SEAT NO. ____________

NED UNIVERSITY OF ENGINEERING & TECHNOLOGY

FINAL YEAR(SOFTWARE ENGINEERING)
FALL SEMESTER EXAMINATIONS 2021
BATCH 2018

Time: 3 Hours

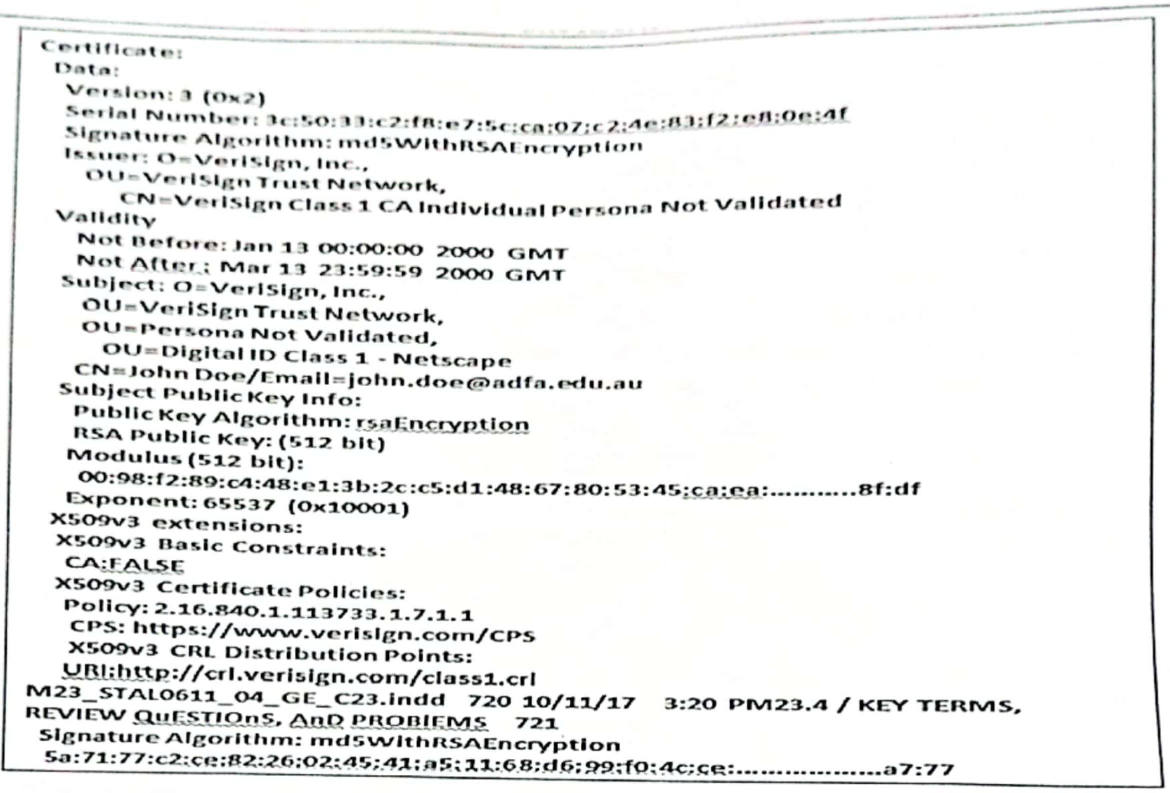
Dated:19-02-2022
Max.Marks:60

Network & Information Security - CT-460

Instructions:

- Attempt ALL questions.
- Make neat and clean diagrams where necessary.
- Questions can be attempted in any order but all parts of a question must be attempted together.

Q1 (a)	**EXPLAIN** the working of **Secure Hash Algorithm (SHA)-512** Algorithm with the help of diagrams of message digest generation and processing of a single block. **[CLO-1]**	[6]
(b)	**DESCRIBE** the Worms and their following attributes. **[CLO-1]** • Multiplatform • Multi-exploit • Ultrafast spreading • Polymorphic • Metamorphic	[6]
Q2 (a)	**EXPLAIN** with the help of diagram the Encryption and Key Generation Process of AES algorithm. ***[CLO-1]***	[6]
(b)	***EXPLAIN*** *the six stages of Intruder Behavior.* **[CLO-1]**	[6]
Q3 (a)	*Suppose you have a new smartphone and are excited about the range of apps available for it. You read about a really interesting new game that is available for your phone. You do a quick Web search for it and see that a version is available from one of the free marketplaces. When you download and start to install this app, you are asked to approve the access permissions granted to it. You see that it wants permission to "Send SMS messages" and to "Access your address-book".* ***[CLO-2]*** ***DETERMINE*** *the answers to the following question.* • *Should you be suspicious that a game wants these types of permissions?* • *What threat might the app pose to your smartphone,* • *Should you grant these permissions and proceed to install it?* • *What the types of malware it might be?*	[4]
(b)	Consider the details of the X.509 certificate shown below. **DETERMINE** the answers to the following questions. **[CLO-2]** a. Identify the key elements in this certificate, including the owner's name and public key, its validity dates, the name of the CA that signed it, and the type and value of signature. b. State whether this is a CA or end-user certificate, and why. c. Indicate whether the certificate is valid or not, and why. d. State whether there are any other obvious problems with the algorithms used in this certificate.	[4]



```
Certificate:
 Data:
  Version: 3 (0x2)
  Serial Number: 3c:50:33:c2:f8:e7:5c:ca:07:c2:4e:83:f2:e8:0e:4f
  Signature Algorithm: md5WithRSAEncryption
  Issuer: O=VeriSign, Inc.,
    OU=VeriSign Trust Network,
      CN=VeriSign Class 1 CA Individual Persona Not Validated
 Validity
   Not Before: Jan 13 00:00:00  2000  GMT
   Not After : Mar 13 23:59:59  2000  GMT
  Subject: O=VeriSign, Inc.,
    OU=VeriSign Trust Network,
    OU=Persona Not Validated,
      OU=Digital ID Class 1 - Netscape
   CN=John Doe/Email=john.doe@adfa.edu.au
  Subject Public Key Info:
   Public Key Algorithm: rsaEncryption
   RSA Public Key: (512 bit)
  Modulus (512 bit):
   00:98:f2:89:c4:48:e1:3b:2c:c5:d1:48:67:80:53:45:ca:ea:..........8f:df
  Exponent: 65537  (0x10001)
 X509v3  extensions:
  X509v3  Basic Constraints:
   CA:FALSE
  X509v3  Certificate Policies:
   Policy: 2.16.840.1.113733.1.7.1.1
    CPS: https://www.verisign.com/CPS
   X509v3  CRL Distribution Points:
   URI:http://crl.verisign.com/class1.crl
M23_STAL0611_04_GE_C23.indd   720 10/11/17    3:20 PM23.4 / KEY TERMS,
REVIEW QuESTIOnS, AnD PROBIEMS    721
 Signature Algorithm: md5WithRSAEncryption
  5a:71:77:c2:ce:82:26:02:45:41:a5:11:68:d6:99:f0:4c:ce:.................a7:77
```

(c) APPLY HILL Cipher to encrypt Message $\begin{bmatrix} A \\ C \\ T \end{bmatrix}$ with the following key. Then generate the original text from the cipher text using the inverse of key matrix modulo 26. **[CLO-2]** **[4]**

$$\begin{bmatrix} 6 & 4 & 1 \\ 13 & 12 & 10 \\ 8 & 7 & 5 \end{bmatrix}$$

Q4

(a) An enterprise network comprises of has different network devices (Routers, Switches etc.), Servers like Web, Email, DNS etc. and end-users. **PREPARE** defense mechanism against DDoS attacks on this organization by taking into consideration organization services. **[CLO-2]** **[6]**

(b) You are Cloud Service Provider (CSP) providing Web Hosting Services to different customers. A Customer wants to host his site **www.mysite.com** in a secure manner. **DETERMINE** how you will secure this site using PKI and HTTPS. **[CLO-2]** **[6]**

Q5

(a) Assume that one of the largest enterprises has been hit by Advanced Persistent Threat (APT) which is class of Malware. You have assigned the task to mitigate the attack in order to minimize the current damage. The other task assigned is to propose a plan in order to protect the organization from such attacks in future. **APPLY** APT countermeasures approach based upon the malware protection recommendations. **[CLO-2]** **[6]**

(b) You are given the following "Informal Firewall Policy" details to be implemented [6]

1. E-mail may be sent using SMTP in both directions through the firewall.
2. Web requests (both insecure and secure) are allowed from any internal user out through the firewall.
3. Web requests (both insecure and secure) are allowed from anywhere on the Internet to the DMZ Web server.
4. DNS lookup requests by internal users are allowed via the DMZ DNS server, which queries to the Internet
5. External DNS requests are provided by the DMZ DNS server.
6. FTP Traffic is allowed to and from the organization.

APPLY suitable packet filter rule sets to be implemented on the Firewall to satisfy the afore-mentioned policy requirements. **[CLO-2]**