Introduction to Information Security (III)

End (Mid) Semester Examination (Spring 2024)

International Institute of Information Technology, Hyderabad

Time: 2 Hours Total Marks: 60

Instructions: **Q1 is mandatory** and answer **ANY FOUR** questions from remaining Q2-Q7.

This is a closed books and notes examination.

Write your answers sequentially as given in the question paper and also all the parts of a question at the same place.

No query is allowed in the examination.

Use of Regular Calculator is allowed.

1. (a) Suppose one attempts to design a cryptosystem with encryption and decryption. What should be the goal of the designer?

   (A) Encryption/decryption should be done in polynomial time, and cryptanalysis can be done also in polynomial time

   (B) Encryption/decryption speed does not matter, but cryptanalysis must be NP-hard

   (C) Encryption/decryption should be done in polynomial time, and cryptanalysis must be also NP-hard

   (D) All encryption, decryption and cryptanalysis should be NP-hard

   (b) Suppose designer A opts for Encryption Scheme 1, whereas designer B opts for Encryption Scheme 2 as follows.

   Encryption scheme 1 (ES1): Have only the encryption and decryption functions and these are kept secret to the sender and receiver only. No key is used in this method.

   Encryption scheme 2 (ES2): Key is being used. However, the encryption and decryption functions are made public.

   Then, which one of the following is TRUE?

   (A) ES2 is always opted, because ES1 is not possible in practice

   (B) Both ES1 and ES2 are fine for a designer

   (C) ES1 is better in terms of security as compared to ES2

   (D) ES2 is better in terms of security as compared to ES1

   (c) For encrypting communications channels, typically two mechanisms work: "link-by-link encryption (LLE)" and "end-to-end encryption (EEE)". To avoid traffic flow analysis, which mechanism is implemented in network security?

   (A) Only EEE

   (B) Only LLE

   (C) Any one of LLE and EEE

   (D) Both LLE and EEE

   (d) In Internet Security Protocol (IPSec), when do you prefer to use the tunnel mode?

   (A) Tunnel mode is used between two routers

   (B) Tunnel mode is used between a host and a router

   (C) Tunnel mode is used between a router and a host

   (D) All of these

   (e) In password management scheme, which one of the password selection strategies is best?

(A) Computer-generated passwords

(B) Proactive password checking

(C) Reactive password checking

(D) User education

(f) In Data Encryption Standard (DES), for which rounds the schedule of left circular shifts requires the number of bits rotated is 1?

(A) (1, 2, 9, 16)

(B) (2, 7, 9, 16)

(C) (1, 3, 7, 16)

(D) (1, 5, 10, 16)

(g) In Data Encryption Standard (DES), the probability of randomly selecting a weak or a semi-weak is _____

(A) 2^{-52}

(B) 2^{-53}

(C) 2^{-48}

(D) 2^{-50}

(h) The value of 3^{90002} mod 11 is

(A) 5

(B) 4

(C) 7

(D) 9

$3^2 \equiv -2 \bmod 11$

$3^4 \equiv 4 \bmod 11$

$3^5 \equiv 1 \bmod 11$

$3^{90002} \equiv 3^2 \bmod 11$

$\equiv 9 \bmod 11$

(i) In an "Intrusion Detection System (IDS)", there are three types of intruders: Masquerader, Misfeasor and Clandestine user. Which one of the following is TRUE?

(A) The masquerade is likely to be an insider; the misfeasor generally is an outsider; and the clandestine user can be either an outsider or an insider

(B) The masquerade is likely to be an outsider; the misfeasor generally is an outsider; and the clandestine user can be either an outsider or an insider

(C) The masquerade is likely to be an outsider; the misfeasor generally is an insider; and the clandestine user can be either an outsider or an insider

(D) The masquerade is likely to be an outsider; the misfeasor generally is an insider; and the clandestine user is outsider

(j) Suppose for Big Data Analytics, you are using an AI/ML algorithm to create a confusion matrix with $n = 165$ as follows: $TN = 50$, $FP = 10$, $FN = 5$ and $TP = 100$. The values of accuracy and precision are _____ and _____, respectively.

(A) 0.89, 0.91

(B) 0.91, 0.89

(C) 0.89, 0.89

(D) 0.91, 0.91

[10 × 2 = 20]

2. (a) Explain the working steps for a general single i^{th} round of the Data Encryption Standard (DES) algorithm.

(b) Explain external error control mechanism used in securing the data link layer.

[6 + 4 = 10]

3. (a) Let two parties A and B agree on the following digital signature scheme. Entity A signs a binary message m of arbitrary length. Entity B can verify this signature by using the public key of A.

Entity A performs the following steps in key generation:
(i) Select two primes p and q such that $q \mid (p-1)$.
(ii) Select a random integer g with $1 < g < p-1$, such that $\alpha = g^{(p-1)/q} (\bmod p)$ and $\alpha > 1$.
(iii) Select a private key a, $1 \leq a \leq q-1$.
(iv) Compute $y = \alpha^a (\bmod p)$.
Public key of A is (p, q, α, y).

After key generation, A generates a signature on m as follows:
(i) Select a random secret integer k, $1 \leq k \leq q-1$.
(ii) Compute $r = \alpha^k \bmod p$, $e = H(m||r)$, and $s = (ae + k) \bmod q$.
(iii) Select two random secret integers u and v, $0 < u < q$ and $0 < v < q$, and compute $r' = r\alpha^{-u}y^v \bmod p$.
(iv) Compute $e' = H(m||r')$ such that $e' = e - v$ and $s' = s - u$.
A then sends the signed message $(m, (e', s'))$ to the verifier B. Here H is a hash function.

Devise a verification algorithm for the party B with correctness proof.

(b) Briefly explain 3DES with three keys encryption and decryption procedures.

[6 + 4 = 10]

4. (a) Consider the following public key encryption scheme:

- Pick an odd number e.
- Pick two prime numbers p and q, where $(p-1)(q-1) - 1$ is evenly divisible by e.
- Multiply p and q to get n.
- Calculate $d = \frac{(p-1)(q-1)(e-1)+1}{e}$.

Is this scheme equivalent to RSA? Show why or why not?

(b) Explain how the Merkle Tree is constructed with 8 transactions, namely Tx_i, for $i = 1, 2, \cdots, 8$. If there transactions are put in a block in the blockchain, how the procedure how to verify the transaction Tx_3 using the Merkle Tree value stored in the block.

[5 + 5 = 10]

5. (a) Suppose Alice and Bob agree on the ElGamal encryption scheme with the parameters $q = 71$ and $\alpha = 7$. Assume that Alice uses Bob's public key $Y_B = 3$ to send two plaintext messages $M = 17$ and $M' = 37$ using the same random integer $X_A = 9$ as the ciphertext messages $(C_1, C_2) = (47, 59)$ and $(C_1', C_2') = (47, 24)$, respectively. Eve intercepts the ciphertexts (C_1, C_2), (C_1', C_2'), and somehow she finds the value of $M = 17$. Show how Eve can use a known-plaintext attack to find the value of M'.

(b) Define "fraud rate" and "insult rate" in an Intrusion Detection System (IDS). Justify–"False negatives are riskier than false positives".

[6 + 4 = 10]

6. (a) Consider a University, say IIT Kharagpur, website that permits its students to view their registration status, grade information and useful information to their email addresses provided they supply their correct login ids and passwords. Let a relational schema in a database be Students (email, passwd,

login_id, full_name, CGPA, dept), where the attributes email, passwd, login_id, full_name, CGPA and dept be, respectively, the e-mail address, password, login id, full name, CGPA and department of a student. Consider the relations students22 and students23, which are the tables of records of all students for 2022 and 2023 batches, respectively.

Present the following SQL injection attacks:

(i) Insert a fake record by an attacker Eve as ('eve@iitkgp.ac.in', 'hello', 'eve', 'Eve', 9.97, CSE) into the relation students22.

(ii) Modify the existing e-mail 'shyam@iitkgp.ac.in' for Shyam Lal by the e-mail address 'eve@iitkgp.ac.in' in the relation students23 so that useful information sent to Shyam will be received by the attacker Eve only.

(b) Discuss the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm used in blockchain.

[5 + 5 = 10]

7. (a) In Distributed Denial-of-Service (DDoS) detection, consider the SYN flood attack, where the victim sees a dis-appropriate number of SYN packets compared to FIN packets in TCP connection. Explain the anomaly detection algorithm based on the "smoothed average" of the previous values of D_i, which is the normalized difference between the number of SYN and FIN packets in the ith observation interval. Also, discuss its limitations.

(b) Discuss briefly "canary" mechanism used in buffer overflow attacks protection.

[6 + 4 = 10]

********** End of Question Paper **********