CS 519
Cryptography and Network Security
Instructor: Ali Aydın Selçuk
Department of Computer Engineering, Bilkent University

Homework #4

Due November 8, 2012, beginning of the class

1. Answer the following questions regarding MD5 and SHA-1:
   (a) Note that a message is still padded even if its length is already a multip le of the block length. Why is this important? I.e., what would the problem be if such messages are dige sted as they are without any padding?
   (b) Discuss the relation between these hash functions and the Davies-Meyer con struction based on a block cipher.
   (c) Why do you think byte operations such as AND, OR, XOR are used instead of S-boxes in the nonlinear F function? What would happen if a structure like the DES F function were used instead of the current functions?

2. Compare the RSA and ElGamal signature schemes' performance in terms of
   - efficiency of the verification operation,
   - ability to pre-compute most of the signature operation in advance.

   Which scheme should be preferred for an SSL certificate? Which scheme should be preferred for a real-time authentication protocol on a restricted device—e.g., an RFID tag on an electronic passport? Explain why.

3. Find the solution of the system

$$\begin{aligned} x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{6} \\ x &\equiv 1 \pmod{7} \end{aligned}$$

   in $\mathbb{Z}_{210}$, using the Chinese Remainder Theorem and the extended Euclid's algorithm. Show all your work.

4. Question 4, the midterm exam of Fall 2010.