UNIVERSITY OF RUHUNA

Faculty of Engineering

End-Semester 8 Examination in Engineering: November 2017

Module Number: EE8204 **Module Name: Information Security**

[Three Hours]

Index No.: ....

Instructions for Candidates:

1. This question paper consists of two parts. PART-A and PART-B carries 20 and 30 marks respectively.

2. PART-A consists of 20 questions. For PART-A, candidates should answer in the same paper (Use the □ space provided for answering). There are 5 answers for each question. More than one ***correct*** answer or true statement may exist for one question. Candidates should mark ' ✓ ' for the ***correct*** answers and ' ✗ ' for the ***incorrect*** answers. There won't be any negative marks given. 0.2 marks are given for marking a ***correct*** answer as correct. 0.2 marks are given for marking an ***incorrect*** answer as incorrect. Unmarked answers are not given any marks.

3. PART-B consists of three essay questions. Candidates should answer them in the given answer book.

PART - A

Q1 Examine the following statements related to classic ciphers.

(a) Ceaser's cipher exhibits diffusion characteristics only. □

(b) Substitution ciphers can be solved by comparing frequencies of letters in the ciphertext with a general plaintext letter frequency characteristic. □

(c) Transposition ciphers exhibits confusion characteristics only. □

(d) Classic ciphers always rely on the XOR operations to do the ciphering. □

(e) One Time Pad (OTP) cipher is a provably secure cipher. □

Q2 In case of a Man in the Middle (MiM) attack, the adversary

(a) has only the plaintext. □

(b) may ask a specific ciphertext to be decrypted. □

(c) may ask a specific plaintext to be encrypted. □

(d) has only the ciphertext. □

(e) may ask to be authenticated. □

Q3 A keyboard which includes the English alphabet and the numbers from 0 to 9 is used to create a case-sensitive six character password. What is the approximated time that might take to crack the password from a password cracking tool capable of attempting 15 samples for a second?

(a) 6 years □

(b) 60 days □

(c) 60 years □

(d) 6 months □

(e) 60 months □

Q4 Evaluate the following statements regarding Advanced Encryption Standard (AES) and Data Encryption Standard (DES).

(a) Fourteen (14) rounds are included in DES. □

(b) AES round function is □
$F = \left[MixColumn \left[ShiftRaw \left[ByteSub \left(a_{ij} \right) \right] \oplus c_{ij} \right] \oplus k_{ij} \right].$

(c) AES has two key sizes. □

(d) DES is based on Vernam cipher. □

(e) The number of rounds in AES depends on the key length. □

Q5 Which of the following mechanism and technique does support integrity?

(a) Access Control □

(b) Digital Signature □

(c) Data Encryption □

(d) ElGamal Algorithm □

(e) Hashed Message Authentication Code (HMAC) □

Q6 Examine the following statements related to the public and the symmetric key cryptography.

(a) Public key systems provide data secrecy. □

(b) Symmetric key systems do not ensure data integrity. □

(c) Both systems provide non-repudiation of origin. □

(d) Both systems provide user authentication. □

(e) Symmetric key systems are faster than public key systems. □

Q7 Evaluate the following statements regarding stream ciphers.

(a) The main operation in stream ciphers would be the XOR operation. □

(b) The key in a stream cipher is relatively shorter and extended to a longer one. □

(c) RC6 is an example for stream ciphers. □

(d) RC4 includes modular operations. □

(e) In A5/1, the majority function is employed to select the operating Linear Feedback Shift Registers (LFSRs). □

Q8 If H(X) is a one way hash function, then

(a) for any given value h, it is computationally feasible to find X such that H(X) = h. □

(b) for some given value h, it is computationally infeasible to find X such that H(X) = h. □

(c) for some given value X, it is computationally infeasible to find h such that H(X) = h. □

(d) for any given values h and X such that H(X) = h, it is computationally infeasible to find Y with X ≠ Y such that H(Y) = h. □

(e) for any given value h, it is feasible to find X and Y with X ≠ Y such that H(X) = H(Y) = h. □

Q9 Evaluate the following statements regarding information hiding techniques.

(a) The purpose of watermarks in information security is to detect acts of misuse. □

(b) Robust watermarks can withstand attacks. □

(c) Fragile watermarks can be used to detect pirated software. □

(d) Image Steganography is achieved by modifying the Least Significant Bits (LSB) of an image byte. □

(e) Steganography was used more than cryptography in the past. □

Q10 Suppose R is a random challenge sent as a plaintext from Alice to Bob, K is a symmetric key known to both Alice and Bob, h is a secure hash function and E(x, y) denotes x encrypted with a key y. Which of the following statements are correct?

(a) $R \oplus K$ is a secure session key. □

(b) E(R, K) is a secure session key. □

(c) E(K, R) is a secure session key. □

(d) h(K, R) is a secure session key. □

(e) h(R, K) is a secure session key. □

Q11 Which of the following statements are correct regarding the Encapsulating Security Payload (ESP) and the Authentication Header (AH)?

(a) AH provides confidentiality. □

(b) ESP provides data integrity. □

(c) AH is capable of securing the integrity of a message. □

(d) AH is vulnerable against replay attacks. □

(e) ESP provides protection against data tampering. □

Q12 Evaluate the following statements on the context of Internet Protocol Security (IPSec).

(a) There are six versions of Internet Key Exchange (IKE) phase 1. □

(b) IKE uses the ephemeral Diffie-Hellman (DH) scheme to establish a session key for every mode which does not achieve perfect forward secrecy. □

(c) Digital Signature - Aggressive mode (AM) of IKE does not secure the anonymity of the users. □

(d) IPSec is an over engineered prtocol. □

(e) IKE phase 1 is comparable to a Secure Socket Layer (SSL) connection. □

Q13 Evaluate the following statements on the context of SSL.

(a) SSL certificate could only be granted from a Certificate Authority (CA). □

(b) SSL certificate could only be issued from a SSL root certificate. □

(c) Details such as host name, host domain name and host IP address are bound by SSL certificate. □

(d) SSL extended validation provides the mutual authentication between users. □

(e) SSL employs four different keys for both sending and receiving. □

Q14 Which of the following statement(s) is/ are true about Access control systems?

(a) Discretionary Access Control (DAC) is implemented using a Lampson's access control matrix. □

(b) Access Control Lists (ACLs) are specifying authorizations being granted for a specific subject. □

(c) Bell-LaPadula (BLP) model deals with confidentiality. □

(d) In Biba's model, the Subject (S) writes the Object (O) if and only if, □

$I(S) <= I(O)$

(e) In Role Based Access Control (RBAC), permissions are granted to names of the users. □

Q15 Evaluate the following statements regarding Intrusion Detection.

(a) Intrusion prevention is offered by authentication, firewalls and virus guards. □

(b) Both Intrusion Detection Systems (IDSs) and firewalls does the same function. □

(c) Anomaly based IDSs are effective against newly generated malware. □

(d) Mathematical models such as Bayesian and Markov models are used in designing signature based IDSs. □

(e) IDSs are only operable once an attack is happened or underway. □

Q16 Which of the following statement(s) is/are true about Kerberos security?

(a) Kerberos system is designed for smaller scale networks. □

(b) Kerberos system uses the public-key cryptography. □

(c) Kerberos Key Distribution Center (KDC) issues the Tickets and the corresponding session keys. □

(d) Timestamp is a critical parameter in a Kerberos system. □

(e) Due to the larger clock skew, replay attacks are possible in a Kerberos system. □

Q17 Consider a Diffie-Hellman scheme with common prime, p = 11 and generator, g = 17. If user A's private exponent is a = 4 and user B's private exponent is b = 7, then

(a) the shared symmetric key would be 9. □

(b) the shared symmetric key would be 4. □

(c) User A's private value is 20. □

(d) User B's private value is 8. □

(e) both A and B users private values are co-prime. □

Q18 Which of the following statement(s) is/are true about malware?

(a) Worms do not depend on hosts to propagate from one place to another. □

(b) SQL slammer was a worm which exploited the buffer overflow vulnerability of Microsoft SQL servers. □

(c) The defining characteristic of viruses is that they are self-replicating computer programs which install themselves without the user's consent. □

(d) Metamorphic viruses are more complex than polymorphic viruses. □

(e) Memory resident viruses are residing in the boot sector of the hard drive. □

Q19 Which of the following statement(s) is/are true about bio-metric authentication schemes?

(a) The identification mode is more difficult than the authentication mode. □

(b) Hand geometry based bio-metric schemes have universal and permanent features. □

(c) The recognition phase should be much precise than the enrollment phase. □

(d) Hand geometry has a lesser Equal Error Rate (EER) compared to a fingerprint scheme. □

(e) Higher accuracy of bio-metric scheme might result in a low insult and a higher fraud rate. □

Q20 Suppose that an error occurs in the i^{th} block of ciphertext C_i on transmission when using the Cipher Block Chaining (CBC) mode. What is the effect produced on the recovered plaintext blocks P_1, P_2, ..., P_i ?

(a) The error propagates to the recovered plaintext blocks P_i and P_{i+1}. □

(b) The error propagates to the recovered plaintext blocks P_{i-1} and P_i. □

(c) The error propagates to the recovered plaintext blocks P_{i-1} and P_{i+1}. □

(d) The error propagates to the recovered plaintext blocks P_{i-1}, P_i and P_{i+1}. □

(e) The error propagates to all plaintext blocks. □