# Symbiosis University of Applied Sciences

## END SEMESTER SEMI ONLINE THEORY EXAMINATION JAN-2022

## FRONT PAGE OF SEMI ONLINE ANSWER BOOK

| Enrollment Number: | 2 | 0 | 1 | 9 | B | T | C | S | 0 | 8 | 8 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

**2019BTCS088**

**Name of Student: Yash Gupta** **Email: 2019BTCS088@student.suas.ac.in**

**Name of Program: B.TECH** **Year: 2021-2022** **Semester: V**

**Name of Paper: Cryptography & Cyber Security** **Paper Code: BTCS0501**

**Date: 31-01-2022** **Day: Monday** **Time: 10:30 AM – 01:30 PM**

**Total No. of Pages: 15**

**Note: Read all instructions carefully provided by Examination Office for Semi Online Exams.**

**Instructions for Examinees:**

1. Fill up all entries required in this page.
2. Merge this .docx page with your scanned answer sheets as a first page in a single PDF file.
3. Write your answers on A4 Ruled Sheet/Register Page.
4. Write End after the last attempted question.
5. Write the page number on every page and mentioned Total No. of Pages on front Page.
6. Don't write Name or Enrollment number on answer sheets.
7. **If the content in the Answer Book of two students or more has found similar, in that case all copied answer will stand cancelled and it will be case of UFM.**

---

## Details of Evaluation

| Section | Question No. | | | | | Total |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | |
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| | | | | | TOTAL | |

**Marks Obtained (In figure) :……Marks Obtained (In words) : …….**

**Maximum Marks (In Figure): 50** **Minimum Pass Marks (In Figure): 20**

**Name of Evaluator: _____Signature & Date of Evaluator:_____**

**Comments (to be given by Evaluator): _____**

**_____**

PAGE NO.: 01
DATE 31/01/2022

## Section-01

Q2 SOURCE_CODE

Ans 2:

```
/* Program_for_implementing_Caesar_Cipher_in_C++
   Author: 2019BICS088
   Day,Date: 31_01_2022; Monday
*/
#include <iostream.h>      // Including Necessary Header Files
#include <string.h>
using namespace std;

char caesar(char);
int main() {
        string input;
        do {
            cout << "Enter Plaintext & Press Enter "<<endl;
            cout << "Enter Blank line to Quit"<<endl;
            getline(cin, input);
            string output = "";
            for(int x = 0; x < input.length(); x++){
                output += caesar(input[x]);
            }
            cout << output << endl;
        }
        while(!input.length() == 0);
}// end main()
char caesar(char c){
        if(isalpha(c))
            { c = toupper(c); //using upper to keep from
                              // having to use seperate for
                              // A-Z, a-z...
            c = (((c-65)+13)%26)+65;
        }
```

```
//If c isn't alpha, just return it.
    return c;
}
```

O/P of the CODE: Enter ciphertext and press enter:-
PlainText: SANFOUNDRY
UpperText: FNASBHADEL
Enter blank line to Quit.

Q3

Ans3:

| MAC | MESSAGE DIGEST |
|---|---|
| 1. MAC stands for Message Authentication Code. | 1. Message Digest is S/W as it only. |
| 2. A message authentication code algorithm takes TWO Inputs :- a) Message b) Secret key | 2. A message digest algorithm only takes a SINGLE INPUT:- a) Message |
| 3. In this algorithm, after taking two inputs it produces a MAC. that allows us to verify & check the integrity and authentication of the Message. generated. | 3. In this algorithm, after taking single input it produces a message digest which Helps us to verify & check the integrity of the message generated. |

| MAC | MESSAGE DIGEST |
|---|---|
| 4. If we change anything in the secret key, or the message, the results in the MAC gets generated differently. | 4. If we change anything in the I/P message, results in the different Hash is being generated. |
| 5. In this algorithm, an attacker cannot identify & validate the correct MAC without the secret key. | 5. In this algorithm, an attacker has NO CLUE about the message, once a Hash is generated. |
| 6. Ex: Most popular MAC are HMAC & MAC. | 6. Most popular message digest algorithms are:- MD5 and SHA-1. |
| 7. HMAC & MAC are generated using DES in CBC Mode. | 7. MD5 and SHA-1 are generated using SHA algorithm. |

Q4
Ans: PROBLEM ASSOCIATED IN EXCHANGING PUBLIC KEYS:

In order to establish secure communications using Public-Key cryptography, we must share our Public Key. The problem with this is:

a) How do I know that the public key I intend to use is REALLY the public key of the party with whom I wish to securely

communicate & not some attacker's key claiming to be the public key of that party?

- If I use the wrong key, the attacker can read my supposedly secure communication & my intended recipient cannot.

For Example: Suppose, you can find my publickey at YashGPK.com and I can state my fingerprint on my any socked media code platfosm (Stackoveflow) for some demonstration purpose, Now anyone can test my publickey against it & He/she can download it.

NOTE: Assuming that it's me who actually done that post.

b) Also, if for large-scale organizations where large Number of parties must pairwise, secretly communicate, many schemes don't scale well.

c) Many possible attacks can be done in RSA Algorithm also.

PAGE NO.: 05
DATE 31/01/2022

## Section-02

Q:

Ans6: **AFFINE CIPHER**: An affine cipher is a type of monoalphabetic substitution cipher, where each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function and converted back to a letter. The formula used means that 'each letter encrypts to one other letter & back again' meaning the cipher is essentially a standard substitution cipher. with a rule governing which letter go to which.

**MATHEMATICAL DESCRIPTION**: In the affine cipher the letters of an alphabet size 'm' are mapped first to the integers in the range 0 . . . m-1. It then uses a modular arithmetic to transform the integer that each plaintext letter corresponds to into another integer that correspond to a ciphertext letter.

The Encryption func$^n$ for single letter is:-

$$E(x) = (ax+b) \bmod m$$

a, b → Keys of the cipher

m → Size of the Alphabet

(a, m) → Must be co-prime

Similarly, the Decryption function for single letter is:-

$$D(x) = a^{-1}(x-b) \bmod m$$

$a^{-1}$ is the Multi-plicative Inverse of a modulo m

$$1 = aa^{-1} \bmod m$$ — such that

**WEAKNESS:** The cipher's primary weakness comes from the fact that if the cryptanalyst can discover (by any means of frequency analysis, bruteforce, guessing) the plaintext of two ciphertext characters then the key can be obtained by solving a simultaneous equation. Since we know 'a' and 'm' are relatively coprime this can be used to discard many "false" keys in an automated system.

**CODE ANALYSIS:**

for Encryption: in C++:

```
string encryptMessage(string msg)
{
    string cipher = "";
    for(int i=0; i<msg.length(); i++)
    {
        if(msg[i] != ' ')
        { cipher = cipher + (char)((((a*(msg[i]-'A'))
                                    +b)%26)+'A');
        }
        else {
            cipher += msg[i];
        }
    return cipher;
}
```

**EXAMPLES:** Plain Text: ~~AFFINE CIPHER~~ TWENTY FIFTEEN

A-Z → [0-25] w.r.t

**ENCRYPTION**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | T | W | E | N | T | Y | F | I | F | T | E | E | N | | |
| x | 19 | 22 | 4 | 13 | 19 | 24 | 5 | 8 | 5 | 19 | 4 | 4 | 13 | | |
| (ax+b)%26 | 5 | 4 | 10 | 7 | 5 | 12 | 1 | 0 | 1 | 5 | 10 | 10 | 7 | | |

Cipher Text: → F E K H F M B A B F K K H

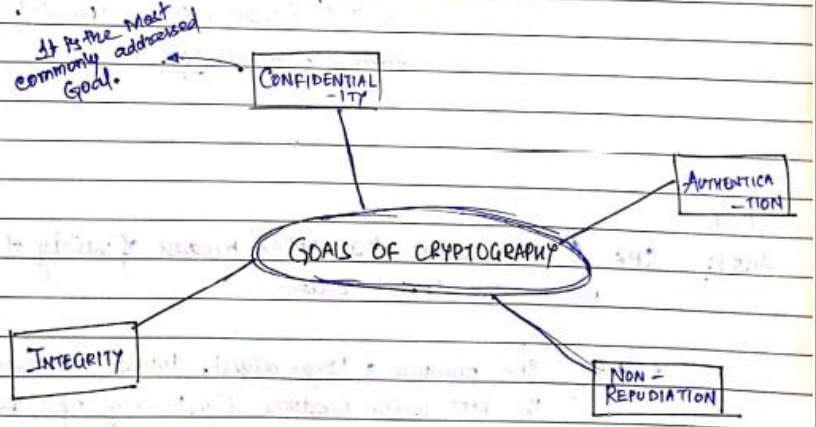
PAGE NO.: 07
DATE 31/01/2022

DECRYPTION :- Encrypted Text: F E K H F M B A B F K K H

| | | |
|---|---|---|
| Value: | 5 4 10 7 5 12 | 1 0 1 5 10 10 7 |
| $23^{*}(x-b) \bmod 26$ : | 19 22 4 13 19 14 | 5 8 5 19 4 4 13 |
| Decrypted Text: | T W E N T Y. | F I F T E E N |

Q8

Ans8: GOALS OF CRYPTOGRAPHY : Cryptography is the study of information hiding and verification by the involvement of the protocols, algorithms and strategies to securely, and consistently prevent or delay unauthorized access to sensitive information and enable verifiability of every component in a communication.




(i) Confidentiality of Data :

- It implies that only an authorized recipent should be able to extract the contents of a message from its encrypted form.
- The Recipent decrypts the Message using a cryptographic key that may or may'nt be the same as the one used by the sender.

2. Data Integrity: It ensures that the message received is the same as the message that was sent using Hashing to create a unique message that is sent along with the message.

3. Data Authentication: It ensures that the receipent should be able to verify from the message, the identity of the sender, the origin of the path it traveled so as to validate claims from emitter or to validated the recipeent expectations.

4. Data Non-Repudiation: It ensures that the re-emitter shouldn't be able to deny the message. It's the ability to ensure that a party to a contract or a communication must accept the authenticity of their signature or a document or the sending of a message.

---

Q7.

Ans7: SHA is more secure than MD5 because of variety of Reasons which are listed below:—

a) Firstly, SHA produces a longer digest, 160 bits as compared to the MD5 which produces digest only upto 128 bits which means BRUTEFORCE attack would be very much difficult to perform over SHA.

b) Also, there are O(ZERO) No. of collisions found for SHA. whereas in case of MD5, a collision can be found for

relatively short period of time.

c) Since, the first introduc of SHA, many newer versions are introduced that are much more secure than the original one.

SHA-256 → uses 512-bit block → 32 bytes Digest produced.
SHA-384 → " → 1024 bit block → 48 bytes "
SHA-512 → " → 1024 bit block → 64 bytes "

↳ It makes the cryptanalysis much more difficult. Also, No known successfull attacks on the newer versions of SHA.

d) SHA is now used in the Digital signature algorithm, which is the US Federal Signature scheme.

e) Also, the construct behind the SHA is that these square measure accustomed generate a Novel Digital Fingerprint of knowledge or measure that is understood as a Hash or Digest.

## Section-03

Q9

Ans 9: A Parasite Virus is a type of virus that spreads by attaching itself to another program. When a program that is infected with a parasitic virus executes, the virus code runs as well, & the computer operating system gives the virus code the same rights as the program. It allows the virus to make changes on the computer, install itself within the computer's memory, or copy itself.

HOW TO RECOGNIZE it? The signs of a parasitic virus infection are similar to those of any virus, slower performance, pop-ups, new tasks running, changes to web-browsers etc.

HOW TO Prevent it? To avoid a parasitic virus infection, users should avoid clicking suspicious links or downloading attachments from unverified emails, as well as visiting suspicious sites. Aside from training users, endpoint protection is key to keeping your network clear of parasitic viruses.

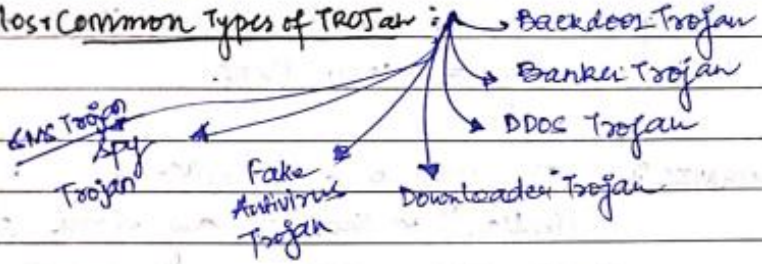
Q10.

Ans 10: TROJAN HORSE ⇒ The name of Trojan Horse is taken from the classical story of the Trojan War.

A Trojan Horse virus is a type of malware that downloads onto a computer disguised as a legitimate program. The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain user's system access by with their software.

For Ex: There is a direct action Trojan Name Js. ExitW. It can be downloaded from many malicious sites. The effect of this makes the computer fall in a Never-Ending loop of start & shutdown. It doesn't cause any serious damage but there are many other Trojans which are very severe.

Most Common Types of TROJan:




Real world Examples of Trojan Horse: (1) Rakhni Trojan: It delivers a spy ransomware or a cryptojacker tool - which enables an attacker to use a device to mine cryptocurrency.

(2) Tiny Banker. It enables Hackers to steal users financial details.

BEST WAY TO RECOGNIZE: (1) Start using a [Trojan & cannes or Malware Removal software]

(2) If computer settings, suddenly changing or loss of computer performance. or any unusual activity taking place.

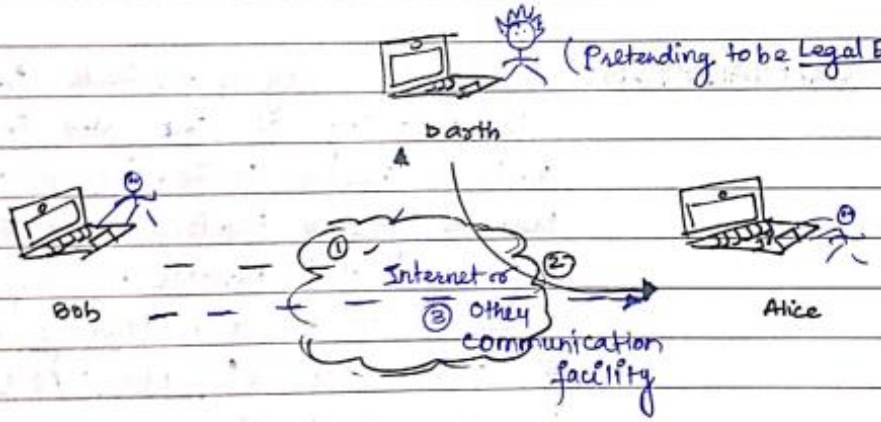
—x—

## Section-04

Q11

Ans11: Masquerade is a type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity. It takes place when one pretends to be a different entity. It usually includes one of the other forms of active attack.

For Ex: Authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.




Q12

Ans12: A boot sector is defined as the reserved section of a disk that contains the code and data needed to start the operating system (OS) of a computer. A boot sector virus is a type of malware that infects a system's boot partition or the Master Boot Record (MBR) of a Hard Disk.

During startup of different processes & before security software can be executed, the virus executes Malicious code.
Once a computer is infected, a boot sector virus will try to infect every disk that is accessed on the infected system.

Ex: A user's pc can get infected by Boot Sector Virus if:—
a) when starting up a machine from an infected USB drive.
b) Email attachments also contain → & after clicking over it, it infects the owner computer as well as other pc's on the Network.

6(3

Ans 13: CRYPTANALYSIS: It is the study of methods for obtaining the meaning of encrypted information, without access to the secret information that is typically required to do so.
Typically, it involves knowing how the system works and finding a secret key.
It is also k/w as "CODEBREAKING" or "cracking the code".

PROCESS INVOLVED: The ciphertext is generally the easiest part of the cryptosystem to obtain & therefore, is an important part of cryptanalysis.
Depending on what information is available & what type of cipher is being analyzed, cryptanalysis can follow one or more attack models to crack a cipher.

Ex: Suppose a ciphertext, having certain alphabets, so as a cryptanalyst it performs cryptanalysis such as:-

| Letter | Number of occurences | Frequency |
|---|---|---|
| E | 8,915 | .127 |
| T | 6,820 | .097 |
| A | 4,320 | .075 |
| I | 1,157 | .073 |
| W | 2,246 | .067 |

— such kind of thing.

Q14

Ans14: **SNIFFING**: It is the process in which all the data packets passing in the Network are Monitored. Sniffers are usually used by Network Admin's to monitor as well as troubleshoot the Network Traffic.
Attackers uses both types of sniffers i.e. Hardware & Software based for capturing data packets to steal & sensitive information containing password & users a/c's.

Eg: Tools used as for SNIFFING:
In Kali Linux (OS), → Wireshark is a GUI based tool used as Network packet analyser. With the help of this tool, we can see what's happening in our Network & apply filters on it.

**SPOOFING**: It is the process in which an intruder introduces fake traffic and pretends to be someone else (legal source or the legitimate authority). This process is achieved by sending packets with incorrect source address over the Network. The best way to

deal and tackle with this attack is to use a digital signature.

Eg: Tools used for Spoofing: MITMPROXY → It is an SSL-capable man-in-the-middle HTTP proxy, providing a console interface that allows traffic flows to be inspected & edited at the moment they are inspected. We can inspect, modify Network Traffic, save HTTP conversations for inspection, SSL inspection and more.

```
[kali-linux]$ mitmproxy . -p 80
                          → PortNumber
```

THE END