



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 6

1. What is the advantage for a hacker using software cracking?
2. Describe how cryptanalysis can be performed through viruses.
3. What is the reason why we do not use keys of length 100.000?
4. Would you use in a system a symmetric key and a public key both of length 56? Give appropriate lengths for both keys.
5. What is a birthday attack?
6. What is a reduced keyspace?
7. What is a nonlinear keyspace?
8. How can a key be verified?
9. Describe the problem with encryption software in a preemptive multitasking system.
10. Describe a protocol for key backup.
11. What are introducers? Explain a simple protocol based on them.