Computer & Network Security '09

Dr. Roberto Di Pietro
Monday 01/06/2009

Instructions: Questions should be answered in English.
The final grade will be the sum of the points divided by 10. Points will be rounded to the nearest half point.
You have 2 hours and 45 minutes to complete this exam. Please read all questions carefully before answering them.

Describe the principles of transposition and permutation ciphers, and report an example of cipher for each type (10).

Report an example of perfect cipher (10).

Report the birthday paradox and provide its mathematical proof (10).
---assignment 2 is a substitute for this question---

Provide the logical scheme (design) of the Feistel cipher and discuss its advantages (10).
---assignment 1 is a substitute for this question---

Report the logical scheme (design) of a cipher operating in CBC mode (10).

Report the Man in the Middle Attack related to the Diffie Helman key exchange (10).

Report all the 9 principles for the design of secure systems, and briefly discuss three of them (10).

In the context of Secure Multicast describe the star scheme, and discuss how an eviction is performed (10).

Describe the differences between Misuse based and Anomaly based IDS (10).

Discuss the ROC curve used to evaluate IDS (10).
---assignment 3 is a substitute for this question---
