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

Curso de Mestrado em Engenharia Informática (2º Ciclo)

Segurança em Sistemas e Redes de Computadores
(Computer Systems and Networks Securty, MSc Level)

1º Sem. 2010/2011

TESTE DE FREQUÊNCIA Nº 1
(Frequency Test 1)

The test has two groups of questions

- Group 1: Answers with closed book: 1 hour
- Group 2: It is possible to use reference documentation and materials: 1 hour

Student Number:	Name:	
LEI/MEI:	Group: SSTC-G____	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)									
1)	2)	3)	4)	5)	6)	7)	8)	9)	10)

GROUP 2									
1)	2)	3)	4)	5)	6)	7)	8)	9)	10)

Question 1

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

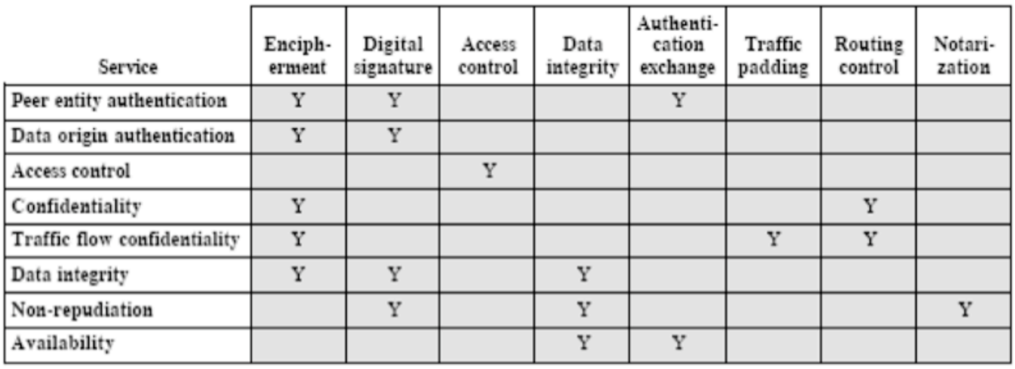
b) List and briefly define categories of passive and active security attacks, as defined in the X.800 framework.

Passive Attacks:
P1 –
P2 –

Active Attacks
A1 –
A2 –
A3 –
A4 –
A5 -

c) From the following table, describing the relationship between security services and security mechanisms, try to fill 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.

If you need to argument your choices, use the indexes M1, M2, etc to justify your answer.



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		**Passive Attacks**		**Acitice attacks**			
(column)		**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-512 Algorithm						
M5	HMAC wityh SHA-1 and/or MD5						
M6	Introduction of random traffic padding in a data-stream message, before encryption						
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	Authentication auditable LOGs maintained by a KDC running the Neddham-Schroeder Algorithm for Key-Distribution						

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 CBC mode.

Question 3

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

C1 = P1s xor Ss ({IV}k) and Ci = Pi xor Ss ({Ci-1}k), for any i

Remembering:

- Ss(X) corresponds to a shift-left operation of b-s bits, of the block X with initial size b, selecting only the most significant s bits for the xor operation (discarding the b-s least significant bits). As you remember, for byte-oriented encryption, s = 8 bits

Write the expression to compute P1 and Ci in the decryption phase:

P1 =

Ci =

Question 4

Why is the middle step of a 3DES (Triple DES) a decryption step, rather than an encryption step ? Justify the answer.

Question 5

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 6

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

b) List the other important properties (complementing the properties above) that a secure hash function must satisfy to be used as a component for a message authentication code (or MAC) scheme. Describe each property.

Question 7

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.

Question 8

a) Which is the generic structure of a HMAC scheme composed by two secure hash-functions ? Explain the motivation to adopt two different secure hash-functions.

b) Which is the generic structure of a CMAC scheme based on a CBC mode ?

c) What are the advantages or disadvantages between HMACs and CMACs to be used as MAC schemes as integrity and non-replaying warranties in the implementation of the the Needham-Schroeder Protocol, as implemented in the first practical work-assignment (TP1) ?

GROUP 2

Question 9 (estimated time: 10 min max.)

Consider the listed program that uses PBE decryption and its logic 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/PKCS5Padding", "BC")

by the line

Cipher eEnc=Cipher.getInstance("DESede/CBC/PKCS7Padding", "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, justifying your answer.

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

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

Question 10 (estimated time: 10 min, max)

a) From the listed program (based in an example discussed in the classroom), simulate a tampering attack (adding lines in the code), resulting in a transfer of 5000000 to the attacker account 9876-5432, just by forging in the encrypted channel a fake message with a fake content: Transfer 5000000 to AC 9876-5432.

b) Explain why your attack has success?

c) Explain if such attack is possible if we change the Counter mode by another byte-oriented mode, such as OFB. Why ?

Question 11 (estimated time: 5 to 10 min)

Considering the context of the TP1 (work assignment): suppose that we will use a fixed ciphersuite using DES as a symmetric algorithm to implement the Needham-Schroeder protocol (Phase 2 of TP1) for the base of the authentication and key-session distribution protocol for chat sessions, knowing that the ciphersuite defined for the sessions can use different symmetric algorithms, namely: AES, Triple DES and Blowfish.

From you opinion does it makes sense? Justify your answer in the perspective that you must warrant the security properties (authentication, confidentiality, integrity and protection against message-relaying) in the communication between principals involved in those different chat sessions.