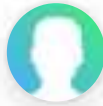


WUOLAH



Silvia_Perez_Valdericeda

www.wuolah.com/student/Silvia_Perez_Valdericeda



2480

Exámenes-cripto.pdf

Exámenes



2º Criptografía y Seguridad Informática



Grado en Ingeniería Informática



Escuela Politécnica Superior
Universidad Carlos III de Madrid



¿Harto de chapar
algo que **no te renta?**

¿Cuál es tu trabajo ideal?

Haz el test aquí

<http://bit.ly/necesitouncambio>



RESUMEN DE PROPUESTAS DE EXAMEN FINAL

SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN GRADO EN INGENIERÍA INFORMÁTICA CURSO 2009-2010

NOTA: Estas preguntas de examen y sus soluciones se publican como información adicional. Las soluciones son informativas (orientativas) y en ningún caso se podrá exigir responsabilidades a los profesores de la asignatura por ellas.

PROPUESTA DE EXAMEN 1 – ORDINARIA 1 - ESPAÑOL.....	3
PREGUNTAS DE RESPUESTA OBJETIVA.....	5
CUESTIONES.....	7
CUESTIÓN 1. Valor = 0,2 pts. Tiempo estimado: 5 min.	7
CUESTIÓN 2. Valor = 0,2 pts. Tiempo estimado: 10 min.	7
PROBLEMAS.....	9
PROBLEMA 1. Valor = 1,5 pto. Tiempo estimado: 20 min.	9
PROBLEMA 2. Valor = 1,5 pts. Tiempo estimado: 45 min.	11
PROPUESTA DE EXAMEN 1 – ORDINARIA 1 - INGLES.....	13
MULTIPLE-CHOICE QUESTIONS.....	15
SHORT-ANSWER QUESTIONS.....	17
QUESTION 1. Value = 0,2 pts. Estimated time: 5 min.	17
QUESTION 2. Value = 0,2 pts. Estimated time: 10 min.	17
PROBLEMS.....	19
PROBLEM 1. Value = 1,5 pt. Estimated time: 20 min.	19
PROBLEM 2. Value = 1,5 pts. Estimated time: 45 min.	21
PROPUESTA DE EXAMEN 1 – ORDINARIA 1 - SOLUCIÓN.....	23
PREGUNTAS DE RESPUESTA OBJETIVA - SOLUCIÓN.....	25
CUESTIONES - SOLUCIÓN.....	27
CUESTIÓN 1. Valor = 0,2 pts. Tiempo estimado: 5 min.	27
CUESTIÓN 2. Valor = 0,2 pts. Tiempo estimado: 10 min.	27
PROBLEMAS - SOLUCIÓN.....	28
PROBLEMA 1. Valor = 1,5 pto. Tiempo estimado: 20 min.	28
PROBLEMA 2. Valor = 1,5 pts. Tiempo estimado: 45 min.	29
PROPUESTA DE EXAMEN 2 – ORDINARIA 2.....	31
PREGUNTAS DE RESPUESTA OBJETIVA.....	33
CUESTIONES.....	35
CUESTIÓN 1. Valor = 0,2 pts. Tiempo estimado: 10 min.	35
CUESTIÓN 2. Valor = 0,2 pts. Tiempo estimado: 10 min.	35
PROBLEMAS.....	37
Problema 1. Valor = 1,5 pts. Tiempo estimado: 20 min.	37
Problema 2. Valor = 1,5 pts. Tiempo estimado: 45 min.	39
PROPUESTA DE EXAMEN 2 – ORDINARIA 2 – INGLÉS.....	41
MULTIPLE-CHOICE QUESTIONS.....	43
SHORT ANSWER QUESTIONS.....	45
QUESTION 1. Value = 0,2 pts. Estimated time: 10 min.	45
QUESTION 2. Value = 0,2 pts. Estimated time: 10 min.	45
PROBLEMS.....	47
PROBLEM 1. Value = 1,5 pts. Estimated time: 20 min.	47
PROBLEM 2. Value = 1,5 pts. Estimated time: 45 min.	49
PROPUESTA DE EXAMEN 2 – ORDINARIA 2 - SOLUCIÓN.....	51
PREGUNTAS DE RESPUESTA OBJETIVA- SOLUCIÓN.....	53
CUESTIONES - SOLUCIÓN.....	55
CUESTIÓN 1. Valor = 0,2 pts. Tiempo estimado: 10 min.	55
CUESTIÓN 2. Valor = 0,2 pts. Tiempo estimado: 10 min.	55
PROBLEMAS - SOLUCIÓN.....	56
Problema 1. Valor = 1,5 pts. Tiempo estimado: 20 min.	56
Problema 2. Valor = 1,5 pts. Tiempo estimado: 45 min.	59



¿Harto de chapar algo que **no te renta?**

Olvida tus apuntes este verano
y ponte a programar 🧑💻

Si no encuentras tu crush, por lo menos
dedícate a algo que te guste.



<http://bit.ly/necesitouncambio>



PROPUESTA DE EXAMEN 3 – EXTRAORDINARIA 1 - ESPAÑOL	61
PREGUNTAS DE RESPUESTA OBJETIVA.....	63
CUESTIONES.....	65
CUESTIÓN 1. Valor = 0,2 ptos. Tiempo estimado: 10 min.	65
CUESTIÓN 2. Valor = 0,2 ptos. Tiempo estimado: 10 min.	65
PROBLEMAS.....	67
Problema 1. Valor = 1,5 ptos. Tiempo estimado: 40 min.....	67
Problema 2. Valor = 1,5 ptos. Tiempo estimado: 40 min.....	71
PROPUESTA DE EXAMEN 3 – EXTRAORDINARIA 1 - INGLÉS.....	73
MULTIPLE-CHOICE QUESTIONS.....	75
SHORT ANSWER QUESTIONS.....	77
QUESTION 1. Value = 0,2 pts. Estimated time: 10 min.	77
QUESTION 2. Value = 0,2 pts. Estimated time: 10 min.	77
PROBLEMS.....	79
Problem 1. Value = 1,5 pts. Estimated time: 40 min.	79
Problem 2. Value = 1,5 pts. Estimated time: 40 min.	83
PROPUESTA DE EXAMEN 3 – EXTRAORDINARIA 1 – SOLUCIÓN.....	85
PREGUNTAS DE RESPUESTA OBJETIVA.....	86
CUESTIONES.....	88
CUESTIÓN 1. Valor = 0,2 ptos. Tiempo estimado: 10 min.	88
CUESTIÓN 2. Valor = 0,2 ptos. Tiempo estimado: 10 min.	88
PROBLEMAS.....	89
Problema 1. (SOLUCIÓN).....	89
Problema 2. (SOLUCIÓN).....	90
PROPUESTA DE EXAMEN 4 – EXTRAORDINARIA 2.....	91
PREGUNTAS DE RESPUESTA OBJETIVA.....	93
CUESTIONES.....	95
CUESTIÓN 1. Valor = 0,2 ptos. Tiempo estimado: 10 min.	95
CUESTIÓN 2. Valor = 0,2 ptos. Tiempo estimado: 10 min.	95
PROBLEMAS.....	97
Problema 1. Valor = 1,5 ptos. Tiempo estimado: 45 min.....	97
Problema 2. Valor = 1,5 ptos. Tiempo estimado: 30 min.....	99
PROPUESTA DE EXAMEN 4 – EXTRAORDINARIA 1 – SOLUCIÓN.....	101
TEORÍA.....	102
CUESTIONES.....	104
QUESTION 1. Value = 0,2 ptos. Estimated time: 10 min.	104
QUESTION 2. Value = 0,2 ptos. Estimated time: 10 min.	104
PROBLEMAS.....	105
Problema 1. Valor = 1,5 ptos. Tiempo estimado: X.....	105
Problema 2. Valor = 1,5 ptos. Tiempo estimado: X.....	107
PROPUESTA DE EXAMEN 5 – ORDINARIA EXTRA 1 - ESPAÑOL	109
PREGUNTAS DE RESPUESTA OBJETIVA.....	111
CUESTIONES.....	113
CUESTIÓN 1. Valor = 0,2 ptos. Tiempo estimado: 10 min.	113
CUESTIÓN 2. Valor = 0,2 ptos. Tiempo estimado: 10 min.	113
PROBLEMAS.....	115
PROBLEMA 1. Valor = 1,5 ptos. Tiempo estimado: 40 min.	115
PROBLEMA 2. Valor = 0,5 ptos. Tiempo estimado: 15 min.	117
PROBLEMA 3. Valor = 1 pto. Tiempo estimado: 25 min.	119
PROPUESTA DE EXAMEN 5 – ORDINARIA EXTRA 1 - INGLÉS.....	121
MULTIPLE-CHOICE QUESTIONS.....	123
SHORT-ANSWER QUESTIONS.....	125
QUESTION 1. Value = 0,2 pt. Estimated time: 10 min.	125
QUESTION 2. Value = 0,2 pt. Estimated time: 10 min.	125
PROBLEMS.....	127
PROBLEM 1. Value = 1,5 pts. Estimated time: 40 min.	127
PROBLEM 2. Value = 0,5 pts. Estimated time: 15 min.	129
Problem 3. Value = 1 pt. Estimated time: 25 min.	131
PROPUESTA DE EXAMEN 5 – ORDINARIA EXTRA 1 - SOLUCIONES.....	133
PREGUNTAS DE RESPUESTA OBJETIVA - SOLUCIÓN.....	135
CUESTIONES - SOLUCIÓN.....	137
CUESTIÓN 1. Valor = 0,2 ptos. Tiempo estimado: 10 min.	137
CUESTIÓN 2. Valor = 0,2 ptos. Tiempo estimado: 10 min.	137
PROBLEMAS – SOLUCIÓN.....	138
Problema 1. Valor: 1,5 ptos. - SOLUCIÓN.....	138
Problema 2. Valor: 0,5 pts. - SOLUCIÓN.....	141
Problema 3. Valor: 1 pto. - SOLUCIÓN.....	141

PROPUESTA DE EXAMEN 1 – ORDINARIA 1 - ESPAÑOL



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria

Leganés – 17 Mayo 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G81 ☐ G82 ☐ G83 ☐ G84

PREGUNTAS DE RESPUESTA OBJETIVA

**Cada pregunta tiene una única opción correcta, que debe señalarse claramente redondeando la letra identificativa de la opción. Cada pregunta contestada incorrectamente será evaluada con menos un cuarto de la nota que se hubiese obtenido si hubiese sido correctamente respondida.
Cada una de las 8 preguntas tiene un valor de 0,2 puntos. Tiempo estimado: 20 min.**

- 1) Señale cuál de las siguientes opciones es un mecanismo de seguridad
 - a) Firma Digital
 - b) Cifrado
 - c) Rellenado de tráfico
 - d) Las opciones a,b y c son mecanismos de seguridad

- 2) Indique cuál de los siguientes **NO** es un cifrador que siga el esquema propuesto por Hors Feistel:
 - a) DES
 - b) 3DES
 - c) AES
 - d) Todos los anteriores son cifradores de Feistel

- 3) Indique cuál de las siguientes propiedades del protocolo Diffie-Hellman **NO** es cierta.
 - a) Diffie-Hellman permite acordar una clave entre dos extremos que no han intercambiado previamente ningún secreto.
 - b) Diffie-Hellman emplea exponenciación modular para derivar la clave compartida.
 - c) Diffie-Hellman permite autenticar a los extremos de la comunicación.
 - d) El tamaño de generador g no es importante para la seguridad del protocolo.

- 4) Seleccione la respuesta correcta:
 - a) La seguridad del algoritmo RSA radica en el problema del logaritmo discreto
 - b) La seguridad del algoritmo El Gamal radica en el problema de las curvas elípticas
 - c) La seguridad del algoritmo RSA radica en el problema de la factorización de números grandes
 - d) Todas las respuestas anteriores son correctas

- 5) Funciones resumen:
 - a) Una función resumen criptográfica $H(x)$ debe estar libre de colisiones, es decir, se puede encontrar un par de números (x, x') con $x \neq x'$ tal que $H(x)=H(x')$.
 - b) Las funciones resumen MD5 y SHA-1 generan salidas de la misma longitud.
 - c) Una colisión supone la existencia de dos entradas distintas con el mismo resumen.
 - d) Todas las anteriores son falsas.

6) Señale la respuesta correcta:

- a) La firma digital de un mensaje permite exclusivamente que el receptor del mismo pueda probar su origen. Por tanto no difiere funcionalmente de la firma manuscrita.
- b) Sean dos usuarios A y B que desean intercambiarse mensajes confidenciales y con garantía de no repudio en origen. Para que ello ocurra respecto de los mensajes remitidos por B a A, estos mensajes deben ser firmados con la clave privada de B y cifrados con la clave pública de A.
- c) La firma digital garantiza la confidencialidad de los mensajes firmados así como su integridad
- d) La firma digital es el mejor mecanismo existente para producir el resumen de un texto en claro.

7) ¿Qué método se emplea en una autenticación basada en contraseña de un solo uso (OTP) mediante desafío?

- a) El usuario cifra, empleando el token OTP, un valor aleatorio (nonce) enviado por el servidor de autenticación (SA) con la clave privada del SA. Posteriormente le devuelve el resultado al SA para que éste lo descifre con su clave pública, y verifique el valor obtenido contra el almacenado internamente.
- b) El usuario cifra simétricamente, empleando el token OTP, un valor aleatorio (nonce) enviado por el servidor de autenticación (SA) con una clave que comparte con SA. Posteriormente le devuelve el resultado al SA para que éste compruebe el valor que recibe contra el calculado internamente.
- c) No es posible implementar un método de autenticación basado en OTP mediante desafío.
- d) Ninguna de las anteriores.

8) Seleccione la opción correcta (Ley 59/2003 de Firma Electrónica):

- a) La firma electrónica siempre se genera con medios bajo el exclusivo control del firmante.
- b) Un dispositivo de verificación de firma es un dispositivo para crear firmas digitales
- c) Una firma electrónica avanzada es, entre otras cosas, aquella que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados por éste.
- d) Un prestador de servicios de certificación debe almacenar copias de los datos de creación de firma.

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria

Leganés – 17 Mayo 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G81 ☐ G82 ☐ G83 ☐ G84

CUESTIONES

CUESTIÓN 1. Valor = 0,2 ptos. Tiempo estimado: 5 min.

Defina brevemente el funcionamiento de un Generador Linear LFSR.


CUESTIÓN 2. Valor = 0,2 ptos. Tiempo estimado: 10 min.

Describa brevemente los principales servicios operacionales en una Infraestructura de Clave Pública para la gestión del ciclo de vida de los certificados digitales, así como las entidades que intervienen en cada uno de ellos.



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA

Examen Final – Convocatoria Ordinaria

Leganés – 17 Mayo 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G81 ☐ G82 ☐ G83 ☐ G84

PROBLEMAS

PROBLEMA 1. Valor = 1,5 pto. Tiempo estimado: 20 min.

Sobre el cifrado simétrico en bloque proporcionado por el algoritmo AES:

a) Complete la siguiente afirmación:

La matriz de estado del AES está formada por filas, donde cada elemento de la matriz es un

El número de rondas depende del tamaño de

b) Complete el siguiente pseudocódigo en relación a los procedimientos llamados en cada una de las rondas del algoritmo:

```
Round(State, RoundKey) {  
    ..... (.....) ;  
    ..... (.....) ;  
    ..... (.....) ;  
    ..... (....., ..... ) ;  
}
```

c) Sea la matriz de estado de entrada a la función ShiftRows de AES

$$\begin{pmatrix} 09 & 93 & 19 & 27 \\ AE & 52 & 11 & 9D \\ 19 & 21 & A5 & 9C \\ A9 & CC & 33 & 30 \end{pmatrix}$$

Halle la matriz de estado a la salida de dicha función.

SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA

Examen Final – Convocatoria Ordinaria

Leganés – 17 Mayo 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G81 ☐ G82 ☐ G83 ☐ G84

PROBLEMA 2. Valor = 1,5 ptos. Tiempo estimado: 45 min.

Alicia desea intercambiar mensajes cifrados con Benito. Tiene dudas acerca de qué método emplear entre los dos siguientes:

Método 1: $C = M^x \bmod 128$ siendo x una clave de sesión simétrica intercambiada mediante el algoritmo de Diffie-Hellman, M el texto en claro y C el texto cifrado.

Método 2: RSA con módulo definido por los siguientes números primos expresados en binario $p=1101_2$ y $q=0111_2$

Considere que se utilizan los siguientes valores:

- D-H. Datos públicos: $g = 2$ (generador), $p' = 19$ (primo). Datos privados: $X_a = 7$ (Alicia), $X_b = 6$ (Benito)
- RSA. Datos privados: $d_a = 13$, $d_b = 29$

a) Si Alicia utiliza el método 1,

- ¿Cuál será la clave de sesión negociada?
- ¿Cuál será el criptograma resultante si cifra el mensaje $M = 123_{10}$?

b) Si Alicia emplea el método 2, ¿cuál será el resultado de cifrar el mensaje $M = 9_{10}$ para su descifrado por parte de Benito?

c) Discuta, en 10 líneas, las debilidades de cada método con los parámetros utilizados.



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria

Leganés – 17 Mayo 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G81 ☐ G82 ☐ G83 ☐ G84

PROPUESTA DE EXAMEN 1 – ORDINARIA 1 - INGLES

SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Ordinary examination session

Leganés – May 25th 2010

Surname:

Name:

Group: ☐ G89

NIA:

MULTIPLE-CHOICE QUESTIONS

Each question has only one correct answer, which ought to be clearly pointed out rounding the letter identifying the option. Each question incorrectly answered will be evaluated as minus one fourth of the mark obtained had it been correctly answered.

Each of the 8 questions has a value of 0,2 points. Estimated time: 20 min.

1) Indicate which of the next concepts is a security mechanism:

- a) Digital Signature
- b) Encryption
- c) Padding
- d) The three concepts are security mechanisms

2) Mark the cipher that does **NOT** follow the Hors Feistel scheme:

- a) DES
- b) 3DES
- c) AES
- d) a),b) and c) are all Feistel based ciphers

3) Indicate which of the next properties of the Diffie-Hellman protocol is **NOT** true.

- a) Diffie-Hellman allows two entities to agree a key with no previously exchanged secret.
- b) Diffie-Hellman uses modular exponentiation to derive the shared key.
- c) Diffie-Hellman authenticates the peers of the communication.
- d) The length of the generator g is not important for the security of the protocol.

4) Indicate the correct statement:

- a) The strength of the RSA algorithm lies on the problem of the discrete logarithm
- b) The strength of the El Gamal algorithm lies on the problem of elliptic curves
- c) The strength of the RSA algorithm lies on the problem of factorizing big numbers
- d) All the previous statements are true

5) Hash functions:

- a) A cryptographic hash function $H(x)$ should minimize the number of collisions, i.e. it must be possible to find a tuple of numbers (x, x') with $x \neq x'$ such that $H(x)=H(x')$.
- b) MD5 y SHA-1 hash functions generate outputs of the same length.
- c) The existence of a collision implies that two different inputs have the same fingerprint.
- d) None of the above.

¿Cuál es tu trabajo ideal?



Haz el test aquí



<http://bit.ly/necesitouncambio>



¿Harto de c h a p a r algo que no te renta?



6) Mark the correct statement:

- a) The digital signature of a message simply allows a receiver to prove the origin of the message. Accordingly, in terms of functionality, it does not differ from the manuscript signature.
- b) Let A and B be two users who wish to exchange confidential messages with non repudiation proof of origin. In order to achieve this goal, and regarding messages sent from B to A, messages should be signed with B's private key and encrypted with A's public key.
- c) Digital signatures guarantee confidentiality and integrity of signed messages.
- d) Digital signatures are the best available mechanism to produce a hash from a cleartext.

7) What method is used in an authentication using a one-time password (OTP) based on a challenge?

- a) The user encrypts a random value (nonce), previously sent by the authentication server (AS), with the AS's private key, using an OTP token. Afterwards, the user returns the result to the AS, which decrypts it with its public key, and verifies the obtained value against the one internally stored.
- b) The user symmetrically encrypts a random value (nonce), previously sent by the authentication server (AS), with a key shared between the user and the AS. Afterwards, the user returns the result to the AS, which verifies the received value against the one internally calculated.
- c) An OTP authentication method based on a challenge cannot be implemented.
- d) None of the above.

8) Indicate the correct statement (Spanish Law 59/2003 on Digital Signature):

- a) Electronic signatures are always created using means that the signatory can maintain under his sole control.
- b) Digital signature verification devices are devices for the generation of digital signatures.
- c) The advanced electronic signature, among other things, it is capable of identifying the signatory and it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
- d) A certificate service provider must store a copy of digital signature creation data.

**SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA**

Final Exam – Ordinary examination session

Leganés – May 25th 2010

Surname:

Name:

Group: ☐ G89

NIA:

SHORT-ANSWER QUESTIONS

QUESTION 1. Value = 0,2 pts. Estimated time: 5 min.

Briefly describe how an LFSR Generator works.

QUESTION 2. Value = 0,2 pts. Estimated time: 10 min.

Briefly describe the main operational services available in a Public Key Infrastructure, related to the management of a digital certificate life-cycle. Also, identify the entities involved in each service.

SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Ordinary examination session

Leganés – May 25th 2010

Surname:

Name:

Group: ☐ G89

NIA:

PROBLEMS

PROBLEM 1. Value = 1,5 pt. Estimated time: 20 min.

Regarding the Advanced Encryption Standard (AES):

a) Complete the following statement:

AES state matrix consists of rows, where each element is a

The number of rounds depends on the length of

b) Complete the following pseudocode regarding the procedures called in each of the rounds of the algorithm:

```
Round(State, RoundKey) {  
    ..... (.....) ;  
    ..... (.....) ;  
    ..... (.....) ;  
    ..... (....., ..... ) ;  
}
```

c) Let the state matrix below be the input to AES ShiftRows function

$$\begin{pmatrix} 09 & 93 & 19 & 27 \\ AE & 52 & 11 & 9D \\ 19 & 21 & A5 & 9C \\ A9 & CC & 33 & 30 \end{pmatrix}$$

Show the output, i.e. the state matrix after AES ShiftRows function.



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Ordinary examination session

Leganés – May 25th 2010

Surname:

Name:

Group: ☐ G89

NIA:

PROBLEM 2. Value = 1,5 pts. Estimated time: 45 min.

Alice wishes to send encrypted messages to Bob. She is not certain about the method to use amongst the following:

Method 1: $C = M^x \bmod 128$ where x is a symmetric session key agreed by means of Diffie-Hellman key exchange algorithm. M is the cleartext and C is the ciphertext.

Method 2: RSA with a modulo defined by the following prime numbers (expressed in binary) $p=1101_2$ y $q=0111_2$

Consider the following values:

- D-H: Public data: $g = 2$ (generator), $p' = 19$ (prime). Private data: $X_a = 7$ (Alice), $X_b = 6$ (Bob)
- RSA: Private data: $d_a = 13$ (Alice), $d_b = 29$ (Bob)

a) If Alice uses the method 1,

- What is the session key x ?
- What is the ciphertext corresponding to the message $M = 123_{10}$?

b) If Alice uses the method 2 to encrypt messages to Bob, ¿what is the result of encrypting the message $M = 9_{10}$?

c) Briefly discuss (no more than 10 lines), the weaknesses of both methods with the parameters used in the exercise.

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria

Leganés – 17 Mayo 2010


SOLUCIÓN

PROPUESTA DE EXAMEN 1 – ORDINARIA 1 - SOLUCIÓN



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria

Leganés – 17 Mayo 2010

SOLUCIÓN

PREGUNTAS DE RESPUESTA OBJETIVA - SOLUCIÓN

**Cada pregunta tiene una única opción correcta, que debe señalarse claramente redondeando la letra identificativa de la opción. Cada pregunta contestada incorrectamente será evaluada con menos un cuarto de la nota que se hubiese obtenido si hubiese sido correctamente respondida.
Cada una de las 8 preguntas tiene un valor de 0,2 puntos. Tiempo estimado: 20 min.**

- 1) Señale cuál de las siguientes opciones es un mecanismo de seguridad
 - a) Firma Digital
 - b) Cifrado
 - c) Rellenado de tráfico
 - d) Las opciones a,b y c son mecanismos de seguridad

- 2) Indique cuál de los siguientes **NO** es un cifrador que siga el esquema propuesto por Hors Feistel:
 - a) DES
 - b) 3DES
 - c) AES
 - d) Todos los anteriores son cifradores de Feistel

- 3) Indique cuál de las siguientes propiedades del protocolo Diffie-Hellman **NO** es cierta.
 - a) Diffie-Hellman permite acordar una clave entre dos extremos que no han intercambiado previamente ningún secreto.
 - b) Diffie-Hellman emplea exponenciación modular para derivar la clave compartida.
 - c) Diffie-Hellman permite autenticar a los extremos de la comunicación.
 - d) El tamaño de generador g no es importante para la seguridad del protocolo.

- 4) Seleccione la respuesta correcta:
 - a) La seguridad del algoritmo RSA radica en el problema del logaritmo discreto
 - b) La seguridad del algoritmo El Gamal radica en el problema de las curvas elípticas
 - c) La seguridad del algoritmo RSA radica en el problema de la factorización de números grandes
 - d) Todas las respuestas anteriores son correctas

- 5) Funciones resumen:
 - a) Una función resumen criptográfica $H(x)$ debe estar libre de colisiones, es decir, se puede encontrar un par de números (x, x') con $x \neq x'$ tal que $H(x)=H(x')$.
 - b) Las funciones resumen MD5 y SHA-1 generan salidas de la misma longitud.
 - c) Una colisión supone la existencia de dos entradas distintas con el mismo resumen.
 - d) Todas las anteriores son falsas.

6) Señale la respuesta correcta:

- a) La firma digital de un mensaje permite exclusivamente que el receptor del mismo pueda probar su origen. Por tanto no difiere funcionalmente de la firma manuscrita.
- b) Sean dos usuarios A y B que desean intercambiarse mensajes confidenciales y con garantía de no repudio en origen. Para que ello ocurra respecto de los mensajes remitidos por B a A, estos mensajes deben ser firmados con la clave privada de B y cifrados con la clave pública de A.
- c) La firma digital garantiza la confidencialidad de los mensajes firmados así como su integridad
- d) La firma digital es el mejor mecanismo existente para producir el resumen de un texto en claro.

7) ¿Qué método se emplea en una autenticación basada en contraseña de un solo uso (OTP) mediante desafío?

- a) El usuario cifra, empleando el token OTP, un valor aleatorio (nonce) enviado por el servidor de autenticación (SA) con la clave privada del SA. Posteriormente le devuelve el resultado al SA para que éste lo descifre con su clave pública, y verifique el valor obtenido contra el almacenado internamente.
- b) El usuario cifra simétricamente, empleando el token OTP, un valor aleatorio (nonce) enviado por el servidor de autenticación (SA) con una clave que comparte con SA. Posteriormente le devuelve el resultado al SA para que éste compruebe el valor que recibe contra el calculado internamente.
- c) No es posible implementar un método de autenticación basado en OTP mediante desafío.
- d) Ninguna de las anteriores.

8) Seleccione la opción correcta (Ley 59/2003 de Firma Electrónica):

- a) La firma electrónica siempre se genera con medios bajo el exclusivo control del firmante.
- b) Un dispositivo de verificación de firma es un dispositivo para crear firmas digitales
- c) Una firma electrónica avanzada es, entre otras cosas, aquella que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados por éste.
- d) Un prestador de servicios de certificación debe almacenar copias de los datos de creación de firma.

SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA

Examen Final – Convocatoria Ordinaria

Leganés – 17 Mayo 2010

SOLUCIÓN

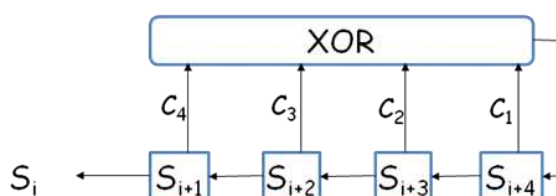
CUESTIONES - SOLUCIÓN

CUESTIÓN 1. Valor = 0,2 ptos. Tiempo estimado: 5 min.

Defina brevemente el funcionamiento de un Generador Linear LFSR.

- ▶ Registro de desplazamiento con realimentación
 - ▶ es una memoria de n celdas cuyo contenido se desplaza con los pulsos de un reloj de control
 - ▶ El contenido de sus celdas se mezcla mediante operaciones lineales, cuyo resultado alimenta la última de las celdas

Ejemplo 4 celdas:



CUESTIÓN 2. Valor = 0,2 ptos. Tiempo estimado: 10 min.

Describa brevemente los principales servicios operacionales en una Infraestructura de Clave Pública para la gestión del ciclo de vida de los certificados digitales, así como las entidades que intervienen en cada uno de ellos.

Los principales servicios incluyen:

- La solicitud de un certificado por parte de un usuario a la Autoridad de Certificación (AC) deseada.
- El proceso de registro de dicho usuario ante la Autoridad de Registro (AR).
- La emisión del certificado digital al usuario por parte de la AC en base a la información proporcionada por la AR.
- La solicitud de renovación del certificado por parte del propietario del certificado a la AC con el fin de extender el periodo de validez del mismo, y así poder seguir operando con las mismas claves asimétricas.
- La solicitud de revocación del estado del certificado por parte del propietario o una entidad autorizada, con el fin de invalidar el certificado antes de su fecha de expiración.
- La consulta del estado de revocación de un certificado por cualquier entidad. El tipo de consulta variará dependiendo del modelo existente para la publicación del estado de revocación de los certificados. En caso de mecanismos basados en CRL, la entidad solicitante generalmente accederá al punto de distribución de la CRL, gestionado por la AC u otra autoridad delegada. En el caso de mecanismos basados en OCSP, la entidad solicitante generalmente accederá al servicio OCSP correspondiente, que podrá ser publicado por la AC u otra entidad externa.

¿Cuál es tu trabajo ideal?



Haz el test aquí

<http://bit.ly/necesitouncambio>



¿Harto de c h a p a r algo que no te renta?

PROBLEMAS - SOLUCIÓN

PROBLEMA 1. Valor = 1,5 pto. Tiempo estimado: 20 min.

Sobre el cifrado simétrico en bloque proporcionado por el algoritmo AES:

d) Complete la siguiente afirmación:

La matriz de estado del AES está formada por filas, donde cada elemento de la matriz es un
El número de rondas depende del tamaño de

e) Complete el siguiente pseudocódigo en relación a los procedimientos llamados en cada una de las rondas del algoritmo:

```
Round(State, RoundKey) {  
    ..... (.....) ;  
    ..... (.....) ;  
    ..... (.....) ;  
    ..... (....., .....) ;  
}
```

f) Sea la matriz de estado de entrada a la función ShiftRows de AES

$$\begin{pmatrix} 09 & 93 & 19 & 27 \\ AE & 52 & 11 & 9D \\ 19 & 21 & A5 & 9C \\ A9 & CC & 33 & 30 \end{pmatrix}$$

Halle la matriz de estado a la salida de dicha función.

a)

La matriz de estado del AES está formada por4... filas, donde cada elemento de la matriz es un ..byte....(2 dígitos Hex).....
El número de columnas depende del tamaño dela clave.....

b)

```
Round(State, RoundKey) {  
    ..... SubBytes ..... (.. State ..) ;  
    ..... ShiftRows ..... (.. State ..) ;  
    ..... MixColumns ..... (.. State ..) ;  
    ..... AddRoundKey ..... (.. State .., .. RoundKey ..) ;  
}
```

SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA

Examen Final – Convocatoria Ordinaria

Leganés – 17 Mayo 2010

SOLUCIÓN

}

c)

09	93	19	27
52	11	9D	AE
A5	9C	19	21
30	A9	CC	33

PROBLEMA 2. Valor = 1,5 pts. Tiempo estimado: 45 min.

Alicia desea intercambiar mensajes cifrados con Benito. Tiene dudas acerca de qué método emplear entre los dos siguientes:

Método 1: $C = M^x \bmod 128$ siendo x una clave de sesión simétrica intercambiada mediante el algoritmo de Diffie-Hellman, M el texto en claro y C el texto cifrado.

Método 2: RSA con módulo definido por los siguientes números primos expresados en binario $p=1101_{(2)}$ y $q=0111_{(2)}$

Considere que se utilizan los siguientes valores:

- D-H. Datos públicos: $g = 2$ (generador), $p' = 19$ (primo). Datos privados: $X_a = 7$ (Alicia), $X_b = 6$ (Benito)
- RSA. Datos privados: $d_a = 13$, $d_b = 29$

a) Si Alicia utiliza el método 1,

- ¿Cuál será la clave de sesión negociada?
- ¿Cuál será el criptograma resultante si cifra el mensaje $M = 123_{(10)}$?

b) Si Alicia emplea el método 2, ¿cuál será el resultado de cifrar el mensaje $M = 9_{(10)}$ para su descifrado por parte de Benito?

c) Discuta, en 10 líneas, las debilidades de cada método con los parámetros utilizados.

a) $Y_a = g^{X_a} \bmod p' = 2^7 \bmod 19 = 2^4 2^3 \bmod 19 = (-3) 8 \bmod 19 = -5 \bmod 19 = 14$

$Y_b = g^{X_b} \bmod p' = 2^6 \bmod 19 = (-3) 4 \bmod 19 = -12 \bmod 19 = 7$

$K = (Y_a)^{X_b} \bmod p' = (Y_b)^{X_a} \bmod p' =$

$(Y_a)^{X_b} \bmod p' = 14^6 \bmod 19 = (-5)^6 \bmod 19 = (-5)^2 (-5)^2 (-5)^2 = 6^3 \bmod 19 = 36 6 \bmod 19 = (-2) 6 \bmod 19 = 7$

$(Y_b)^{X_a} \bmod p' = 7^7 \bmod 19 = 7^2 7^5 \bmod 19 = (-8)^3 7 \bmod 19 = 7 (-8) 7 \bmod 19 = 11 (-8) \bmod 19 = 7$

$K = 7$

$C = M^x \bmod 128 = 123^7 \bmod 128 = ((-5)^3)^2 (-5) \bmod 128 = (-125)^2 (-5) \bmod 128 = 3^2 (-5) \bmod 128 = -45 \bmod 128 = 83$

$$b) p=1101_2=13_{(10)} \text{ y } q=111_2=7_{(10)}$$

$$\text{Luego } n = 13 \cdot 7 = 91$$

$$e_b d_b = 1 \bmod \phi(n)$$

$$29 e_b = 1 \bmod \phi(91)$$

$$\phi(91) = \phi(13) \cdot \phi(7) = (12 \cdot 6) = 72$$

$$29 e_b = 1 \bmod 72 \quad 1 = 29 - 14 \cdot 2$$

$$72 = 29 \cdot 2 + 14 \quad 1 = 29 - 2(72 - 29 \cdot 2)$$

$$29 = 14 \cdot 2 + 1 \quad 1 = 29 - 2 \cdot 72 + 4 \cdot 29$$

$$1 = 5 \cdot 29 - 2 \cdot 72$$

$$e_b = 5$$

$$C = M^{e_b} \bmod n = 9^5 \bmod 91 = 9^2 \cdot 9^2 \cdot 9 \bmod 91 = (-10)^2 \cdot 9 \bmod 91 = 81$$

c) La mayor debilidad del método 1 es que el espacio de claves que se pueden intercambiar es pequeño (sólo 19 claves distintas) por lo que sería sencillo realizar un ataque de fuerza bruta. Además con los valores públicos proporcionados es sencillo deducir los valores privados.

La mayor debilidad del método 2 (RSA) es que al ser n pequeño es fácilmente factorizable y de la clave pública se puede obtener la privada. p y q deberían de tener, a día de hoy, un tamaño de al menos 512 bits cada uno y en el problema su tamaño es de 4 bits.

Además el intercambio de claves de Diffie-Hellman es vulnerable a un ataque de hombre en el medio y en ambos métodos, en las condiciones del problema, el espacio de mensajes es pequeño.

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria

Colmenarejo – 25 Mayo 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G80 ☐ G81

NIA:

PROPUESTA DE EXAMEN 2 – ORDINARIA 2



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria

Colmenarejo – 25 Mayo 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G80 ☐ G81

NIA:

PREGUNTAS DE RESPUESTA OBJETIVA

**Cada pregunta tiene una única opción correcta, que debe señalarse claramente redondeando la letra identificativa de la opción. Cada pregunta contestada incorrectamente será evaluada con menos un cuarto de la nota que se hubiese obtenido si hubiese sido correctamente respondida.
Cada una de las 8 preguntas tiene un valor de 0,2 puntos. Tiempo estimado: 20 min.**

1) Señale la respuesta correcta:

- a) La interceptación es un ejemplo de amenaza activa, que trata de modificar los datos.
- b) Un ejemplo típico de ataque de modificación es la falsificación de direcciones IP.
- c) Los sniffers remiten cantidades ingentes de datos a un servidor hasta colapsarlo.
- d) La interrupción es un ejemplo de amenaza activa, que atenta contra la confidencialidad de la información.

2) Señale la respuesta correcta:

- a) En la sustitución polialfabeto periódica la frecuencia de los caracteres del texto en claro se transmite íntegra al texto cifrado.
- b) El índice de coincidencia es la probabilidad de que dos letras (seleccionadas aleatoriamente) de un texto sean la misma.
- c) El método Kasiski es útil para criptoanalizar textos cifrados mediante el método Vernam.
- d) La máquina enigma utilizaba el cifrado Vigenere.

3) Suponga que se cifra un mensaje en claro de 1028 bits usando un LFSR de 10 celdas cuyo polinomio asociado es primitivo. En estas condiciones:

- a) El mensaje no se debe cifrar, ya que el mensaje es más largo que la secuencia pseudoaleatoria que el LFSR genera.
- b) Se rellena con ceros la secuencia de cifrado hasta alcanzar la longitud requerida, ya que el mensaje es más largo que la secuencia pseudoaleatoria que el LFSR genera.
- c) La secuencia aleatoria generada servirá para cifrar el mensaje, ya que un LFSR con polinomio asociado primitivo está diseñado para generar secuencias largas.
- d) Ninguna de las anteriores.

4) Indique cuál de las siguientes afirmaciones es verdadera:

- a) Los sistemas de clave secreta son más lentos que los de clave pública y se han quedado obsoletos.
- b) Un sistema de clave pública requiere un mayor número total de claves.
- c) La clave pública puede ser enviada por cualquier canal inseguro.
- d) Ninguna de las anteriores es cierta.

5) Señale la respuesta correcta:

- a) Una función resumen criptográfica genera resúmenes de longitud fija.
- b) Al hecho de que una función resumen criptográfica genere el mismo resultado a partir de dos mensajes distintos se le llama Colisión.
- c) Las funciones resumen criptográficas deben ser eficientes, deterministas y con alta difusión ante pequeños cambios en un mensaje.
- d) Las opciones a,b y c son correctas.

6) Sobre la firma digital:

- a) La operación de firma digital proporciona confidencialidad y no repudio de los datos.
- b) La validación de la firma digital reside en la comprobación de la vigencia del certificado digital del firmante, entre otras.
- c) En España, la Ley 59/2003 de Firma electrónica define varios tipos de firma electrónica: reconocida, avanzada y digital.
- d) Todas las anteriores son correctas.

7) Sobre la infraestructura de clave pública (PKI):

- a) La recepción por parte de A de un documento M acompañado de un certificado digital de B implica que A cree a ciegas en B, por lo que A no ha de acudir a ninguna autoridad para creer en la autenticidad del documento M.
- b) Un certificado digital X.509 contiene, entre otros datos, un número de serie, la identidad de la AC que lo emite, la fecha de caducidad, la clave privada del usuario o entidad que solicitó el certificado y los algoritmos utilizados.
- c) Tras recibir un certificado digital de A, B debe acudir a la CRL (Listado de revocación de certificados) de la AC que emitió el certificado de A, para comprobar su validez, y sólo lo aceptará en el caso de recibir la confirmación de que el mismo no se encuentra en la CRL.
- d) Ninguna de las anteriores.

8) Señale la respuesta **INCORRECTA**:

- a) El protocolo SSL sirvió como base del estándar TLS.
- b) Los protocolos SSL y TLS se usan, entre otras, en aplicaciones de comercio electrónico por Internet.
- c) El protocolo SSL ofrece confidencialidad, integridad y compresión (opcional) de los datos.
- d) En el protocolo SSL nunca es posible autenticar al cliente, sólo al servidor.

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria

Colmenarejo – 25 Mayo 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G80 ☐ G81

NIA:

CUESTIONES

CUESTIÓN 1. Valor = 0,2 ptos. Tiempo estimado: 10 min.

Defina brevemente el concepto de “ataque de hombre interpuesto” (*Man in the middle*).


CUESTIÓN 2. Valor = 0,2 ptos. Tiempo estimado: 10 min.

Defina de manera concisa los conceptos de firma electrónica, firma electrónica avanzada y firma electrónica reconocida recogidos en la Ley 59/2003 de firma electrónica.



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA

Examen Final – Convocatoria Ordinaria

Colmenarejo – 25 Mayo 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G80 ☐ G81

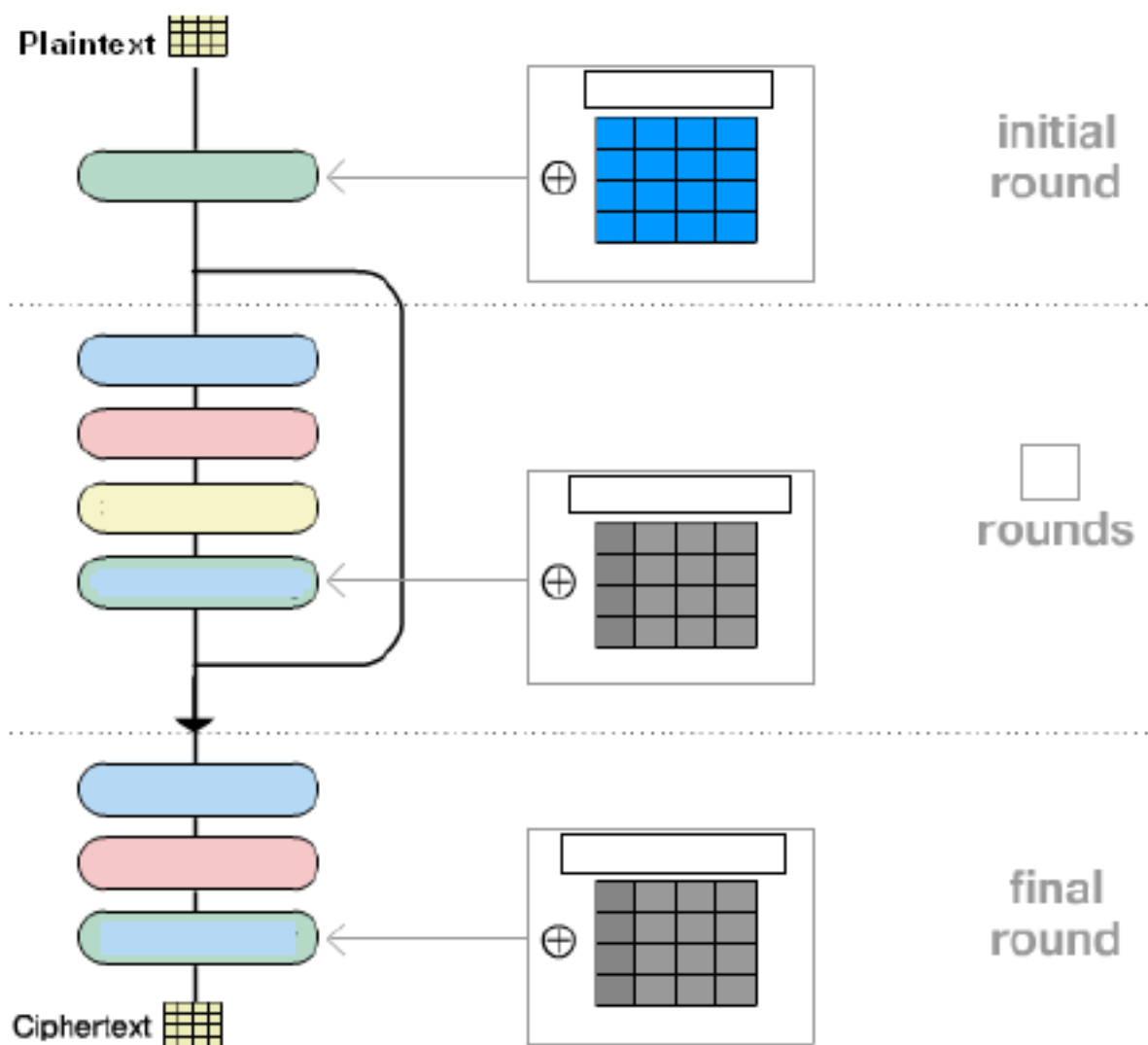
NIA:

PROBLEMAS

Problema 1. Valor = 1,5 ptos. Tiempo estimado: 20 min.

Sobre el cifrado simétrico en bloque proporcionado por el algoritmo AES:

- a) El proceso de cifrado del algoritmo AES se compone de una serie de funciones que se aplican al bloque de entrada a lo largo de un número determinado de rondas. Típicamente, podemos representar el **proceso general con el siguiente diagrama**, al que se le han borrado las etiquetas descriptivas. **Rellene** cada etiqueta del diagrama con los datos apropiados.



b) Considerando AES-128 y la siguiente matriz estado a la salida de la ronda 0:

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

Halle la matriz de estado a la salida de las funciones en la ronda 1 que a continuación se piden:

Matriz Matriz
Tras aplicar la 1ªFunción Tras aplicar la 2ªFunción

		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 7. S-box: substitution values for the byte xy (in hexadecimal format).

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria

Colmenarejo – 25 Mayo 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G80 ☐ G81

NIA:

Problema 2. Valor = 1,5 ptos. Tiempo estimado: 45 min.

A y B desean intercambiar mensajes. Para garantizar la autenticidad en dicho intercambio, los mensajes serán firmados por los interlocutores mediante el algoritmo RSA.

Una AC en la que confían A y B certifica sus claves públicas. El algoritmo utilizado por la AC es RSA y los certificados emitidos constan únicamente de la firma del exponente de la clave pública correspondiente.


Considerando que AC, A y B trabajan con el mismo módulo $n=85$, que los certificados son $C_A=30$ y $C_B=9$ y que la clave pública de la AC es $(e_{AC}, n)=(3, 85)$

- a) Obtenga las claves públicas de A y B a partir de sus certificados
- b) Suponga que $e_A=55$ y que el mensaje que A pretende enviar a B es $M=5$. Calcule la firma que A envía a B.
- c) Realice los cálculos que lleva a cabo B, para verificar la firma de A.



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Extraordinary examination session (EXTRA) Leganés – May 31st 2010

Surname:

Name:

Group: ☐ G89

NIA:

PROPUESTA DE EXAMEN 2 – ORDINARIA 2 – INGLÉS

SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Extraordinary examination session (EXTRA) Leganés – May 31st 2010

Surname:

Name:

Group: ☐ G89

NIA:

MULTIPLE-CHOICE QUESTIONS

Each question has only one correct answer, which ought to be clearly pointed out rounding the letter identifying the option. Each question incorrectly answered will be evaluated as minus one fourth of the mark obtained had it been correctly answered.

Each of the 8 questions has a value of 0,2 points. Estimated time: 20 min.

1) Mark the correct statement:

- a) Interception is an example of an active threat that tries to modify data.
- b) A typical example of a modification attack is IP spoofing.
- c) Sniffers send huge amounts of data to a server to collapse it.
- d) Interruption is an example of an active threat against confidentiality of information.

2) Mark the correct statement:

- a) The frequency of plaintext characters is maintained in ciphertext in periodical polyalphabetic substitution.
- b) The index of coincidence is the probability that two letters from a text (randomly selected) are the same.
- c) Kasiski method is useful for cryptanalysis of ciphertexts encrypted by means of Vernan cipher.
- d) Enigma machine used Vigènere encryption.

3) A plaintext of 1028 bits is encrypted by means of a 10-cell LFSR which associated polynomial is primitive. Given these conditions:

- a) The plaintext should not be encrypted because the plaintext is longer than the pseudorandom sequence produced by the LFSR.
- b) Due to the plaintext is larger than the pseudorandom sequence the LFRS generate the sequence is filled up with zeros to reach the required length.
- c) The produced sequence is appropriate to encrypt the message because an LFSR with an associated polynomial that is primitive is designed to produce maximal sequences.
- d) None of the above is true.

4) Mark the correct statement:

- a) Symmetric key cryptosystems are slower than public key ones and have become obsolete.
- b) A public key cryptosystem requires a higher total number of keys than a symmetric key one.
- c) Public keys can be sent through any channel, even an insecure one.
- d) None of the above is true.

5) Mark the correct statement:

- a) The output of a cryptographic hash function has always the same length.
- b) A collision occurs when two messages produce the same output in a cryptographic hash function.
- c) Cryptographic hash functions must be efficient and deterministic. Moreover, they must produce high diffusion based on small changes in the input message.
- d) All a, b and c are correct.

¿Cuál es tu trabajo ideal?



Haz el test aquí



<http://bit.ly/necesitouncambio>



¿Harto de c h a p a r algo que no te renta?

IRON
HACK

6) Regarding digital signatures:

- a) A digital signature protects the confidentiality and non repudiation of the data.
- b) A digital signature validation requires checking the validity of the signer's certificate, among other operations.
- c) In Spanish Law 59/2003 on Electronic Signatures (based on EU Directive 1999/93/EC), several kinds of signatures are defined: digital, advanced and recognized.
- d) All a, b and c are correct.

7) Regarding public key infrastructures (PKI):

- a) The reception by A of a document M along with B's public key certificate implies that A trusts blindly in B, so A does not need to consult any trusted third party (authority) to verify the authenticity of document M.
- b) An X.509 public key certificate contains, among other data, a serial number, the identification of the issuer (Certificate Authority), expiration date, the private key of the certificate owner and the used algorithms.
- c) After receiving A's public key certificate, B must consult the corresponding CRL (Certificate Revocation List) to check A's certificate validity. B would only accept A's certificate if it is not listed in the CRL.
- d) None of the above is true.

8) Mark the **INCORRECT** statement:

- a) SSL served as a basis for TLS.
- b) SSL and TLS are employed in e-commerce applications as well as in other scenarios.
- c) SSL provides confidentiality, integrity and (optionally) data compression.
- d) It is not possible to authenticate the client in SSL, only the server can be authenticated in this protocol.

SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Extraordinary examination session (EXTRA) Leganés – May 31st 2010

Surname:

Name:

Group: ☐ G89

NIA:

SHORT ANSWER QUESTIONS

QUESTION 1. Value = 0,2 pts. Estimated time: 10 min.

Briefly define the “man in the middle” attack.

QUESTION 2. Value = 0,2 pts. Estimated time: 10 min.

Define in a precise manner the electronic signature, advanced electronic signature and the qualified electronic signature concepts included in the 59/2003 Spanish Law on electronic signatures and the European Directive 1999/93/CE.

SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Extraordinary examination session (EXTRA) Leganés – May 31st 2010

Surname:

Name:

Group: ☐ G89

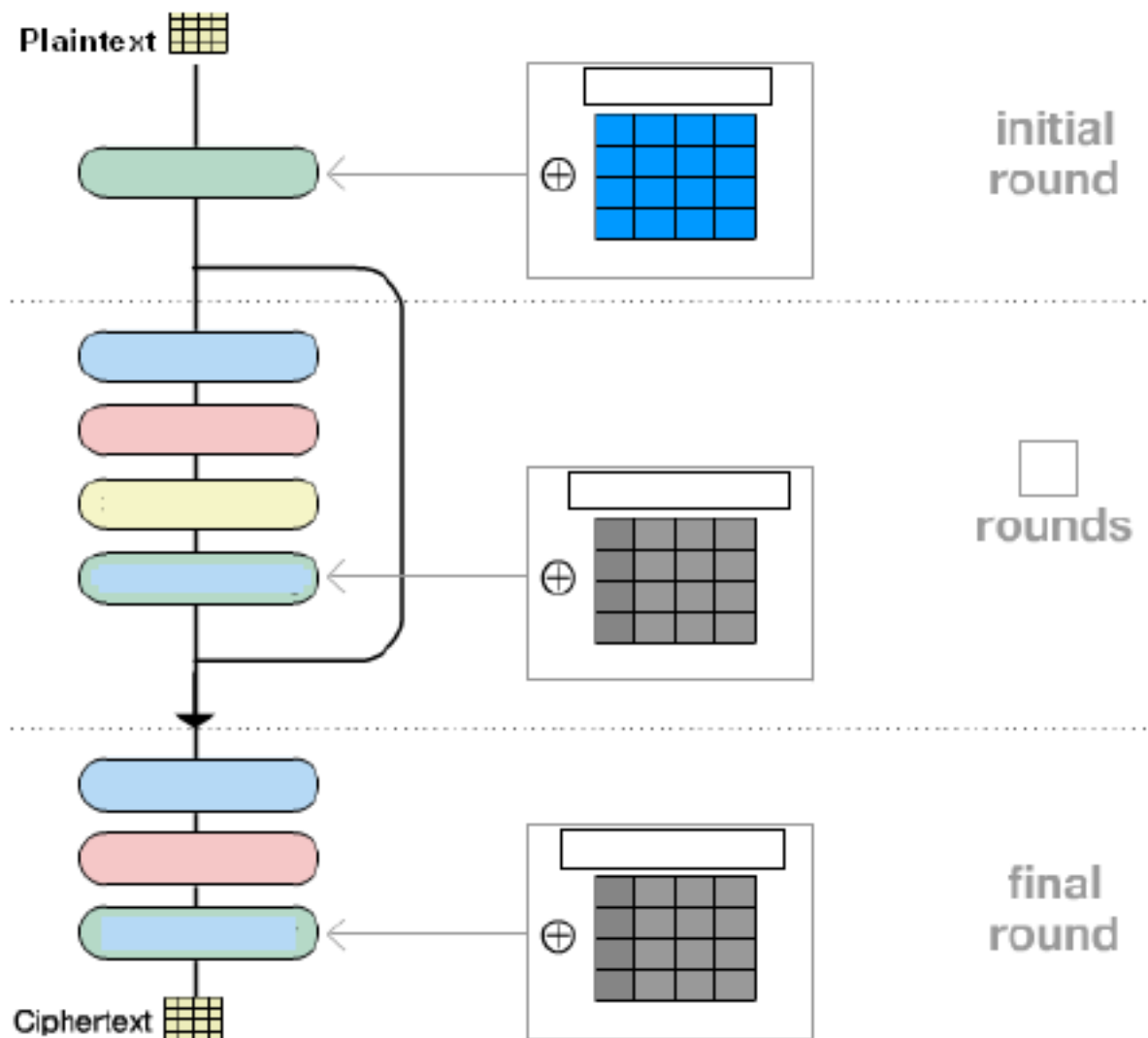
NIA:

PROBLEMS

PROBLEM 1. Value = 1,5 pts. Estimated time: 20 min.

About the symmetric block encryption provided by AES:

- a) AES encryption process consists of a series of stages executed for each message block in a set of rounds. Typically, we can represent the overall process with the following diagram, on which we have deleted titles of each phase and labels. **Fill** each element of the diagram with tags for those stages and AES items.



¿Cuál es tu trabajo ideal?



Haz el test aquí



<http://bit.ly/necesitouncambio>



¿Harto de c hapar algo que no te renta?



- b) Consider AES-128 and the following state matrix as output of the initial round:

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

Compute the state matrix at round 1 after applying the AES functions requested below:

Matrix
After applying first function

Matrix
After applying second function

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 7. S-box: substitution values for the byte xy (in hexadecimal format).

SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Extraordinary examination session (EXTRA) Leganés – May 31st 2010

Surname:

Name:

Group: ☐ G89

NIA:

PROBLEM 2. Value = 1,5 pts. Estimated time: 45 min.

A and B want to exchange messages. To authenticate the transmitted data, messages will be signed with RSA algorithm.

Both A and B trust in a Certification Authority (CA) to certify their public keys. The CA uses RSA for this purpose, and the resulting certificates only contain the signature of the public key exponent.

Assuming that the RSA algorithm uses $n=85$, the certificates are $C_A=30$ and $C_B=9$ and the CA public key is $(e_{CA}, n)=(3, 85)$, answer the following questions:

- a) Get the public keys of A and B, using the information contained in their certificates.
- b) Suppose that $e_A=55$ and that the message A tries to send to B is $M=5$. Calculate the signature that A sends to B.
- c) Carry out the calculations that B makes to verify the signature of A.

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria

Colmenarejo – 25 Mayo 2010

SOLUCIÓN

PROPUESTA DE EXAMEN 2 – ORDINARIA 2 - SOLUCIÓN



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria

Colmenarejo – 25 Mayo 2010

SOLUCIÓN

PREGUNTAS DE RESPUESTA OBJETIVA- SOLUCIÓN

Cada pregunta tiene una única opción correcta, que debe señalarse claramente redondeando la letra identificativa de la opción. Cada pregunta contestada incorrectamente será evaluada con menos un cuarto de la nota que se hubiese obtenido si hubiese sido correctamente respondida.

Cada una de las 8 preguntas tiene un valor de 0,2 puntos. Tiempo estimado: 20 min.

1) Señale la respuesta correcta:

- e) La interceptación es un ejemplo de amenaza activa, que trata de modificar los datos.
- f) Un ejemplo típico de ataque de modificación es la falsificación de direcciones IP.
- g) Los sniffers remiten cantidades ingentes de datos a un servidor hasta colapsarlo.
- h) La interrupción es un ejemplo de amenaza activa, que atenta contra la confidencialidad de la información.

2) Indique cual de las siguientes opciones es cierta:

- a) En la sustitución polialfabeto periódica la frecuencia de los caracteres del texto en claro se transmite al texto cifrado.
- b) El índice de coincidencia es la probabilidad de que dos letras (seleccionadas aleatoriamente) de un texto sean la misma.
- c) El método Kasiski es útil para criptoanalizar textos cifrados con el método Vernam.
- d) La máquina enigma utilizaba el cifrado Vigenere.

3) Suponga que se cifra un mensaje en claro de 1028 bits usando un LFSR de 10 celdas cuyo polinomio de conexión es primitivo. En estas condiciones:

- a) El mensaje no se debe cifrar, ya que el mensaje es más largo que la secuencia pseudoaleatoria que el LFSR genera.
- b) Se rellena con ceros la secuencia de cifrado hasta alcanzar la longitud requerida, ya que el mensaje es más largo que la secuencia pseudoaleatoria que el LFSR genera.
- c) La secuencia aleatoria generada servirá para cifrar el mensaje, ya que un LFSR con polinomio de conexión primitivo está diseñado para generar secuencias largas.
- d) Ninguna de las anteriores.

4) Indique cuál de las siguientes afirmaciones es verdadera:

- a) Los sistemas de clave secreta son más lentos que los de clave pública y se han quedado obsoletos.
- b) Un sistema de clave pública requiere un mayor número total de claves.
- c) La clave pública puede ser enviada por cualquier canal inseguro.
- d) Ninguna de las anteriores es cierta.

5) Seleccione la opción correcta

- a) Una función resumen genera resúmenes de longitud fija.
- b) Al hecho de que una función resumen genere el mismo resultado a partir de dos mensajes distintos se le llama colisión.
- c) Las funciones resumen criptográficas deben ser eficientes, deterministas y con alta difusión ante pequeños cambios en un mensaje.
- d) Las opciones a,b y c son correctas.

6) Firma digital

- a) La operación de firma digital proporciona confidencialidad y no repudio de los datos.
- b) [La validación de la firma digital reside en la comprobación de la vigencia del certificado digital del firmante, entre otras.](#)
- c) En España, la Ley 59/2003 de Firma electrónica define varios tipos de firma electrónica: reconocida, avanzada y digital.
- d) Todas las anteriores son correctas.

7) PKI

- a) La recepción por A de un documento M acompañado de un certificado digital de B implica que A cree a ciegas en B, por lo que A no ha de acudir a ninguna autoridad para creer en la autenticidad del documento M.
- b) Un certificado digital X.509 contiene, entre otros datos, un número de serie, la identidad de la AC que lo emite, la fecha de caducidad, la clave privada del usuario o entidad que solicitó el certificado y los algoritmos utilizados.
- c) [Tras recibir un certificado digital de A, B debe acudir a la CRL \(Listado de revocación de certificados\) de la AC que emitió el certificado de A, para comprobar su validez, y sólo lo aceptará en el caso de recibir la confirmación de que el mismo no se encuentra en la CRL.](#)
- d) Ninguna de las anteriores.

8) Señale la respuesta **INCORRECTA**:

- a) El protocolo SSL sirvió como base del estándar TLS.
- b) Los protocolos SSL y TLS se usan, entre otras, en aplicaciones de comercio electrónico por Internet.
- c) El protocolo SSL ofrece confidencialidad, integridad y compresión (opcional) de los datos.
- d) [En el protocolo SSL nunca es posible autenticar al cliente, sólo al servidor.](#)

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria

Colmenarejo – 25 Mayo 2010

SOLUCIÓN

CUESTIONES - SOLUCIÓN

CUESTIÓN 1. Valor = 0,2 ptos. Tiempo estimado: 10 min.

Defina brevemente el concepto de “ataque de hombre interpuesto” (*Man in the middle*).

El atacante controla el canal

Suplanta a A frente a B y a B frente a A

Realiza un D-H con cada uno de ellos

Ni A ni B pueden descubrirlo, puesto que no se utiliza ningún mecanismo de autenticación

CUESTIÓN 2. Valor = 0,2 ptos. Tiempo estimado: 10 min.

Defina de manera concisa los conceptos de firma electrónica, firma electrónica avanzada y firma electrónica reconocida recogidos en la Ley 59/2003 de firma electrónica.

Respuesta: La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

La firma electrónica reconocida es una firma electrónica avanzada basada en un certificado reconocido y generada por un dispositivo seguro de creación de firma.

¿Cuál es tu trabajo ideal?



Haz el test aquí

<http://bit.ly/necesitouncambio>



¿Harto de c hapar algo que no te renta?

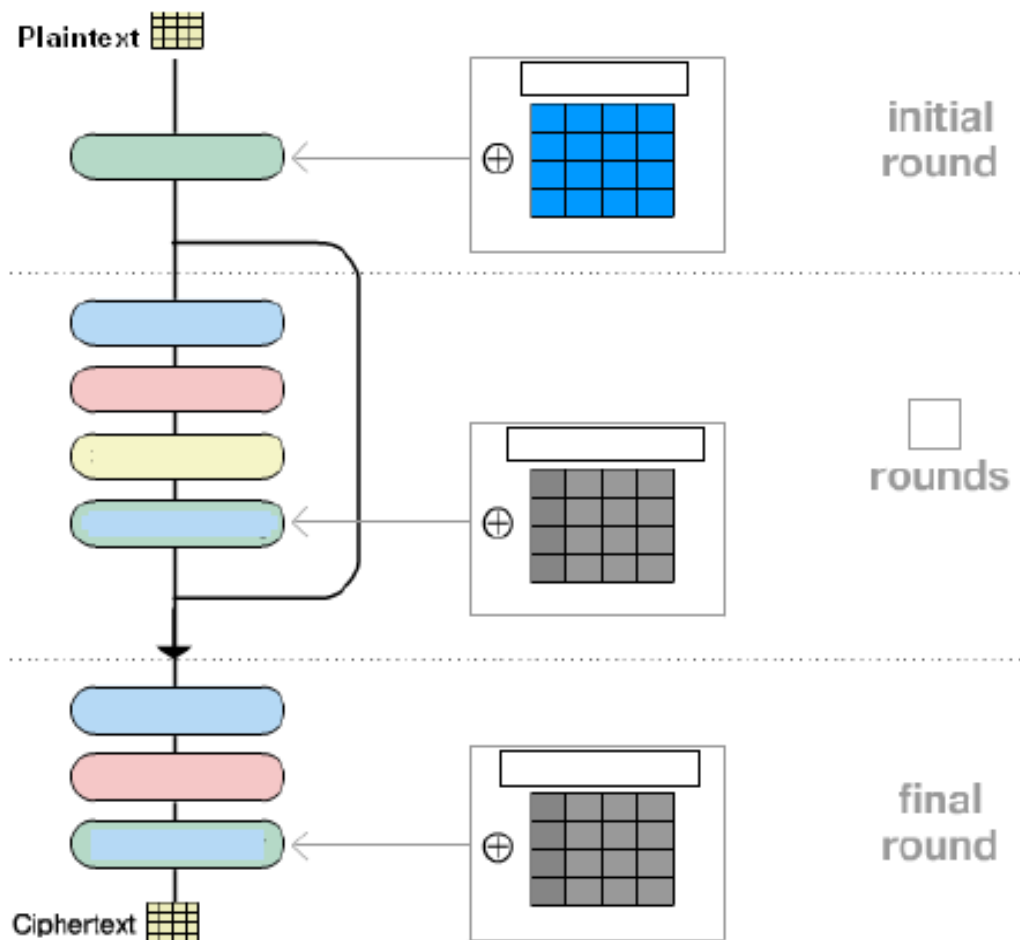
IRON
HACK

PROBLEMAS - SOLUCIÓN

Problema 1. Valor = 1,5 pts. Tiempo estimado: 20 min.

Sobre el cifrado simétrico en bloque proporcionado por el algoritmo AES:

- b) El proceso de cifrado del algoritmo AES se compone de una serie de funciones que se aplican al bloque de entrada a lo largo de un número determinado de rondas. Típicamente, podemos representar el **proceso general con el siguiente diagrama**, al que se le han borrado las etiquetas descriptivas. **Rellene** cada etiqueta del diagrama con los datos apropiados.



SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA

Examen Final – Convocatoria Ordinaria

Colmenarejo – 25 Mayo 2010

SOLUCIÓN

c) Considerando AES-128 y la siguiente matriz estado a la salida de la ronda 0:

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

Halle la matriz de estado a la salida de las funciones en la ronda 1 que a continuación se piden:

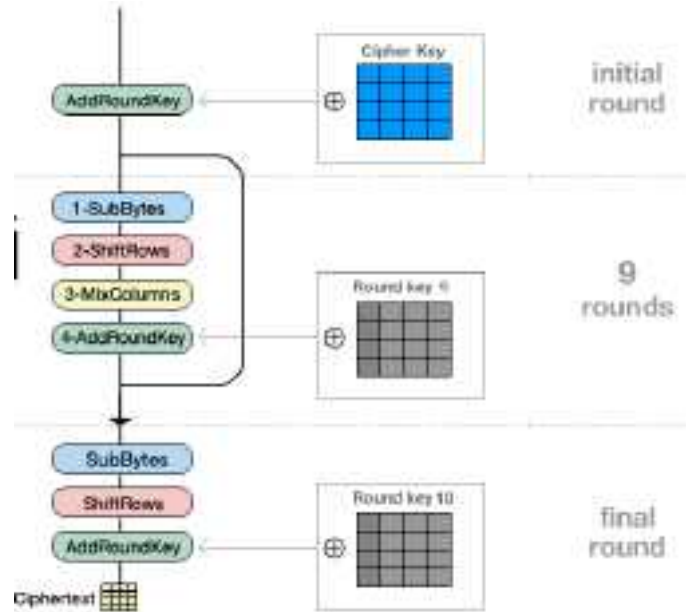
Matriz
Tras aplicar la 1ªFunción

Matriz
Tras aplicar la 2ªFunción

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 7. S-box: substitution values for the byte xy (in hexadecimal format).

a)



b)

d4	e0	b8	1e	d4	e0	b8	1e
27	bf	b4	41	bf	b4	41	27
11	98	5d	52	5d	52	11	98
ae	f1	e5	30	30	ae	f1	e5

SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA

Examen Final – Convocatoria Ordinaria

Colmenarejo – 25 Mayo 2010

SOLUCIÓN

Problema 2. Valor = 1,5 pts. Tiempo estimado: 45 min.

A y B desean intercambiar mensajes. Para garantizar la autenticidad en dicho intercambio, los mensajes serán firmados por los interlocutores mediante el algoritmo RSA.

Una AC en la que confían A y B certifica sus claves públicas. El algoritmo utilizado por la AC es RSA y los certificados emitidos constan únicamente de la firma del exponente de la clave pública correspondiente.

Considerando que AC, A y B trabajan con el mismo módulo $n=85$, que los certificados son $C_A=30$ y $C_B=9$ y que la clave pública de la AC es $(e_{AC}, n)=(3, 85)$

- d) Obtenga las claves públicas de A y B a partir de sus certificados
- e) Suponga que $e_A=55$ y que el mensaje que A pretende enviar a B es $M=5$. Calcule la firma que A envía a B.
- f) Realice los cálculos que lleva a cabo B, para verificar la firma de A.
- a) $C_A=30 = e_A^{d_{AC}}$; $e_A = 30^{e_{AC}} = 30^3 \text{ mód } 85 = (3 \cdot 10)^3 \text{ mód } 85 = 3^3 \cdot 15 \cdot 10 \text{ mód } 85 = 15 \cdot 15 \text{ mód } 85 = 55$ **(0,3 puntos)**
 $C_B=9 = e_B^{d_{AC}}$; $e_B = 9^{e_{AC}} = 9^3 \text{ mód } 85 = 49$ **(0,3 puntos)**

Si el procedimiento es correcto, y sólo el resultado está mal se valora con la mitad de puntuación. En el resto de los casos no se valora el ejercicio

- b) $F_A = M^{d_A} \text{ mod } n$; $d_A = e_A^{-1} \text{ mód } \Phi(n) = 55^{-1} \text{ mód } 64$
 Aplicando Euclides modificado

	1	6
64	55	9
9	1	

$$9 = 64 - 55$$

$$1 = 55 - 9 \cdot 6 = 55 - 6(64 - 55) = 7 \cdot 55 - 6 \cdot 64$$

Por lo que $d_A=7$ **(0,3 puntos)**

Nota: Se acepta también como solución $d_A=71$ que también pertenece a Z_{85}

$$F_A = 5^7 \text{ mod } 85 = 5^3 \cdot 5^3 \cdot 5 \text{ mod } 85 = (4 \cdot 10)^2 \cdot 5 \text{ mod } 85 = 16 \cdot 15 \cdot 5 \text{ mod } 85 = -5 \cdot 15 \text{ mod } 85 = -75 \text{ mod } 85 = 10$$
 (0,3 puntos)

Si el procedimiento es correcto, y sólo el resultado está mal se valora con la mitad de puntuación. En el resto de los casos no se valora el ejercicio


- c) $M = F_A^{e_A} = 10^{55} \text{ mod } 85 = 5$ **(0,3 puntos)**

Si el procedimiento es correcto, y sólo el resultado está mal se valora con la mitad de puntuación. En el resto de los casos no se valora el ejercicio



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



PROPUESTA DE EXAMEN 3 – Extraord. 1

PROPUESTA DE EXAMEN 3 – EXTRAORDINARIA 1 - ESPAÑOL

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Extraordinaria

Leganés – 30 Junio 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G81 ☐ G82 ☐ G83 ☐ G84 **NIA:**

PREGUNTAS DE RESPUESTA OBJETIVA

**Cada pregunta tiene una única opción correcta, que debe señalarse claramente redondeando la letra identificativa de la opción. Cada pregunta contestada incorrectamente será evaluada con menos un cuarto de la nota que se hubiese obtenido si hubiese sido correctamente respondida.
Cada una de las 8 preguntas tiene un valor de 0,2 puntos. Tiempo estimado: 20 min.**

1) Seleccione la afirmación que **NO** es correcta:

- a) El algoritmo de cifrado DES descompone el mensaje en claro en bloques y cifra cada uno de ellos con la misma clave.
- b) Los algoritmos de cifrado en bloque tienen como ventaja su baja velocidad de cifrado.
- c) DES, AES e IDEA son algoritmos de cifrado en bloque.
- d) DES usa una longitud de clave de 64 bits, aunque 8 de ellos son de paridad.

2) Sobre cifradores de flujo, indique cuál de las siguientes afirmaciones es verdadera:

- a) El cifrador de flujo más antiguo es el de Vigenére.
- b) Si la clave es más corta que el mensaje, hay que repetirla, y el cifrador de flujo se convierte en un cifrador de bloque modo CTR.
- c) Si la clave es periódica, tiene que ser muy larga, al menos tan larga como el mensaje.
- d) En modo autosíncrono no se propagan los errores de transmisión.

3) Señale la respuesta correcta:

- a) En una red compuesta de n nodos, con $n > 5$, en la que todos los nodos tienen que disponer de claves de cifrado y descifrado con el resto de nodos, se precisa un menor número de claves si se decide usar en la red criptografía asimétrica en lugar de simétrica.
- b) En la actualidad, y según la mayoría de los expertos en Criptografía, la aparición de la criptografía asimétrica supone el abandono a medio plazo de la simétrica.
- c) La fortaleza de un cifrador radica en el desconocimiento de su algoritmo, aunque la clave sea de público conocimiento.
- d) Ninguna de las respuestas anteriores es cierta.

4) Indique cuál es la complejidad computacional para realizar un ataque a una función MAC consistente en generar un mensaje M' diferente de uno M dado, con una longitud de clave k bits y una longitud de MAC de n bits, tal que $MAC(K, M') = MAC(K, M)$.

- a) $1 / 2^k$
- b) $1 / 2^n$
- c) $\min(1 / 2^k, 1 / 2^n)$
- d) $\max(1 / 2^k, 1 / 2^n)$

5) Seleccione la respuesta correcta:

- a) Una firma digital garantiza la integridad del mensaje recibido.
- b) Una firma digital no garantiza el repudio.
- c) Una firma digital asegura la confidencialidad.
- d) Las opciones a,b y c son correctas.

¿Cuál es tu trabajo ideal?



Haz el test aquí

<http://bit.ly/necesitouncambio>



¿Harto de c h a p a r a l g o q u e n o t e r e n t a ?

IRON
HACK

6) Seleccione la afirmación sobre los certificados digitales que es verdadera:

- a) El proceso de validación de un certificado X509 en el modelo de confianza PGP depende de la validez del certificado de la AC.
- b) Las ACs no disponen de sus propios certificados públicos, ya que sus claves privadas asociadas son empleadas por las AC para firmar directamente los certificados que emiten.
- c) Los certificados de "entidad final" a veces certifican la identidad de servidores web.
- d) Los certificados son documentos que recogen ciertos datos de su titular y su clave pública y están cifrados electrónicamente por la Autoridad de Certificación utilizando su clave pública.

7) Seleccione la respuesta correcta. La autenticación de entidades basada en tokens...:

- a) se basa en la posesión de un objeto capaz de generar contraseñas desechables.
- b) evita la necesidad de identificar a los usuarios.
- c) autentica las identidades mediante números que los usuarios autorizados memorizan para posteriores autenticaciones.
- d) típicamente, permiten modificar la contraseña de autenticación mensualmente.

8) ¿Qué regula la Ley 59/2003 de firma electrónica?

- a) Las tecnologías concretas que pueden utilizarse para generar firmas electrónicas que actúen como medio de autenticación.
- b) La Infraestructura de Clave Pública (PKI) del DNI electrónico, y sus posibles usos, entre otros.
- c) Transpone al ámbito nacional el formato de los certificados X.509 y las listas de revocación de certificados (CRL) definidos en el estándar internacional IETF RFC 5280.
- d) El concepto de firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Extraordinaria

Leganés – 30 Junio 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G81 ☐ G82 ☐ G83 ☐ G84 **NIA:**

CUESTIONES

CUESTIÓN 1. Valor = 0,2 ptos. Tiempo estimado: 10 min.

Defina el concepto de amenaza a un sistema y clasifíquelas respecto a su actuación.

CUESTIÓN 2. Valor = 0,2 ptos. Tiempo estimado: 10 min.

Enumere las diferentes etapas del protocolo de negociación (*handshake*) en SSL cuando no se requiere autenticación de cliente y el servidor emplea autenticación basada en certificado digital.

SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA

Examen Final – Convocatoria Extraordinaria

Leganés – 30 Junio 2010

Apellidos:

Nombre:

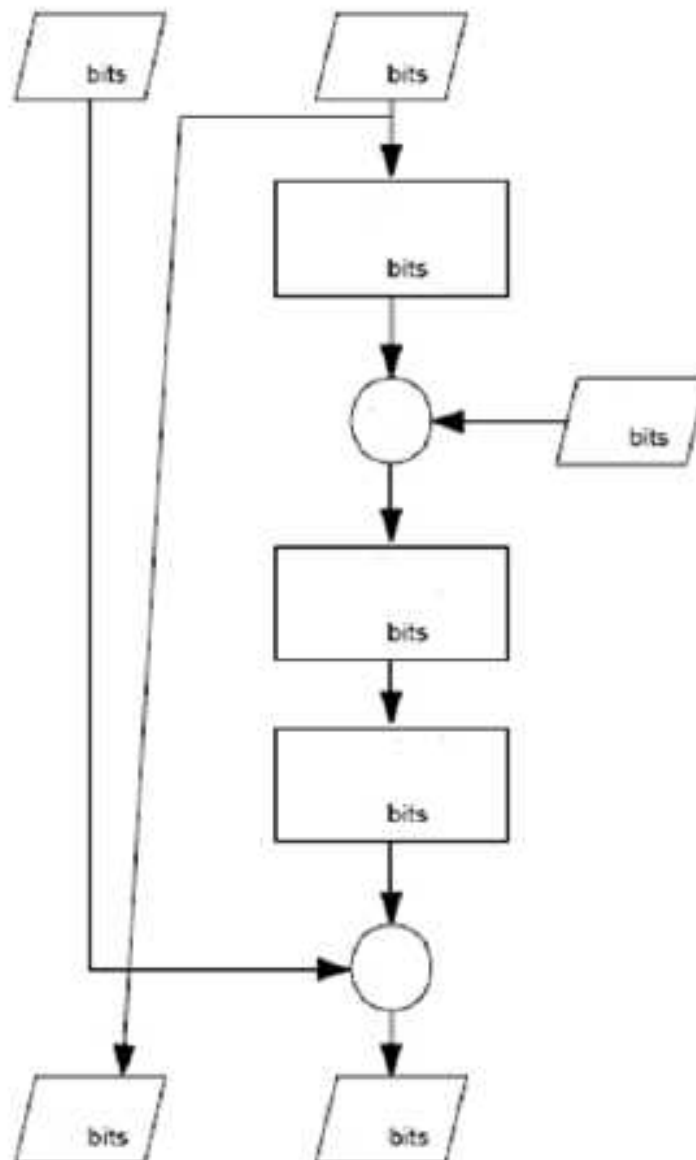
Grupo reducido: ☐ G81 ☐ G82 ☐ G83 ☐ G84 NIA:

PROBLEMAS

Problema 1. Valor = 1,5 ptos. Tiempo estimado: 40 min.

Sobre el cifrado simétrico en bloque proporcionado por el algoritmo DES:

a) La función F de la red de Feistel en DES se compone de una serie de fases y operaciones ejecutadas para cada bloque en una serie de rondas. Típicamente, podemos representar el **proceso general de una ronda con el siguiente diagrama de bloques**, al que le hemos borrado el título de cada fase, los símbolos de operación y sub-bloques y las etiquetas del número de bits por bloque en cada fase. **Rellene** cada elemento del diagrama con: el nombre correspondiente (nombre de la fase, de la operación o del dato) y el tamaño del bloque de la salida, así como los símbolos necesarios.



¿Cuál es tu trabajo ideal?



Haz el test aquí

<http://bit.ly/necesitouncambio>



¿Harto de c hapar algo que no te renta?



b) Sabiendo que la entrada a las cajas-S es:

101111001011111010011010100011010011000111101011

¿Cuál es la salida?

Fila	Columna																S-Caja
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S ₁
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S ₂
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S ₃
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	5	2	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	S ₄
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	15	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	S ₅
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	0	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	S ₆
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	0	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	S ₇
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	15	2	8	4	8	15	11	1	10	9	3	14	5	0	12	7	S ₈
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

S-cajas del algoritmo DES

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Extraordinaria

Leganés – 30 Junio 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G81 ☐ G82 ☐ G83 ☐ G84 **NIA:**

c) Sabiendo que la salida de R_0 es:

00000000111111101100110010000100

y que la sub-clave K_i es

000000111111000000111111000000111111000000111111

¿Cuál será la entrada a la Fase de Sustitución?

Caja E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Extraordinaria

Leganés – 30 Junio 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G81 ☐ G82 ☐ G83 ☐ G84 **NIA:**

Problema 2. Valor = 1,5 ptos. Tiempo estimado: 40 min.

A y B desean intercambiar mensajes. Para garantizar la autenticidad en dicho intercambio, los mensajes serán firmados por los interlocutores mediante el algoritmo RSA.

Una AC en la que confían A y B certifica sus claves públicas. El algoritmo utilizado por la AC es RSA y los certificados emitidos constan exclusivamente de la firma del exponente de la clave pública RSA correspondiente.

Considerando que los criptosistemas RSA de todas las entidades participantes operan con el mismo módulo $n=85$, que los certificados son $C_A=30$ y $C_B=9$ y que la clave pública de la AC es $(e_{AC}, n)=(3, 85)$

a) Calcule las claves privadas de A y B. Tenga en cuenta que no debería poder hacerlo si los números empleados correspondiesen a un sistema real, pero dado el tamaño de los números dados, es posible calcular dichas claves privadas sin gran dificultad


b) Suponga que $e_B=49$ y que el mensaje que B pretende enviar a A es $M=5$. Calcule la firma que B envía a A.

c) Realice los cálculos que lleva a cabo A, para verificar la firma de B.



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Extraordinary examination session

Leganés – June 1st 2010

Surname:

Name:

Group: ☐ G89

NIA:

PROPUESTA DE EXAMEN 3 – EXTRAORDINARIA 1 - INGLÉS

SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Extraordinary examination session

Leganés – June 1st 2010

Surname:

Name:

Group: ☐ G89

NIA:

MULTIPLE-CHOICE QUESTIONS

Each question has only one correct answer, which ought to be clearly pointed out rounding the letter identifying the option. Each question incorrectly answered will be evaluated as minus one fourth of the mark obtained had it been correctly answered.

Each of the 8 questions has a value of 0,2 points. Estimated time: 20 min.

1) Mark the **INCORRECT** statement:

- a) DES encryption algorithm divides the plain message in blocks and encrypts each of them with the same key.
- b) Block cipher algorithms present the advantage of being very slow.
- c) DES, AES and IDEA are block cipher algorithms.
- d) DES key length is 64 bits, but 8 of these bits are parity bits.

2) Regarding stream ciphers, mark the correct sentence:

- a) Vigenère is the oldest stream cipher algorithm.
- b) If the key is shorter than the message, it has to be reused, and the stream cipher becomes a block cipher working in CTR operation mode.
- c) If the key is periodic, it has to be very long, at least as long as the message.
- d) In auto-synchronous mode, transmission errors do not propagate.

3) Mark the correct statement:

- a) In a network composed of n nodes, with $n > 5$, where every node needs to have encryption and decryption keys, the use of asymmetric cryptography instead of symmetric cryptography implies the generation of fewer keys.
- b) According to experts in cryptography, the emergence of asymmetric cryptography will lead to stop using symmetric cryptography in the upcoming years.
- c) The strength of a cipher lies on the obscurity of the algorithm, regardless the key is publicly known.
- d) None of the above is true.

4) Indicate what is the computational complexity to perform an attack on a MAC function that consists of generating a message M' different to a given M , with a key length of k bits and a MAC length of n bits such that $\text{MAC}(K, M') = \text{MAC}(K, M)$.

- a) $1 / 2^k$
- b) $1 / 2^n$
- c) $\text{Min} (1 / 2^k, 1 / 2^n)$
- d) $\text{Max} (1 / 2^k, 1 / 2^n)$

5) Marck the correct statement:

- a) Electronic signatures guarantee integrity of received messages
- b) Electronic signatures do not guarantee repudiation
- c) Electronic signatures guarantee confidentiality.
- d) Sentences a, b and c are correct

¿Cuál es tu trabajo ideal?



Haz el test aquí



<http://bit.ly/necesitouncambio>



¿Harto de c h a p a r a l g o q u e n o t e r e n t a ?



6) Mark the correct statement:

- a) In PGP web-of-trust model, X509 certificate validation relies on verifying that CA's certificate is valid.
- b) The CAs do not have their own public certificates, as their associated private keys are used by the CAs to sign certificates directly.
- c) User certificates generally certify the identity of web servers.
- d) X509 certificates are documents that collect several details for the certificate owner and his public key, and also are encrypted by the CA's public key.

7) Choose the correct answer. User authentication based on tokens...:

- a) relies on the possession of an object that is able to generate one-time passwords.
- b) avoids the necessity of identifying users.
- c) authenticates the identities by means of numbers that authorized users memorize for future authentications.
- d) generally allows the modification of the authentication password once a month.

8) What does the 59/2003 Spanish Law (or the corresponding European Directive) on electronic signatures regulate?

- a) The specific technologies that can be employed to generate electronic signatures to be used as authentication means.
- a) The Public Key Infrastructure (PKI) of the Spanish electronic identity card (e-DNI), and its potential uses, among others.
- b) It incorporates into national law the format of X.509 certificates and certificate revocation lists (CRL) defined in the international standard IETF RFC 5280.
- c) The electronic signature concept, its legal effectiveness and the certification services supply.

SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Extraordinary examination session

Leganés – June 1st 2010

Surname:

Name:

Group: ☐ G89

NIA:

SHORT ANSWER QUESTIONS

QUESTION 1. Value = 0,2 pts. Estimated time: 10 min.

Define the concept of threat to a system and classify the possible threats regarding their operation mode.

QUESTION 2. Value = 0,2 pts. Estimated time: 10 min.

Enumerate the different stages of the SSL handshake protocol when client authentication is not required and the server is authenticated by means of a digital certificate.

SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Extraordinary examination session

Leganés – June 1st 2010

Surname:

Name:

Group: ☐ G89

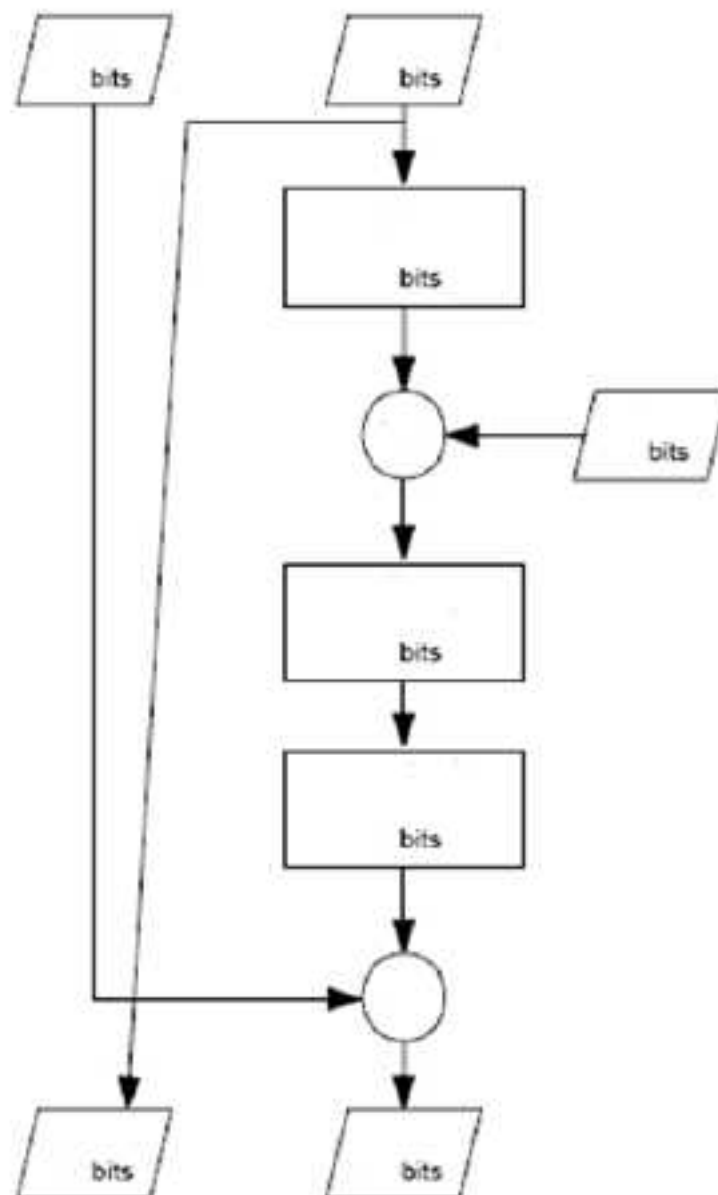
NIA:

PROBLEMS

Problem 1. Value = 1,5 pts. Estimated time: 40 min.

Regarding a symmetric block encryption algorithm provided by DES:

a) Feistel F function consists of a number of stages and operations on each message block in a set of rounds. Typically, we can represent the overall process with the following diagram. The title of each phase, the operation symbols and labels as well as the number of bits per block in each phase have been deleted. Fill each element of the diagram: label the phases, the operations and the data blocks, the size of the output data block, and the necessary symbols.



¿Cuál es tu trabajo ideal?



Haz el test aquí

<http://bit.ly/necesitouncambio>



¿Harto de c hapar algo que no te renta?

IRON
HACK

b) Let the following stream be the input to S-boxes:

101111001011111010011010100011010011000111101011

Compute the output.

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S ₁
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S ₂
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S ₃
13	7	0	8	3	4	6	10	2	8	5	14	12	11	15	1	
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	S ₄
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	S ₅
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	S ₆
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	S ₇
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
15	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	S ₈
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Extraordinary examination session

Leganés – June 1st 2010

Surname:

Name:

Group: ☐ G89

NIA:

c) Let the following stream be the R_0 sub-block

00000000111111101100110010000100

and the corresponding sub-key K_i is

000000111111000000111111000000111111000000111111

Compute the input to the substitution stage.

E-Box

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Extraordinary examination session

Leganés – June 1st 2010

Surname:

Name:

Group: ☐ G89

NIA:

Problem 2. Value = 1,5 pts. Estimated time: 40 min.

A and B want to exchange messages. To authenticate the transmitted data, messages will be signed with RSA algorithm.

Both A and B trust in a Certification Authority (CA) to certify their public keys. The CA uses RSA for this purpose, and the resulting certificates only contain the signature of the public key exponent.

Assuming that the RSA algorithm uses $n=85$, the certificates are $C_A=30$ and $C_B=9$ and the CA public key is $(e_{CA}, n)=(3, 85)$, answer the following questions:

- a) Get the public keys of A and B, using the information contained in their certificates.
- b) Suppose that $e_B=49$ and that the message B tries to send to A is $M=5$. Calculate the signature that B sends to A.
- c) Carry out the calculations that A makes to verify the signature of B



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



PROPUESTA DE EXAMEN 3 – Extraord. 1 - SOLUCIÓN

PROPUESTA DE EXAMEN 3 – EXTRAORDINARIA 1 – SOLUCIÓN

PREGUNTAS DE RESPUESTA OBJETIVA

1) **TEST.** Seleccione la afirmación incorrecta.

- a) El método de cifrado DES descompone el mensaje en claro en bloques y cifra cada uno de ellos con la misma clave
- b) Los métodos de cifrado en bloque tienen como ventaja su baja velocidad de cifrado
- c) DES, AES e IDEA son cifradores de bloque
- d) DES usa una longitud de clave de 64 bits, aunque 8 de ellos son de paridad

2) **Sobre Cifradores de flujo.**

Indique cuál de las siguientes afirmaciones es verdadera:

- a) El cifrador de flujo más antiguo es el de Vigenére.
- b) Si la clave es más corta que el mensaje, hay que repetirla, y el cifrador de flujo se convierte en un cifrador de bloque.
- c) Si la clave es periódica, tiene que ser muy larga, al menos tan larga como el mensaje.
- d) En modo autosíncrono no se propagan los errores de transmisión.

3) Señale la respuesta correcta:

- a) ☒ En una red compuesta de n nodos, con $n > 5$, en la que todos los nodos disponen de claves de cifrado y descifrado con el resto de nodos, se precisa un menor número de claves si se decide usar en la red criptografía asimétrica en lugar de simétrica
- b) ☐ En la actualidad, y según la mayoría de los expertos en Criptografía, la aparición de la criptografía asimétrica supone el abandono a medio plazo de la simétrica
- c) ☐ La fortaleza de un cifrador radica en el desconocimiento de su algoritmo, aunque la clave sea de público conocimiento
- d) ☐ Ninguna de las respuestas anteriores es cierta

4) **Pregunta (Test):** Indique cuál es la complejidad computacional para realizar un ataque a una función MAC consistente en generar un mensaje M' diferente de un M dado, con una longitud de clave k bits y una longitud de MAC n bits.

Question (Test): Indicate what is the computational complexity to perform an attack on a MAC function that consists of generating a message M' different to a given M , with a key length of k bits and a MAC length of n bits.

Respuesta:

- a) $1 / 2^k$
- b) $1 / 2^n$
- c) $\text{Min} (1 / 2^k, 1 / 2^n)$
- d) $\text{Max} (1 / 2^k, 1 / 2^n)$

5) **TEST.** Seleccione la opción correcta

- a) Una firma digital garantiza la integridad del mensaje recibido
- b) Una firma digital no garantiza el repudio
- c) Una firma digital asegura la confidencialidad
- d) Las opciones a,b y c son correctas

6) **CERTIFICADOS DIGITALES**

- a) El proceso de validación de un certificado X509 en el modelo de confianza PGP depende de la validez del certificado de la AC.
- b) Las ACs no disponen de sus propios certificados públicos, ya que sus claves privadas asociadas son empleadas por las AC para firmar directamente los certificados que emiten.

PROPUESTA DE EXAMEN 3 – Extraord. 1 - SOLUCIÓN

- c) Los certificados de "entidad final" a veces designan servidores web (y entonces los certificados se emplean dentro del protocolo SSL).
- d) Los certificados son documentos que recogen ciertos datos de su titular y su clave pública y están cifrados electrónicamente por la Autoridad de Certificación utilizando su clave pública.

7) La autenticación de entidades basada en tokens

- ☒ se basa en la posesión de un objeto capaz de generar contraseñas desechables
- ☐ evita la necesidad de identificar a los usuarios
- ☐ autentica las identidades mediante números que los usuarios autorizados memorizan para posteriores autenticaciones
- ☐ típicamente, permiten modificar la contraseña de autenticación mensualmente

8) Pregunta (Test): ¿Qué regula la Ley 59/2003 de firma electrónica?

Question (Test): What does the 59/2003 Spanish Law on electronic signatures regulate?

Respuesta:

- a) Las tecnologías concretas que pueden utilizarse para generar firmas electrónicas que actúen como medio de autenticación.
- b) La Infraestructura de Clave Pública (PKI) del DNI electrónico, y sus posibles usos, entre otros.
- c) Transpone al ámbito nacional el formato de los certificados X.509 y las listas de revocación de certificados (CRL) definidos en el estándar internacional IETF RFC 5280.
- d) El concepto de firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

¿Cuál es tu trabajo ideal?



Haz el test aquí

<http://bit.ly/necesitouncambio>



¿Harto de c h a p a r algo que no te renta?

IRON
HACK

CUESTIONES

CUESTIÓN 1. Valor = 0,2 ptos. Tiempo estimado: 10 min.

Defina el concepto de amenaza a un sistema y clasifíquelas respecto a su actuación.

Amenaza: Potencial violación (accidental o intencionada) de la seguridad de la información. Es cualquier acción que ponga en peligro los objetivos de la seguridad
Clasificación de amenazas según su actuación:

Pasivas: Interceptación (Sniffers)

Activas: Interrupción (Inundación: SYN, Smurf, ...)

Modificación (Falsificación de direcciones IP, Suplantación de DNS)

Generación (Secuestro de la sesión)

CUESTIÓN 2. Valor = 0,2 ptos. Tiempo estimado: 10 min.

Pregunta (Teoría): Enumere las diferentes etapas del protocolo de negociación (*handshake*) en SSL cuando no se requiere autenticación de cliente y el servidor emplea autenticación basada en certificado digital.

Question (Theory): Enumerate the different stages of the SSL handshake protocol when client authentication is not required and the server is authenticated by means of a digital certificate.

Respuesta:

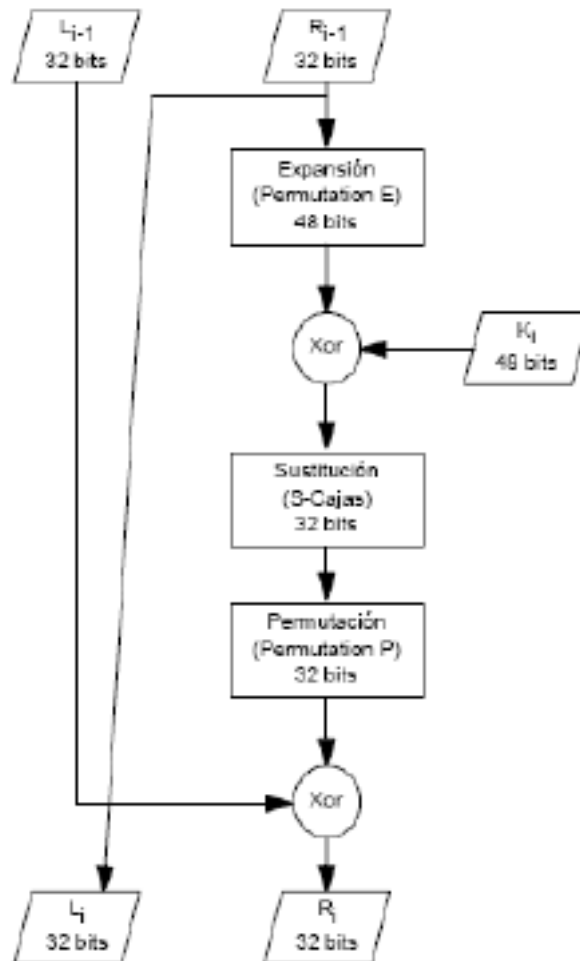
- 1) **Client Hello:** El cliente genera un valor aleatorio C y envía al servidor el número de versión, el valor aleatorio C, y ciphersuite (opciones de intercambio de claves y autenticación, algoritmos de cifrado y funciones resumen).
- 2) **Server Hello:** El servidor genera un valor aleatorio S y envía al cliente el número de versión, el valor aleatorio S, y ciphersuite (seleccionado en base al enviado por el cliente).
- 3) El Servidor envía su certificado digital junto con la cadena de certificación.
- 4) El Servidor envía el mensaje *Server Hello Done* al Cliente.
- 5) El Cliente verifica el certificado del servidor, y, en caso que éste sea correcto y confíe en él, calcula el valor de *pre-master-secret key*, y se la envía al servidor cifrada con la clave pública contenida en el certificado de servidor.
- 6) Tanto Servidor como Cliente componen la *master-secret key* a partir de los valores C, S y *pre-master-secret key*.
- 7) El Cliente y el Servidor se intercambian sendos mensajes indicando que ha finalizado la negociación, y pasan a modo cifrado. En estos mensajes se incorporan los valores MAC de todos los mensajes intercambiados hasta el momento, y empleando la *master-secret key*.

PROPUESTA DE EXAMEN 3 – Extraord. 1 - SOLUCIÓN

PROBLEMAS

Problema 1. (SOLUCIÓN)

a)



b) 101111 001011 111010 011010 100011 010011 000111 101011
 7 2 10 4 8 1 7 10

En binario: 0111 0010 1010 0010 1000 0001 0111 1010

c)

E(R₀) = 000000 000001 011111 111101 011001 011001 010000 001000

Ahora hay que realizar la suma OR exclusiva con la clave K_i.

0000000000001011111111101011001011001010000001000

000000111111000000111111000000111111000000111111

000000111110011111000010011001100110010000110111

Problema 2. (SOLUCIÓN)

a) $C_A=30=e_A^{d_{AC}}$; $e_A=30^e_{AC}=30^3 \bmod 85 = (3 \cdot 10)^3 \bmod 85 = 3^3 \cdot 15 \cdot 10 \bmod 85 = 15 \cdot 15 \bmod 85 = 55$ **(0,25 puntos)**

$$d_A = e_A^{-1} \bmod \Phi(n) = 55^{-1} \bmod 64$$

Aplicando Euclides modificado

	1	6
64	55	9
9	1	

$$9 = 64 - 55$$

$$1 = 55 - 9 \cdot 6 = 55 - 6(64 - 55) = 7 \cdot 55 - 6 \cdot 64$$

Por lo que $d_A=7$ **(0,25 puntos)**

Nota: Se acepta también como solución $d_A=71$ que también pertenece a \mathbb{Z}_{85}

$C_B=9=e_B^{d_{BC}}$; $e_B=9^e_{AC}=9^3 \bmod 85 = 49$ **(0,25 puntos)**

$$d_B = e_B^{-1} \bmod \Phi(n) = 49^{-1} \bmod 64$$

Aplicando Euclides modificado

	1	3	3	1
64	49	15	4	3
15	4	3	1	

$$15 = 64 - 49$$

$$4 = 49 - 15 \cdot 3$$

$$3 = 15 - 4 \cdot 3$$

$$1 = 4 - 3 = 4 - (15 - 4 \cdot 3) = 4 \cdot 4 - 15 = 4(49 - 15 \cdot 3) - 15 = 4 \cdot 49 - 13 \cdot 15 = 4 \cdot 49 - 13(64 - 49) = 17 \cdot 49 - 13 \cdot 64$$

Por lo que $d_B=17$ **(0,25 puntos)**

Nota: Se acepta también como solución $d_B=81$ que también pertenece a \mathbb{Z}_{85}

Si el procedimiento es correcto, y sólo el resultado está mal se valora con la mitad de puntuación. En el resto de los casos no se valora el ejercicio

b) $F_B = M^{d_B} \bmod n$; $F_B = 5^{17} \bmod 85$
 $5^7 \bmod 85 = 5^3 \cdot 5^3 \cdot 5 \bmod 85 = (4 \cdot 10)^2 \cdot 5 \bmod 85 = 16 \cdot 15 \cdot 5 \bmod 85 = -5 \cdot 15 \bmod 85 = -75 \bmod 85 = 10$
 $F_B = 5^{17} \bmod 85 = 10^2 \cdot 5^3 \bmod 85 = 15 \cdot 4 \cdot 10 \bmod 85 = 5$ **(0,25 puntos)**

Si el procedimiento es correcto, y sólo el resultado está mal se valora con la mitad de puntuación. En el resto de los casos no se valora el ejercicio

c) $M = F_B^{e_B} = 5^{49} \bmod 85 = 5$ **(0,25 puntos)**

Si el procedimiento es correcto, y sólo el resultado está mal se valora con la mitad de puntuación. En el resto de los casos no se valora el ejercicio

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Extraordinaria

Colmenarejo – 22 Junio 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G80 ☐ G81


NIA:

PROPUESTA DE EXAMEN 4 – EXTRAORDINARIA 2



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Extraordinaria

Colmenarejo – 22 Junio 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G80 ☐ G81

NIA:

PREGUNTAS DE RESPUESTA OBJETIVA

**Cada pregunta tiene una única opción correcta, que debe señalarse claramente redondeando la letra identificativa de la opción. Cada pregunta contestada incorrectamente será evaluada con menos un cuarto de la nota que se hubiese obtenido si hubiese sido correctamente respondida.
Cada una de las 8 preguntas tiene un valor de 0,2 puntos. Tiempo estimado: 20 min.**

- 1) ¿Cómo pueden eliminarse los riesgos de seguridad en un sistema informático?
 - a) Mediante medidas técnicas, organizativas, legales y físicas.
 - b) Únicamente mediante medidas técnicas, como cifrado de datos o autenticación de usuarios.
 - c) Si un sistema informático se diseña correctamente, no es necesario afrontar riesgos de seguridad.
 - d) Los riesgos nunca pueden eliminarse, sino que se mitigan.
- 2) Sobre el cifrado polialfabeto, indique cuál de las siguientes afirmaciones es verdadera:
 - a) El cifrado de Vigenère equivale a una sustitución monoalfabeto con clave.
 - b) Los cifradores polialfabeto aplican el mismo mensaje como clave principal.
 - c) El cifrador autoclave es una variante del algoritmo Vigenère donde la clave es tan larga como el mensaje.
 - d) Ninguna de las anteriores es cierta.
- 3) Seleccione la opción correcta:
 - a) Los cifradores de flujo descomponen el mensaje en símbolos (caracteres o bits)
 - b) En el cifrado de flujo síncrono emisor y receptor no tienen porqué estar sincronizados
 - c) Existen algoritmos finitos que generan sucesiones realmente aleatorias
 - d) Normalmente los cifradores de flujo son más lentos que los cifradores de bloque
- 4) El cifrado asimétrico:
 - a) Se conoce también como cifrado de clave secreta.
 - b) Se utiliza exclusivamente para lograr la confidencialidad de las comunicaciones.
 - c) Es más rápido que el cifrado simétrico.
 - d) Suele utilizarse para cifrar claves de sesión simétricas.
- 5) ¿Cuál de las siguientes propiedades de seguridad no la aporta un esquema de firma digital?
 - a) Confidencialidad.
 - b) Integridad.
 - c) No repudio.
 - d) Autenticación.
- 6) Seleccione la opción que **NO** es correcta:
 - a) Una lista CRL contiene un listado de certificados revocados.
 - b) Las Autoridades de Certificación están organizadas de acuerdo a un modelo jerárquico.
 - c) Un certificado x.509 puede pertenecer, entre otros, a una persona jurídica.
 - d) Las opciones a,b y c son falsas.

7) El protocolo *handshake* de SSL:

- a) Se encarga de cifrar la información entre cliente y servidor.
- b) Se encarga de la autenticación del cliente y, opcionalmente, del servidor.
- c) Sirve para negociar la clave simétrica de cifrado entre cliente y servidor.
- d) Se encarga de alertar al cliente y al servidor cuando algún paquete no presenta la MAC correcta.

8) En relación a los aspectos legales:

- a) En la Ley 59/2003 de España de firma electrónica denomina a las autoridades de certificación como Prestadores de servicios de certificación.
- b) La firma electrónica avanzada es la firma electrónica basada en un certificado reconocido y generada por un dispositivo seguro de creación de firma.
- c) No existe en la actualidad ninguna ley española que permita proteger cualquier tipo de información que se transmita por redes de comunicaciones electrónicas mediante procedimientos de cifrado.
- d) Todas las anteriores son falsas.

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Extraordinaria

Colmenarejo – 22 Junio 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G80 ☐ G81

NIA:

CUESTIONES

CUESTIÓN 1. Valor = 0,2 ptos. Tiempo estimado: 10 min.

Indique al menos 2 ventajas y 2 inconvenientes de la criptografía de clave pública en comparación con la criptografía simétrica.


CUESTIÓN 2. Valor = 0,2 ptos. Tiempo estimado: 10 min.

Describa brevemente el concepto de sistema de autenticación biométrica y los problemas que presenta.



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA

Examen Final – Convocatoria Extraordinaria

Colmenarejo – 22 Junio 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G80 ☐ G81

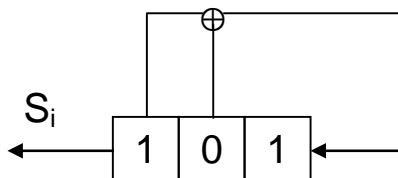
NIA:

PROBLEMAS

Problema 1. Valor = 1,5 ptos. Tiempo estimado: 45 min

Alicia desea enviar confidencialmente a Benito el mensaje $M=218$. Para lograrlo utiliza un sistema de cifrado híbrido (análogo al empleado en PGP) basado en el criptosistema RSA y en el algoritmo de clave secreta $E(M, J) = (M + J) \bmod 256$, donde J representa la clave de sesión. La clave pública de Benito es $K_{Bu}=(e_b, n_b)=(5, 69)$ y la de Alicia $K_{Au}=(e_a, n_a)=(7, 65)$. Alicia genera la clave de sesión seleccionando los 6 primeros bits que proporciona un LFSR cuyo polinomio de conexión viene definido por $C(D)=D^3 + D^2 + 1$.

- a) Calcule la clave de sesión generada teniendo en cuenta que el estado actual del LFSR es 101. Indique, además, el periodo de la secuencia generada por el LFSR y si éste es máximo.



- b) Ignore el resultado del apartado anterior y suponga que $J=111001_2$. Calcule y explicita el mensaje completo que Benito recibe de Alicia, sabiendo que Benito no dispone del LFSR.
- c) Ignore el resultado del apartado anterior y suponga que Benito recibe el valor 8 como resultado del cifrado simétrico realizado por Alicia y el valor 9 como resultado del cifrado asimétrico de la correspondiente clave de sesión. Realice las operaciones que ha de acometer Benito para descifrar el criptograma recibido y obtenga el texto en claro (calcule aquellos datos que usted precise y que Benito conoce).

(NOTA: $57^2 \bmod 69 = 6$)

SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA

Examen Final – Convocatoria Extraordinaria

Colmenarejo – 22 Junio 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G80 ☐ G81

NIA:

Problema 2. Valor = 1,5 ptos. Tiempo estimado: 30 min

Alicia desea transmitir a Benito el día del examen. Para ello cifra el mensaje en claro. Alicia usa el criptosistema ElGamal con:

- $p=17$
- $g=7$
- $X_B=5$
- $k=9$


- El día del examen es el 15 de Mayo de 2010, es decir $M=15$

- a) Obtenga el cifrado (r, s) que Alicia debe transmitir.
- b) Realice los cálculos que Benito debe realizar para descifrar el mensaje.



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



PROPUESTA DE EXAMEN 4 – Extraord. 2 - SOLUCIÓN

PROPUESTA DE EXAMEN 4 – EXTRAORDINARIA 1 – SOLUCIÓN

TEORÍA

Pregunta (Test): ¿Cómo pueden eliminarse los riesgos de seguridad en un sistema informático?

Question (Test): How can IT security risks be eliminated?

Respuesta:

- a) Mediante medidas técnicas, organizativas, legales y físicas.
- b) Únicamente mediante medidas técnicas, como cifrado de datos o autenticación de usuarios.
- c) Si un sistema informático se diseña correctamente, no es necesario afrontar riesgos de seguridad.
- d) Los riesgos nunca pueden eliminarse, sino que se mitigan.

Answer:

- a) By means of technical, organizational, legal and physical mechanisms.
- b) Only by means of technical mechanisms, like data encryption or user authentication.
- c) If an IT system is correctly designed, it is not necessary to face IT security risks.
- d) Risks are never eliminated, but mitigated.

1. Sobre Cifrado Polialfabeto.

Indique cuál de las siguientes afirmaciones es verdadera:

- a) El cifrado de Vigenère equivale a una sustitución monoalfabeto con clave.
- b) Los cifradores polialfabeto aplican el mismo mensaje como clave principal.
- c) **El cifrador autoclave es una variante del algoritmo Vigenère donde la clave es tan larga como el mensaje.**
- d) Ninguna de las anteriores es cierta.

TEST. Seleccione la opción correcta

- a) **Los cifradores de flujo descomponen el mensaje en símbolos (caracteres o bits)**
- b) En el cifrado de flujo síncrono emisor y receptor no tienen porqué estar sincronizados
- c) Existen algoritmos finitos que generan sucesiones realmente aleatorias
- d) Normalmente los cifradores de flujo son más lentos que los cifradores de bloque

5.- El cifrado asimétrico

- a) ☐ se le conoce también como cifrado de clave secreta
- b) ☐ se utiliza exclusivamente para lograr la confidencialidad de las comunicaciones
- c) ☐ es más rápido que el cifrado simétrico
- d) ☒ suele utilizarse para cifrar claves de sesión simétricas

Pregunta (Test): ¿Cuál de las siguientes propiedades de seguridad no la aporta un esquema de firma digital?

Question (Test): What security property is not provided by a digital signature scheme?

Respuesta:

- a) Confidencialidad
- b) Integridad
- c) No repudio
- d) Autenticación

Answer:

PROPUESTA DE EXAMEN 4 – Extraord. 2 - SOLUCIÓN

- a) Confidentiality
- b) Integrity
- c) Non-repudiation
- d) Authentication

TEST. Seleccione la opción incorrecta:

- a) Una lista CRL contiene un listado de certificados revocados
- b) Las Autoridades de Certificación están organizadas de acuerdo a un modelo jerárquico
- c) Un certificado x.509 puede pertenecer, entre otros, a una persona jurídica
- d) Las opciones a,b y c son falsas

10.- El protocolo *handshake* de SSL

- a) ☐ se encarga de cifrar la información entre cliente y servidor
- b) ☐ se encarga de la autenticación del cliente y, opcionalmente, del servidor
- c) ☒ sirve para negociar la clave simétrica de cifrado entre cliente y servidor
- d) ☐ se encarga de alertar al cliente y al servidor cuando algún paquete no presenta la MAC correcta

ASPECTOS LEGALES

- a) En la Ley 59/2003 de España de firma electrónica denomina a las autoridades de certificación como Prestadores de servicios de certificación.
- b) La firma electrónica avanzada es la firma electrónica basada en un certificado reconocido y generada por un dispositivo seguro de creación de firma.
- c) No existe en la actualidad ninguna ley española que permita proteger cualquier tipo de información que se transmita por redes de comunicaciones electrónicas mediante procedimientos de cifrado.
- d) Todas las anteriores son falsas.

¿Cuál es tu trabajo ideal?



Haz el test aquí 

<http://bit.ly/necesitouncambio>



¿Harto de c h a p a r algo que no te renta?

IRON
HACK

CUESTIONES

QUESTION 1. Value = 0,2 ptos. Estimated time: 10 min.

Pregunta (Teoría): Indique al menos 2 ventajas y 2 inconvenientes de la criptografía de clave pública en comparación con la criptografía simétrica.

Question (Theory): Indicate, at least, 2 advantages and 2 disadvantages of public key cryptography compared with the secret key cryptography.

Respuesta:

Ventajas → no exige la existencia de un canal seguro / la gestión de claves es más sencilla, por lo que los sistemas escalan mejor ante mayor número de usuarios.

Desventajas → la propia naturaleza de los criptosistemas exige la existencia de 2 claves diferentes (asimetría) / son más lentos que los criptosistemas simétricos.

QUESTION 2. Value = 0,2 ptos. Estimated time: 10 min.

TEORÍA. Describa brevemente el sistema de autenticación biométrica y los problemas que presenta

El sistema autentica al usuario basándose en rasgos biométricos (característica física única e irrepetible)

Existe un proceso de registro en el sistema (extracción del patrón biométrico y almacenamiento)

El proceso de autenticación implica la obtención del patrón biométrico del usuario, y su comparación con el patrón almacenado

Múltiples técnicas biométricas (huella dactilar, iris, vascular, geometría de la mano, escritura y firma manuscrita, voz, ...)

Diferentes tasas de eficacia (falsos positivos / falsos negativos)

PROPUESTA DE EXAMEN 4 – Extraord. 2 - SOLUCIÓN

PROBLEMAS

Problema 1. Valor = 1,5 pts. Tiempo estimado: X

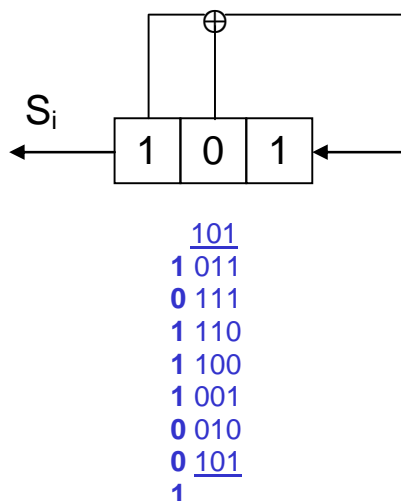
Alicia desea enviar confidencialmente a Benito el mensaje $M=218$. Para lograrlo utiliza un sistema de cifrado híbrido (análogo al empleado en PGP) basado en el criptosistema RSA y en el algoritmo de clave secreta $E(M, J) = (M + J) \bmod{256}$, donde J representa la clave de sesión. La clave pública de Benito es $K_{Bu}=(e_b, n_b)=(5, 69)$ y la de Alicia $K_{Au}=(e_a, n_a)=(7, 65)$. Alicia genera la clave de sesión seleccionando los 6 primeros bits que proporciona un LFSR cuyo polinomio de conexión viene definido por $C(D)=D^3 + D^2 + 1$.

- d) Calcule la clave de sesión generada teniendo en cuenta que el estado actual del LFSR es 101. Indique, además, el periodo de la secuencia generada por el LFSR y si éste es máximo.
- e) Ignore el resultado del apartado anterior y suponga que $J=111001_{(2)}$. Calcule y explice el mensaje completo que Benito recibe de Alicia, sabiendo que Benito no dispone del LFSR.
- f) Ignore el resultado del apartado anterior y suponga que Benito recibe el valor 8 como resultado del cifrado simétrico realizado por Alicia y el valor 9 como resultado del cifrado asimétrico de la correspondiente clave de sesión. Realice las operaciones que ha de acometer Benito para descifrar el criptograma recibido y obtenga el texto en claro (calcule aquellos datos que usted precise y que Benito conoce).

(NOTA: $57^2 \bmod{69} = 6$)

Problema 1. (SOLUCIÓN)

a)



La clave de sesión es $J=101110_{(2)}=46_{(10)}$. El periodo de la secuencia es 7. El periodo de un LFSR es máximo si el polinomio de conexión es primitivo (como en este caso) y viene dado por $2^L - 1$, siendo L el grado de su polinomio de conexión. En el problema planteado, $L=3$ y el periodo es $T=2^3 - 1=7$, por lo que es máximo.

b)

$J=111001_{(2)}=57_{(10)}$

Alicia cifra simétricamente el mensaje M con la clave J:

$$E(M,J) = E(218, 57) = 218 + 57 \text{ mód. } 256 = 19$$

Alicia cifra asimétricamente la clave J con la clave pública de Benito:

$$E_{KBu}(J) = E_{KBu}(57) = 57^2 \cdot 57^2 \cdot 57 \text{ mód. } 69 = 6 \cdot 6 \cdot (-12) \text{ mód. } 69 = -3 \cdot 6 \text{ mód. } 69 = 51$$

ó alternativamente:

$$E_{KBu}(J) = E_{KBu}(57) = 57^5 \text{ mód. } 69 = (-12)^5 \text{ mód. } 69 = -(4 \cdot 3)^5 \text{ mód. } 69 = -(-5 \cdot 16 \cdot 12 \cdot 3) \text{ mód. } 69 = 5 \cdot 4^3 \cdot 3^2 \text{ mód. } 69 = 5 \cdot 2^6 \cdot 3^2 \text{ mód. } 69 = 5 \cdot 2^3 \cdot 3 \text{ mód. } 69 = 2 \cdot (-9) \text{ mód. } 69 = 51$$

Finalmente, Alicia le envía a Benito ambos resultados **$(E(M,J), E_{KBu}(J)) = (19, 51)$**

c)

Para descifrar el mensaje, Benito ha de descifrar $E_{KBu}(J') = 9$ con su clave privada para obtener J' . Después descifrá $E(M',J') = 8$ con la clave obtenida.

Cálculo de la clave privada de Benito:

$$5 \text{ d mód. } \Phi(69) = 1$$

$$\Phi(69) = \Phi(3 \cdot 23) = 2 \cdot 22 = 44$$

$$5 \text{ d mód. } 44 = 1$$

$$\mathbf{d=9}$$

$$J' = D_{KBu}(E_{KBu}(J')) = (E_{KBu}(J'))^d \text{ mód. } 69 = 9^9 \text{ mód. } 69 = 81 \cdot 81 \cdot 81 \cdot 81 \cdot 9 \text{ mód. } 69 = 12 \cdot 12 \cdot 12 \cdot 12 \cdot 9 \text{ mód. } 69 = 4^4 \cdot 3^6 \text{ mód. } 69 = 4^3 \cdot 4 \cdot 81 \cdot 3^2 \text{ mód. } 69 = -5 \cdot 4 \cdot 12 \cdot 3^2 \text{ mód. } 69 = 9 \cdot 4 \cdot 3^2 \text{ mód. } 69 = 81 \cdot 4 \text{ mód. } 69 = 12 \cdot 4 \text{ mód. } 69 = \mathbf{48}$$

$$\mathbf{M' = D(E(M',J'),J') = D(8, 48) = 8 - 48 \text{ mód. } 256 = \mathbf{216}}$$

PROPUESTA DE EXAMEN 4 – Extraord. 2 - SOLUCIÓN

Problema 2. Valor = 1,5 ptos. Tiempo estimado: X

Alicia desea transmitir a Benito el día del examen. Para ello cifra el mensaje en claro. Alicia usa el criptosistema ElGamal con:

- $p=17$
- $g=7$
- $X_B=5$
- $k=9$

- El día del examen es el 15 de Mayo de 2010, es decir $M=15$

c) Obtenga el cifrado (r, s) que Alicia debe transmitir. **(1 punto)**

d) Realice los cálculos que Benito debe realizar para descifrar el mensaje. **(0,5 puntos)**

Problema 2. (SOLUCIÓN)

a)

$$r = g^k \pmod{p} = 7^9 \pmod{17} = (7^2)^4 \cdot 7 \pmod{17} = (-2)^4 \cdot 7 \pmod{17} = (-1) \cdot 7 \pmod{17} = 10 \quad \textbf{(0,25 puntos)}$$

$$Y_B = g^{X_B} \pmod{p} = 7^5 \pmod{17} = (7^2)^2 \cdot 7 \pmod{17} = (-2)^2 \cdot 7 \pmod{17} = 4 \cdot 7 \pmod{17} = 11 \quad \textbf{(0,25 puntos)}$$

$$s = M \cdot Y_B^k \pmod{p} = 15 \cdot 11^9 \pmod{17} = (-2) \cdot (11^2)^4 \cdot 11 \pmod{17} = (-2) \cdot (2)^4 \cdot 11 \pmod{17} = (-2) \cdot (-1) \cdot 11 \pmod{17} = 5 \quad \textbf{(0,5 puntos)}$$

$$C = (r, s) = (10, 5)$$


b)

$$M = r^{p-1-X_B} \cdot s \pmod{p} = 10^{16-5} \cdot 5 \pmod{17} = 10^{11} \cdot 5 \pmod{17} = (10^2)^5 \cdot 10 \cdot 5 \pmod{17} = (-2)^5 \cdot 10 \cdot 5 \pmod{17} = (-1) \cdot (-2) \cdot (-1) \pmod{17} = 15 \quad \textbf{(0,5 puntos)}$$



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



PROPUESTA DE EXAMEN 5 – Ord. EXTRA 1

PROPUESTA DE EXAMEN 5 – ORDINARIA EXTRA 1 - ESPAÑOL

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria (EXTRA)

Leganés – 1 Junio 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G81 ☐ G82 ☐ G83 ☐ G84

NIA:

PREGUNTAS DE RESPUESTA OBJETIVA

Cada pregunta tiene una única opción correcta, que debe señalarse claramente redondeando la letra identificativa de la opción. Cada pregunta contestada incorrectamente será evaluada con menos un cuarto de la nota que se hubiese obtenido si hubiese sido correctamente respondida.

Cada una de las 8 preguntas tiene un valor de 0,2 puntos. Tiempo estimado: 20 min.

1) En relación a criptoanálisis:

- a) Cuando sólo se tiene acceso al criptograma el ataque de criptoanálisis más apropiado se denomina de texto cifrado elegido.
- b) Cuando se tiene acceso al criptograma y a una parte del texto en claro el ataque de criptoanálisis más apropiado se denomina de texto cifrado elegido.
- c) Cuando sólo se tiene acceso al criptograma elegido y a su descifrado el ataque de criptoanálisis más apropiado se denomina de texto cifrado elegido.
- d) Cuando sólo se tiene acceso al criptograma elegido y a su descifrado el ataque de criptoanálisis más apropiado se denomina de texto en claro elegido.

2) Sobre generadores LFSR de series cifrantes, determine cuál de las siguientes características corresponde a una secuencia generada con un LFSR representado por un polinomio primitivo:

- a) El periodo T de la secuencia depende de la semilla.
- b) T no depende de la semilla, y será máxima con $T_{\max} = 2^n - 1$
- c) Se generan secuencias de periodo $T_{\max} = 2^n - 1$
- d) Se generan secuencias de periodo $T_{\max} = 2^{n-1}$

3) Seleccione la opción **INCORRECTA**:

- a) El artículo seminal de Diffie-Hellman en 1976 supuso el nacimiento de los sistemas de clave pública.
- b) El protocolo Diffie-Hellman no es autenticado, permite ataques de hombre interpuesto.
- c) La criptografía de clave pública emplea dos tipos de claves, la pública y la privada.
- d) Una condición imprescindible en criptografía de clave pública es que la clave privada sea fácilmente deducible a partir de la clave pública.

4) En relación a las funciones resumen criptográficas podemos afirmar que:

- a) La longitud de la huella digital de un mensaje M viene determinada por el tamaño de M.
- b) Las funciones resumen se usan exclusivamente para facilitar la firma digital.
- c) La probabilidad de hallar dos mensajes diferentes, M1 y M2, que produzcan la misma huella digital es mayor que la probabilidad de encontrar un mensaje, M1, que produzca la misma huella digital que otro dado M2.
- d) Ninguna de las anteriores es cierta

5) ¿En qué campo de un certificado X.509 v3 se incluye los posibles usos autorizados de las claves criptográficas correspondientes?

- a) En las extensiones del certificado, al ser información opcional.
- b) En el campo obligatorio donde se incluye la información de la clave pública.
- c) Se define en la política del certificado, ajena a la estructura del certificado.
- d) No es posible restringir los usos de las claves criptográficas.

¿Cuál es tu trabajo ideal?



Haz el test aquí



<http://bit.ly/necesitouncambio>



¿Harto de c hapar algo que no te renta?



6) Seleccione la opción correcta:

- a) Un token OTP genera una contraseña válida para varias sesiones.
- b) Un token OTP se basa en la aleatoriedad, evitando ataques por predicción.
- c) En los token OTP síncronos existe sincronía entre el reloj del cliente y el del servidor de autenticación.
- d) En un token OTP basado en desafíos la generación de un OTP depende del OTP anterior.

7) En relación a los protocolos criptográficos:

- a) Una de las fases básicas del protocolo SSL consiste en negociar, entre ambas partes, el algoritmo de cifrado que se usará en la comunicación.
- b) En la fase de intercambio de claves públicas y autenticación SSL en ocasiones no se requiere que el cliente envíe su certificado digital.
- c) Tras el establecimiento de sesión SSL el tráfico no se transmite en claro, se cifra con cifrado simétrico.
- d) Todas las anteriores son correctas.

8) Tomando como referencia la Ley 59/2003 de Firma Electrónica española y la Directiva Europea 1999/93/CE, seleccione la opción correcta:

- a) La firma electrónica avanzada es la firma digital del resumen (o huella digital) de un mensaje.
- b) La firma electrónica garantiza la autoría e integridad del mensaje que se firma.
- c) La firma electrónica reconocida es la que se ejecuta en un PC de propósito general con la clave privada del firmante.
- d) La firma electrónica avanzada garantiza la integridad, la autoría y el no repudio de los mensajes firmados.

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria (EXTRA)

Leganés – 1 Junio 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G81 ☐ G82 ☐ G83 ☐ G84

NIA:

CUESTIONES

CUESTIÓN 1. Valor = 0,2 ptos. Tiempo estimado: 10 min.

Relacione los conceptos de vulnerabilidad, amenaza, riesgo y ataque.

CUESTIÓN 2. Valor = 0,2 ptos. Tiempo estimado: 10 min.

Explique el protocolo de firma digital con apéndice de un mensaje M.

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria (EXTRA)

Leganés – 1 Junio 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G81 ☐ G82 ☐ G83 ☐ G84

NIA:

PROBLEMAS

PROBLEMA 1. Valor = 1,5 ptos. Tiempo estimado: 40 min.

Alicia y Benito acuerdan intercambiarse mensajes firmados digitalmente. Para ello, han establecido que, en primer lugar, emplearán una función resumen *especial* $H(M)$ basada en las cajas S del DES. Esta función consiste en lo siguiente:

- Se agrupa el mensaje M en bloques de 6 bytes (48 bits). Si hay que usar relleno en el último bloque, se añaden tantos bits a cero como sea necesario.
- Paso 1. Cada bloque i entra en las cajas S estándar (véase tabla adjunta), dando como salida un resumen de 32 bits:
 - $r_i = \text{CajaS}(\text{bloque}_i)$
- Paso 2. El resumen final $H(M)$ de 32 bits se produce a partir de la fórmula siguiente:
 - $H(M) = \sum r_i$donde la operación suma es xor, \oplus .

Para $M = \text{"AQUI_NO_HAY_PLAYA"}$, los resúmenes para los dos primeros bloques son:

$r_1 = 0011\ 0001\ 0000\ 0010\ 0101\ 1101\ 1101\ 0001$

$r_2 = 0110\ 1000\ 1101\ 0000\ 1000\ 1101\ 1011\ 0111$

La representación en binario de cada uno de los caracteres es la siguiente:

A =	0100 0001	N =	0100 1110	H =	0100 1000	P =	0101 0000
Q =	0101 0001	O =	0100 1111	A =	0100 0001	L =	0100 1100
U =	0101 0101	_ =	0010 0000	Y =	0101 1001	A =	0100 0001
I =	0100 1001			_ =	0010 0000	Y =	0101 1001
_ =	0010 0000					A =	0100 0001

- a) Calcule el resumen r_3 del tercer bloque de texto y el resumen final $H(M)$.
- b) Sabiendo que la función resumen empleada sigue el algoritmo descrito, deseamos firmar los resúmenes resultantes con RSA y con los siguientes datos:

$p = 25.621$; $q = 187.163$; $n = p \cdot q = 25.621 \cdot 187.163 = 4.795.303.223$,
 $\phi(n) = (p-1)(q-1) = (25.620)(187.162) = 4.795.090.440$,
 $e = 770.011$; $d = 2.658.042.571$

¿Son válidos el módulo de trabajo y esas claves? Justifique su respuesta.

- c) Sabiendo que la función resumen empleada sigue el algoritmo descrito, deseamos firmar los resúmenes resultantes con ElGamal considerando el primo $p' = 2.147.483.647$. ¿Es válido el módulo de trabajo? Justifique su respuesta.

Datos adicionales:

p, p' y q son primos

$$p' = 2^{31} - 1$$

$$2^{32} = 4.294.967.296$$

$$770.011 = 11 \cdot 70.001 \text{ (ambos primos)}$$

$$770.011 \cdot 2.658.042.571 = 2.046.722.018.138.281 = 426.837 \cdot 4.795.090.440 + 1$$

¿Cuál es tu trabajo ideal?



Haz el test aquí



<http://bit.ly/necesitouncambio>



¿Harto de c hapar algo que no te renta?



Fila	Cajas S															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S₁																
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S₂																
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S₃																
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S₄																
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S₅																
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S₆																
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S₇																
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S₈																
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria (EXTRA)

Leganés – 1 Junio 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G81 ☐ G82 ☐ G83 ☐ G84

NIA:

PROBLEMA 2. Valor = 0,5 ptos. Tiempo estimado: 15 min.

Considere un escenario en el Alicia y Benito se intercambian claves mediante el esquema de Diffie-Hellman con un número primo común $p = 11$ y una raíz primitiva $g = 2$.

1. Si la clave pública de Alicia es $Y_a = 9$, ¿cuál es su clave privada X_a ?
2. Si, además del dato del apartado anterior, se sabe que la clave pública de Benito es $Y_b = 3$, ¿cuál es la clave secreta K acordada?
3. ¿En qué problema matemático se basa la seguridad del intercambio de claves de Diffie-Hellman? ¿Son apropiados para dicho intercambio los parámetros escogidos en este ejercicio? En caso negativo indique cuál o cuáles deberían ser modificados. Justifique su respuesta.

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria (EXTRA)

Leganes – 1 Junio 2010

Apellidos:

Nombre:

Grupo reducido: ☐ G81 ☐ G82 ☐ G83 ☐ G84

NIA:

PROBLEMA 3. Valor = 1 pto. Tiempo estimado: 25 min.

Falsifique la firma del mensaje $M=3$, para que imite la de un remitente cuya clave pública RSA es $(e, n)=(77, 143)$.

(Nota: $3^5 \bmod 143 = 100$; $100^3 \bmod 143 = 1$)



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Ordinary examination session (EXTRA)

Leganés –June 1st 2010

Surname:

Name:

Group: ☐ G89

NIA:

PROPUESTA DE EXAMEN 5 – ORDINARIA EXTRA 1 - INGLÉS

SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Ordinary examination session (EXTRA)

Leganés –June 1st 2010

Surname:

Name:

Group: ☐ G89

NIA:

MULTIPLE-CHOICE QUESTIONS

Each question has only one correct answer, which ought to be clearly pointed out rounding the letter identifying the option. Each question incorrectly answered will be evaluated as minus one fourth of the mark obtained had it been correctly answered.

Each of the 8 questions has a value of 0,2 points. Estimated time: 20 min.

1) Regarding cryptanalysis attacks:

- a) When a cryptanalyst has access only to the cryptogram, the cryptanalysis attack is called chosen-ciphertext.
- b) When a cryptanalyst has access to the cryptogram and part of the plaintext, the cryptanalysis attack is called chosen-ciphertext.
- c) When a cryptanalyst can obtain the ciphertexts corresponding to a particular set of plaintexts, the cryptanalysis attack is called chosen-ciphertext.
- d) When a cryptanalyst has access only to a chosen cryptogram to which he knows the corresponding plaintext, the cryptanalysis attack is called chosen-plaintext.

2) Considering a keystream generated by an LFSR with a primitive polynomial associated:

- a) The period T of the generated keystream depends on the seed chosen.
- b) The period T of the generated keystream does not depend on the choice of seed and the length of the keystream will be maximum $T_{\max} = 2^n - 1$
- c) The generated keystream will be of maximum length $T_{\max} = 2^n - 1$
- d) The generated keystream will be of maximum length $T_{\max} = 2^{n-1}$

3) Mark the **INCORRECT** statement:

- a) Diffie-Hellman's seminal article published in 1976 was the birth of Public Key Cryptosystems.
- b) Diffie-Hellman's protocol does not provide authentication, it is vulnerable to the Man in the Middle attack.
- c) Public key cryptography is based on the use of two different keys, one public and the other one private.
- d) An indispensable condition in public key cryptography is that the private key has to be easily obtained from the public key.

4) Regarding cryptographic hash functions, it is true that:

- a) The hash of a message M depends on the size of the message M.
- b) They are exclusively used to facilitate digital signatures.
- c) The probability of finding two different messages M1 y M2, that produce the same hash is greater than the probability of finding a message, M1, that produces the same hash of a given message M2.
- d) None of the above is true

5) What field of an X.509 v3 certificate includes the authorized usages of the corresponding public key?

- a) An extension field, as it is optional information.
- b) A mandatory field where the public key information is included.
- c) This information is defined in the certificate policy, outside the certificate structure.
- d) It is not possible to restrict public key usages.

¿Cuál es tu trabajo ideal?



Haz el test aquí



<http://bit.ly/necesitouncambio>



¿Harto de c h a p a r a l g o q u e n o t e r e n t a ?



6) Mark the correct statement:

- a) An OTP token generates a password valid for several sessions.
- b) An OTP token is based on randomness, avoiding prediction attacks.
- c) In synchronous OTP tokens, the client and the authentication server clocks are synchronized.
- d) In a challenge based OTP token, the generation of an OTP depends on the previous OTP.

7) Regarding cryptographic protocols:

- a) In a SSL stage the client and server negotiate a combination of cryptographic algorithms to be used for the connection.
- b) In key exchange and authentication SSL stages, client certificate authentication is not always required.
- c) Once a SSL session is established, the following transmissions are encrypted.
- d) All of the above are correct.

8) Taking as reference the 59/2003 Spanish Law on electronic signatures and on the European Directive 1999/93/CE, mark the correct statement:

- a) Advanced electronic signature is the digital signature of the hash of a message.
- b) Electronic signature guarantees authorship and integrity of signed messages.
- c) Recognized electronic signature is the one that is executed in a general purpose PC with the signatory's private key.
- d) Advanced electronic signature guarantees authorship, integrity and non-repudiation of signed messages.

SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Ordinary examination session (EXTRA)

Leganés –June 1st 2010

Surname:

Name:

Group: ☐ G89

NIA:

SHORT-ANSWER QUESTIONS

QUESTION 1. Value = 0,2 pt. Estimated time: 10 min.

Relate the vulnerability, threat, risk and attack concepts.

QUESTION 2. Value = 0,2 pt. Estimated time: 10 min.

Explain the digital signature with appendix protocol of a message M.

SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Ordinary examination session (EXTRA)

Leganés –June 1st 2010

Surname:

Name:

Group: ☐ G89

NIA:

PROBLEMS

PROBLEM 1. Value = 1,5 pts. Estimated time: 40 min.

Alice and Bob agree to exchange digitally signed messages. To do this, they also agree to initially use a special hash function $H(M)$ based on DES S-boxes. This function is as follows:

- Message M is divided into blocks of 6 bytes (48 bits). If you have to use padding in the last block, add as many zero-bits as needed.
- Step 1: Each block $_i$ is processed using the standard S-boxes (see table enclosed), which outputs summaries of 32 bits
 - $r_i = \text{S-boxes}(\text{block}_i)$
- Step 2: The final hash $H(M)$ of 32 bits is computed by the following formula:
 - $H(M) = \sum r_i$
where add operation is or-exclusive.

Let $M = \text{"AQUI_NO_HAY_PLAYA"}$ be the plaintext and the resulting first and second hashes are:

$r_1 = 0011\ 0001\ 0000\ 0010\ 0101\ 1101\ 1101\ 0001$

$r_2 = 0110\ 1000\ 1101\ 0000\ 1000\ 1101\ 1011\ 0111$

The binary representation of each character is:

A =	0100 0001	N =	0100 1110	H =	0100 1000	P =	0101 0000
Q =	0101 0001	O =	0100 1111	A =	0100 0001	L =	0100 1100
U =	0101 0101	_ =	0010 0000	Y =	0101 1001	A =	0100 0001
I =	0100 1001			_ =	0010 0000	Y =	0101 1001
_ =	0010 0000					A =	0100 0001

- a) Calculate the hash r_3 (for the third block) and the final $H(M)$.
- b) Considering the hash algorithm previously described, we intend to sign any resulting hash value using the RSA algorithm with:

$$p = 25.621; q = 187.163; n = p \cdot q = 25.621 \cdot 187.163 = 4.795.303.223$$

$$\phi(n) = (p-1)(q-1) = (25.620)(187.162) = 4.795.090.440$$

$$e = 770.011$$

$$d = 2.658.042.571$$

Are the modulus and the keys valid for the task? Justify your answer.

- c) Considering the hash algorithm previously described, we intend to sign any resulting hash value using the ElGamal algorithm with $p' = 2.147.483.647$. Is the chosen parameter valid for the task? Justify your answer.

Note that:

p, p' and q are primes

$$2^{32} = 4.294.967.296$$

$$p' = 2^{31} - 1$$

$$770.011 = 11 \cdot 70.001 \text{ (both primes)}$$

$$770.011 \cdot 2.658.042.571 = 2.046.722.018.138.281 = 426.837 \cdot 4.795.090.440 + 1.$$

¿Cuál es tu trabajo ideal?



Haz el test aquí

<http://bit.ly/necesitouncambio>



¿Harto de c h a p a r algo que no te renta?



S-boxes

		<u>C o l u m n s</u>															
Row		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S₁																	
0		14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1		0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2		4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3		15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S₂																	
0		15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1		3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2		0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3		13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S₃																	
0		10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1		13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2		13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3		1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S₄																	
0		7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1		13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2		10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3		3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S₅																	
0		2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1		14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2		4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3		11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S₆																	
0		12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1		10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2		9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3		4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S₇																	
0		4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1		13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2		1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3		6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S₈																	
0		13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1		1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2		7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3		2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Ordinary examination session (EXTRA)

Leganés –June 1st 2010

Surname:

Name:

Group: ☐ G89

NIA:

PROBLEM 2. Value = 0,5 pts. Estimated time: 15 min.

Consider a Diffie-Hellman scheme with a common prime $p=11$ and a primitive root $g=2$.

1. If Alice has public key $Y_a=9$, what is Alice's private key X_a ?
2. If Bob has public key $Y_b=3$, what is the shared secret key K ?
3. What is the mathematical problem Diffie-Hellman bases its security on? Are the parameters used in this exercise appropriate for the task at issue? In negative case, state which parameter/s must be modified.

SECURITY IN INFORMATION TECHNOLOGY
GRADO EN INGENIERÍA INFORMÁTICA

Final Exam – Ordinary examination session (EXTRA)

Leganés –June 1st 2010

Surname:

Name:

Group: ☐ G89

NIA:

Problem 3. Value = 1 pt. Estimated time: 25 min.


Assuming that the RSA public key of a signatory is $(e,n)=(77,143)$, forge the signature of the message $M=3$.

(Note: $3^5 \bmod 143 = 100$; $100^3 \bmod 143 = 1$)



¿Harto de c hapar algo que no te renta?

¿Cuál es tu trabajo ideal? 

Haz el test aquí 

<http://bit.ly/necesitouncambio>



**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria (EXTRA)

Leganés – 1 Junio 2010

SOLUCIÓN

**PROPUESTA DE EXAMEN 5 – ORDINARIA EXTRA 1 -
SOLUCIONES**

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria (EXTRA)

Leganés – 1 Junio 2010

SOLUCIÓN

PREGUNTAS DE RESPUESTA OBJETIVA - SOLUCIÓN

1) En relación a criptoanálisis:

- a) Cuando sólo se tiene acceso al criptograma el ataque de criptoanálisis más apropiado se denomina de texto cifrado elegido.
- b) Cuando se tiene acceso al criptograma y a una parte del texto en claro el ataque de criptoanálisis más apropiado se denomina de texto cifrado elegido.
- c) Cuando sólo se tiene acceso al criptograma elegido y a su descifrado el ataque de criptoanálisis más apropiado se denomina de texto cifrado elegido.
- d) Cuando sólo se tiene acceso al criptograma elegido y a su descifrado el ataque de criptoanálisis más apropiado se denomina de texto en claro elegido.

2) Sobre generadores LFSR de series cifrantes, determine cuál de las siguientes características corresponde a una secuencia generada con un LFSR representado por un polinomio primitivo:

- a) El periodo T de la secuencia depende de la semilla.
- b) T no depende de la semilla, y será máxima con $T_{\max} = 2^n - 1$
- c) Se generan secuencias de periodo $T_{\max} = 2^n - 1$
- d) Se generan secuencias de periodo $T_{\max} = 2^{n-1}$

3) Seleccione la opción **INCORRECTA**:

- a) El artículo seminal de Diffie-Hellman en 1976 supuso el nacimiento de los sistemas de clave pública.
- b) El protocolo Diffie-Hellman no es autenticado, permite ataques de hombre interpuesto.
- c) La criptografía de clave pública emplea dos tipos de claves, la pública y la privada.
- d) Una condición imprescindible en criptografía de clave pública es que la clave privada sea fácilmente deducible a partir de la clave pública.

4) En relación a las funciones resumen criptográficas podemos afirmar que:

- a) La longitud de la huella digital de un mensaje M viene determinada por el tamaño de M.
- b) Las funciones resumen se usan exclusivamente para facilitar la firma digital.
- c) La probabilidad de hallar dos mensajes diferentes, M1 y M2, que produzcan la misma huella digital es mayor que la probabilidad de encontrar un mensaje, M1, que produzca la misma huella digital que otro dado M2.
- d) Ninguna de las anteriores es cierta

5) ¿En qué campo de un certificado X.509 v3 se incluye los posibles usos autorizados de las claves criptográficas correspondientes?

- e) En las extensiones del certificado, al ser información opcional.
- f) En el campo obligatorio donde se incluye la información de la clave pública.
- g) Se define en la política del certificado, ajena a la estructura del certificado.
- h) No es posible restringir los usos de las claves criptográficas.

¿Cuál es tu trabajo ideal?



Haz el test aquí



<http://bit.ly/necesitouncambio>



¿Harto de c h a p a r algo que no te renta?



6) Seleccione la opción correcta:

- a) Un token OTP genera una contraseña válida para varias sesiones.
- b) Un token OTP se basa en la aleatoriedad, evitando ataques por predicción.
- c) En los token OTP síncronos existe sincronía entre el reloj del cliente y el del servidor de autenticación.
- d) En un token OTP basado en desafíos la generación de un OTP depende del OTP anterior.

7) En relación a los protocolos criptográficos:

- a) Una de las fases básicas del protocolo SSL consiste en negociar, entre ambas partes, el algoritmo de cifrado que se usará en la comunicación.
- b) En la fase de intercambio de claves públicas y autenticación SSL en ocasiones no se requiere que el cliente envíe su certificado digital.
- c) Tras el establecimiento de sesión SSL el tráfico no se transmite en claro, se cifra con cifrado simétrico.
- d) Todas las anteriores son correctas.

8) Tomando como referencia la Ley 59/2003 de Firma Electrónica española y la Directiva Europea 1999/93/CE, seleccione la opción correcta:

- a) La firma electrónica avanzada es la firma digital del resumen (o huella digital) de un mensaje.
- b) La firma electrónica garantiza la autoría e integridad del mensaje que se firma.
- c) La firma electrónica reconocida es la que se ejecuta en un PC de propósito general con la clave privada del firmante.
- d) La firma electrónica avanzada garantiza la integridad, la autoría y el no repudio de los mensajes firmados.

**SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA**

Examen Final – Convocatoria Ordinaria (EXTRA)

Leganés – 1 Junio 2010

SOLUCIÓN

CUESTIONES - SOLUCIÓN

CUESTIÓN 1. Valor = 0,2 ptos. Tiempo estimado: 10 min.

Relacione los conceptos de vulnerabilidad, amenaza, riesgo y ataque.

Respuesta: Una vulnerabilidad es una exposición a una amenaza, y cuya explotación viola la política de seguridad del sistema TI. Así, una amenaza es una potencial violación (accidental o intencionada) de la seguridad de la información. La probabilidad de que una amenaza se materialice aprovechando una vulnerabilidad causando daño (impacto) en un proceso o sistema se llama riesgo. Por último, un ataque es una acción maliciosa encaminada a explotar una o varias vulnerabilidades, y es un tipo de amenaza intencionada.

CUESTIÓN 2. Valor = 0,2 ptos. Tiempo estimado: 10 min.

Explique el protocolo de firma digital con apéndice de un mensaje M.

Respuesta:

1. Obtener el resumen $H(M)$ y su firma $S(H(M))$ (obtenida con la clave privada del remitente)
2. Enviar el par $(M, S(H(M)))$
3. El receptor calcula $H(M)$ a partir del primer elemento del par (el mensaje M)
4. El receptor evalúa la validez de la firma recibida ejecutando el algoritmo de verificación de firma V y la clave pública del remitente a partir del resumen calculado $H(M)$, la firma recibida $S(H(M))$. Se acepta el mensaje si el resultado del algoritmo es verdadero y se rechaza en caso contrario

PROBLEMAS – SOLUCIÓN

Problema 1. Valor: 1,5 ptos. - SOLUCIÓN

Alicia y Benito acuerdan intercambiarse mensajes firmados digitalmente. Para ello, han establecido que, en primer lugar, emplearán una función resumen *especial* $H(M)$ basada en las cajas S del DES. Esta función consiste en lo siguiente:

- Se agrupa el mensaje M en bloques de 6 bytes (48 bits). Si hay que usar relleno en el último bloque, se añaden tantos bits a cero como sea necesario.
- Paso 1. Cada bloque i entra en las cajas S estándar (véase tabla adjunta), dando como salida un resumen de 32 bits:
 - $r_i = \text{CajaS}(\text{bloque}_i)$
- Paso 2. El resumen final $H(M)$ de 32 bits se produce a partir de la fórmula siguiente:
 - $H(M) = \sum r_i$
 donde la operación suma es xor, \oplus .

Para $M = \text{"AQUI_NO_HAY_PLAYA"}$, los resúmenes para los dos primeros bloques son:

$r_1 = 0011\ 0001\ 0000\ 0010\ 0101\ 1101\ 1101\ 0001$

$r_2 = 0110\ 1000\ 1101\ 0000\ 1000\ 1101\ 1011\ 0111$

La representación en binario de cada uno de los caracteres es la siguiente:

A = 0100 0001	N = 0100 1110	H = 0100 1000	P = 0101 0000
Q = 0101 0001	O = 0100 1111	A = 0100 0001	L = 0100 1100
U = 0101 0101	_ = 0010 0000	Y = 0101 1001	A = 0100 0001
I = 0100 1001		_ = 0010 0000	Y = 0101 1001
_ = 0010 0000			A = 0100 0001

- d) Calcule el resumen r_3 del tercer bloque de texto y el resumen final $H(M)$.
- e) Sabiendo que la función resumen empleada sigue el algoritmo descrito, deseamos firmar los resúmenes resultantes con RSA y con los siguientes datos:

$p = 25.621$; $q = 187.163$; $n = p \cdot q = 25.621 \cdot 187.163 = 4.795.303.223$,
 $\phi(n) = (p-1)(q-1) = (25.620)(187.162) = 4.795.090.440$,
 $e = 770.011$; $d = 2.658.042.571$

¿Son válidos el módulo de trabajo y esas claves? Justifique su respuesta.

- f) Sabiendo que la función resumen empleada sigue el algoritmo descrito, deseamos firmar los resúmenes resultantes con ElGamal considerando el primo $p' = 2.147.483.647$. ¿Es válido el módulo de trabajo? Justifique su respuesta.

Datos adicionales:

p, p' y q son primos

$2^{32} = 4.294.967.296$

$770.011 \cdot 2.658.042.571 = 2.046.722.018.138.281 = 426.837 \cdot 4.795.090.440 + 1$

$p' = 2^{31} - 1$

$770.011 = 11 \cdot 70.001$ (ambos primos)

Cajas S																
Columna																
Fila	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA

Examen Final – Convocatoria Ordinaria (EXTRA)

Leganés – 1 Junio 2010

SOLUCIÓN

S₁																	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
S₂																	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
S₃																	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
S₄																	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
S₅																	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
S₆																	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
S₇																	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
S₈																	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

a) El tercer bloque de 48 bits que es el que se pide es PLAYA \Re (\Re es un relleno de 8 ceros)

Caja S₁

Entrada: 010100

Fila: 0

Columna: 10

Salida: 6

Bits: **0110**

Caja S₂

Entrada: 000100

Fila: 0

Columna: 2

Salida: 8

Bits: **1000**

Caja S₃

Entrada: 110001

Fila: 3

Columna: 8

Salida: 4

Bits: **0100**

Caja S₄

Entrada: 000001

Fila: 1

Columna: 0

Salida: 13

Bits: **1101**

(0,25 puntos)

¿Cuál es tu trabajo ideal?



Haz el test aquí

<http://bit.ly/necesitouncambio>



¿Harto de c h a p a r algo que no te renta?



Caja S₅

Entrada: 010110

Fila: 0

Columna: 11

Salida: 15

Bits: 1111

Caja S₆

Entrada: 010100

Fila: 0

Columna: 10

Salida: 3

Bits: 0011

Caja S₇

Entrada: 000100

Fila: 0

Columna: 2

Salida: 2

Bits: 0010

Caja S₈

Entrada: 000000

Fila: 0

Columna: 0

Salida: 13

Bits: 1101

(0,25 puntos)

Resumen $r_3 = 0110\ 1000\ 0100\ 1101\ 1111\ 0011\ 0010\ 1101$

El resumen final $H(M)$ será $r_1 \oplus r_2 \oplus r_3$ es decir:

Resumen $r_1 = 0011\ 0001\ 0000\ 0010\ 0101\ 1101\ 1101\ 0001$

Resumen $r_2 = 0110\ 1000\ 1101\ 0000\ 1000\ 1101\ 1011\ 0111$

Resumen $r_3 = 0110\ 1000\ 0100\ 1101\ 1111\ 0011\ 0010\ 1101$

\oplus

$H(M) = 0011\ 0001\ 1001\ 1111\ 0010\ 0011\ 0100\ 1011$

$H(M)_{16} = 31\ 9F\ 23\ 4B$ (0,25 puntos)

- b) Para un sistema de firma RSA tenemos que $n = p \cdot q = 25.621 \cdot 187.163 = 4.795.303.223$, valor que es ligeramente superior a $2^{32} = 4.294.967.296$ dado como dato, luego el cuerpo de trabajo es correcto ya que podrán cifrarse (firmarse) todos los resúmenes posibles. (0,25 puntos)

En este sistema, $\phi(n) = (p-1)(q-1) = (25.620)(187.162) = 4.795.090.440$. La clave pública e se elige de forma que no tenga factores en común con $\phi(n)$ y se cumple puesto que 4.795.090.440 no es divisible por 11 ni por 70.001 dados como dato. La clave privada d debe ser la inversa de la clave pública e en $\phi(n)$ de forma que se cumpla que $e \cdot d \bmod \phi(n) = 1$. Según los datos dados en el examen se ve que esto se cumple. Luego el sistema es correcto. (0,25 puntos)

- c) En este entorno no puede usarse la firma de ElGamal con un valor primo $p' = 2.147.483.647$ puesto que, aunque cumple con la condición de ser primo, es menor que el valor máximo del resumen que podemos obtener que sería una cadena de 32 unos ($2^{32} - 1$) y el valor dado aquí es justo un bit menos ($2^{31} - 1$). La única solución en este caso sería dividir la función hash $H(M)$ en, por ejemplo, dos bloques de 16 bits cada uno y hacer la firma del documento por partes. (0,25 puntos)

SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN
GRADO EN INGENIERÍA INFORMÁTICA

Examen Final – Convocatoria Ordinaria (EXTRA)

Leganés – 1 Junio 2010

SOLUCIÓN

Problema 2. Valor: 0,5 pts. - SOLUCIÓN

Considere un escenario en el Alicia y Benito se intercambian claves mediante el esquema de Diffie-Hellman con un número primo común $p = 11$ y una raíz primitiva $g = 2$.

1. Si la clave pública de Alicia es $Y_a = 9$, ¿cuál es su clave privada X_a ?
2. Si, además del dato del apartado anterior, se sabe que la clave pública de Benito es $Y_b = 3$, ¿cuál es la clave secreta K acordada?
3. ¿En qué problema matemático se basa la seguridad del intercambio de claves de Diffie-Hellman? ¿Son apropiados para dicho intercambio los parámetros escogidos en este ejercicio? En caso negativo indique cuál o cuáles deberían ser modificados.

1. $9 = Y_a = g^{X_a} \bmod p = 2^{X_a} \bmod 11$
Hemos de probar con los elementos de $Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
 $2^6 \bmod 11 = 64 \bmod 11 = 9$
Por tanto, $X_a = 6$

2. $3 = Y_b = g^{X_b} \bmod p = 2^{X_b} \bmod 11$

[Hemos de probar con los elementos de $Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
 $2^6 \bmod 11 = 64 \bmod 11 = 9$
 $2^8 \bmod 11 = 2^2 \cdot 2^6 \bmod 11 = 4 \cdot 9 \bmod 11 = 4 \cdot (-2) \bmod 11 = -8 \bmod 11 = 3$
Por tanto, $X_b = 8$
 $K = Y_a^{X_b} \bmod p = 9^8 \bmod 11 = (9^2)^4 \bmod 11 = 4^4 \bmod 11 = 5^2 \bmod 11 = 3 = Y_b^{X_a} \bmod p = 3^6 \bmod 11 = (3^2)^3 \bmod 11 = (-2)^3 \bmod 11 = -8 \bmod 11 = 3$]

Realmente, No hace falta calcular X_b .

La solución se obtiene del apartado 1 haciendo $K = Y_b^{X_a} \bmod p = 3^6 \bmod 11 = 3$

3. En el problema del logaritmo discreto para p grande. Debería modificarse p para que tuviera unos 200 dígitos y no se pudiese realizar un ataque de fuerza bruta para deducir las claves privadas.

Problema 3. Valor: 1 pto. - SOLUCIÓN

Falsifique la firma del mensaje $M=3$, para que imite la de un remitente cuya clave pública RSA es $(e, n) = (77, 143)$.

(Nota: $3^5 \bmod 143 = 100$; $100^3 \bmod 143 = 1$)

Podemos realizar la falsificación al ser n un número pequeño. De este modo podemos calcular la clave privada a partir de la clave pública.

$n = 11 \cdot 13$; $\phi(143) = 10 \cdot 12 = 120$
 $77d \bmod 120 = 1$
 $120 = 1 \cdot 77 + 43$
 $77 = 1 \cdot 43 + 34$
 $43 = 1 \cdot 34 + 9$
 $34 = 3 \cdot 9 + 7$
 $9 = 1 \cdot 7 + 2$
 $7 = 3 \cdot 2 + 1$

$$1 = 7 - 3 \cdot 2$$

...

$$1 = 19 \cdot 77 - 34 \cdot 120 + 34 \cdot 77$$

$$1 = 53 \cdot 77 - 34 \cdot 120$$

$$d = 53$$

También es fácil calcular de por el teorema chino del resto:

$$77x_1 \equiv 1 \pmod{3};$$

$$77x_2 \equiv 1 \pmod{5};$$

$$77x_3 \equiv 1 \pmod{8};$$

$$\text{Entonces } x_1 = 2; x_2 = 3; x_3 = 5;$$

Para el cálculo de y_i se obtiene:

$$40y_1 \equiv 1 \pmod{3};$$

$$24y_2 \equiv 1 \pmod{5};$$

$$15y_3 \equiv 1 \pmod{8};$$

$$\text{Entonces } y_1 = 1; y_2 = 4; y_3 = 7;$$

La solución es $d = 40 \cdot 2 \cdot 1 + 24 \cdot 3 \cdot 4 + 15 \cdot 5 \cdot 7 = 53 \pmod{120}$

$$F(M) = 3^{53} \pmod{143} = (3^5)^{10} 3^3 \pmod{143} = 100 3^3 \pmod{143} = 126$$