In the name of God

Sharif University of Technology
Department of Computer Engineering

CE 693: Advanced Computer Networks

Mehdi Kharrazi *Aban 21st, 1390*

Homework 1

Please email your answers/report in **PDF format** to Zhaleh Milanian "zhaleh.milanian@gmail.com" and CC me at "kharrazi@sharif.edu". The HW file name should be **"Your Lastname-442k-HW-1"**. It should be used as the subject of your email, too. In order for us not to miss your homework please follow the formatting. This homework is due by **Aban 30th, 11:59 PM**. There may also be a face-to-face delivery, the time of which will be announced later.

Part I

1. Decipher the following cipher text, which was enciphered using the Caesar cipher:

   GIFMZUZEX PFLI RJJZXEDVEK KF JFDVFEV VCJV ZJ TFEJZUVIVU TYVRKZEX FE PFLI SVYRCW.

2. We covered the DES algorithm in the class, and you should read FIPS 46-3 for more details. In each round of DES a function is calculated which takes a 32 bits input plus the round key and outputs 32 bits. The diagram for this operation is in Figure 2 of FIPS 46-3. Given the following information, calculate the 32 bits output of the function. Show your results at each step. This is doable by hand, so no programming is required.

   - R = 01010101010101010101010101010101 (32 bits)
   - *K:* The 48 bit key for each round is calculated based on Figure 3 of FIPS 46-3. Assume that we are calculating the function for round 1, C_0 = 10101010101010101010101010 (28 bits), and D_0 = 10101010101010101010101010 (28 bits).

3. Suppose Alice want to receive a secret message from Bob using the RSA protocol. She has chosen two prime numbers: $p = 3$ and $q = 11$.

   (a) Calculate the following for her:
   - n
   - $\phi(n)$
   - e
   - d

   (b) What will be transmitted to Bob as the public key?

   (c) Encrypt the message "2" with the public key you calculated as if you are Bob. Show your results.

   (d) Decrypt the cipher text Alice would receive from Bob. It should match the message "2". Show your results.

   Show all steps in detail to get full points.

4. It is well known that RSA is much slower than DES or AES. Then what are the advantages in using RSA over AES/DES? List any pros and cons for each case.

5. Is it better to first sign and then encrypt or encrypt and then sign the message? Elaborate on your answer. List any pros and cons for each case.

6. How does a Firewall differ from an Intrusion Detection System? Compare the two. Are they similar in any way?

Part II

In this part of the assignment you will compare the performance of 3 encryption techniques:

1. AES with 128 bit key

2. Blowfish with 128 bit key

3. DES with 56 bit key

All the above technique should be run in the CBC mode, and you may choose a random key. You may also find the appropriate code for the noted encryption techniques on the web. You should encrypt the following file: http://sharif.edu/ kharrazi/courses/respCondRsrch640x480.swf

with each of the above noted techniques and calculate the time each technique takes. Similarly the decryption time should be calculated with each technique. Use a simple scripting/programming language in order to execute these technique and measure an accurate time. You should submit a plot showing how these techniques compare and note the processor used for the experiments, additionally all files used in the experiments should be submitted.