Soluciones

5. Semana 5

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

1. *a*) Protocolo:

   A y B deben acordar utilizar una función resumen $H(\cdot)$.

A envía:	$C = \mathrm{E}_B(M)$ y $h = H(M)$
B recibe:	C y h
calcula:	$\mathrm{E}_B^{-1}(C) = \mathrm{E}_B^{-1}\,\mathrm{E}_B(M) = M$ y $H(M)$
y verifica:	si $H(M) = h$

   b) Protocolo:

   A y B deben acordar utilizar una función resumen $H(\cdot)$ y una firma. Acuerdan que la firma será el resumen del mensaje.

A calcula:	$C = \mathrm{E}_B(M)$, $h = H(M)$ y $f = \mathrm{E}_A^{-1}(h)$
envía:	C y f
B recibe:	C y f
calcula:	$\mathrm{E}_B^{-1}(C) = \mathrm{E}_B^{-1}\,\mathrm{E}_B(M) = M$, $\mathrm{E}_A(f) = \mathrm{E}_A\,\mathrm{E}_A^{-1}(h) = h$, y $H(M)$
y verifica:	si $H(M) = h$

   Observemos que si $H(M) = h$ el receptor B verifica la firma de A y la integridad del mensaje.

2. *a*) Incorrecta.

   b) Correcta.

3. *a*) Correcto. El protocolo garantiza confidencialidad del mensaje Para obtener M:
   interceptando C, se necesita E_A^{-1} (privada)
   interceptando C', se necesita E_B^{-1} y E_A^{-1} (privadas)
   interceptando C'', se necesita E_B^{-1} (privada)

   b) Incorrecto. Cualquiera puede enviar a A un mensaje cifrado con la clave pública de A.

   c) Incorrecto. Las funciones de cifrado E_A y E_B son públicas. El mensaje puede enviarlo cualquiera.

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

1. *a*) $(\mathbb{Z}_{13}^*, \cdot)$ es un grupo porque $(\cdot)$ es asociativo, tiene elemento neutro (1) y todos los elementos tienen inverso (13 es primo).

b) 4.

c) Los divisores positivos de 12 son $1, 2, 3, 4, 6, 12$.

$$\begin{array}{ll} 2^1 \equiv 2 \not\equiv 1 \pmod{13}, & 2^2 \equiv 4 \not\equiv 1 \pmod{13}, \\ 2^3 \equiv 8 \not\equiv 1 \pmod{13}, & 2^4 \equiv 3 \not\equiv 1 \pmod{13}, \\ 2^6 \equiv 12 \not\equiv 1 \pmod{13}, & \end{array}$$

$\mathrm{ord}(2) = 12$. Por tanto, 2 es un generador de $(\mathbb{Z}_{13}^*, \cdot)$.

d) 4.

2. a) La información enviada por A es $y_A = 4$.
   b) La información enviada por B es $y_B = 8$.
   c) La clave intercambiada es $K = 12$.

3. $K = 10$.

4. a) $(31, 3, 17)$.
   b) $(19, 6)$.
   c) $M = 16$.

5. a) La factorización de $138 = 2 \cdot 3 \cdot 23$. Los elementos de $\mathbb{Z}_{139}^*$ son de órdenes $2, 3, 6, 23$ o mayores que 23. Los elementos de órdenes menores o iguales que 6 son
$$\{1, 138, 42, 96, 43, 97\}.$$
Los restantes tienen orden mayor o igual que 23.
   b) $(139, 9, 86)$.
   c) $M = 100$.

6. a) $(r_1 = 313, s_1 = 1032)$, $(r_2 = 313, s_2 = 901)$.
   b) Dado que $r_1 = r_2$, se tiene que
$$M_2 \equiv s_2 s_1^{-1} M_1 \equiv 200 \pmod{p}.$$

5.3. Criptosistema RSA

1. Sabemos que $\phi(n) = (p-1)(q-1) = n + 1 - (p+q)$. Es decir
$$p + q = n + 1 - \phi(n).$$
Podemos obtener p, q resolviendo el sistema:
$$\left. \begin{array}{l} pq = 7811 \\ p + q = 7811 + 1 - 7632 = 180 \end{array} \right\}$$
De la segunda ecuación obtenemos $q = 180 - p$.
Sustituyendo en la primera
$$p(180 - p) = 7811 \Rightarrow p^2 - 180p + 7811 = 0 \Rightarrow \left\{ \begin{array}{l} p = 73,\ q = 107 \\ \text{o} \\ p = 107,\ q = 73. \end{array} \right.$$

2. $d = 349$

3. $(p, q, d) = (13, 11, 17)$

4.
   a) El cifrado de 2 es 17.
   b) El descifrado de 3 es 48.

5. El descifrado de 20 es 25.

6. El número total de mensajes es 10573. El número de mensajes que quedan sin cifrar es 10573.

7. $13, 19$ son primos relativos. Utilizamos el algoritmo de Euclides extendido para calcular u, v tales que $1 = u13 + v19$. Obtenemos:

   $$1 = 3 \cdot 13 + (-2) \cdot 19.$$

   Entonces

   $$M \equiv M^{3\cdot 13+(-2)\cdot 19} \equiv M^{3\cdot 13} \cdot M^{(-2)\cdot 19} \equiv (M^{13})^3 \cdot (M^{19})^{(-2)} \equiv 377^3 \cdot 346^{-2}$$
   $$\equiv 377^3 \cdot (346^{-1})^2 \mod 527.$$

   Calculamos $346^{-1} \mod 527$ aplicando el algoritmo extendido de Euclides. Obtenemos:

   $$346^{-1} \equiv 428 \mod 527.$$

   Calculamos $377^3 \mod 527$, $428^2 \mod 527$ aplicando el algoritmo de potenciación modular. Obtenemos:

   $$377^3 \equiv 435 \mod 527, \quad 428^2 \equiv 315 \mod 527.$$

   Por tanto,

   $$M \equiv 435 \cdot 315 \equiv 137025 \equiv 5 \mod 527.$$
   $$M = 5.$$

   Comprobación:

   Cifrando $M = 5$ con la clave pública de A obtenemos

   $$5^{13} \equiv 377 \mod 527$$

   y cifrando $M = 5$ con la clave pública de B obtenemos

   $$5^{19} \equiv 346 \mod 527.$$

8.
   $$C \equiv M^{19} \equiv 114 \mod 187.$$

   El ataque cíclico consiste en hacer

   - $C_0 = C$

- Calcular sucesivos cifrados $C_i \equiv C_{i-1}^e \mod n$, hasta que $C_i = C$.
- Entonces $M \equiv C_{i-1} \mod n$.

Utilizamos el algoritmo de potenciación modular para calcular los cifrados sucesivos:

i	C_i
0	$C_0 \equiv 114 \mod 187$
1	$C_1 \equiv 114^{19} \equiv 113 \mod 187$
2	$C_2 \equiv 113^{19} \equiv 158 \mod 187$
3	$C_3 \equiv 158^{19} \equiv 91 \mod 187$
4	$C_4 \equiv 91^{19} \equiv 114 \mod 187$

$$M \equiv C_3 \equiv 91 \mod 187$$