UNIVERSITY OF RUHUNA

Faculty of Engineering

End-Semester 8 Examination in Engineering: November 2016

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).
3. 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.
4. 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 confusion characteristics only. □

(b) Substitution cipher exhibits confusion only characteristics. □

(c) Double transposition cipher exhibits both confusion and diffusion. □

(d) Classic codebook ciphers only exhibits diffusion characteristics. □

(e) Vernam cipher is not a provably secure cipher. □

Q2. In case of a Chosen Plaintext Attack (CPA), 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) has the ciphertext and the plaintext that was enciphered. □

Q3. A keyboard which includes the English alphabet and the numbers from 0 to 9 is used to create a case-sensitive five character password. A password cracking tool, which is capable of attempting 20 samples for a second is used to crack the password. What is the approximated time that might take to crack the password?

(a) 2.5 years □

(b) 44 days □

(c) 17.5 months □

(d) 9 months □

(e) 99 days □

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

(a) Sixteen (16) rounds are included in DES. □

(b) AES is bit oriented. □

(c) AES has three key sizes. □

(d) DES is based on Lucifer cipher. □

(e) In each round, AES performs three functions. □

Q5. Following mechanisms and techniques support confidentiality.

(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 usually slower than the public key systems. □

Q7. Evaluate the following statements regarding stream ciphers.

(a) Main operation in stream ciphers would be XOR operation. □

(b) Encryption is carried out for block wise inputs. □

(c) RC5 is an example for stream ciphers. □

(d) RC4 employs a self-modifying lookup table. □

(e) In A5/1, the plaintexts are encrypted through the use of Linear Feedback Shift Registers (LFSR). □

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 perspective is to detect acts of misuse. □

(b) Robust watermarks are vulnerable against attacks. □

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

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

(e) It is not possible to practice steganography in High Definition (HD) images. □

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 eight versions of Internet Key Exchange (IKE) phase 1. □

(b) IKE uses the static Diffie-Hellman (DH) scheme to establish a session key for every mode. □

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

(d) IPSec is a more efficient protocol than Secure Socket Layer (SSL). □

(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 does not provide the mutual authentication between users. □

(e) SSL employs 4 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) iff, 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 (IDS) and firewalls does the same function. □

(c) Anomaly based IDS 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 symmetric-key cryptography. □

(c) Kerberos Key Distribution Center (KDC) issues the Ticket Granting Ticket (TGT) 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 = 13 and generator, g = 7. If user A's private exponent is a = 3 and user B's private exponent is b = 5, then

(a) the shared symmetric key would be 3. □

(b) the shared symmetric key would be 5. □

(c) A's private value is 18. □

(d) B's private value is 11. □

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

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

(a) Worms are dependent on other hosts when propagating from one place to another. □

(b) Stuxnet was a worm which exploited the vulnerabilities of Supervisory Control and Data Acquisition (SCADA) systems. □

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

(d) Polymorphic viruses are difficult to detect through signature scanning. □

(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) Recognition phase should be much precise than 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. □

```
KeyGenerator keygenerator = KeyGenerator.getInstance("DES");
SecretKey myDesKey = keygenerator.generateKey();
Cipher cipher;
cipher = cipher.getInstance("DES/ECB/PKCS5Padding");
```

Listing 1

Q20. Consider the code fragment given in Listing 1. Which of the following statement(s) is/are correct?

(a) This cipher is created for DES symmetric key encryption scheme. □

(b) *PKCS5Padding* is the block cipher mode mentioned in the code fragment. □

(c) Cipher could be changed to TripleDES, CBC mode with No padding by modifying the above code to □

```
cipher = cipher.getInstance("3DES/CBC/NoPadding");
```

(d) Cipher could be changed to AES, ECB mode with No padding by modifying the above code to □

```
cipher = cipher.getInstance("AES/CBC/NoPadding");
```

(e) The above cipher should be initialized to *ENCRYPT_MODE* in order to be used for encrypting a text. □