uc3m | Universidad Carlos III de Madrid

Criptografía y seguridad informática
Cryptography and computer security

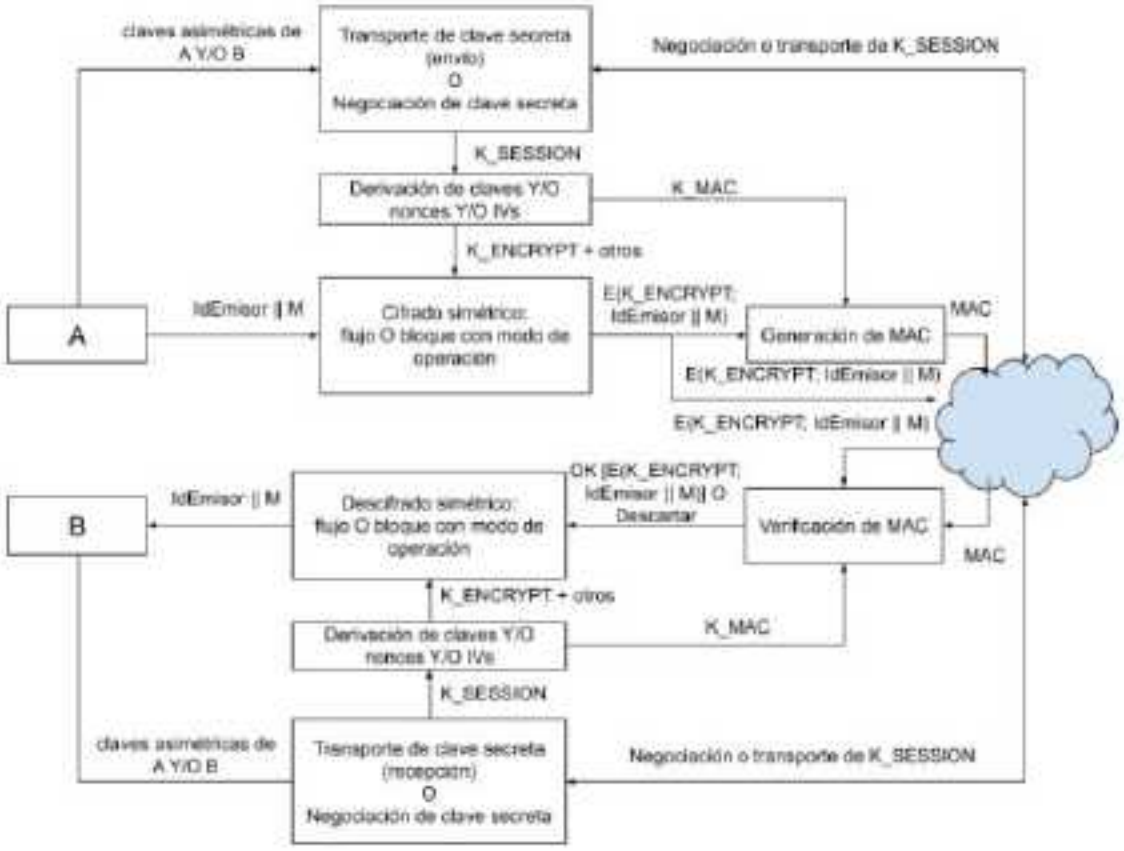
Grado en Ingeniería Informática
Bachelor in Computer Science and Engineering
Doble Grado en Ingeniería Informática y Administración de Empresas

Examen final / Final exam

Convocatoria ordinaria / Ordinary sitting
9 de Junio 2020 / June 9th 2020

DESCRIPCIÓN DEL SISTEMA

Dos entidades denominadas [A] y [B] se van a comunicar de forma segura utilizando un sistema que sigue el siguiente diseño.



El diseño del sistema considera los siguientes algoritmos o esquemas:

Intercambio de clave secreta	**Cifrado simétrico**
Transporte_EG	Bloque_CFB
Firma o autenticación del mensaje	**Firma de certificados de clave pública**
MAC_Bloque_Modo_operación	Firma_Cert_EG_con_Resumen

En este sistema que sigue el modelo Encrypt-then-MAC, si [A] quiere enviar un mensaje a [B], debe seguir los siguientes pasos:

1. Intercambio de clave secreta:
    a. [A] y [B] intercambian una clave secreta K_SESSION.
2. Cifrado del mensaje en claro y autenticación del mensaje cifrado
    a. [A] deriva a partir de la clave secreta K_SESSION los valores que necesitará para los siguientes pasos. La función de derivación de claves KDF se define más adelante.
    b. [A] cifra simétricamente el mensaje precedido de su identificador: C = E(K_ENCRYPT; IdEmisor || M). El cifrador simétrico CIPHER se define más adelante.
    c. [A] genera un código de autenticación MAC sobre el mensaje cifrado C: MAC = MACF(K_MAC; C). La función MACF específica se define más adelante.

[A] y [B] poseen los pares de claves asimétricas que se muestran en la siguiente tabla, estando la clave pública certificada por la Autoridad de Certificación AC. Las claves de la Autoridad de Certificación también se muestran en la tabla, estando también la clave pública de la Autoridad de Certificación certificada, en este caso por ella misma.

Uso de las claves y propietario	**Privada**	**Pública**	**Certificado**
Emisión de certificados; AC	X_AC=4	p=17,g=3,Y_AC=13	CertAC = (p,,g,Y_AC, σ_CertAC) = (17,3,13,(11,13))
Cifrado EG; [A]	X_A=16	p=17,g=3,Y_AC=14	CertA = (p,,g,Y_A, σ_CertA) = (17,3,14,(11,12))
Cifrado EG; [B]	X_B=5	p=17,g=7,Y_B=11	CertB = (p,,g,Y_B, σ_CertB) = (17,7,11,?)

La firma de los certificados emitidos por AC se genera sobre el resultado de aplicar la función resumen H_cert sobre los elementos de la clave pública incluidos en el certificado. La función H_CERT se define más adelante.

σ_CertX = Sign(PRIV_KEY_AC; H_CERT(elementos certificado X))

Representación de datos

El alfabeto considerado se detalla en la siguiente tabla, así como su codificación numérica en valor decimal:

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Por tanto, cada elemento del mensaje en hexadecimal, se representará en binario con 4 bits.

Definición de KDF

KDF = DESPLAZAMIENTO_1_bit_IZQ (BIN(key)) xor DC
Se aplica una rotación de un bit a la izquierda por cada bloque de cuatro bits. Los cuatro bits más significativos (izquierda) se convertirán en la K_ENCRYPT del cifrador del mensaje y los cuatro menos significativos (derecha) pasarán a ser la K_MAC.
Por ejemplo: K = 12 = 0001 0010 □ desplazamiento 0010 0100 □ 0010 0100 xor 1101 1100 (DC) = 1111 1000, de modo que K_ENCRYPT = 1111 y K_MAC=1000

Definición de CIPHER modo CFB

CIPHER=4bitsMasSignificativos(NOT[ByteSub(IV ; K_ENCRYPT)]), donde el IV necesario tiene el valor C (1100 bin).
1)Se calcula la salida de la función ByteSub (del algoritmo AES);
2) A la salida, en binario, se le aplica la operación NOT;
3) El resultado se corresponde con los 4 bit más significativos (izquierda)

Definición de MACF modo CBC

MACF=DESPLAZAMIENTO_1_bit_IZQ[NOT(input)] xor K_MAC , donde el IV necesario se corresponde con 8 (1000 bin)

1) A la entrada se aplica la operación NOT;
2) Se rota un bit a la izquierda;
3) Se hace un XOR con K_MAC

Definición de H_CERT

H_CERT = p xor g xor Y ,
Si un número está compuesto por más de un dígito, se realizará xor de los dígitos independientemente. Cada dígito se convertirá en 4 bits para realizar el xor. Por ejemplo: si p=23 g=8 e Y=16
HASH = 2 XOR 3 XOR 8 XOR 1 XOR 6 = 0010 xor 0011 xor 1000 xor 0001 xor 0110

CUESTIONES A RESOLVER

Parte 1: Certificados de clave pública (0,6 puntos)

a) Calcule la firma del certificado de clave pública de B.
b) Verifique el certificado de A Cert_A, incluyendo la verificación de la cadena de certificación.

Parte 2: Intercambio de clave secreta (0,25 puntos)

c) A elige el valor decimal 35 como clave secreta K_SESSION. Calcule cómo A le transmite a B dicha K_SESSION en el sistema dado. Utilice el valor k=9 si es necesario.
d) Muestre cómo B obtiene K_SESSION de lo que le ha enviado A en el apartado anterior.

Parte 3: Derivación de claves (0,15 puntos)

e) Calcule los valores K_ENCRYPT y K_MAC, utilizando el valor de K_SESSION indicado anteriormente.

Parte 4: Cifrado del mensaje (0,5 puntos)

f) Muestre cómo A cifra el mensaje de 3 caracteres hexadecimales M = 62E, usando los valores obtenidos en el apartado anterior. Recuerde que debe preceder este mensaje del identificador de A, que es “5”.

Parte 5: Generación del MAC (0,5 puntos)

g) Muestre cómo A calcula el MAC sobre el mensaje cifrado obtenido en el apartado anterior, usando la clave K_MAC obtenida en el apartado e.