|  |  |
| --- | --- |
| **Institute of Statistical Studies and Research**  **Cairo University** | |
| **Department of Computer and Information Sciences**  **Course Title: Selected Topics in Computer Science**  **Course Code: CS 515 & IS 517** | **Examination Date: 03/11/2015**  **Examination time: 1 hours**  **Total Marks: 20 marks** |

|  |
| --- |
| **The Examination consists of seven Questions in One Page** |

**Answer all the following questions**

**PART A- (5 x 1 =5 marks)**

1. What is the difference between Monoalphabetic and Polyalphabetic substitution ciphers?
2. How many times is the PC-2 used in the DES?
3. What is the number of possible keys in the Substitution Cipher under Z26?
4. Why is Time Pad unbreakable?
5. Why did the DES use the S-boxes?

**PART B - (15 marks)**

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

YFND LTYN FFUN FLCU RNFF (3 marks)

(b) Encrypt “**Eve has found the key”** with the substitution:

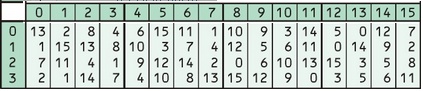
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

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 (3 marks)

(c) Decrypt **“slxp1mlalaeme”** by Columnar transposition using the key K=3. (3 marks)

1. (a) Given S-box 8 of the S-boxes in the DES algorithm, find the following three blocks:

**110111,** **001100**, and **000000**: (3 marks)

****

(c) In the DES algorithm, let the key which is the output of PC-1 is **1111 0000 1100**

**1100 1010 1010 1111 0101 0101 0101 0110 0111 1000 1111**. Find C1D1, and

C2D2. (3 marks)

With my best wishes ☺

Dr. Abd El-Aziz Ahmed