|  |  |
| --- | --- |
| **1Faculty of Science**  **Cairo University** | |
| **Department of Mathematics**  **Course Title: Information Security**  **Course Code: 402** | **Examination Date: 29/07/2015**  **Examination time: 1 hours**  **Total Marks: 15 marks** |

|  |
| --- |
| **The Examination Consists of Seven Questions in One Page** |

**Answer all the following questions**

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

1. What is the difference between symmetric and asymmetric encryption algorithms?
2. Why shift cipher is not secure under Z26?
3. What is the difference between Affine and Vigenere ciphers?
4. Describe the K in Affine cipher under Z26 and mention the number of possible keys of length m in a Vigenere Cipher .
5. Define a cryptosystem system.

**PART B - (3 x 5 = 15 marks)**

1. Encrypt and decrypt the plaintext “math” using the Hill cipher for

k= 11 8

3 7

1. Let m = 6 and the keyword is CIPHER, encrypt and decrypt the plaintext

”math” using the Vigenere cipher.

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.

With my best wishes ☺

Dr. Abd El-Aziz Ahmed