JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR SCIENCE IN SECURITY AND FORENICS

3RD YEAR 1ST SEMESTER 2015/2016 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: IIT 3315

COURSE TITLE: FUNDAMENTALS OF CRYPTOGRAPHY AND STEGANOGRAPHY

EXAM VENUE: **STREAM: BSC COMP SECURITY**

DATE: DECEMBER 2016 **EXAM SESSION:**

TIME: 2.00 HOURS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other two questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

QUESTION ONE [30 MARKS]

(a) Define the following terms and concepts as applies to cryptography; [4 Marks]

(i) Steganalysis (iii) Quantum Teleportation

(ii) Hash Functions (iv) Feistel Ciphers

(b) “Steganography is best used in conjunction with another data-hiding method”. Do you agree with the statement? Explain. [3 Marks]

(c) Explain the three ways of characterizing cryptographic systems. [3 Marks]

(d) Consider an *m*-round Feistel network where key size is equal to half the block size and the round function f(K,R) = K⊕R. Analyze how (in)secure this cipher is against ciphertext only attacks and known plaintext attacks when *m* is arbitrary. [4 Marks]

(e) Explain the four possible approaches to attacking the RSA algorithm. [4 Marks]

(f) Compare and contrast the following classification of cryptosystems; [8 Marks]

(i) Symmetric and Asymmetric (ii) Classical and Quantum

(g) There has been increased emphasis on the cryptanalytic attacks on Data Encryption Standard (DES) and other symmetric block ciphers. Explain the two most powerful and promising approaches to that applies here. [4 Marks]

QUESTION TWO [20 MARKS]

(a) Describe the Caesar Cipher. [4 Marks]

(b) Describe at least two ways of breaking a Caesar Cipher on an English-language message. [4 Marks]

(c) Show that DES decryption is, infact, the inverse of DES encryption. [4 Marks]

(d) Compute the bits number 1, 16, 33, and 48 at the output of the first round of the DES decryption, assuming that the ciphertext block is composed of all ones and the external key is composed of all ones. [8 Marks]

QUESTION THREE [20 MARKS]

(a) Using a suitable example in each case, briefly explain the following; [4 Marks]

(i) Polygraphic Ciphers (ii) Polyalphabetic Ciphers

(b) Compare the security of features of Hill Cipher with that of Vigenère Cipher. [4 Marks]

(c) Encrypt the message "**For sure you must be honest in whatever you are telling me**" using the Hill Cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Display your workings. [6 Marks]

(d) Show your workings for corresponding decryption of the ciphertext to recover the original plaintext. [6 Marks]

QUESTION FOUR [20 MARKS]

(a) Discuss the Elliptic Curve Digital Signature Algorithm (DSA) under the following headings: [8 Marks]

(i) Signature Generation Algorithm

(ii) Signature Verification Algorithm

(b) Name and explain ANY TWO approaches used to distribute public keys in asymmetric cryptosystems. [4 Marks]

(c) Below is a table summarizing the characteristics comparison between some examples of symmetric encryption algorithms. Fill in the blank spaces with appropriate information. [8 Marks]

	Blowfish	Rijndael (AES)
Key Size		
Block Size		
Rounds		
Security Level		

QUESTION FIVE [20 MARKS]

(a) Using a suitable diagram in each case, describe the **four modes of operation** for block cipher. [8 Marks]

(b) While referring to quantum key generation protocol and using a practical real life example, explain the implementation of the following phases as applies in quantum cryptography; [8 Marks]

(i) Error Correction (ii) Privacy Amplification

(c) Differentiate between ***Digital Signature Algorithm (DSA)*** and ***Digital Signature Standard (DSS)***. [4 Marks]

- END –