Redes de Comunicaciones 2
25 de abril de 2022

Apellidos: ____
Nombre: ____

Problema 1	Problema 2	Total Problemas

Supón que estás intentando espiar la comunicación entre Alice y Bob. Esto es lo que has logrado averiguar:

- Están intercambiando mensajes con un método que preserva la confidencialidad, la integridad y la autenticidad de los mensajes.
- La estructura de cada mensaje enviado es sobre digital + cifrado simétrico de (mensaje + firma digital), con 2 dígitos dedicados al sobre digital y otros 2 a la firma digital. El sobre digital contiene la clave simétrica, cifrada para que sea confidencial.
- Para la firma digital se usa la función de hash H(m) = (3m + 5) mod 19. Esta función se aplica sobre el mensaje completo.
- Para el cifrado simétrico se usa un cifrado por bloques en modo CBC. El algoritmo, conocido, calcula $C_i = E_k[(P_i + C_{i-1}) \; mod \; 10]$, donde k es la clave simétrica, de acuerdo con la tabla definida más abajo. Para utilizarlo, considera cada dígito del texto en claro un bloque. El vector de inicialización es VI = 7.
- Conoces la clave pública de Alice. $K_A^+ = (43, 85)$.
- Conoces la clave pública de Bob. $K_B^+ = (29, 95)$.
- Interceptas el mensaje 254883157624.

	$(P_i + C_{i-1}) \; mod \; 10$										
Clave de cifrado		0	1	2	3	4	5	6	7	8	9
	0	9	1	3	5	4	2	0	5	8	5
	1	9	7	9	9	8	8	1	8	0	8
	2	4	0	1	1	7	2	4	6	0	2
	3	5	3	5	5	3	7	7	9	3	0
	4	4	5	8	2	3	1	0	0	0	1
	5	6	5	1	0	8	3	9	7	2	4
	6	8	1	1	6	7	0	3	8	1	7
	7	9	1	7	4	0	8	2	3	6	5
	8	0	4	9	6	5	7	2	1	5	6
	9	0	0	5	7	9	8	2	4	5	3

A partir de esta información debes:

1) (4 pts) Criptoanalizar el mensaje y obtener el correspondiente mensaje en claro

Interceptamos el mensaje completo 254883157624
Sabemos que $K_B^+ = (29, 95)$. Como el módulo (95) es pequeño, podemos factorizarlo, y enseguida observamos que
5 * 19 = 95, luego $p_B = 5$, $q_B = 19$. Entonces z = 72.
Luego $e.d \equiv 1 \; mod \; 72 = (1 + k.72) \rightarrow d = {}^{(1+k.72)}/_{29}. Si \; k = 2, d = 5.$
Luego $K_B^- = (5, 95)$.

Los 2 primeros dígitos (25) tienen que ser el sobre del mensaje, es decir, la clave simétrica cifrada con la clave pública de Bob.
Si $K_B^+(K_s) = 25 \rightarrow K_s = K_B^-(25) = 25^5\ mod\ 95 = 5$.

Ahora vamos a descifrar 4883157624. Si para cifrar hacemos Cifrado = $K_E[(P_i + C_{i-1})\ mod\ 10]$, entonces descifrado = $K_D(C_i) - C_{i-1}$

$P_1 = (K_D(4) - 7)\ mod\ 10 = (9 - 7)\ mod\ 10 = 2$
$P_2 = (K_D(8) - 4)\ mod\ 10 = (4 - 4)\ mod\ 10 = 0$
$P_3 = (K_D(8) - 8)\ mod\ 10 = (4 - 8)\ mod\ 10 = 6$
$P_4 = (K_D(3) - 8)\ mod\ 10 = (5 - 8)\ mod\ 10 = 7$
$P_5 = (K_D(1) - 3)\ mod\ 10 = (2 - 3)\ mod\ 10 = 9$
$P_6 = (K_D(5) - 1)\ mod\ 10 = (1 - 1)\ mod\ 10 = 0$
$P_7 = (K_D(7) - 5)\ mod\ 10 = (7 - 5)\ mod\ 10 = 2$
$P_8 = (K_D(6) - 7)\ mod\ 10 = (0 - 7)\ mod\ 10 = 3$

Los dos últimos dígitos corresponden a la firma digital, así no interesan.
El mensaje es entonces m = 20679023

2) (2 pts) ¿Qué mensaje deberías enviar a Bob para que crea que el mensaje en claro que Alice le envía es 123456?

Nuevo mensaje= 123456
Igual que hicimos con la clave de Bob, sabemos que $K_A^+ = (43, 85)$. Factorizamos el módulo (85). Enseguida se observa que 17 * 5 = 85, luego $p_A = 17, q_B = 5$. Luego $z = (p-1)(q-1) = 64$
Como debe ser
$e.d \equiv 1 \, mod \, 64 = (1 + k.64) \rightarrow d = {}^{(1+k.64)}/_{43} . Si \, k = 2, d = 3.$
Luego $K_A^- = (3, 85)$.

Primero calculamos la firma digital
H(123456) = (3*123456 + 5) mod 19 = 6
$firma =$ K_A^-(H(m)) = K_A^-(6) = $6^3 \, mod \, 85 = 46$
$K_S(m + firma) = K_S(12345646)$

$$C_1 = K_E[(P_1 + VI) \, mod \, 10] = K_E[(1+7) \, mod \, 10] \quad = 2$$
$$C_2 = K_E[(P_2 + C_1) \, mod \, 10] = K_E[(2+2) \, mod \, 10] \quad = 8$$
$$C_3 = K_E[(P_3 + C_2) \, mod \, 10] = K_E[(3+8) mod \, 10] \quad = 5$$
$$C_4 = K_E[(P_4 + C_3) \, mod \, 10] = K_E[(4+5) \, mod \, 10] \quad = 4$$
$$C_5 = K_E[(P_5 + C_4) \, mod \, 10] = K_E[(5+4) mod \, 10] \quad = 4$$
$$C_6 = K_E[(P_6 + C_5) \, mod \, 10] = K_E[(6+4) mod \, 10] \quad = 6$$
$$C_7 = K_E[(P_7 + C_6) \, mod \, 10] = K_E[(4+6) mod \, 10] \quad = 6$$
$$C_8 = K_E[(P_8 + C_7) \, mod \, 10] = K_E[(6+6) mod \, 10] \quad = 1$$

Luego el mensaje que debemos enviar a Bob es 2528544661

Alternativa:
Si el cálculo se hizo con clave pública de Alice = (37,85), entonces la correspondiente clave privada sería (45, 85), y la firma digital sería:
$firma =$ K_A^-(H(m)) = K_A^-(6) = $6^{45} \, mod \, 85 = 61.$
Con lo cual el cifrado de los 2 últimos dígitos sería:
$$C_7 = K_E[(P_7 + C_6) \, mod \, 10] = K_E[(6+6) mod \, 10] \quad = 1$$
$$C_8 = K_E[(P_8 + C_7) \, mod \, 10] = K_E[(1+1) mod \, 10] \quad = 1$$

Con lo cual el mensaje que enviaríamos a Bob sería 2528544611