Cryptography 2

1. 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.

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

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

4. 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?

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

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

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

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

9. 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.