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 2018/2019 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: **IIT 3315**

COURSE TITLE: **FUNDAMENTALS OF CRYPTOGRAPHY AND STEGANOGRAPHY**

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

DATE: DECEMBER 2018 **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**

Candidates must hand in their answer booklets to the invigilator while in the examination room

QUESTION ONE **[30 MARKS]**

(a) Define the following as applies to cryptography and steganography: [8 Marks]

(i) Cryptology

(ii) Digital Signatures

(iii) Polygraphic

(iv) Symmetric Ciphers

(b) Using well aided examples, explain the three ways in which cryptographic systems can be categorized. [6 Marks]

(c) Encrypt the message "Janet is always awesome and that is why many of us get along with her" using the Hill cipher with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$. Show your calculations. Also show the calculation for the corresponding decryption of the ciphertext to recover the original plaintext. [7 Marks]

(d) Steganography can be used for a variety of purposes. Do you agree with the statement? Explain your answer. [3 Marks]

(e) Consider a case where Bob uses the RSA cryptosystem with a very large modulus *n* for which the factorization cannot be found in a reasonable amount of time and Alice sends a message to Bob by representing each alphabetic character as an integer between 0 and 25, and then encrypting each number separately using RSA with large *e* and large *n*. With a supporting reason, comment on the security of this method. [3 Marks]

(f) Use a suitable example to explain the implementation of *quantum key distribution*. [3 Marks]

QUESTION TWO **[20 MARKS]**

(a) This problem explores the use of a one-time pad version of the Vigenère cipher. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 8 24 10…, then the first letter of plaintext is encrypted with a shift of 8 letters, the second with a shift of 24 letters, the third with a shift of 10 letters, and so on.

(i) Encrypt the plaintext **givemoremoney** with the key stream [6 Marks]

10 1 2 8 24 16 22 15 12 12 3 9 10

(ii) Using the ciphertext produced in part (a), find a key so that the cipher text decrypts to the plaintext **moneyrequired.** [6 Marks]

(b) DES is considered insecure because of its short key length (56 bits). An improvement, proposed by Rivest, is DESX. DESX has key length 120 bits, seen as a pair (k_1, k_2), where k_1 is 56 bits and k_2 is 64 bits. The encryption of a one-block message m is $DESX(k_1,k_2)(m) = DES_{k1}(m \oplus k_2) \oplus k_2$

(i) Explain how decryption is done. [4 Marks]

(ii) Explain why the inner xor is necessary, i.e. explain an attack against $DESX'_{(k1, k2)}(m) = DES_{k1}(m) \oplus k_2$ that is much better than brute force. [4 Marks]

QUESTION THREE **[20 MARKS]**

(a) "When a block cipher is used to encrypt a message of arbitrary length, techniques known as modes of operation are used for the block cipher. Any block cipher can be operated in one of the several modes of operation". Discuss. [12 Marks]

(b) Consider a block cipher using 8-bit blocks that is based on the basic DES architecture (Feistel network) with two rounds and no initial or final permutation. The scrambling function for round *i* is $f_i(x, K) = (2i \cdot K)^x \bmod 15$, for i = 1, 2, where the key K is a member of Z_{15}. If K = 7 and the ciphertext is 00111111. With the aid of a diagram of the Feistel Cipher network, calculate the plaintext and show your intermediate results. [8 Marks]

QUESTION FOUR **[20 MARKS]**

(a) While referring to RC5 symmetric encryption block cipher, discuss it under objectives of its design, its characteristics, design parameters, its security and area of applications. [8 Marks]

(b) Consider the following scheme by which B encrypts a message for A.

1. A chooses two large primes *P* and *Q* that are also relatively prime to (*P*-1) and (*Q*-1).
2. A publishes $N = PQ$ as its public key.
3. A calculates *P*' and *Q*' such that $PP' \equiv 1 \pmod{Q\text{-}1}$ and $QQ' \equiv 1 \pmod{P\text{-}1}$.
4. B encrypts message *M* as $C = M^N \bmod N$.
5. A finds *M* by solving $M \equiv C^{P'} \pmod{Q}$ and $M \equiv C^{Q'} \pmod{P}$.
   (i) Briefly explain how this scheme works. [4 marks]
   (ii) Compare this scheme with that of RSA. [4 Marks]
   (iii) Give two advantages to RSA compared to this scheme. [4 Marks]

QUESTION FIVE **[20 MARKS]**

(a) Give <u>two</u> weaknesses and <u>two</u> strengths of public key cryptography. [4 Marks]

(b) Using a suitable example, explain the implementation of Diffie-Hellman Key Exchange in the management of key exchange in public-key Infrastructure. [8 Marks]

(c) Using four areas of reference, compare classical cryptography with quantum cryptography. [8 Marks]

- END –