**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 2014-2015**

**Assessment 1**

Time: 90 minutes Max: 35 marks

**PART- A (Answer all: 10 x 2 =20)**

1. Define a cryptosystem system.
2. What is the difference between Cryptography, Cryptanalysis, and Cryptology?
3. List the goals of the cryptology.
4. What are the pros and cons of block and stream ciphers.
5. What is the difference between symmetric and asymmetric encryption algorithms?
6. Why shift cipher is not secure under Z26?
7. What is the difference between Affine and Vigenere ciphers?
8. Describe the K in Affine cipher under Z26 and mention the number of possible keys of length m in a Vigenere Cipher .
9. What is the difference between Cryptanalyticand Brute-force attack?
10. What is the difference between the transposition and substitution ciphers?

**PART- B (Answer only one: 15 marks)**

1. (a). Encrypt and decrypt the plaintext “ISSR” using the Hill cipher for

 k= 11 8

 3 7 (10 marks)

 (b). Determine the number of keys in an Affine cipher over Zm , where m=70 &

 80. (5 marks)

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

 ”ISSR” usingVigenere cipher. (10 marks)

 (b). Determine the element of keys in an Affine cipher over Z15. (5 marks)