## National University of Computer and Emerging Sciences

FAST School of Computing

F 201-2022

Johannahad Campus

0025

CS-3002: Information

Security (DSN)

Serial No:

Sessional Exam-II

Total Time: 1 Hour

Total Marks: 50

Wednesday: 9th November, 2011

Course Instructors

Dr. Zainab Abaid

Signature of Invivilator

Ali Komal 19I-1865 N

DO NOT OPEN THE QUESTION BOOK OR START UNTIL INSTRUCTED.

Instructions:

 Attempt on question paper. Attempt all of them. Read the question carefully, understand the question, and then attempt it.

No additional sheet will be provided for rough work. Use the back of the last page for rough.

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 a questions.

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

Islamabad Campus

Question 1 [12 Marks]

National C mark

A. Discuss whether a code injection attack is possible on sample code of not. If you think injection would inject some code (and the exact statements you would inject some code) A. Discuss whether a code injection attack is possible on sample.

A. Discuss whether a code injection attack is possible on sample.

It is possible, then state how you would inject some code (and the exact statements you would inject in possible, then state how you would inject some code (and the exact statements you would inject in possible, then state how you would inject some code (and the exact statements you would inject in possible). A. Discuss whether a code injection is possible, then state how you would inject some code (and the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the code should allow any user (not just the username ali) to enter the username ali) to enter the code should allow any user (not just the username ali) to enter the username ali) to website. Explain your answer. [5 marks]

Note: Code injection follows the basic principles of SQL injection attacks covered in class. Instead

```
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

-Entering " or 1:1 in text box would make the it condition like this: hence making the if condition adways some true statement). - one to this, it will allow any user to enter into it condition, thus andering website. **FAST School of Computing** 

Fall-2022

Islamabad Campus

n. Do a code injection attack on the given code in a way that it displays "helio 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) & prind "Lello injected wole"; 36

This input has enimal conimolon and closing puotations in visitor vortable, which will enter complete the previous print statement. Some complete the previous print statement.

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

whitelist input ophions that on be extred, 2 only relevant things about to be extred.

I hoper former of cool is have the proper former of cool is extred values one

Stored, and not anywhere else

## National University of Computer and Emerging Sciences Islamabad Campus

Ouestion 2 [15 Marks]

A new email provider. MailPro. is developing a cryptographic system for their users. The design

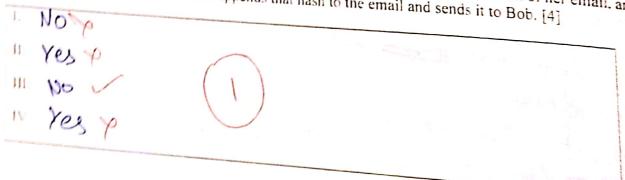
- The emails should be encrypted to secure against eavesdropping attacks (confidentiality)
- The emails should be encrypted to secure against cavesuropping.

  The users must be able to verify that the contents of the email are exactly as the original sender sent. 1
- (integrity)
  Users should have an option of enabling high security mode, in which no sender is able to deny 111
- that they sent an email

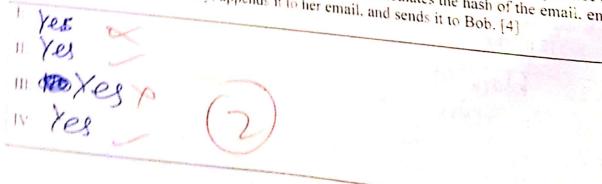
  MailPro will develop their own mobile application and the encryption should be end-to-end, i.e. IV MailPre will develop their own mobile apprecation and mobile devices (which may be resource

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<sub>Dub</sub> and  $B_{pos}$  respectively, and their private keys are  $A_{prv}$  and  $B_{prv}$  respectively.

- 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.
  - Alice encrypts her email using (Plaintext XOR Bpub). She then calculates the hash of her email, and encrypts the hash with B<sub>put</sub>. She appends that hash to the email and sends it to Bob. [4]



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]



FAST School of Computing

Full-2022

Islamabad Campus

Alice energpts her email using the AliS-23n-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]

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

RSJ Could be used it has private key a had could be stored on feel years another alwies of one used for decryptons, mobile alwies to one used for decryptons, was path fufilling points 1,11,000 ove also covered what RSA, as de compted, digital signature when very in 111 ) provider dosa

## National University of Computer and Emerging Sciences

Fall-2022

Islamabad Campus

00%

FAST School of Computing Question 3 [23 Marks]

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: Px2 => 221



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

O(n): (p-1)x(2-1)=) (16)x(12)=) 192



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

Ode mod n=1

SERVE STORES TO THE

Q3 d mod 2000 Q(N) = 1 = 1823 mod 192=1

Establish Solve for I through hit and try method

\$ 823 x(7) mod (92 = 1

5761 mod 192:1

( 1: 1 =) (192 x30: 5760 =) 1 remainder

## Sptional University of Computer and Emerging Sciences LAST School of Computing Fall-2022 Islamsbad Campus

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

e: 80-3

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

d=7 - 0.j

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

PT: 56

CT: PTe mod N

56823 mod 221 => OC

= Calculator gives

moth error

Value too lorge.

5.5/2

Fall-2022

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

PT = and nod N Since we don't love exact value of (

Since we don't love exact value of (

to make error in calculator, loss large

complete got all the part of back to it PT = ( mod 221

Atlent 156 bit - 5/2 bit RSA Icey.

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 southering key in Secure marrier in symmetric key manyphon Secure marrier in symmetric key manyphon There was also issue of data non-organization. in symmetric key imprography i e there in symmetric key imprography i e there is so no so grander the soul a specific were send that the data e.g. they were sould always back a off and say they will say data, and since keys are public, there's and way to verify if was public, there's and way to verify if asymmetric leay = encryption i.e when
public and private keys i-e no issue of
securely showing leays or data
non-repudiation.