Total No. of Questions : 8] **SEAT No. :**

P439 **[Total No. of Pages : 2**

[6003]-543

T.E. (Artificial Intelligence and Data Science)

CYBER SECURITY

(2019 Pattern) (Semester-II) (317530)

Time : 2½ Hours] ***[Max. Marks : 70***

Instructions to the candidates:

1) ***Answer Q.1 or Q.2, Q.3 or Q.4, Q.5 or Q.6, Q.7 or Q.8.***
2) ***Neat diagrams must be drawn wherever necessary.***
3) ***Draw neat figures wherever necessary.***
4) ***Figures to the right side indicate full marks.***
5) ***Use of Calculator is allowed.***
6) ***Assume suitable data if necessary.***

Q1) a) Describe the Deffie-Hellman Key Exchange in detail. **[6]**

b) Identify and explain the authentication methods. **[6]**

c) Distinguish between Kerberos and X.509 authentication service. **[5]**

OR

Q2) a) What is Digital Signature Standard? Explain the DSS approach. **[6]**

b) Explain the RSA algorithm in detail with the help of diagram. **[6]**

c) Explain Message Digest algorithm in detail. **[5]**

Q3) a) Explore Secure Socket Layer Handshake protocol in detail. **[6]**

b) What is VPN? Explain types of VPN. **[6]**

c) Describe IPSec Protocol with its components and Security Services. **[6]**

OR

Q4) a) Distinguish between PGP and S/MIME. **[6]**

b) Explain ISAKMP protocol of IPSec. **[6]**

c) Identify Threats to web Security and figure out how any of two among listed are countered by particular feature of SSL. **[6]**

P.T.O.

Q5) a) Differentiate packet filtering router and stateful Inspection firewall. **[6]**

b) What is trusted system? Explain in brief. **[6]**

c) List limitations of Firewall. **[5]**

OR

Q6) a) Illustrate Screened subnet firewall Architecture. **[6]**

b) List and Explain types of intrusion detection system (IDS) **[6]**

c) Identify and explore any two-password management practice. **[5]**

Q7) a) Identify and explore the different types of Cyber stalker attacks. **[6]**

b) Illustrate life cycle of cyber forensics? **[6]**

c) List VoIP hacking types and explore any 3? What are the counter measures for it. **[6]**

OR

Q8) a) Who are cyber criminals? What are types of cyber crimes. **[6]**

b) What is Botnet? How to protect from botnet? **[6]**

c) Explain the terms: **[6]**

i) Virus

ii) Phishing

iii) Spoofing

iv) Phone phishing

v) Internet pharming

vi) Cyber Forensic

❖ ❖ ❖

Shree Ramchandra Education Society's
SHREE RAMCHANDRA COLLEGE OF ENGINEERING
Lonikand, Pune – 412216
Department of Artificial Intelligence and Data Science

TE-AI&DS- CYBER SECURITY

Unit-3

[MAY-2024]

Q1) Describe the Deffie-Hellman Key Exchange in detail. [6]

[MAY-2024]

Ans –

Diffie-Hellman algorithm:

The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

- For the sake of simplicity and practical implementation of the algorithm, we will consider only 4 variables, one prime P and G (a primitive root of P) and two private values a and b.
- P and G are both publicly available numbers. Users (say Alice and Bob) pick private values a and b and they generate a key and exchange it publicly. The opposite person receives the key and that generates a secret key, after which they have the same secret key to encrypt.
  - tep-by-Step explanation is as follows:

Alice	**Bob**
Public Keys available = P, G	Public Keys available = P, G
Private Key Selected = a	Private Key Selected = b

Alice	Bob
Exchange of generated keys takes place	
Key received = y	key received = x
Generated Secret Key =	Generated Secret Key =
Algebraically, it can be shown that	
Users now have a symmetric secret key to encrypt	

- **Example:**

- Step 1: Alice and Bob get public numbers P = 23, G = 9

  Step 2: Alice selected a private key a = 4 and
  Bob selected a private key b = 3

  Step 3: Alice and Bob compute public values
  Alice: x =(9^4 mod 23) = (6561 mod 23) = 6
  Bob: y = (9^3 mod 23) = (729 mod 23) = 16

  Step 4: Alice and Bob exchange public numbers

  Step 5: Alice receives public key y =16 and
  Bob receives public key x = 6

  Step 6: Alice and Bob compute symmetric keys
  Alice: ka = y^a mod p = 65536 mod 23 = 9
  Bob: kb = x^b mod p = 216 mod 23 = 9

  Step 7: 9 is the shared secret.

Q.2) Identify and explain the authentication methods. [6]

[MAY-2024]

Ans-

Authentication is the process of verifying the identity of a user or information. User authentication is the process of verifying the identity of a user when that user logs in to a computer system.

The main objective of authentication is to allow authorized users to access the computer and to deny access to unauthorized users. Operating Systems generally identify/authenticates users using the following 3 ways: Passwords, Physical identification, and Biometrics. These are explained as following below.

1. **Passwords:** Password verification is the most popular and commonly used authentication technique. A password is a secret text that is supposed to be known only to a user. In a password-based system, each user is assigned a valid username and password by the system administrator. The system stores all usernames and Passwords. When a user logs in, their user name and password are verified by comparing them with the stored login name and password. If the contents are the same then the user is allowed to access the system otherwise it is rejected.
2. **Physical Identification:** This technique includes machine-readable badges(symbols), cards, or smart cards. In some companies, badges are required for employees to gain access to the organization's gate. In many systems, identification is combined with the use of a password i.e the user must insert the card and then supply his /her password. This kind of authentication is commonly used with ATMs. Smart cards can enhance this scheme by keeping the user password within the card itself. This allows authentication without the storage of passwords in the computer system. The loss of such a card can be dangerous.
3. **Biometrics:** This method of authentication is based on the unique biological characteristics of each user such as fingerprints, voice or face recognition, signatures, and eyes.
4. A scanner or other devices to gather the necessary data about the user.
5. Software to convert the data into a form that can be compared and stored.
6. A database that stores information for all authorized users.
7. **Facial Characteristics –** Humans are differentiated on the basis of facial characteristics such as eyes, nose, lips, eyebrows, and chin shape.
8. **Fingerprints –** Fingerprints are believed to be unique across the entire human population.

9. **Hand Geometry –** Hand geometry systems identify features of the hand that includes the shape, length, and width of fingers.
10. **Retinal pattern –** It is concerned with the detailed structure of the eye.
11. **Signature –** Every individual has a unique style of handwriting, and this feature is reflected in the signatures of a person.
12. **Voice –** This method records the frequency pattern of the voice of an individual speaker.

Q.3) Distinguish between Kerberos and X.509 authentication service. [5] [MAY-2024]

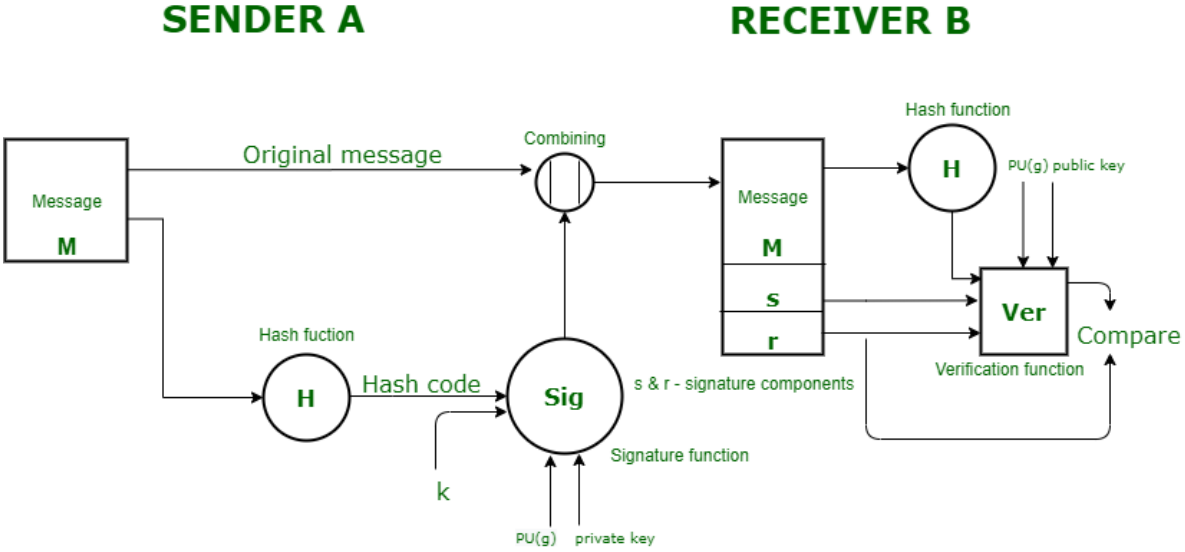
Ans -

S.No.	Kerberos	SSL
1.	Kerberos is an open source software and offers free services.	SSL does not offer free service as it is patented.
2.	Kerberos is generally implemented in microsoft products like Windows 2000, Windows XP and later windows.	SSL is implemented in web browsing, messaging and other protocols like FTP.
3.	Kerberos depends on a reliable third party.	SSL is asynchronous as it depends on the certificate.
4.	Kerberos works on the private key encryption.	While SSL works on the public key encryption.
5.	Kerberos is best suited for the WWW.	SSL is appropriate and effective for the networked environments.
6.	In kerberos, key cancellation is achieved by disabling any user on authentication server.	In SSL, revocation server control records of the bad certificate for key cancellation.

Q 4) What is Digital Signature Standard? Explain the DSS approach. [6] [MAY-2024]

Ans-

signature is a way of authenticating the data coming from a trusted individual. Similarly, digital signature is a way of authenticating a digital data coming from a trusted source. **Digital Signature Standard (DSS)** is a Federal Information Processing Standard(FIPS) which defines algorithms that are used to generate digital signatures with the help of Secure Hash Algorithm(SHA) for the authentication of electronic documents. DSS only provides us with the digital signature function and not with any encryption or key exchanging strategies.



Sender Side : In DSS Approach, a hash code is generated out of the message and following inputs are given to the signature function –

1. The hash code.
2. The random number ‘k’ generated for that particular signature.
3. The private key of the sender i.e., PR(a).
4. A global public key(which is a set of parameters for the communicating principles) i.e., PU(g).

These input to the function will provide us with the output signature containing two components – ‘s’ and ‘r’. Therefore, the original message concatenated with the signature is sent to the receiver. **Receiver Side :** At the receiver end, verification of the sender is done. The hash code of the sent message is generated. There is a verification function which takes the following inputs –

1. The hash code generated by the receiver.
2. Signature components ‘s’ and ‘r’.
3. Public key of the sender.

4. Global public key.

The output of the verification function is compared with the signature component ‘r’. Both the values will match if the sent signature is valid because only the sender with the help of it private key can generate a valid signature.

Q. 5) Explain the RSA algorithm in detail with the help of diagram. [6] [MAY-2024]

Ans-

RSA encryption algorithm is a type of public-key encryption algorithm. To better understand RSA, lets first understand what is public-key encryption algorithm.

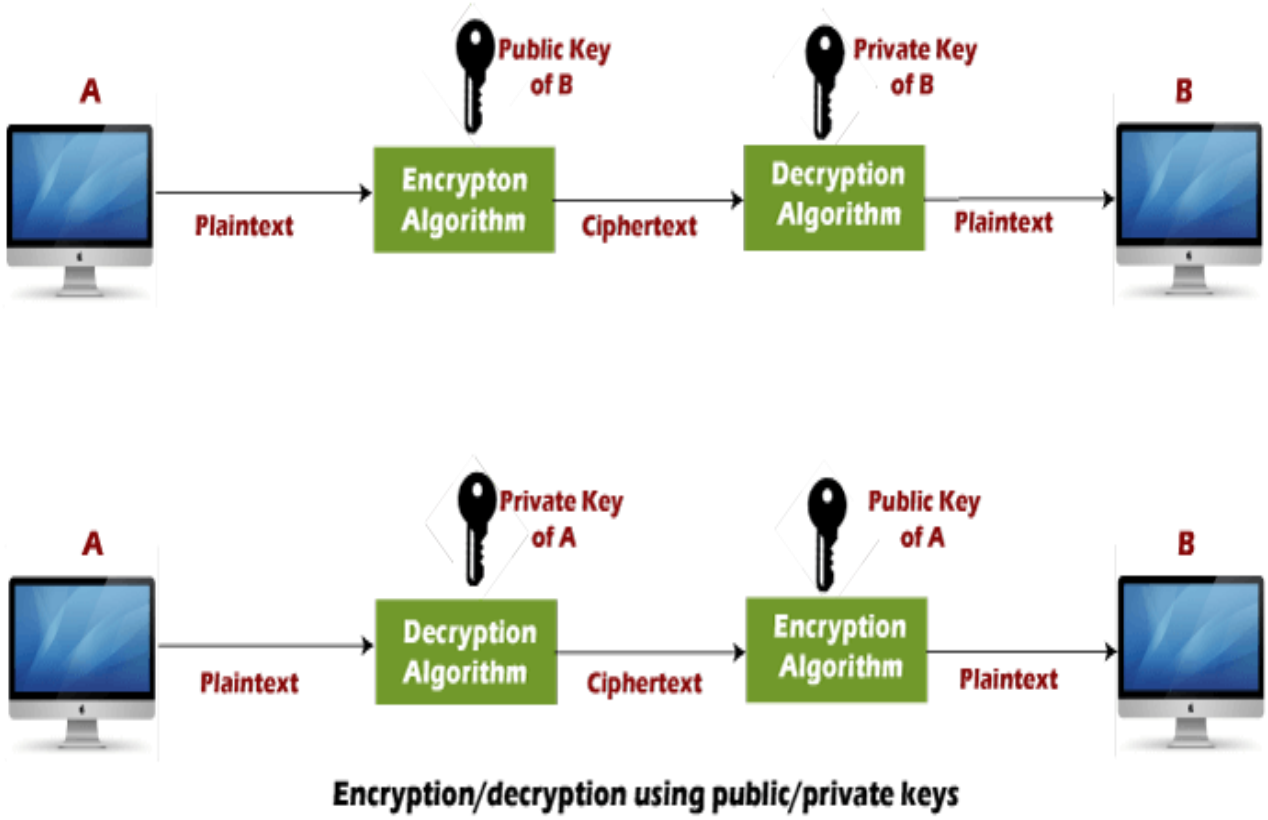
Public key encryption algorithm:

Public Key encryption algorithm is also called the Asymmetric algorithm. Asymmetric algorithms are those algorithms in which sender and receiver use different keys for encryption and decryption. Each sender is assigned a pair of keys:

- **Public key**
- **Private key**

The **Public key** is used for encryption, and the **Private Key** is used for decryption. Decryption cannot be done using a public key. The two keys are linked, but the private key cannot be derived from the public key. The public key is well known, but the private key is secret and it is known only to the user who owns the key. It means that everybody can send a message to the user using user's public key. But only the user can decrypt the message using his private key.

The Public key algorithm operates in the following manner:

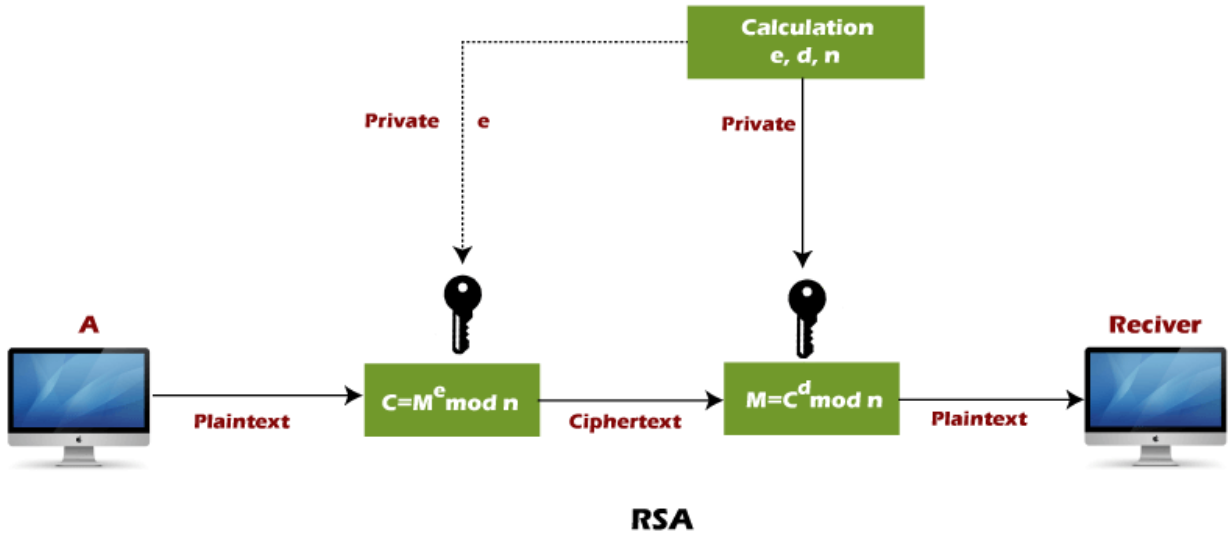


Encryption/decryption using public/private keys

- The data to be sent is encrypted by sender **A** using the public key of the intended receiver
- B decrypts the received ciphertext using its private key, which is known only to B. B replies to A encrypting its message using A's public key.
- A decrypts the received ciphertext using its private key, which is known only to him.

RSA encryption algorithm:

RSA is the most common public-key algorithm, named after its inventors **Rivest, Shamir, and Adelman (RSA).**



RSA

RSA algorithm uses the following procedure to generate public and private keys:

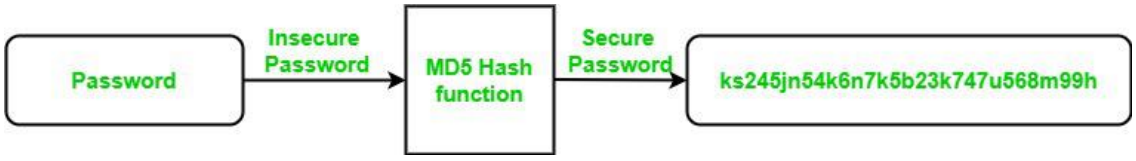
- Select two large prime numbers, p and **q**.
- Multiply these numbers to find **n = p x q,** where **n** is called the modulus for encryption and decryption.
- Choose a number **e** less than **n**, such that n is relatively prime to **(p - 1) x (q -1).** It means that **e** and **(p - 1) x (q - 1)** have no common factor except 1. Choose "e" such that 1<e < φ (n), e is prime to φ (n),
  gcd (e,d(n)) =1
- If **n = p x q,** then the public key is <e, n>. A plaintext message **m** is encrypted using public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C.
  $C = m^e \bmod n$
  Here**, m** must be less than **n**. A larger message (>n) is treated as a concatenation of messages, each of which is encrypted separately.
- To determine the private key, we use the following formula to calculate the d such that:
  $D_e \bmod \{(p - 1) \times (q - 1)\} = 1$
  Or
  $D_e \bmod \varphi(n) = 1$

- The private key is <d, n>. A ciphertext message **c** is decrypted using private key <d, n>. To calculate plain text **m** from the ciphertext c following formula is used to get plain text m.
  $m = c^d \bmod n$

Q. 6) Explain Message Digest algorithm in detail. [5]
[MAY-2024]

Ans-
MD5 is a cryptographic hash function algorithm that takes the message as input of any length and changes it into a fixed-length message of 16 bytes. MD5 algorithm stands for the **message-digest algorithm**. MD5 was developed as an improvement of MD4, with advanced security purposes. The output of MD5 (Digest size) is always **128 bits. MD5** was developed in 1991 by **Ronald Rivest.**

Use Of MD5 Algorithm:
- It is used for file authentication.
- In a web application, it is used for security purposes. e.g. Secure password of users etc.
- Using this algorithm, We can store our password in 128 bits format.



MD5 Algorithm

Working of the MD5 Algorithm:

MD5 algorithm follows the following steps

1. Append Padding Bits: In the first step, we add padding bits in the original message in such a way that the total length of the message is 64 bits less than the exact multiple of 512.
Suppose we are given a message of 1000 bits. Now we have to add padding bits to the original message. Here we will add 472 padding bits to the original message. After adding the padding bits the size of the original message/output of the first step will be 1472 i.e. 64 bits less than an exact multiple of 512 (i.e. 512*3 = 1536).

Length(original message + padding bits) = 512 * i – 64 where i = 1,2,3 . . .
2. Append Length Bits: In this step, we add the length bit in the output of the first step in such a way that the total number of the bits is the perfect multiple of 512. Simply, here we add the 64-bit as a length bit in the output of the first step.
i.e. output of first step = 512 * n – 64
length bits = 64.
After adding both we will get **512 * n** i.e. the exact multiple of 512.
3. Initialize MD buffer: Here, we use the 4 buffers i.e. J, K, L, and M. The size of each buffer is 32 bits.

- J = 0x67425301
- K = 0xEDFCBA45
- L = 0x98CBADFE
- M = 0x13DCE476

4. Process Each 512-bit Block: This is the most important step of the MD5 algorithm. Here, a total of 64 operations are performed in 4 rounds. In the 1st round, 16 operations will be performed, 2nd round 16 operations will be performed, 3rd round 16 operations will be performed, and in the 4th round, 16 operations will be performed. We apply a different function on each round i.e. for the 1st round we apply the F function, for the 2nd G function, 3rd for the H function, and 4th for the I function.
We perform OR, AND, XOR, and NOT (basically these are logic gates) for calculating functions. We use 3 buffers for each function i.e. K, L, M.

- F(K,L,M) = (K AND L) OR (NOT K AND M)
- G(K,L,M) = (K AND L) OR (L AND NOT M)
- H(K,L,M) = K XOR L XOR M
- I(K,L,M) = L XOR (K OR NOT M)

After applying the function now we perform an operation on each block. For performing operations we need

- add modulo 2^{32}
- M[i] – 32 bit message.
- K[i] – 32-bit constant.
- <<<n – Left shift by n bits.

Now take input as initialize MD buffer i.e. J, K, L, M. Output of K will be fed in L, L will be fed into M, and M will be fed into J. After doing this now we perform some operations to find the output for J.

- In the first step, Outputs of K, L, and M are taken and then the function F is applied to them. We will add modulo 2^{32} bits for the output of this with J.
- In the second step, we add the M[i] bit message with the output of the first step.
- Then add 32 bits constant i.e. K[i] to the output of the second step.
- At last, we do left shift operation by n (can be any value of n) and addition modulo by 2^{32}.

After all steps, the result of J will be fed into K. Now same steps will be used for all functions G, H, and I. After performing all 64 operations we will get our message digest.

Output:

After all, rounds have been performed, the buffer J, K, L, and M contains the MD5 output starting with the lower bit J and ending with Higher bits M.