**CB3491-CRYPTOGRAPHY AND CYBER SECURITY**

UNIT I INTRODUCTION TO SECURITY

**PART-A**

**1 What is Security attack, Security mechanism and Security service?**

**Security attack:** Any action that compromises the security of information owned by an organization.

**Security mechanism:** A mechanism that is designed to detect, present or recover from a security attack.

**Security service:** A service that enhances the security of the data processing systems and

the information transfer of an organization.

**2 Define confidentiality.**

Confidentiality ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties. This type of access includes printing, displaying, and other forms of disclosure.

**3 Define integrity.**

Integrity ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing, deleting, creating and delaying or replaying of transmitted messages.

**4 Define Authentication, Nonrepudiation, Availability and Access control.**

**Authentication:** Ensures that the origin of a message is correctly identified, with an assurance that the identity is not false.

**Nonrepudiation:** Requires that neither the sender nor the receiver of a message be able to deny the transmission.

**Availability:** Requires that computer system assets be available to authorized parties

when needed.

**Access control:** Requires that access to information resource may be controlled by or for the target system.

**5 List 4 general categories of attack.**

* Interruption
* Interception
* Modification
* Fabrication

**6 Differentiate between Interruption and Interception.**

**Interruption Interception**

An asset of the system is destroyed or becomes unavailable or unusable

An authorized party gains access to the asset

This is an attack on availability This is an attack on confidentiality

**E.g.:** Destruction of a piece of hardware, the

cutting of a communication line, the disabling

of the file management system.

**E.g.:** Wiretapping to capture data in a

network, illicit copying of files or

programs.

**7 Differentiate between Modification and Fabrication.**

Interruption Interception

An unauthorized party not only gains access to

but tampers with an asset

An unauthorized party inserts

counterfeit objects into the system.

This is an attack on integrity This is an attack on authenticity

**E.g.:** Changing values in a data file, altering a

program so that it performs differently

**E.g.:** Insertion or spurious message in a

network or the addition of records to a

file

**8 Compare active and passive attack (Dec 2020)**

**Active attack Passive attack**

These attacks involve some modification of the data stream or creation of false stream

They are in the nature of eavesdropping, on or monitoring of transmissions

The types of active attacks are

* Masquerade
* Replay
* Modification
* Messages

The types of passive attacks are

* Release of message contents
* Traffic analysis

It is difficult to prevent active attacks

absolutely.

They are very difficult to detect

(because they do not move any

alternation to data). But it is feasible to

prevent the success of these attacks.

**9 List the components involved in network security (i.e. Model for network security)**

* Message
* Two principals (Source and Destination)
* Trusted third party
* Opponent

**10 List the 4 basic tasks in designing a particular security service.**

* Design an algorithm for performing the security-related Transformation
* Generate the secret information to be used with the algorithm
* Develop methods for the distribution and sharing of secret information
* Specify a protocol to be used by the two principals.

**UNIT II - SYMMETRIC CIPHERS**

PART-A

**1 What is symmetric key encryption?**

Symmetric key encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process.

**2 List the 5 main components of a symmetric encryption system.**

* Plaintext
* Encryption algorithm
* Secret key
* Ciphertext
* Decryption algorithm

**3 Give the 5 modes of operations of block cipher. (Dec 2020)**

* Electronic codebook (ECB)
* Cipher block chaining (CBC)
* Cipher feedback (CFB)
* Output feedback (OFB)
* Counter (CTR)

**4 List the parameters for the 3 AES version**

Parameters AES-128 AES-192 AES-256

Plaintext block size (bits) 128 128 128

Key size (bits) 128 192 256

Number of rounds 10 12 14

**5 Compare DES and AES**

Parameters DES AES

Developed 1977 2002

Key length 56 bits 128,192 or 256 bits

Cipher type Symmetric block cipher Symmetric block cipher

Block type 64 bits 128 bits

Security Proven inadequate Considered secure

**6 Brief the strengths of triple DES**

Triple DES is based on the DES algorithm, therefore it is very easy to modify existing software to use triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the attacks (i.e. Triple DES systems are significantly more

secure than single DES)

**7 Determine the GCD of (24140,16762) using Euclid‟s algorithm**

GCD (24140, 16762) = GCD (16762, 7378)

= GCD (7378, 2006)

= GCD (2006, 1360)

= GCD (1360, 646)

= GCD (646, 68)

= GCD (68, 34) = GCD (34,0) = 34

**8 Determine the GCD of (1970,1066) using Euclid‟s algorithm**

GCD (1970,1066) = GCD (1066,904)

= GCD (904, 162)

= GCD (162, 94)

= GCD (94, 68)

= GCD (68, 26)

= GCD (26, 16)

= GCD (16,10)

= GCD (10,6)

= GCD (6,4)

= GCD (4,2)

= GCD (2,0)=2

**9 Define finite field?**

A field (F, +, .) is called a finite field if the set F is finite. A field is a ring in which the multiplication operation is commutative, has no zero divisors, and includes an identity element and an inverse element.

**10 Define field and ring in number theory (Dec 2020)**

A ring is a set of elements that is closed under two binary operations, addition and multiplication, with the following: the addition operation is a group that is commutative; the multiplication operation is associative and is distributive over the addition operation.

A field is a ring in which the multiplication operation is commutative, has no zero divisors, and includes an identity element and an inverse element.

**UNIT-III ASYMMETRIC CRYPTOGRAPHY**

**PART-A**

**1 Define primality testing.**

A primality test in an algorithm for determining whether an input number is prime

(i.e. Given an number n, check if it is prime or not)

**2 State whether symmetric and asymmetric cryptography algorithm needs key exchange**

* In symmetric key encryption all parties involved in communication have to exchange the key (a secret key) used to encrypt the data before they can decrypt it (This is the main disadvantage of symmetric encryption)
* Asymmetric key encryption uses two keys. A public key is made freely available to anyone who might want to send you a message. The second key, private key is kept secret.

**3 Find the GCD of (2740, 1760) using Euclid‟s Algorithm.**

GCD (2740,1760) = GCD (1760,980)

= GCD (980, 780)

= GCD (780, 200)

= GCD (200, 180)

= GCD (180, 20)

= GCD (20, 0)

= 20

**4 For p = 11 and q = 19 and choose d = 17. Apply RSA algorithm where Cipher message= 80 and thus find the plain text.**

n = pq = 11 × 19 = 209.

C=Me mod n ; C=517mod 209 ; C = 80 mod 209.

So the plain text is 5

**5 What is meet in the Middle Attack?**

* A Meet-in-the-Middle (MitM) Attack is a kind of cryptanalytic attack where the attacker uses some kind of space or time tradeoff to aid the attack.
* MitMs can take the form of dividing the target communication into two so that each piece can be addressed individually.
* It could mean transforming an attack requiring X amount of time into one requiring Y time and Z space. The aim is to significantly reduce the effort needed to perform a brute-force attack.

**6. Write the formula for Encryption and Decryption in RSA (NOV/DEC 2021).**

For Decryption C = Me mod n

For Encryption M = C d mod n

**7. What is the use of Fermat’s theorem?(NOV/DEC 2021)**

* This theorem is central to the calculus method of determining maxima and minima: in one dimension, one can find extreme by simply computing the stationary points (by computing the zeros of the derivative), the non- differentiable points, and the boundary points, and then investigating this set to determine the extreme.
* One can do this either by evaluating the function at each point and taking the maximum, orby analyzing the derivatives further, using the first derivative test, the second derivative test, or the higher-order derivative test.
* In dimension above 1, one cannot use the first derivative test any longer, but the second derivative test and higher-order derivative test generalize.

**8. Describe Chinese remainder theorem.**

The Chinese remainder theorem is a result about congruences in number theory and its generalizations in abstract algebra. In its basic form, the Chinese remainder theorem will determine a number n that when divided by some given divisors leave given remainders.

**9. Define Euler’s theorem and it’s application? (APRIL/MAY 18)**

Euler’s theorem states that for every a and n that is relatively prime:

a Φ(n)≡ 1 mod n

**10.Define Euler’s totient function or phi function and their applications?**

The Eulers totient function states that, it should be clear for a prime number p,

Φ(p) =p-1

**UNIT-IV INTEGRITY AND AUTHENTICATION ALGORITHMS**

PART-A

**1 Write a simple authentication dialogue used in Kerberos.**

(1) C → AS 1Dc||Pc||1Dv

(2) AS → C Ticket

(3) C → V 1Dc||Ticket

Ticket = EKv [1Dc||ADc||1Dv]

where

C= Client

A= Authentication server

V= Server

1Dc= Identifier of user on C

1Dv= Identifier of user on V

Pc= Password of user on C

ADc= Network address of C

KV= Secret encryption key shared by A, S and V.

||= Concatenation

**2 Contrast various SHA algorithms.**

Properties SHA-1 SHA-224 SHA-256 SHA-384 SHA-512

Message Digest Size 160 224 256 384 512

Message Size <264 <264 <264 <2128 <2128

Block size 512 512 512 1024 1024

Word size 32 32 32 64 64

**3 What is digital signature?**

A digital signature is an authentication mechanism that allows the sender to attach an electronic code with the message in order to ensure its authenticity and integrity. This electronic code acts as the signature of the sender and, hence is named digital signature.

Digital signature uses the public-key cryptographic technique. The sender uses his private key and a signing algorithm creates a digital signature, and the signed document can be made public. The receiver uses the public key of the sender and a verifying algorithm to verify the digital signature.

**4 What is realm in Kerberos?**

A Kerberos realm is a set of managed nodes that share the same Kerberos database. The Kerberos database resides on the Kerberos master computer system, which should be kept in a physically secure room. A read-only copy of the Kerberos database might also reside on other Kerberos computer systems. However, all changes to the database must be made on the master computer system. Changing or accessing the contents of a Kerberos database requires the Kerberos master password.

**5 What entities constitute a full service in Kerberos environment?**

A full-service environment consists of a

* Kerberos server
* A number of clients
* A number of application servers

**6 How digital signatures differ from authenticator protocols?**

Digital signature Authentication Protocol

* A digital signature is an authentication mechanism

that allows the sender to attach an electronic code

with the message in order to ensure its authenticity

and integrity.

* This electronic code acts as the signature of the

sender and, hence is named digital signature.

Digital signature uses the public-key

cryptographic technique.

* The sender uses his private key and a signing

algorithm to create a digital signature, and the

signed document can be made public.

* The receiver uses the public key of the sender and

a verifying algorithm to verify the digital signature

**7 State the requirements of a digital signature**

The signature must be a bit pattern that depends on the message being signed.

* The signature must use some information unique to the sender to prevent both forgery and denial.
* It must be relatively easy to produce the digital signature.
* It must be relatively easy to recognize and verify the digital signature.
* It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.
* It must be practical to retain a copy of the digital signature in storage.

**8 Show how SHA is more secure than MD5**

* It produces a largest digest (160-bit compared to 128 bits, so a brute force attack

would be more difficult to carry out)

* No known collisions have been formed for SHA
* Never version have been introduced in SHA (SHA-256, SHA-384, SHA-512) that are much more secure than the original.

**9 What do you mean by one-way properly in hash function?**

One-way function is easy to compute but it is very difficult to compute their inverse

functions. Thus, having data n, it is easy to calculate f(n) but, knowing the value of f(n) it

is quite difficult to calculate the value of X,

* One-way hash functions fulfill all conditions of one-way functions.
* A one-way hash function should be collision-free
* Algorithms of one-way hash functions are often to the public.

**10 What is weak collision resistance?**

Given n, is infeasible to find y such that H(y)=H(n)

**UNIT-V CYBER CRIMES AND CYBER SECURITY**

PART-A

**1 Define Cybercrime.**

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device .Cybercrime is committed by cybercriminals or hackers who want to Make money. Cybercrime is carried out by individuals or organizations.

**2 Define Information Security.**

Information security means to consider available countermeasures or controls stimulated through uncovered vulnerabilities and identify an area where more work is needed. The purpose of data security management is to make sure business continuity and scale back business injury by preventing and minimizing the impact

of security incidents.

**3 List the need for information Security**

* Protecting the functionality of the organization
* Enabling the safe operation of applications
* Protecting the data that the organization collects and use
* Safeguarding technology assets in organizations

**4 What are the category of cybercrime?**

* Cybercrimes against persons.
* Cybercrimes against property.
* Cybercrimes against government.

**5 What is the purpose of password cracking?**

* To recover a forgotten password.
* As a preventive measure by system administrators to check for easily crack able passwords.
* To gain unauthorized access to a system,

**6 What are the types of password cracking attacks?**

* Online attacks
* Offline attacks
* Non-electronic attacks

**7 Define Key loggers.**

Keystroke logging, often called keylogging, is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is Unaware that such action are being monitored. It can be classified as software key logger and hardware key logger.

**8 Define Software Key loggers.**

Software keyloggers are software programs installed on the computer systems which usuallyare located between the OS and the keyboard hardware, and every keystroke is recorded. Software keyloggers are installed on a computer system by Trojans or viruses without the knowledge of the user.

**9 What is Hardware Key loggers.**

Hardware keyloggers are small hardware devices. These are connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device.

Cybercriminals install such devices on ATM machines to capture ATM Cards’ PINs. Each Key press on the keyboard of the ATM is registered by these key loggers.

**10 Define Spyware.**

Spyware is a type of malware that is installed on computers which collects information about users without their knowledge. It is clearly understood from the term Spyware that it secretly monitors the user.