**Institute of Statistical Studies and Research**

**Department of Computer and Information Sciences**

**Cairo University**

**Dr. Abd El-Aziz Ahmed**

**Information Security**

**CS515 - IS517**

 **Winter term 2015-2016**

**Sheet 2**

1. Decrypt the following, which has been encrypted with a Caesar cipher.

YFND LTYN FFUN FLCU RNFF UTYL TBTY LTBZ

 WRNF FUTY LTBT FLCU TYLT BNFF U

1. Why is it important for a cipher to have a large number of keys?
2. Why is time pad unbreakable?
3. Find the key used to get the cipher

 FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDK

APRKDLYEVLRHHRH

By applying an Affine Cipher .

1. Explain how a substitution cipher works by encrypting **Eve has found the key** with the substitution :

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

T H E Q U I C K B R O W N F X J M P S V L A Z Y D G

1. Alice and Bob wish to use the same substitution for both encryption and decryption. What property must the substitution have, considered as a permutation of the alphabet?
2. If Eve knows that the same substitution is used for both encryption and decryption,

does it make her job of breaking the cipher any easier? Why?

1. In the F-function of DES, the expansion permutation is one of the inner functions. Describe what this function does and why?
2. Why is the key space of the DES algorithm only 256 , when the key input to

 the algorithm consists of 8 bytes (64 bits)?

1. Assume that K is a key which is used in the DES algorithm and comp-K is the complement key of K (i.e. for each 0 in K there is a 1 in comp-K and for each 1 in K there is a 0 in comp-K). Also assume that the cipher text C is created by using K on the plain text P, and the cipher text D is created by using comp-K on the plain text comp-P, where comp-P is the complement of P. What is the cipher text D equal to? Choose your answer below (You do not have to motivate your answer).
* The same as C
* The complement of C
* The plain text P
* The complement of P
* The key K
* None of the above
1. Prove that **DES** decryption can be done by applying the **DES** encryption algorithm to the ciphertext with the key schedule reversed.
2. Using S-box in Des algorithm calculate the following:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Input |  Box 1  | Box 2  | Box 3  | Box 4 |  Box 5  | Box 6  | Box 7  | Box 8 |
| 11111111  |  |   |   |  |  |  |   |  |

1. Make two round using AES for encrypt the plaintext 0123456789ABCDEF using the key 0123456789ABCDEF.
2. If 0123456789ABCDEF is the ciphertext, make one round of the decryption in AES.
3. Compare between Feistel and DES.
4. Compare between AES and DES.
5. Which is the better DES or AES? and why?.