Department of Higher Education
University of Computer Studies, Yangon
Fourth Year (B.C.Tech.)
Final Examination
Cryptography (CT-405)
October, 2018

Answer All Questions: **Time Allowed: 3 hours**

1. Choose the correct answers:

(i) The attack threatening availability of information is --------.

A. routing control B. modification

C. access control D. DOS

(ii) The attack, ----------, does not modify data or harm the system that continues with its normal operation.

A. active attack B. passive attack

C. snooping D. traffic analysis

(iii) There are four types of cryptanalysis attacks: Ciphertext-only, ---------- , Chosen-plaintext and Chosen-ciphertext.

A. Statistical attack B. Pattern attack

C. Known-plaintext attack D. Brute-Force attack

(iv) Additive ciphers are sometimes referred to as shift ciphers or -------.

A. ElGamal cipher B. Caesar cipher

C. RSA cipher D. Schnoor cipher

(v) The cipher changes the location of the symbols by ----------.

A. substitution B. transposition

C. permutation D. addition

(vi) Hidden the relationship between the ciphertext and the plaintext is--------.

A. Completeness effect B. Confusion

C. Diffusion D. Avalanche effect

(vii) The key in a ------- stream cipher is independent of the plaintext or ciphertext.

A. nonsynchronous B. synchronous

C. non-Feistel D. Feistel

(viii) DES function is made up of an expansion P-box, a whitener , a group of S-boxes and ------.

A. a straight P-box B. a compression P-box

C. a splitter D. a swapper

(ix) Each n-bit block is encrypted independently with the same cipher key: ---------.

A. ECB B. CBC

C. CFB D. CTR

(x) RSA cryptosystem uses --------.

A. one key B. two keys

C. three key D. no key

2(a) List and define some security mechanisms recommended by ITU.T(X.800) to provide the security services.

(b) Apply the Vigenere Cipher to encrypt and decrypt the message "**We are computer students**." using "**LUCKY**" keyword. What cipher is a special case of Vigenere cipher in which m=1.

3(a) Create a linear feedback shift register with 5 cells $b_4 = b_3 \oplus b_2 \oplus b_0$ and show the value of output for 20 transitions (shifts) if the seed is $(1001)_2$. What is the maximum period of LFSR?

(b) Show the result of the Hexa decimal data "01B0 1020 0A00 0010" after passing if through the Initial Permutation in Table 1.

Table 1. Initial Permutation

58	50	42	34	26	18	10	02
60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06
64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01
59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05
63	55	47	39	31	23	15	07

(c) What is the DES Challenges? Describe the DES function process?

4(a) Show the diagram for encryption and decryption in the OFB mode when r = n. Why OFB mode creates a synchronous stream cipher?

(b) In A5/1, find the maximum period of each LFSR and the expression of the Majority Function. What is the size of the data unit in A5/1?

5(a) In ElGamal public key cryptosystem, Bob chooses 19 as p. He then chooses d=3 and e1= 2 (primitive root of Z^*_p).

i. Calculate Bob's public key and private key.

ii. Encrypt and decrypt the plaintext P = 10.

iii. List the two attacks on ELGamal cryptosystem.

(b) What are the strengths and weaknesses of public-key? Alice's RSA public key {e, n} is {5,22} and Bob's RSA public key { e, n } is {3, 77}. Alice want to send the plaintext P = 10 to Bob. Show how to encrypt and decrypt the RSA cryptosystem by using these facts.