Departamento de Informática
Faculdade de Ciências e Tecnologia
UNIVERSIDADE NOVA DE LISBOA

Mestrado em Engenharia Informática (2º Ciclo)
Segurança em Sistemas e Redes de Computadores
(Computer Systems and Networks Securty, MSc Course)

1º Sem. 2010/2011

Mid-Term Evaluation: Frequency Test #1, 22/Oct/2012

Test: 2 hours
The test has two groups of questions

- Group 1: Answers with closed book: 1 hour
- Group 2: Answers with open book, documentation and class-materials: 1 hour

Student Number:	Name:	
LEI/MEI:	Group (Practical Evaluation): _____	Total number of pages:

You should number each page in the form: Page Number/TOTAL

EVALUATION TABLE (to be used by the teacher)

GROUP 1 (Closed book)									

GROUP 2									

PART I – Closed Book

Question 1

a) Explain the difference between "confidentiality" and "privacy", according with the conceptualization of security properties as defines in security frameworks like OSI X.800 or FIPS 100 - CIA (Confidentiality, Integrity and Availability) Triad.

Confidentiality:

Privacy:

b) Explain the following concepts in the OSI X.800 Security Architecture, giving examples of each category.

B1 – Security Mechanism is

Security Mechanisms – Examples:

B2 – Security Service is

Security Service – Examples:

c) According with the X.800 Security Framework, what are the differences between passive and active threats?

d) List and briefly define examples of passive and active security attacks, as defined in the X.800 framework.

Passive Attacks:

P1 –

P2 –

Active Attacks

A1 –

A2 –

A3 –

A4 –

A5 -

e) From the following table, describing the relationship between security services and security mechanisms, try to fill (using the letter Y) a table representing similar relationships between the specific represented security mechanisms and a list of passive and active attacks, as mentioned in b). You must consider in the table the same passive and active attacks mentioned in P1, P2, A1, A2, A3, A4 and A5, with the same interpretation. If you need to argument your choices, use the indexes M1, M2, etc to justify your answer (using the white sheets distributed with the test).

Service	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

	Mechanism (column)	**Passive Attacks**		**Acitice attacks**			
		P1	**P2**	**A1**	**A2**	**A3**	**A4**
M1	AES Algorithm						
M2	CMAC with 3DES and CBC						
M3	Switched LAN Access Control based on assigned MAC addresses (in each switch port)						
M4	SHA-2 (SHA-512) Algorithm						
M5	HMAC witvh SHA-1 and/or MD5						
M6	Support provided by an Authentication Exchange Protocol in a Key-Distribution Service						
M7	Encryption of a Message Digest with a RSA private Key						
M8	Encryption with a RSA public key						
M9	PKCS#7 used in plaintext encrypted with AES and CBC Mode						
M10	A Notarization Service						

Question 2

Explain how you can implement a stream cipher, usable as a structure for real-time bit stream encryption, using a block cipher algorithm in the COUNTER mode, as a primitive box.
(Suggestion: you can sketch a picture with fundamental processing blocks and a legend explaining the purpose of each processing block)

For the ENCRYPTION process:

For the DECRYPTION process:

Question 3

a) In the Output Feedback Mode (OFB), the encryption of a message composed by a number of N blocks, each one with size b bits, is expressed in the following way:

$$C_i = Pi \text{ xor } \{C_{i-1} \text{ xor } P_{i-1}\}_K$$
$$C_1 = P_1 \text{ xor } \{Nonce\}_K$$

for any block i encrypted with the key K, generating the cipher sequence C1, C2, … Cn. As you know, $\{M\}_K$ is a notation for the Block-Encryption Function of the Plaintext block M using a Key K. Write the expression to compute P1 and Pi in the decryption phase

P1 =

Pi =

Question 4

Knowing the different encryption modes as studied, when do you choose to use CTR? You must answer mentioning first the advantages or drawbacks of the CTR mode, and from the advantages, you must justify the CTR choice for the proposed application scenario requirements.

Question 5

As you know, 3-DES is a possible approach for more robustness using the base DES algorithm as the base block-cipher. The algorithm is used in practice, minimizing brute-force-attacks and DES cryptanalysis attacks. Why the same technique is not adopted in practice for algorithms like AES, for example using a Tripe AES approach?

PART II – Open Book

Question 6

When certain cipher modes of operation are used, we only need an algorithm implementing the encryption function, because the decryption is done also with the encryption function. Show how this can be done?

Question 7

a) Explain the difference between weak-collision resistance and strong-collision resistance as different properties in a secure hashing function.

b) If we use a secure hashing function, subjacent to a digital signature of a software distribution (ex., a software package with the binary installation archive, signed by the company that distributes the software) using a Public Key Scheme (as represented), what is important to have as the minimal guarantees of the secure hash function used: Strong Collision Resistance or Weak Collision Resistance ? Make your argumentation.

Package: the SW Package downloaded to be installed
KpubD, KprivD: Asymmetric key pair - Public Key and Private Key of the origin company (ex., Apple)
KpubI, KprivI: Asymmetric key pair of the installer (ex., you in your computer)
H() Secure Hash Function, ex., SHA-2 family, example SHA-512
Pad1: The padding used in the signature, ex., PKCS#7
Pad 2: the padding useed in a symmetric encryption process
Legal-Terms: A text with the legal terms for your installation.
||: Concatenation
TN = Timestamp || Nonce: A timestamp concatenated with a generated random nonce
Ks – Encryption Key for Symmetric Encryption Algorithm (ex., AES-128)

Suppose you received the software distribution as a multi-part message as follow. Suppose you know the separation of each part, as well as, the separation and the expected size of all cryptographic objects in each part of the message.

KEY-ENVELOPE || SIGNATURE || BODY

KEY-ENVELOPE PART: {Ks || TN}KpubI
SIGNATURE PART: { H(Package) || H(Ks || TN) || H(Legal-Terms) || Pad1}Kpriv
BODY PART: { Legal-Terms || Package || Pad2 }Ks

Answer
For the case, it is necessary for H() to provide: _____ COLLISION RESISTANCE as the necessary and sufficient condition.
Because:

Question 8

a) When using a PBE encryption scheme to encrypt a message M, the values of the password, salt and counter that are used used as parameters must be kept secret and shared between the two principal making the encryption and the decryption computation. True or False ? Justify your answer.

b) What are the security concerns regarding the security guarantees, when a PBE-Encryption scheme is adopted in a solution? Justification.

Question 9

Consider the listed program in
http://asc.di.fct.unl.pt/cns/classes/P/aprat/EX5/PBEWithoutParamsExample.java
(test annex)
The program uses a PBE technique to decrypt a ciphertext previously obtained by a non-PBE encryption scheme, from an initial plaintext message. You must know why this program works fine and why the PBE decryption obtains the initial plaintext in a correct way (as shown in the printed output)

a) If you change the line:

Cipher cEnc= Cipher.getInstance("DESede/CBC/PKCS7Padding", "BC")

by the line

Cipher eEnc=Cipher.getInstance("DESede/CBC/PKCS5Padding", "BC")

the output of the program (last 4 lines) will change or not ? By other words, the PBE decryption will obtain the correct plaintext as previously or not? Explain why.

b) Repeat your answer if the same code line is changed by the following line:

Cipher eEnc=Cipher.getInstance("DESede/CBC/NoPadding", "BC")

Question 10

Consider the program in:

http://asc.di.fct.unl.pt/cns/classes/P/aprat/EX3/Exemplos-modos-cifra-ecb-cbc/SimpleCBCExample.java
(test annex)

You want to use AES with a 256 bit key as a substitution for the DES/CBC/PKCS5Padding cipher-suite.

What are all the modifications you need for this purpose (maintaining the same functionality of the program).

Explain your solution.