Universidad
Carlos III de Madrid

Grupo COSEC· Dpto. Informática

Universidad Carlos III de Madrid

Elaboración de un esquema de comunicación seguro

COSEC
Curso 2019/2020

1 Instrucciones

El objetivo de esta actividad es que acabéis de diseñar un sistema de comunicación seguro (autenticación de mensajes y confidencialidad) siguiendo cierto modelo e incluyendo determinados algoritmos y esquemas criptográficos. Además de la especificación del sistema, tendréis que utilizar el sistema para que A envíe un mensaje a B y B conteste a A con otro mensaje, proporcionando los cálculos en detalle.

A cada grupo se le indicará un modelo que su sistema debe seguir y una variante que determinará algunos de los algoritmos que debe utilizar.

La sección Modelos generales explica los dos modelos que los sistemas pueden seguir. La sección Algoritmos y esquemas describe los algoritmos y esquemas criptográficos que los sistemas podrían incluir. El Anexo A. Lista de variantes lista los algoritmos y esquemas concretos que están asociados a cada variante, y el Anexo B. Plantilla para el informe contiene una plantilla para guiaros en la elaboración del documento que tenéis que entregar. La sección 5 Criterios de evaluación detalla los criterios de evaluación.

2 Modelos generales

2.1 Modelo Sign-then-Encrypt

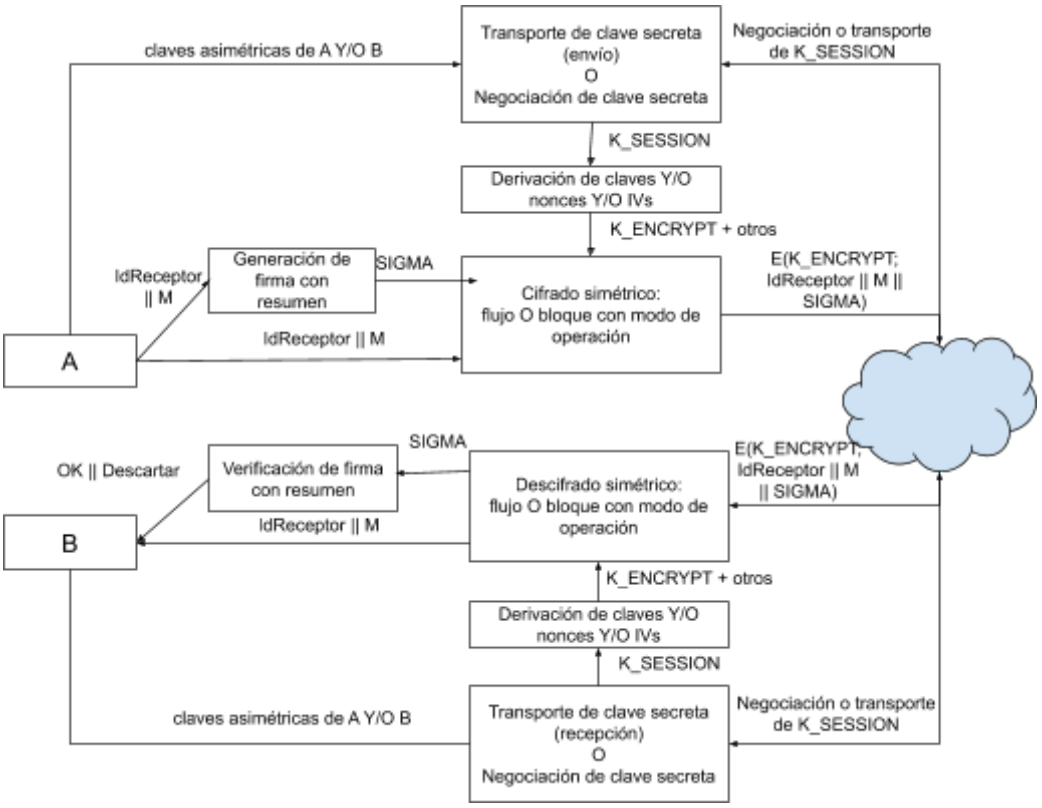

Figura 1: Modelo Sign-then-Encrypt

Explicaremos el modelo como si A fuera a enviar un mensaje a B, pero se debe tener en cuenta que funcionaría de forma similar en la dirección contraria (B envía un mensaje a A).

En el modelo Sign-then-Encrypt, si A quiere enviar un mensaje a B:

1. Determina la clave secreta K_SESSION que se utilizará en esta sesión (para ambos sentidos de la comunicación), bien mediante negociación con el otro interlocutor (negociación de clave) o bien eligiendo dicha clave y cifrándola para enviarla de forma segura al interlocutor.
2. Adjunta el identificador del destinatario al mensaje M (IdReceptor || M) y firma ambos con un esquema de firma combinada con función resumen H: SIGMA = S(K_{V,A}; H(IdReceptor || M))
3. Deriva a partir de la clave secreta K_SESSION la clave simétrica de cifrado K_ENCRYPT y/o otros datos (eg., IV, NONCE, SEED...) que sean necesarios para proceder al cifrado simétrico del mensaje firmado.
4. Cifra simétricamente el mensaje firmado: C = E(K_ENCRYPT; IdReceptor || M || SIGMA)

Tras recibir el mensaje protegido de A, B deberá obtener la clave secreta K_SESSION (bien mediante negociación o descifrándola), derivar la clave simétrica de cifrado K_ENCRYPT (y/o otros posibles datos), descifrar el mensaje firmado (IdReceptor || M || SIGMA) y, por último, verificar la firma SIGMA sobre el mensaje (IdReceptor || M).

2.2 Modelo Encrypt-then-MAC

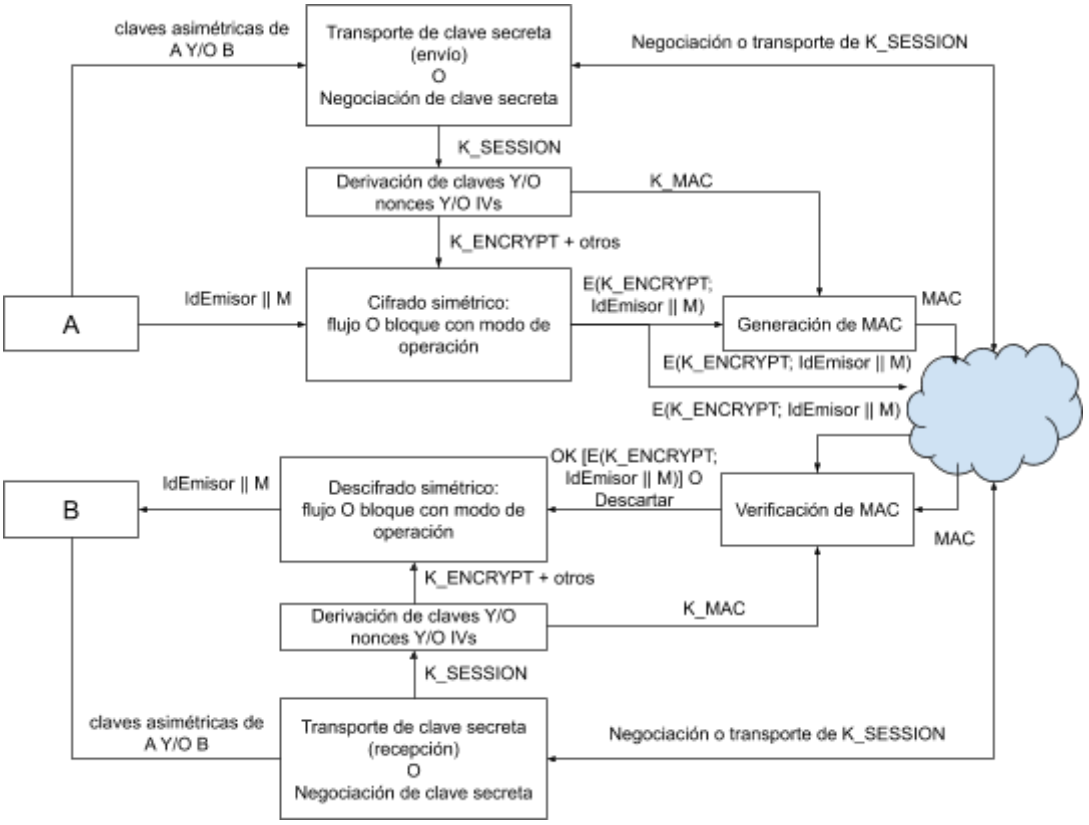

Figura 2: Modelo Encrypt-then-MAC

Explicaremos el modelo como si A fuera a enviar un mensaje a B, pero se debe tener en cuenta que funcionaría de forma similar en la dirección contraria (B envía un mensaje a A).

En el modelo Encrypt-then-MAC, si A quiere enviar un mensaje a B:

1. Determina la clave secreta K_SESSION que se utilizará en esta sesión (para ambos sentidos de la comunicación), bien mediante negociación con el otro interlocutor (negociación de clave) o bien eligiendo dicha clave y cifrándola para enviarla de forma segura al interlocutor.
2. Deriva a partir de la clave secreta K_SESSION la clave simétrica de cifrado K_ENCRYPT y/o otros datos (eg., IV, NONCE, SEED...) que sean necesarios para proceder al cifrado simétrico del mensaje. También derivará una segunda clave simétrica K_MAC que se utilizará para generar códigos de autenticación.
3. Cifra simétricamente el mensaje precedido del identificador del emisor: C = E(K_ENCRYPT; IdEmisor || M)
4. Genera un código de autenticación MAC sobre el mensaje cifrado C.

Tras recibir el mensaje protegido de A, B deberá obtener la clave secreta K_SESSION (bien mediante negociación o descifrándola), derivar la clave simétrica de cifrado K_ENCRYPT (y/o otros posibles datos) y la clave de autenticación K_MAC, verificar el código de autenticación MAC y, por último, descifrar el mensaje cifrado C.

3 Algoritmos y esquemas

3.1 Intercambio de clave secreta

Los dos modelos consideran que los interlocutores se intercambian una clave secreta (denominada K_SESSION) a partir de la cual ambos interlocutores derivarán otros secretos necesarios para cifrar el mensaje de forma simétrica o generar códigos de autenticación de mensajes. Esta clave es la misma para toda la sesión considerada en la comunicación, por tanto, solo se ejecutará una única vez. Se proponen tres posibles variantes:

- **Negociación_DH** indica que ambos interlocutores ejecutan el protocolo de intercambio de clave secreta Diffie-Hellman. Nótese que se requiere que las claves públicas utilizadas en este protocolo estén autenticadas para evitar ataques de Persona-en-el-Medio.
- **Transporte_RSA** especifica que el interlocutor que inicia la comunicación elige la clave secreta y la envía al otro interlocutor cifrándola asimétricamente con el algoritmo de cifrado RSA (es lo que se ha denomina algunas veces en el material del curso como cifrado híbrido).
- **Transporte_EG** especifica que el interlocutor que inicia la comunicación elige la clave secreta y la envía al otro interlocutor cifrándola asimétricamente con el algoritmo de cifrado EG (es lo que se ha denomina algunas veces en el material del curso como cifrado híbrido).

3.2 Funciones de derivación de claves

Una vez ambos interlocutores conocen la clave secreta K_SESSION, dependiendo del

modelo/variante, necesitarán un conjunto de datos/secretos para proceder con la autenticación y/o el cifrado del mensaje. Estos datos pueden ser NONCE (para inicialización de modo de operación CTR), IV (para inicializar otros modos de operación), SEED (semilla para inicializar un LFSR), K_MAC (como clave de autenticación en el caso que se tenga que generar un MAC), …

Deberéis elegir cómo se deben derivar estos nuevos datos/secretos. Pueden ser procesamientos sencillos (un NOT, un XOR con una constante, …) o podéis utilizar un LFSR o una función resumen… La cuestión es que ambos interlocutores generen el material suficiente a partir de K_SESSION.

3.3 Cifrado simétrico

En cada modelo se especifica la utilización de un algoritmo de cifrado simétrico según las siguientes opciones:

- **Bloque_CBC.** Se utilizará un cifrador de bloque operado bajo el modo de operación CBC. Deberéis especificar el cifrador de bloque concreto de forma similar a los utilizados en los problemas de la asignatura (por ejemplo, como los de los problemas del examen parcial del curso 2018-2019).
- **Bloque_CFB.** Se utilizará un cifrador de bloque operado bajo el modo de operación CFB. Deberéis especificar el cifrador de bloque concreto de forma similar a los utilizados en los problemas de la asignatura (por ejemplo, como los de los problemas del examen parcial del curso 2018-2019).
- **Bloque_OFB.** Se utilizará un cifrador de bloque operado bajo el modo de operación OFB. Deberéis especificar el cifrador de bloque concreto de forma similar a los utilizados en los problemas de la asignatura (por ejemplo, como los de los problemas del examen parcial del curso 2018-2019).
- **Bloque_CTR.** Se utilizará un cifrador de bloque operado bajo el modo de operación CTR. Deberéis especificar el cifrador de bloque concreto de forma similar a los utilizados en los problemas de la asignatura (por ejemplo, como los de los problemas del examen parcial del curso 2018-2019).
- **Flujo_LFSR.** Se utilizará para cifrar un cifrador de flujo con secuencia cifrante (*keystream*) generada por un LFSR. Deberéis especificar el polinomio de conexión del LFSR[1].

3.4 Firma del mensaje / Generación de MAC

Cada modelo incluye bien la Firma del mensaje (modelo Sign-then-Encrypt) o Generación de MAC (Encrypt-then-MAC) para autenticar los mensajes intercambiados.

- **Firma_Mensaje_RSA_con_Resumen** utilizará el algoritmo de firma RSA combinado con una función resumen (que no se especifica) para generar firmas sobre los mensajes. Deberéis especificar una función resumen concreta (similar a las utilizadas en los problemas de la asignatura).
- **Firma_Mensaje_EG_con_Resumen** utilizará el algoritmo de firma ElGamal

[1] Podéis buscar polinomios adecuados aquí [1] o aquí [2].

combinado con una función resumen (que no se especifica) para generar firmas sobre los mensajes. Deberéis especificar una función resumen concreta (similar a las utilizadas en los problemas de la asignatura).
- **MAC_HMAC_con_Resumen** generará un MAC basándose en HMAC. Deberéis especificar una función resumen concreta (similar a las utilizadas en los problemas de la asignatura).
- **MAC_Bloque_Modo_operación** generará un MAC basándose en un cifrador de bloque operado bajo cierto modo de operación (recordad que el MAC es la salida del procesamiento del último bloque). Deberéis especificar un cifrador de bloque concreto de forma similar a los utilizados en los problemas de la asignatura (por ejemplo, como los de los problemas del examen parcial del curso 2018-2019).

3.5 Firma de certificados de clave pública

Todas las claves públicas utilizadas en el sistema deberán estar certificadas por una Autoridad de Certificación. Deberéis incluir en la memoria la descripción de la generación de dichos certificados (incluyendo también la inicialización de las claves y certificados de la Autoridad de Certificación).

La primera vez que un interlocutor utilice una clave pública deberá verificar el correspondiente certificado. Nótese que A y B deberán poseer parejas de claves diferentes para el intercambio de claves secretas (DH), el cifrado de mensajes y la firma de mensajes (en cada caso se especificarán solo las que se deban utilizar en el modelo/variante concreto asignado) .

Cada modelo considera que la Autoridad de Certificación utiliza determinado algoritmo de firma para firmar los certificados de clave pública entre los dos siguientes:

- **Firma_Cert_RSA_con_Resumen.** La AC utilizará el algoritmo RSA combinado con una función resumen (que no se especifica) para generar la firma. Deberéis especificar una función resumen concreta (similar a las utilizadas en los problemas de la asignatura).
- **Firma_Cert_EG_con_Resumen.** La AC utilizará el algoritmo ElGamal (de firma) combinado con una función resumen (que no se especifica) para generar la firma. Deberéis especificar una función resumen concreta (similar a las utilizadas en los problemas de la asignatura).

4 Notas adicionales

Reutilización de algoritmos de diseño propio

En el caso que se deban utilizar en diferentes sitios del sistema algoritmos del mismo tipo que no hayan sido definidos en este documento y, por el contrario, deban ser especificados por los estudiantes (e.g., función resumen, cifrador de bloque, LFSR…), será posible reutilizarlos.

Coherencia entre las representaciones de datos y el tamaño de los espacios de trabajo

Se debe tener especial cuidado en que la representación de datos y su procesamiento por bloques (función resumen, cifrado simétrico,...) sea coherente con los tamaños de los espacios de trabajo de los algoritmos. Por ejemplo, si las claves simétricas de cifrado tienen una longitud de 8 bits (256 posibles valores), y se debe cifrar con RSA o ElGamal, el módulo debe ser suficientemente grande para poder representar y procesar dichos valores sin problemas.

5 Criterios de evaluación

Deberéis elaborar un informe en Google Docs, compartiendo desde el principio una carpeta dedicada a la actividad y el propio documento con los profesores de teoría/problemas de vuestros grupos. Al finalizar la actividad, entregaréis un enlace al documento y una versión en PDF. El informe debe satisfacer la guía en Anexo B. Plantilla para el informe.

	Muy deficiente	Insuficiente	Suficiente-Bien	Bien-Notable	Sobresaliente
Especificación del sistema de acuerdo a las instrucciones	0	0.15	0.3	0.45	0.6
Detalle de los cálculos de la comunicación entre las partes	0	0.15	0.3	0.45	0.6
Corrección del sistema y los cálculos	0	0.1	0.2	0.3	0.4
Presentación del informe y explicaciones aportadas	0	0.1	0.2	0.3	0.4

Anexo A. Lista de variantes

Variantes	Modelo	Intercambio de clave secreta	Cifrado simétrico	Firma del mensaje/Generación de MAC	Firma de certificados de clave pública
Var1	**Sign-then-Encrypt**	Negociación_DH	Bloque_CBC	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_RSA_con_Resumen
Var2	**Sign-then-Encrypt**	Negociación_DH	Bloque_CBC	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_EG_con_Resumen
Var3	**Sign-then-Encrypt**	Negociación_DH	Bloque_CFB	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_RSA_con_Resumen
Var4	**Sign-then-Encrypt**	Negociación_DH	Bloque_CFB	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_EG_con_Resumen
Var5	**Sign-then-Encrypt**	Negociación_DH	Bloque_OFB	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_RSA_con_Resumen
Var6	**Sign-then-Encrypt**	Negociación_DH	Bloque_OFB	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_EG_con_Resumen
Var7	**Sign-then-Encrypt**	Negociación_DH	Bloque_CTR	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_RSA_con_Resumen
Var8	**Sign-then-Encrypt**	Negociación_DH	Bloque_CTR	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_EG_con_Resumen
Var9	**Sign-then-Encrypt**	Negociación_DH	Flujo_LFSR	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_RSA_con_Resumen
Var10	**Sign-then-Encrypt**	Negociación_DH	Flujo_LFSR	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_EG_con_Resumen
Var11	**Sign-then-Encrypt**	Transporte_RSA	Bloque_CBC	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_RSA_con_Resumen
Var12	**Sign-then-Encrypt**	Transporte_RSA	Bloque_CBC	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_EG_con_Resumen
Var13	**Sign-then-Encrypt**	Transporte_RSA	Bloque_CFB	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_RSA_con_Resumen
Var14	**Sign-then-Encrypt**	Transporte_RSA	Bloque_CFB	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_EG_con_Resumen
Var15	**Sign-then-Encrypt**	Transporte_RSA	Bloque_OFB	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_RSA_con_Resumen
Var16	**Sign-then-Encrypt**	Transporte_RSA	Bloque_OFB	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_EG_con_Resumen
Var17	**Sign-then-Encrypt**	Transporte_RSA	Bloque_CTR	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_RSA_con_Resumen
Var18	**Sign-then-Encrypt**	Transporte_RSA	Bloque_CTR	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_EG_con_Resumen
Var19	**Sign-then-Encrypt**	Transporte_RSA	Flujo_LFSR	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_RSA_con_Resumen
Var20	**Sign-then-Encrypt**	Transporte_RSA	Flujo_LFSR	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_EG_con_Resumen

Var21	**Sign-then-Encrypt**	Transporte_EG	Bloque_CBC	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_RSA_con_Resumen
Var22	**Sign-then-Encrypt**	Transporte_EG	Bloque_CBC	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_EG_con_Resumen
Var23	**Sign-then-Encrypt**	Transporte_EG	Bloque_CFB	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_RSA_con_Resumen
Var24	**Sign-then-Encrypt**	Transporte_EG	Bloque_CFB	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_EG_con_Resumen
Var25	**Sign-then-Encrypt**	Transporte_EG	Bloque_OFB	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_RSA_con_Resumen
Var26	**Sign-then-Encrypt**	Transporte_EG	Bloque_OFB	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_EG_con_Resumen
Var27	**Sign-then-Encrypt**	Transporte_EG	Bloque_CTR	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_RSA_con_Resumen
Var28	**Sign-then-Encrypt**	Transporte_EG	Bloque_CTR	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_EG_con_Resumen
Var29	**Sign-then-Encrypt**	Transporte_EG	Flujo_LFSR	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_RSA_con_Resumen
Var30	**Sign-then-Encrypt**	Transporte_EG	Flujo_LFSR	Firma_Mensaje_RSA_con_Resumen	Firma_Cert_EG_con_Resumen
Var31	**Sign-then-Encrypt**	Negociación_DH	Bloque_CBC	Firma_mensaje_EG_con_Resumen	Firma_Cert_RSA_con_Resumen
Var32	**Sign-then-Encrypt**	Negociación_DH	Bloque_CBC	Firma_mensaje_EG_con_Resumen	Firma_Cert_EG_con_Resumen
Var33	**Sign-then-Encrypt**	Negociación_DH	Bloque_CFB	Firma_mensaje_EG_con_Resumen	Firma_Cert_RSA_con_Resumen
Var34	**Sign-then-Encrypt**	Negociación_DH	Bloque_CFB	Firma_mensaje_EG_con_Resumen	Firma_Cert_EG_con_Resumen
Var35	**Sign-then-Encrypt**	Negociación_DH	Bloque_OFB	Firma_mensaje_EG_con_Resumen	Firma_Cert_RSA_con_Resumen
Var36	**Sign-then-Encrypt**	Negociación_DH	Bloque_OFB	Firma_mensaje_EG_con_Resumen	Firma_Cert_EG_con_Resumen
Var37	**Sign-then-Encrypt**	Negociación_DH	Bloque_CTR	Firma_mensaje_EG_con_Resumen	Firma_Cert_RSA_con_Resumen
Var38	**Sign-then-Encrypt**	Negociación_DH	Bloque_CTR	Firma_mensaje_EG_con_Resumen	Firma_Cert_EG_con_Resumen
Var39	**Sign-then-Encrypt**	Negociación_DH	Flujo_LFSR	Firma_mensaje_EG_con_Resumen	Firma_Cert_RSA_con_Resumen
Var40	**Sign-then-Encrypt**	Negociación_DH	Flujo_LFSR	Firma_mensaje_EG_con_Resumen	Firma_Cert_EG_con_Resumen
Var41	**Sign-then-Encrypt**	Transporte_RSA	Bloque_CBC	Firma_mensaje_EG_con_Resumen	Firma_Cert_RSA_con_Resumen
Var42	**Sign-then-Encrypt**	Transporte_RSA	Bloque_CBC	Firma_mensaje_EG_con_Resumen	Firma_Cert_EG_con_Resumen
Var43	**Sign-then-Encrypt**	Transporte_RSA	Bloque_CFB	Firma_mensaje_EG_con_Resumen	Firma_Cert_RSA_con_Resumen

Var44	**Sign-then-Encrypt**	Transporte_RSA	Bloque_CFB	Firma_mensaje_EG_con_Resumen	Firma_Cert_EG_con_Resumen
Var45	**Sign-then-Encrypt**	Transporte_RSA	Bloque_OFB	Firma_mensaje_EG_con_Resumen	Firma_Cert_RSA_con_Resumen
Var46	**Sign-then-Encrypt**	Transporte_RSA	Bloque_OFB	Firma_mensaje_EG_con_Resumen	Firma_Cert_EG_con_Resumen
Var47	**Sign-then-Encrypt**	Transporte_RSA	Bloque_CTR	Firma_mensaje_EG_con_Resumen	Firma_Cert_RSA_con_Resumen
Var48	**Sign-then-Encrypt**	Transporte_RSA	Bloque_CTR	Firma_mensaje_EG_con_Resumen	Firma_Cert_EG_con_Resumen
Var49	**Sign-then-Encrypt**	Transporte_RSA	Flujo_LFSR	Firma_mensaje_EG_con_Resumen	Firma_Cert_RSA_con_Resumen
Var50	**Sign-then-Encrypt**	Transporte_RSA	Flujo_LFSR	Firma_mensaje_EG_con_Resumen	Firma_Cert_EG_con_Resumen
Var51	**Sign-then-Encrypt**	Transporte_EG	Bloque_CBC	Firma_mensaje_EG_con_Resumen	Firma_Cert_RSA_con_Resumen
Var52	**Sign-then-Encrypt**	Transporte_EG	Bloque_CBC	Firma_mensaje_EG_con_Resumen	Firma_Cert_EG_con_Resumen
Var53	**Sign-then-Encrypt**	Transporte_EG	Bloque_CFB	Firma_mensaje_EG_con_Resumen	Firma_Cert_RSA_con_Resumen
Var54	**Sign-then-Encrypt**	Transporte_EG	Bloque_CFB	Firma_mensaje_EG_con_Resumen	Firma_Cert_EG_con_Resumen
Var55	**Sign-then-Encrypt**	Transporte_EG	Bloque_OFB	Firma_mensaje_EG_con_Resumen	Firma_Cert_RSA_con_Resumen
Var56	**Sign-then-Encrypt**	Transporte_EG	Bloque_OFB	Firma_mensaje_EG_con_Resumen	Firma_Cert_EG_con_Resumen
Var57	**Sign-then-Encrypt**	Transporte_EG	Bloque_CTR	Firma_mensaje_EG_con_Resumen	Firma_Cert_RSA_con_Resumen
Var58	**Sign-then-Encrypt**	Transporte_EG	Bloque_CTR	Firma_mensaje_EG_con_Resumen	Firma_Cert_EG_con_Resumen
Var59	**Sign-then-Encrypt**	Transporte_EG	Flujo_LFSR	Firma_mensaje_EG_con_Resumen	Firma_Cert_RSA_con_Resumen
Var60	**Sign-then-Encrypt**	Transporte_EG	Flujo_LFSR	Firma_mensaje_EG_con_Resumen	Firma_Cert_EG_con_Resumen
Var61	**Encrypt-then-MAC**	Negociación_DH	Bloque_CBC	MAC_HMAC_con_Resumen	Firma_Cert_RSA_con_Resumen
Var62	**Encrypt-then-MAC**	Negociación_DH	Bloque_CBC	MAC_HMAC_con_Resumen	Firma_Cert_EG_con_Resumen
Var63	**Encrypt-then-MAC**	Negociación_DH	Bloque_CFB	MAC_HMAC_con_Resumen	Firma_Cert_RSA_con_Resumen
Var64	**Encrypt-then-MAC**	Negociación_DH	Bloque_CFB	MAC_HMAC_con_Resumen	Firma_Cert_EG_con_Resumen
Var65	**Encrypt-then-MAC**	Negociación_DH	Bloque_OFB	MAC_HMAC_con_Resumen	Firma_Cert_RSA_con_Resumen
Var66	**Encrypt-then-MAC**	Negociación_DH	Bloque_OFB	MAC_HMAC_con_Resumen	Firma_Cert_EG_con_Resumen

Var67	**Encrypt-then-MAC**	Negociación_DH	Bloque_CTR	MAC_HMAC_con_Resumen	Firma_Cert_RSA_con_Resumen
Var68	**Encrypt-then-MAC**	Negociación_DH	Bloque_CTR	MAC_HMAC_con_Resumen	Firma_Cert_EG_con_Resumen
Var69	**Encrypt-then-MAC**	Negociación_DH	Flujo_LFSR	MAC_HMAC_con_Resumen	Firma_Cert_RSA_con_Resumen
Var70	**Encrypt-then-MAC**	Negociación_DH	Flujo_LFSR	MAC_HMAC_con_Resumen	Firma_Cert_EG_con_Resumen
Var71	**Encrypt-then-MAC**	Transporte_RSA	Bloque_CBC	MAC_HMAC_con_Resumen	Firma_Cert_RSA_con_Resumen
Var72	**Encrypt-then-MAC**	Transporte_RSA	Bloque_CBC	MAC_HMAC_con_Resumen	Firma_Cert_EG_con_Resumen
Var73	**Encrypt-then-MAC**	Transporte_RSA	Bloque_CFB	MAC_HMAC_con_Resumen	Firma_Cert_RSA_con_Resumen
Var74	**Encrypt-then-MAC**	Transporte_RSA	Bloque_CFB	MAC_HMAC_con_Resumen	Firma_Cert_EG_con_Resumen
Var75	**Encrypt-then-MAC**	Transporte_RSA	Bloque_OFB	MAC_HMAC_con_Resumen	Firma_Cert_RSA_con_Resumen
Var76	**Encrypt-then-MAC**	Transporte_RSA	Bloque_OFB	MAC_HMAC_con_Resumen	Firma_Cert_EG_con_Resumen
Var77	**Encrypt-then-MAC**	Transporte_RSA	Bloque_CTR	MAC_HMAC_con_Resumen	Firma_Cert_RSA_con_Resumen
Var78	**Encrypt-then-MAC**	Transporte_RSA	Bloque_CTR	MAC_HMAC_con_Resumen	Firma_Cert_EG_con_Resumen
Var79	**Encrypt-then-MAC**	Transporte_RSA	Flujo_LFSR	MAC_HMAC_con_Resumen	Firma_Cert_RSA_con_Resumen
Var80	**Encrypt-then-MAC**	Transporte_RSA	Flujo_LFSR	MAC_HMAC_con_Resumen	Firma_Cert_EG_con_Resumen
Var81	**Encrypt-then-MAC**	Transporte_EG	Bloque_CBC	MAC_HMAC_con_Resumen	Firma_Cert_RSA_con_Resumen
Var82	**Encrypt-then-MAC**	Transporte_EG	Bloque_CBC	MAC_HMAC_con_Resumen	Firma_Cert_EG_con_Resumen
Var83	**Encrypt-then-MAC**	Transporte_EG	Bloque_CFB	MAC_HMAC_con_Resumen	Firma_Cert_RSA_con_Resumen
Var84	**Encrypt-then-MAC**	Transporte_EG	Bloque_CFB	MAC_HMAC_con_Resumen	Firma_Cert_EG_con_Resumen
Var85	**Encrypt-then-MAC**	Transporte_EG	Bloque_OFB	MAC_HMAC_con_Resumen	Firma_Cert_RSA_con_Resumen
Var86	**Encrypt-then-MAC**	Transporte_EG	Bloque_OFB	MAC_HMAC_con_Resumen	Firma_Cert_EG_con_Resumen
Var87	**Encrypt-then-MAC**	Transporte_EG	Bloque_CTR	MAC_HMAC_con_Resumen	Firma_Cert_RSA_con_Resumen
Var88	**Encrypt-then-MAC**	Transporte_EG	Bloque_CTR	MAC_HMAC_con_Resumen	Firma_Cert_EG_con_Resumen
Var89	**Encrypt-then-MAC**	Transporte_EG	Flujo_LFSR	MAC_HMAC_con_Resumen	Firma_Cert_RSA_con_Resumen

Var90	**Encrypt-then-MAC**	Transporte_EG	Flujo_LFSR	MAC_HMAC_con_Resumen	Firma_Cert_EG_con_Resumen
Var91	**Encrypt-then-MAC**	Negociación_DH	Bloque_CBC	MAC_Bloque_Modo_operación	Firma_Cert_RSA_con_Resumen
Var92	**Encrypt-then-MAC**	Negociación_DH	Bloque_CBC	MAC_Bloque_Modo_operación	Firma_Cert_EG_con_Resumen
Var93	**Encrypt-then-MAC**	Negociación_DH	Bloque_CFB	MAC_Bloque_Modo_operación	Firma_Cert_RSA_con_Resumen
Var94	**Encrypt-then-MAC**	Negociación_DH	Bloque_CFB	MAC_Bloque_Modo_operación	Firma_Cert_EG_con_Resumen
Var95	**Encrypt-then-MAC**	Negociación_DH	Bloque_OFB	MAC_Bloque_Modo_operación	Firma_Cert_RSA_con_Resumen
Var96	**Encrypt-then-MAC**	Negociación_DH	Bloque_OFB	MAC_Bloque_Modo_operación	Firma_Cert_EG_con_Resumen
Var97	**Encrypt-then-MAC**	Negociación_DH	Bloque_CTR	MAC_Bloque_Modo_operación	Firma_Cert_RSA_con_Resumen
Var98	**Encrypt-then-MAC**	Negociación_DH	Bloque_CTR	MAC_Bloque_Modo_operación	Firma_Cert_EG_con_Resumen
Var99	**Encrypt-then-MAC**	Negociación_DH	Flujo_LFSR	MAC_Bloque_Modo_operación	Firma_Cert_RSA_con_Resumen
Var100	**Encrypt-then-MAC**	Negociación_DH	Flujo_LFSR	MAC_Bloque_Modo_operación	Firma_Cert_EG_con_Resumen
Var101	**Encrypt-then-MAC**	Transporte_RSA	Bloque_CBC	MAC_Bloque_Modo_operación	Firma_Cert_RSA_con_Resumen
Var102	**Encrypt-then-MAC**	Transporte_RSA	Bloque_CBC	MAC_Bloque_Modo_operación	Firma_Cert_EG_con_Resumen
Var103	**Encrypt-then-MAC**	Transporte_RSA	Bloque_CFB	MAC_Bloque_Modo_operación	Firma_Cert_RSA_con_Resumen
Var104	**Encrypt-then-MAC**	Transporte_RSA	Bloque_CFB	MAC_Bloque_Modo_operación	Firma_Cert_EG_con_Resumen
Var105	**Encrypt-then-MAC**	Transporte_RSA	Bloque_OFB	MAC_Bloque_Modo_operación	Firma_Cert_RSA_con_Resumen
Var106	**Encrypt-then-MAC**	Transporte_RSA	Bloque_OFB	MAC_Bloque_Modo_operación	Firma_Cert_EG_con_Resumen
Var107	**Encrypt-then-MAC**	Transporte_RSA	Bloque_CTR	MAC_Bloque_Modo_operación	Firma_Cert_RSA_con_Resumen
Var108	**Encrypt-then-MAC**	Transporte_RSA	Bloque_CTR	MAC_Bloque_Modo_operación	Firma_Cert_EG_con_Resumen
Var109	**Encrypt-then-MAC**	Transporte_RSA	Flujo_LFSR	MAC_Bloque_Modo_operación	Firma_Cert_RSA_con_Resumen
Var110	**Encrypt-then-MAC**	Transporte_RSA	Flujo_LFSR	MAC_Bloque_Modo_operación	Firma_Cert_EG_con_Resumen
Var111	**Encrypt-then-MAC**	Transporte_EG	Bloque_CBC	MAC_Bloque_Modo_operación	Firma_Cert_RSA_con_Resumen
Var112	**Encrypt-then-MAC**	Transporte_EG	Bloque_CBC	MAC_Bloque_Modo_operación	Firma_Cert_EG_con_Resumen

Var113	**Encrypt-then-MAC**	Transporte_EG	Bloque_CFB	MAC_Bloque_Modo_operación	Firma_Cert_RSA_con_Resumen
Var114	**Encrypt-then-MAC**	Transporte_EG	Bloque_CFB	MAC_Bloque_Modo_operación	Firma_Cert_EG_con_Resumen
Var115	**Encrypt-then-MAC**	Transporte_EG	Bloque_OFB	MAC_Bloque_Modo_operación	Firma_Cert_RSA_con_Resumen
Var116	**Encrypt-then-MAC**	Transporte_EG	Bloque_OFB	MAC_Bloque_Modo_operación	Firma_Cert_EG_con_Resumen
Var117	**Encrypt-then-MAC**	Transporte_EG	Bloque_CTR	MAC_Bloque_Modo_operación	Firma_Cert_RSA_con_Resumen
Var118	**Encrypt-then-MAC**	Transporte_EG	Bloque_CTR	MAC_Bloque_Modo_operación	Firma_Cert_EG_con_Resumen
Var119	**Encrypt-then-MAC**	Transporte_EG	Flujo_LFSR	MAC_Bloque_Modo_operación	Firma_Cert_RSA_con_Resumen
Var120	**Encrypt-then-MAC**	Transporte_EG	Flujo_LFSR	MAC_Bloque_Modo_operación	Firma_Cert_EG_con_Resumen

Anexo B. Plantilla para el informe

A continuación se presenta el índice del informe que se debe presentar:

1. Datos de identificación

   Identificador del grupo, identificación de los integrantes del grupo, identificación del modelo y variante asignados.

2. Especificación del sistema

   2.1. Representación de datos
   Se detallará cómo se han representado los datos a procesar (alfabeto considerado, representación numérica o siguiendo algún estándar como ASCII, B64…)

   2.2. Algoritmos y esquemas
   Se describirán los algoritmos y esquemas que se utilicen en el sistema que los estudiantes hayan debido diseñar. Por ejemplo, funciones resumen, cifradores de bloque…

   2.3. Claves asimétricas
   Se listarán todas las parejas de claves asimétricas utilizadas en el sistema, incluyendo los certificados asociados a las claves públicas.

   2.4. Coherencia de representaciones y tamaños de bloques y espacios de trabajo
   Se justificará que las representaciones, tamaños de bloques y de espacios de trabajo de los algoritmos son coherentes.

3. Comunicación de las partes

   En esta parte del informe se utilizará el sistema para que A envíe un mensaje a B y B le envíe un mensaje de respuesta a A.

   Se deben detallar los cálculos que llevan a cabo ambas partes, tanto en la transmisión como en la recepción.

   Esta parte si se desea puede adoptar el formato típico de un problema de examen pero no es necesario. Sería suficiente con que se muestre como A genera el mensaje a transmitir (detallando cada paso según se considera en cada modelo), B lo recibe y procesa, y de forma similar para la respuesta de B a A.

Referencias

[1] https://en.wikipedia.org/wiki/Linear-feedback_shift_register#Some_polynomials_for_maximal_LFSRs

[2] https://users.ece.cmu.edu/~koopman/lfsr/index.html