Ejercicios

5. Semana 5

5.1. Características de la Criptografía de clave pública. Complejidad computacional. Servicios de seguridad

1. Sean A y B dos usuarios. Sean E_A y E_B las funciones de cifrado de un cifrado de clave pública de A y B, respectivamente.

   a) Describir un protocolo para que A envíe a B un mensaje M cifrado, con autenticidad de contenido.

   b) Describir un protocolo para que A envíe a B un mensaje M cifrado, con autenticidad de contenido y autenticidad de origen.

2. Sea $N > 1$ un número entero. Sea $\mathcal{M} = \mathcal{C} = \mathbb{Z}_N$. Consideremos un criptosistema afín $C \equiv (aM + b) \mod N$, con a y b enteros positivos, $\mathrm{mcd}(a, N) = 1$, y $M \in \mathbb{Z}_N$. Decidir si las siguientes afirmaciones son correctas o incorrectas:

   a) Es un cifrado de clave pública.

   b) El coste computacional de obtener la clave de descifrado (a', b') con $a' \equiv a^{-1} \mod N$ y $b' \equiv -a^{-1}b \mod N$ a partir de la clave de cifrado (a, b) es polinomial.

3. En un criptosistema de clave pública, sean $(\mathrm{E}_A, \mathrm{E}_A^{-1})$ y $(\mathrm{E}_B, \mathrm{E}_B^{-1})$ las funciones de cifrado y descifrado de A y B, respectivamente. Las funciones de cifrado son tales que $\mathrm{E}_A \mathrm{E}_B = \mathrm{E}_B \mathrm{E}_A$.

   Estudiemos el *cifrado de Massey-Omura*: El usuario A pretende enviar un mensaje M a B cifrado de manera segura.

   Protocolo:

Paso 1.	A envía a B:	$C = \mathrm{E}_A(M)$
Paso 2.	B envía a A:	$C' = \mathrm{E}_B \mathrm{E}_A(M)$
Paso 3.	A envía a B:	$C'' = \mathrm{E}_A^{-1} \mathrm{E}_B \mathrm{E}_A(M)$
Paso 4.	B:	obtiene el mensaje M

   Estudiar si:

   a) El protocolo garantiza confidencialidad del mensaje.

   b) En el paso 1 se garantiza autenticidad de contenido.

   c) En el paso 2 se garantiza autenticidad de origen.

5.2. Logaritmo discreto. Intercambio de claves de Diffie-Hellman. Criptosistema ElGamal

1. *a*) ¿$(\mathbb{Z}_{13}^*, \cdot)$ es un grupo? Justificar la respuesta.

   b) Calcular el número de generadores de $(\mathbb{Z}_{13}^*, \cdot)$.

   c) Comprobar que 2 es un generador de $(\mathbb{Z}_{13}^*, \cdot)$.

d) Calcular $\log_2 3 \mod 13$.

2. Dos usuarios A y B pretenden intercambiar una clave secreta por el método de Diffie-Hellman. La información pública es el número primo $p = 13$ y el generador $g = 2$ de $\mathbb{Z}_{13}^*$.

   A elige un número secreto $x_A = 2$ y B elige un número secreto $x_B = 3$.

   a) ¿Cuál es la información enviada por A?

   b) ¿Cuál es la información enviada por B?

   c) ¿Cuál es la clave intercambiada?

3. Dos usuarios A y B pretenden intercambiar una clave secreta por el método de Diffie-Hellman. La información pública es el número primo $p = 11$ y el generador $g = 8$ de $\mathbb{Z}_{11}^*$. Interceptamos la información enviada por A, $y_A = 10$, y la información enviada por B, $y_B = 2$. Sabiendo que $\log_8 10 = 5 \mod 11$, obtener la clave intercambiada.

4. Un usuario A quiere generar una clave pública para un criptosistema ElGamal. Para ello elige el número primo $p = 31$, el número 3 como generador de $\mathbb{Z}_{31}^*$ y $x = 7$ como clave privada.

   a) Generar la clave pública de A.

   b) Cifrar el mensaje $M = 23$ mediante el criptosistema ElGamal para enviárselo a A, eligiendo $b = 4$.

   c) Si A recibe el mensaje cifrado $(15, 27)$, hallar el mensaje en claro que ha sido enviado a A.

5. Sea el número primo $p = 139$. Pretendemos generar un par clave pública-clave privada para un cifrado de ElGamal, para lo cual vamos a seleccionar un elemento g del grupo multiplicativo $\mathbb{Z}_{139}^*$ que posea un orden "grande". Sabemos que $g^{\mathrm{ord}(g)} \equiv 1 \mod 139$. Nuestro objetivo es trabajar dentro del conjunto

$$\{g, g^2, \ldots, g^{\mathrm{ord}(g)}\}.$$

   a) Se pide seleccionar un elemento g de orden mayor o igual que 23.

   b) Suponiendo que elegimos $g = 9$ y la clave privada $x = 131$, hallar la clave pública correspondiente.

   c) Un usuario A con las claves pública-privada del apartado anterior recibe el mensaje $(113, 13)$. Descifrar el mensaje.

6. Es importante no utilizar repetidamente el valor aleatorio b para cifrar en cifrados ElGamal. Supongamos que la clave pública para un cifrado ElGamal de un usuario A es $(p, g, y) = (1163, 701, 543)$.

   Un usuario B pretende enviar a A confidencialmente los mensajes $M_1 = 100$ y $M_2 = 200$. Para ello elige $b = 207$ y cifra los dos mensajes con el mismo valor de b:

$$\begin{array}{ll} r_1 \equiv g^b \mod p, & r_2 \equiv g^b \mod p, \\ s_1 \equiv M_1 y^b \mod p, & s_2 \equiv M_2 y^b \mod p. \end{array}$$

a) Calcular los mensajes cifrados (r_1, s_1) y (r_2, s_2).

b) Un adversario intercepta la comunicación, obtiene (r_1, s_1) y (r_2, s_2) y consigue conocer M_1. Demostrar que puede descifrar el segundo mensaje, siempre que exista s_1^{-1} mód p.

5.3. Criptosistema RSA

1. Supongamos
$$n = pq = 7811, \quad \phi(n) = 7632,$$
con p, q primos distintos. Calcular p y q.

2. La clave pública RSA de un usuario es $(n, e) = (391, 117)$ y la clave privada $(p, q, d) = (17, 23, d)$. Calcular d.

3. La clave pública RSA de un usuario es $(n, e) = (143, 113)$. Descubrimos que $\phi(143) = 120$. Encontrar la clave privada.

4. La clave pública RSA de un usuario es $(n, e) = (55, 9)$. La clave privada es $(p, q, d) = (11, 5, 9)$.

   a) Cifrar $M = 2$.

   b) Descifrar $C = 3$.

5. La clave pública RSA de un usuario es $(n, e) = (55, e)$. La clave privada es (p, q, d). Ciframos $M_1 = 50$ y obtenemos $C_1 = 30$. Supongamos que calculamos
$$\log_{30} 50 = 3 \mod 55.$$
Descifrar $C_2 = 20$.

6. Calcular el número total de mensajes y el número de ellos que quedan sin cifrar con el algoritmo RSA para $p = 97$, $q = 109$, $e = 865$.

7. Las claves públicas RSA de los usuarios A, B son:
$$(n, e_A) = (527, 13), \quad (n, e_B) = (527, 19).$$
El cifrado del mensaje M es:
$$C_A = 377, \quad C_B = 346.$$
Calcular M por un ataque de módulo común.

8. La clave pública RSA de un usuarios A es $(n, e) = (187, 19)$. El cifrado de un mensaje M es $C = 114$. Obtener M por un ataque cíclico.