Examen Ordinario Criptografia y Seguridad Informatica.

Declaro que he realizado la prueba evaluación conforme a las indicaciones facilitadas y sin haber utilizado ningun recurso que no haya sido autorizado expresamente por el profesorado, asumiendo toda la responsabilidad administrativa y disciplinaria que pudiera derivarse de la utilización de medios defraudatorios.

Asignatura: Criptografia y Seguridad Informatica.

Titulación: Ingenieria Informatica.

Fecha: 09/06/2020

Nombre y Apellidos: Jorge Rodriguez Fraile.

DNI: 02592368S

NIA: 100405951

Firma: Jorge R

Parte 1:

a) $F(Cert_B)$ declave pública. $p=17$ $g=7$ $Y_B=11$ $x_B=5$

$Cert_B=(17,7,11,H(H))$ Hallamos la firma ElGamal de $(17,7,11)$

$\sigma_{Cert_B} = Sign(priv\_key; H_{cert}) = ElGamal(4,1)$

$H\_Cert = p \text{ XOR } g \text{ XOR } Y = 1 \text{ XOR } 7 \text{ XOR } 7 \text{ XOR } 1 \text{ XOR } 1 = 1$

$$\begin{array}{r} 0001 \\ 0001 \\ 0111 \\ \oplus\ 0111 \\ 0001 \\ \hline 0001 \end{array}$$

$ElGamal(4,1)$

$r = g^k \bmod p = 3^4 \bmod 17 = 13$

$s = (H\_Cert - x_B \cdot r)\, k^{-1} \bmod p-1 = (1+4\cdot 13)\cdot 4 \bmod 16 = 212 \bmod 16 = 4$

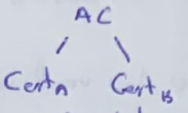
$k^{-1} = 13^{-1} = 1 \bmod 17 = 4$

$17 = 13\cdot 1 + 4$ $\quad 1 = 13 - 3(17-13) = 13 - 3\cdot 17 + 3\cdot 13 = 4\cdot 13 + 17$

$13 = 4\cdot 3 + 1$ $\quad 1 = 13 - 4\cdot 3$

La firma es: $(r,s) = (11,4)$

6) Verificar Cert_A y su cadena.



Cert_A(17, 3, 14, (11, 12))

Hallamos el hash de los datos para hacer la verificación ElGamal.

$H(Cert\_A) = 1 \oplus 7 \oplus 3 \oplus 1 \oplus 4 =$ 0100 ⊕ 0001 ⊕ 0111 ⊕ 0011 ⊕ 0001 $= 0000 = 0$

Verificamos con AC

$V_1 = y_{AC}^{r} \cdot r^{s} \bmod p = 13^{11} \cdot 11^{13} \bmod 17 = (13^{5})^{2} \cdot 13 \cdot (11^{4})^{3} \bmod 17 = 1$

($13^2 \cdot 13 \cdot 4^3$; $4 \cdot 13$)

$V_2 = g^{H} \bmod p = 3^{0} \bmod 17 = 1$

Coinciden V_1 y V_2 verificado el certificado de A expedido por AC

Verificar AC

$H(Cert\_AC) = 1 \oplus 7 \oplus 3 \oplus 1 \oplus 3 =$ 0001 ⊕ 0111 ⊕ 0011 ⊕ 0001 ⊕ 0011 $= 0111 = 7$

$V_1 = 13^{11} \cdot 11^{13} \bmod 17 = 4 \cdot 13 \cdot 11 \bmod 17 = 13^3 \cdot 4^3 \cdot 11 \bmod 17 = 11$

$V_2 = 3^{7} \bmod 17 = 11$

Coincide V_1 y V_2, verificada la autofirma de AC, por lo tanto son correctos los certificados.

Parte 2:

c) $k\_Session = 35$ $k = 9$ Como $A \xrightarrow[\text{ElGamal}]{\text{Transport}} B$

$C_1 = g^{k} \bmod p = 7^{9} \bmod 17 = 10$ Para poder hallar k_s desde B

$k = y_B^{k} \bmod p = 11^{9} \bmod 17 = 6$ Clave

$C_2 = k\_Session \cdot k \bmod p = 35 \cdot 6 \bmod 17 = 6$ Cifrado

A le enviará a B: $C_1 = 10$ $C_2 = 6$ y B con su X_B lo podrá descifrar y conseguir el 35.

d) $C_1 = 10$ $C_2 = 6$ $X\_B = 5$

$k = C_1^{X\_B} \bmod p = 10^{5} \bmod 17 = 6$

$k\_Session = C_2 k^{-1} \bmod p = 6 \cdot 3 \bmod 17 = 1 + 17 \cdot 2 = 35$

$6^{-1} = 1 \bmod 17 = 3$

$17 = 6 \cdot 2 + 5$ $\quad 1 = 6 - 17 + 2 \cdot 6 = 3 \cdot 6 - 17$

$6 = 5 \cdot 1 + 1$ $\quad 1 = 6 - 5$

B ha descifrado ela k-session, pero al ser mod 17 le da 1, que es congruente con 1+17·2

Jorge R.F

Parte 3:

e) k_Encrypt y k_MAC a partir de k_sesion=35, derivo mediante kDF

kDF = Desplazamiento_1_bit_izq(Bin(k_sesion)) xor DC

35 = 10 00 11 = 0010 0011

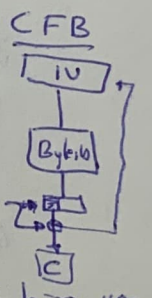
DC = 1101 1100
13 12

kDF = 0101 0110 XOR 1101 1100 = 1000 1010
más significativos menos significativos.

k_Encrypt = 1000
k_MAC = 1010

Parte 4:

f) A cifra M = 62E ID_A = 5 IV = 1100 = 12



M = 62E = 0110 0010 1110

C = E(k_Encrypt; ID_A || M) = E(1000; 0101 0110 0010 1110)M

CYPHER = 4 bits significativos(Not Bytesub(1100;1000))

Suponiendo que se refiere a que es byte izq = 1100 y byte derecho = 1000

1º bloque) Bytesub(C8) = e8

0101 Not(e8) = 0001 0111

C_1 = 0001 XOR 0101 = 0100

2º bloque 0110, IV = 0100 i Bytesub(4 8) = 52
0101 0010

Not(52) = 1010 1101

C_2 = 1010 XOR 0110 = 1000

3º bloque 0010, IV = 1000 i Byte sub(8 8) = C4
1100 0100

Not(C4) = 0011 1011

C_3 = 0011 XOR 0010 = 0001

4º bloque 1110, IV = C_3 = 0001) Byte sub(1 8) = AD
1010 1101

NOT(AD) = 0101 0010

C_4 = 0101 XOR 1110 = 1011

El mensaje M=62E cifrado con el ID_A=5, da lugar a: 0100 1000 0001 1011
C = 481B$_{16}$

3

Parte 5:

g) Calcular MAC sobre C= 481B K_MAC= 1010
IV= 1000

MAC= MACF(K_MAC; C) Al ser CBC, nos quedamos solo con la salida del último bloque.

MACF = Desplazamiento_1_bit_izq [Not (input)] xor k_MAC

1er bloque 0100, IV=1000) Not(1000 ⊕ 0100) = Not(1100) = 0011
Desplazamiento izq (0011) = 0110
0110 ⊕ 1010 = 1100

2° bloque 1000, IV=1100) Not(1000 ⊕ 1100) = Not(0100) = 1011
1011 ⇒ 0111
0111 ⊕ 1010 = 1101

3° bloque 0001, IV=1101) Not(0001 ⊕ 1101) = 0011
0011 ⇒ 0110
0110 ⊕ 1010 = 1100

4° bloque 1011, IV=1100) Not(1011 ⊕ 1100) = Not(0111) = 1000
1000 ⇒ 0001
0001 ⊕ 1010 = 1011

El código de autenticación MAC sobre el mensaje $C = 481B_{(16)}$ con la clave $K\_MAC = 1010_{(2)}$ es:

$MAC(1010_{(2)}; 481B)_{(16)} = 1011_{(2)} = B_{(16)} = 11_{(10)}$