataque de *diccionario* por parte de un adversario pasivo que pueda escuchar el protocolo de establecimiento de claves. También les preocupa que un adversario activo pueda iniciar el protocolo pretendiendo ser el otro o que intente un ataque *de hombre en el medio.* A Alicia y Roberto les gustaría usar una variante del protocolo básico de Diffie y Hellman en el cual Alicia le envía a Roberto g^x para x elegido al azar en $\{1,\ldots,p-1\}$, Roberto le envía a Alicia g^y para y elegido al azar en $\{1,\ldots,p-1\}$ y la clave establecida es $K = g^{xy}$ (donde toda la aritmética se realiza módulo p).

Para lograr sus objetivos Alicia y Roberto consideran dos posibles esquemas:

> (i).- Usar $K = g^{xy} + \omega \bmod p$ en vez de $K = g^{xy}$ (aquí asumimos que ω se puede interpretar como un elemento en $\mathbb{Z}_p$).
>
> (ii).- En vez de enviar g^x, Alicia envía $E_\omega(g^x)$ donde E es la función de encripción de un criptosistema simétrico pre-establecido (i.e., Alicia encripta g^x con la clave ω). Análogamente, Roberto en vez de enviar g^y, envía $E_\omega(g^y)$. Alicia y Roberto decriptan los mensajes recibidos y proceden como en el caso típico de Diffie y Hellman.

Compare la seguridad de ambos esquemas. ¿Qué recomendaciones le haría a Alicia y Roberto?