UNIVERSITY OF NEW YORK TIRANA
Komuna e Parisit,Tirana, Albania
Tel.: 00355-(0)4-273056-8 – Fax: 00355-(0)4-273059
***Web Site Address*: http://www.unyt.edu.al**

Security Engineering
Spring 2010

Course : **Security Engineering (4 credit hours)**
Instructor : **Dr. Marenglen Biba**
Office : **Faculty building 1st floor**
Office Hours : **Tuesday 3-5 PM or by appointment**
Phone : **42273056 / ext. 112**
E-mail : **marenglenbiba@unyt.edu.al**
Course page : **http://www.marenglenbiba.net/seceng/**

SAMPLE TEST

Lesson 1

1. Describe the design hierarchy for security engineering.
2. What is a principal and what are the types of principals.
3. What is the difference between trust and trustworthy?
4. Explain the difference between confidentiality, privacy and secrecy.
5. Describe the ways to authenticate people to devices.
6. Describe the types of attacks on a system.

Lesson 2

1. Describe password retry counters and the related two types of attacks.
2. Describe the attack based on the audit trail. Give an example.
3. What is a pre-computed dictionary attack?
4. Describe the categories of weak passwords.
5. Describe phishing.
6. What is a two-channel authentication. Give an example.

7. Describe the access control at the middleware level.
8. What is a sandbox?
9. Describe the security elements of the ARM processor.
10. Describe a stack smashing attack.
11. Describe a race condition attack.

Lesson 3

1. What is a chosen-plaintext attack?
2. Describe the elements that are used to measure the complexity of attacks.
3. What is steganography. Give an example of this.
4. What are the types of substitution ciphers? Describe them briefly.
5. What is a one-time pad (OTP)? What are the properties of its key and what is property proven by Shannon?
6. Give the definition of a protocol. What are the main characteristics of a security protocol?.
7. Describe the steps of a simple symmetric cryptographic protocol. What are the problems with this protocol?
8. What is a trapdoor one-way function?
9. What is a MAC?
10. What is the advantage of public-key versus symmetric protocols?
11. Describe a hybrid cryptosystem.
12. Describe the digital signature protocol with a one-way hash function.
13. What is the property for a sequence to be cryptographically secure pseudo-random?

Lesson 4

1. Describe the steps of Key Exchange with Symmetric Cryptography. What is the problem with this protocol?
2. Describe the man-in-the-middle attack.
3. Describe the interlock protocol.
4. What is Salt and why it makes much harder the dictionary attack?
5. Describe the Needham-Schroeder protocol.
6. How does multiple-key public key cryptography work?
7. Give an example of secret splitting.
8. What is a threshold scheme for secret sharing?
9. Describe a cryptographic protection of a database.
10. What is an undeniable digital signature?

11. Describe a protocol on Group Signatures with a Trusted Arbitrator.
12. What is the concept of Fail-stop digital signatures?
13. Describe a bit commitment protocol.