National University of Computer and Emerging Sciences
FAST School of Computing | Fall-2022 | Islamabad Campus

0025

CS-3002: Information Security

Serial No:

Sessional Exam-II
Total Time: 1 Hour
Total Marks: 50

Tuesday, 8th
~~Wednesday, 9th~~ November, 2022

Signature of Invigilator

Course Instructors

Dr. Zainab Abaid

Ali Kamal	19I-1865	N	085
Student Name	Roll No.	Course Section	Student Signature

DO NOT OPEN THE QUESTION BOOK OR START UNTIL INSTRUCTED.

Instructions:

1. Attempt on question paper. Attempt all of them. Read the question carefully, understand the question, and then attempt it.
2. No additional sheet will be provided for rough work. Use the back of the last page for rough work.
3. If you need more space write on the back side of the paper and clearly mark question and part number etc.
4. After asked to commence the exam, please verify that you have eight (8) different printed pages including this title page. There are a total of 3 questions.
5. Calculator sharing is strictly prohibited.
6. Use permanent ink pens only. Any part done using soft pencil will not be marked and cannot be claimed for rechecking.

	Q-1	Q-2	Q-3	Total
Marks Obtained	10	9	15	34
Total Marks	12	15	23	50

Question 1 [12 Marks]

10

A. Discuss whether a code injection attack is possible on sample code or not. If you think injection is possible, then state how you would inject some code (and the exact statements you would inject) to bypass the condition, i.e. the code should allow any user (not just the username ali) to enter the website. Explain your answer. **[5 marks]**

Note: Code injection follows the basic principles of SQL injection attacks covered in class. Instead of injecting a rogue SQL query, here you are injecting pseudo code.

```
string myVar;

myVar = TextBox.Text; // taking input from user

if (myVar == "ali")
{
   print("hello :" + myVar);
   enterWebsite();
}
else
   print("enter wrong username");
```

(**Note:** The given code is not in a specific programing language; you can write pseudo code in your answer.)

myVar : "" or 1=1 if ("" or 1=1 == ali:

-Entering " or 1=1 in text box would make the if condition like this:

if (myVar == "ali " or 1=1) { } (3)

hence making the if condition always true as we wrote "or 1=1" (an always true statement).

- Due to this, it will allow any user to enter into if condition, thus entering website.

B. Do a code injection attack on the given code in a way that it displays "hello injected code" infinite times on the screen (this will hang the server on which this script is running). [5 marks]

```
string visitor;
visitor = TextBox.Text; // taking input form user
var time = new Time(); // get current time
if (time >"6:00" and time < "12:00")
        print("good Morning :" + visitor);
else if (time >"18:00" and time < "20:00")
        print("good evening :" + visitor);
else
        print("have a nice day :" + visitor);
```

visitor = "); while(true){ print "Hello injected code";}

- This input has semi-colon and closing quotations in visitor variable, which will complete the previous print statement. Now, infinite loop will run printing desired output.

5

C. How would you fix the code in A and B such that it is not vulnerable to code injection any more? [2 marks]

- I would blacklist certain characters e.g " etc so as to restrict injection attacks.
- Whitelist input options that can be entered, only relevant things allowed to be entered.
- Proper format of code i.e have proper fields where user entered values are stored, and not anywhere else.

2

Question 2 [15 Marks] 9

A new email provider, MailPro, is developing a cryptographic system for their users. The design requirements and constraints are as follows.

I. The emails should be encrypted to secure against eavesdropping attacks (*confidentiality*).
II. The users must be able to verify that the contents of the email are exactly as the original sender sent (*integrity*).
III. Users should have an option of enabling high security mode, in which no sender is able to deny that they sent an email.
IV. MailPro will develop their own mobile application and the encryption should be end-to-end, i.e. emails must be encrypted and decrypted on the users' mobile devices (which may be resource constrained).

Keeping these requirements in mind, answer the questions that follow. In all questions, Alice is assumed to be the sender of an email and Bob is the receiver. Alice and Bob's public keys are A_{pub} and B_{pub} respectively, and their private keys are A_{prv} and B_{prv} respectively.

a) For each of the following proposed encryption schemes, suggested by different employees of MailPro, state YES or NO for whether requirements I – IV above are met by the scheme.

i. Alice encrypts her email using (Plaintext XOR B_{pub}). She then calculates the hash of her email, and encrypts the hash with B_{pub}. She appends that hash to the email and sends it to Bob. [4]

I. No ✗
II. Yes ✗
III. No ✓
IV. Yes ✗

(1)

ii. Alice and Bob first use public key cryptography to exchange a 40-bit symmetric key. Alice encrypts her email using RC4 with the symmetric key. She then calculates the hash of the email, encrypts it with the same symmetric key, appends it to her email, and sends it to Bob. [4]

I. Yes ✗
II. Yes ✓
III. ~~No~~ Yes ✗
IV. Yes ✓

(2)

iii) Alice encrypts her email using the AES-256-bit cipher. She then attaches a digital signature to the email and sends it to Bob. This means Bob has to verify whether both her digital certificate and signature are valid. [4]

I: Yes
II: Yes
III: Yes
IV: No

(4)

b) Suggest an ideal encryption scheme that will achieve all four goals stated above. [3]

RSA digital signature of file could be used. Id of private key that could be stored on end users mobile devices and used for decryption, fulfilling point IV. Points I, II, and III are also covered under RSA, as data is encrypted, digital signature will verify integrity, and asymmetric cryptography (RSA) provides data authentication (point II) as no users can decrypt sending email as they have private keys.

(2)

Question 3 [23 Marks]

15

Solve the following RSA encryption/decryption problems. Only the answers will not be awarded marks; show clear working.

Given two prime numbers p=17, q=13

a) What is the value of n? **[1 mark]**

$n = p \times 2 \Rightarrow 221$ ✓(1)

b) What is the value of $\Phi(n)$? **[2 marks]**

$\phi(n) = (p-1)\times(q-1) \Rightarrow (16)\times(12) \Rightarrow 192$ ✓(2)

c) Given e=823, what is the value of d? **[5 marks]**

$de \bmod n = 1$

$823\, d \bmod \phi(n) = 1 = 823 \bmod 192 = 1$

Solve for d through hit and try method

$823 \times (7) \bmod 192 = 1$

$823 \times 7 = 5761$

$5761 \bmod 192 = 1$

$1 = 1 \Rightarrow (192 \times 30 = 5760 + 1 \text{ remainder})$ ✓(5)

$d = 7$

d) What is the value of the public key? [1 mark]

e: 823 ✓ 0.5

e) What is the value of the private key? [1 mark]

d: 7 — 0.5

f) Given a message M=56. What is the ciphertext, C? [5 marks]

P_T: 56

$C_T = P_T^e \bmod N$

$56^{823} \bmod 221 \Rightarrow$ ⊗C ✓ (1)

= Calculator gives math error

Value too large.

g) Show the decryption steps clearly to recover the message. [5 marks]

Decryption steps (Assuming C is encrypted text, P_T is original plain text) (2)

$P_T = C^d \bmod N$

$P_T = C^7 \bmod 221$

Since we don't know exact value of C due to math error in calculator, (too large value of e), we can't really compute original C back to plain text as we don't have exact value of C.

original message

h) What is the current recommendation for RSA key size? [1 mark]

Atleast 256 bit - 512 bit RSA key. (1)
Although nowadays 2048 bits key are also used.

i) Describe in detail why RSA was developed, i.e. what were the disadvantages of symmetric key encryption algorithms that it overcomes? [2 marks]

- There was problem of sharing key in secure manner in symmetric key encryption
- There was also issue of data non-repudiation in symmetric key cryptography i.e there was no way of guaranteeing that a specific user sent the data e.g they could always back off and say they didn't send data, and since keys are public, there's no way to verify if user did or did not send data. (2)

-RSA solves both of these issues, as it is asymmetric key encryption i.e has public and private keys i.e no issue of securely sharing keys or data non-repudiation.