Data Security

Final Exam 18.12.2014

The maximum amount of points is 50.

1. Give brief definitions for the terms substitution and permutation (transposition). Where are these methods used in cryptography? (5 p)
2. Explain the basic functionality of a symmetric cryptosystem. How is security achieved in a symmetric cryptosystem? Give an example of an application in which symmetric cryptography is used. (10 p)
3. What is the difference between a block cipher and a stream cipher? Describe the basic functionality of a block cipher. Give a few examples of existing block cipher methods. Why (or where) are modes of operations for block ciphers needed? (10 p)
4. Describe the basic functionality of a pseudorandom number generator. Where are pseudorandom numbers needed in cryptography? (5 p)
5. Explain the basic functionality of a public-key cryptosystem. How is security achieved in a public-key cryptosystem? Give an example of an application in which public-key cryptography is used. (10 p)
6. Give a definition for a cryptographic hash function. (5 p)
7. What are message authentication codes and digital signatures? For what purpose are they used? (5 p)