Cryptography 1

1. Answer the following questions briefly:
   a. What is the OSI security architecture?
   b. What is the difference between passive and active security attacks?
   c. List and briefly define categories of passive and active security attacks.
   d. List and briefly define categories of security services.

2. Is it possible to design a cryptographic system that needs no secret information and supports confidentiality?

3. Is it possible to support both confidentiality and nonrepudiation using shared key cryptography?

4. What properties of the following are required for any shared key encryption algorithm and why:
   a. $A \neq B \rightarrow E(k, A) \neq E(k, B)$
   b. $k_1 \neq k_2 \rightarrow E(k_1, A) \neq E(k_2, A)$
   c. $k_1 \neq k_2 \rightarrow D(k_2, E(k_1, A)) \neq A$
   d. $\mathrm{D}\big(\mathrm{k}, \mathrm{E}(\mathrm{k}, \mathrm{A})\big) = \mathrm{A}$

5. Prove the above properties (for which your answer was '*yes*') for Caesar Cipher.

6. In order to strengthen Caesar cipher, one of your colleagues came out with the following idea: rather than using a single number in the key (k), which leads to only 26 possible keys, he suggested to use *n* numbers and apply the Caesar algorithm *n* times using these numbers to further confuse the message. For example if n equals 2, the algorithm receives two keys and apply the original Caesar with the first then the second. What can you say about the strength of this algorithm compared with the original Caesar cipher?

7. A generalization of the Caesar cipher, knows as the affine Caesar cipher, has the following form: For each plaintext letter p, substitute the ciphertext letter C:

   C = E([a, b], p) = (ap + b) mod 26

   A basic requirement of any encryption algorithm is that it be one-to-one. That is, if $p \neq q$, then $E(k, p) \neq E(k, q)$ (see problem 3). The affine Caesar cipher is not one-to-one for all values of a. For example, for a = 2 and b = 3, then E([a, b], 0) = E([a, b], 13) = 3.

   a. Are there any limitations on the value of b? Explain why or why not.
   b. Determine which values of a are not allowed.

c. Provide a general statement of which values of a are and are not allowed. Justify your statement.

8. Write a program that can encrypt and decrypt using the general Caesar cipher.
9. What is the problem with the following approximation of the one time pad: Using 1024 bits key and then repeating it every 1K of plain text to be encrypted.

10. What is the effective key size of a simple transposition cipher with *n* columns?

11. Show that the ideal block cipher needs $n \times 2^n$ key.

12. The following protocol was used to generate a shared key between Alice and Bob:

$$Alice \rightarrow KDC: E(k_{Alice-KDC}, Bob)$$
$$KDC \rightarrow Alice: E(k_{Alice-KDC}, k_{Alice-Bob})$$
$$KDC \rightarrow Bob: E(k_{Bob-KDC}, k_{Alice-Bob})$$

a. By the end of this protocol (and assuming the KDC is not compromised) will Alice and Bob share a common session key?
b. Assume that *Eve* was able to get a copy of this protocol run and compromised $k_{Alice-Bob}$, how can she impersonate *Alice*?
c. How can you change the protocol to prevent the previous type of attack?

13. What are the advantages and disadvantages of link encryption as compared to end-to-end encryption for providing confidentiality?

14. What is the maximum key length of 3DES?

15. What is the main advantage of AES over 3DES?

16. What is the main advantage of 3DES over AES?

17. Write a simple command line program that reads a file and either encrypts or decrypts it using DES. You can use C, C++, Jave, or C# and utilize any open source libraries you may need.