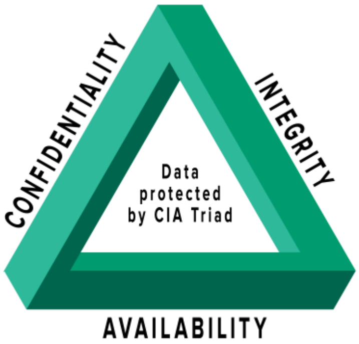
Notes for CSS (Cryptography and system security)

Q1.Explain CIA triad.

- The CIA triad is benchmark model in information security designed to govern and evaluate how an organization handles data, when it is stored, transmitted or processed.
- Each attribute of triad represents critical components of information security.



- Confidentiality:

  Data should not be accessed or read without authentication.

  It ensures that only authorized parties have access.

  Attacks against confidentiality are disclosure attacks.
- Integrity:

  Data should not be modified or compromised in anyway.

  It ensures that data remains in its intended state and can only be edited by authorized parties.

  Attacks against integrity are alteration attacks.
- Availability:

  Data should be accessible upon legitimate request.

  It ensures authorized parties have unimpeded access to data when required.

  Attacks against availability are destruction attacks.

Q2.Explain cipher modes of encryption.

Types of cipher modes:

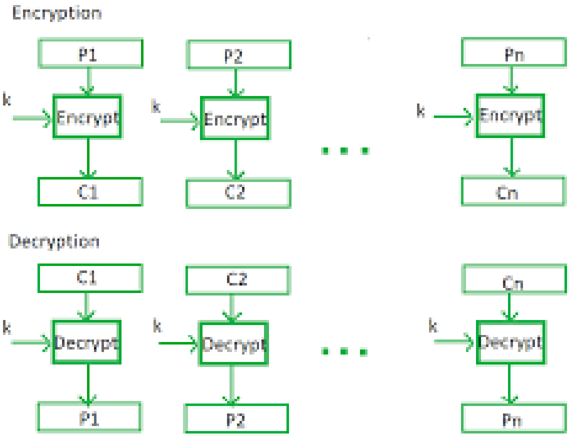
1) Electronic code book (ECB) mode
2) Cipher block chaining (CBC) mode
3) Cipher feedback (CFB) mode
4) Output feedback (OFB) mode

5) Counter (CTR) mode

[i] Electronic code book (ECB) mode:

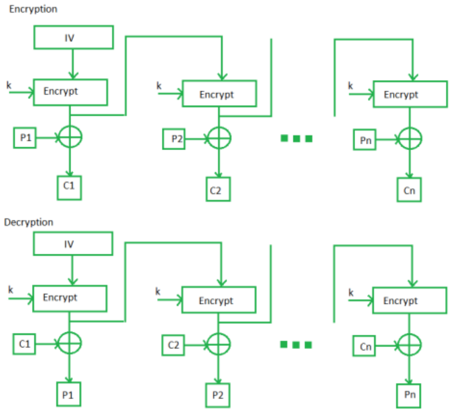
- Electronic code book is simplest mode of operation of block cipher.
- It works on processing series of sequencially listed message blocks but 64-bit block at a time.
- Each block is separately encrypted.
- The ECB mode is deterministic as the same.
- Encryption -> Ci=E_k (Pi)

  Decryption -> Pi=D_k(Ci)



[ii] Cipher block chaining (CBC) mode:

- CBC can be called as advancement of ECB.
- Here, at the sender side, the plain text is divided into blocks.
- In this mode, initialization vector is used, which can be random block of text.
- IV is used to make ciphertext of each block unique since the key is same for encryption as we use for ECB.

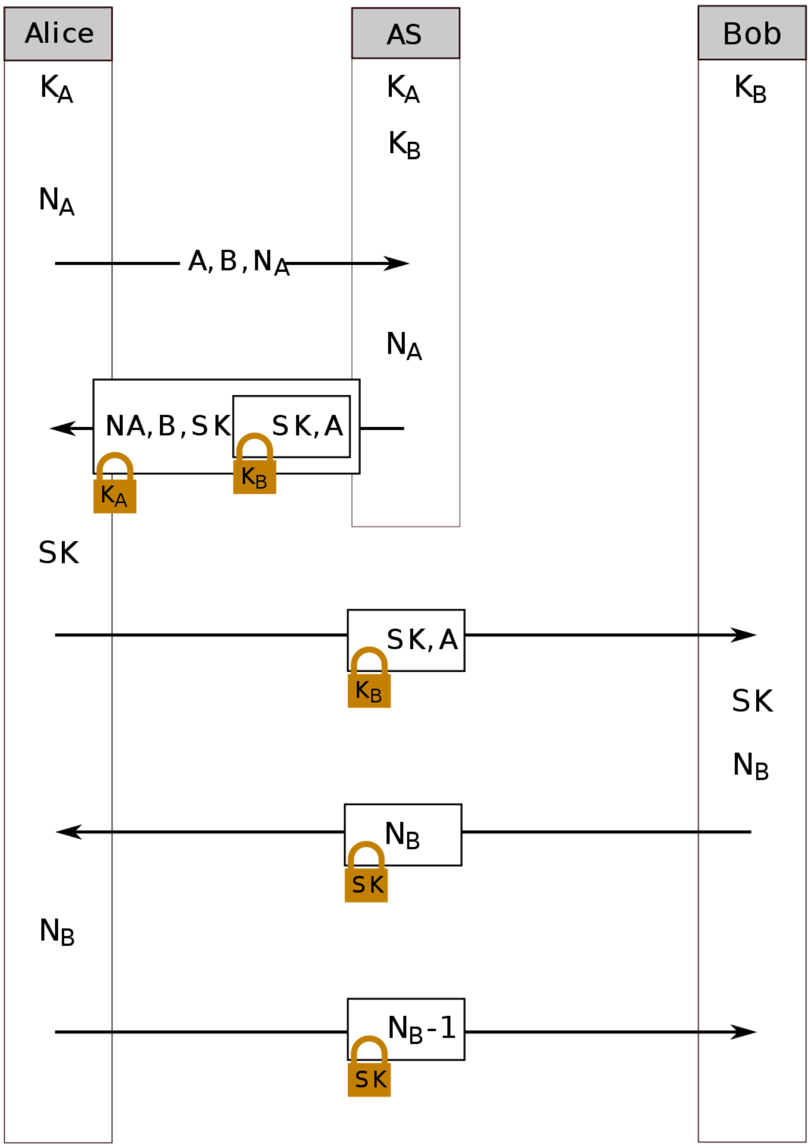


Q3. AES vs DES.

SR.NO.	AES	DES
1	AES stand for advanced encryption standard.	DES stands for data encryption standard.
2	AES is byte-oriented.	DES is bit oriented.
3	Key length can be 128 bits, 192 bits, 256 bits.	Key length is 56 bits.
4	The structure is based on substitution-Permutation network.	The structure is based on Feistel network.
5	The design rational for AES is open.	The design rational for DES is closed.
6	AES is more secure than DES.	DES can be broken easily.
7	AES is flexible.	DES is not flexible.
8	AES is faster than DES.	DES is slower than AES.

Q.4. Needham - Schroeder Protocol :

1. The Needham – Schroeder public-key protocol is based on public-key cryptography.
2. This protocol is intended to provide mutual authentication between two parties communicating on network.
3. Suppose Alice (A) initials the communication to Bob (B). S is server (KDC) trusted by both parties.
    - KAS is symmetric key known only to A and S.
    - KBS is symmetric key known only to B and S.
    - NA and NB are nonces generated by A and B.
    - KAB is symmetric key generated which will be session key between A and B.



Q.5 Hashing and hashing techniques.

I. Hashing is method of cryptography that converts any form of data into unique string of text. Any piece of data can be hashed, no matter its size and type.

II. Hashing is a mathematical operation that is easy to perform, but extremely difficult to reverse.

III. The difference between hashing and encryption is that encryption can be reversed or decrypted using a specific key.

IV. Most widely used hashing functions are MD5, SHA 1 and SHA-256.

V. Hashing techniques :

- Message integrity
- Message authentication
- Message authentication code (MAC)
- Hash based MAC
- Cipher based machine authentication code (CMAC)
- Cryptographic hash functions.

Q.6 Cryptographic hash functions :

1. Hash functions are commonly used to create a one-way password file.
2. It can be used for intrusion detection and virus detection.
3. There are two categories of possible attacks on has functions, brute force and cryptanalysis.
4. Properties of hash function :
   - Pre-image resistance
   - Second pre-image resistance
   - Collision resistance

1. Pre-image resistance :

   Means it should be completely hard to reverse it.
2. Second pre-image resistance :

   Means give input & its hash, it should find different input with same hash.
3. Collision resistance :
   - Also called as collision free hash function.
   - It should be hard to find two different input at any length.

	MD5	SHA1
Full form	MD5 stands for digest.	SHA1 stands for secure hash algorithm.
Length of message digest	The message digest length for MD5 is 128 bits.	The message digest length for SHA1 is 160 bits.
Complexity	Simple	Complicated
Speed	It is faster.	It is slower.
Developed	1992	1995

Q.7 Authentication? Types of authentication?

1. Authentication is used by server when the server needs to know exactly who is accessing their information or site.
2. Authentication is used by client when clients needs to known that server is system claims to be.
3. In authentication the user or computer has to prove its identity to server or client.

Types of authentication :

A. Passwords
B. Fixed passwords
C. One time password

A. Passwords :
   - Password authentication is most common way to implement authentication.
   - User enters login and password to log in to server.
   - Login name identifies user and password authenticates user.

B. Fixed passwords :

   Fixed password indicates same password will be used for every access.

   Approach 1 : Hashing password

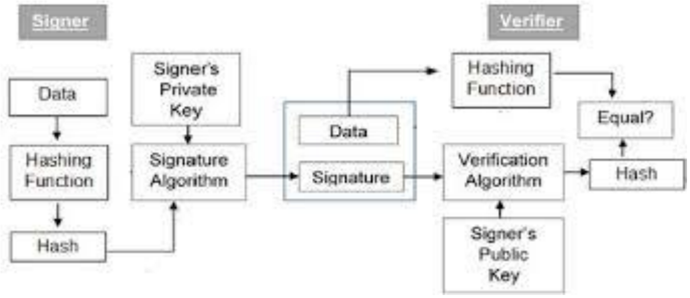
   Approach 2 : Salting password

   Approach 3 : Combining two identification techniques.

C. One time password :
   - A one time password is one which can be used only once to access system.
   - This makes eavesdropping & salting useless.

Q.8 Digital signature :

1. A digital signature is mathematical technique used to validate the authenticity and integrity of message, software or digital document.
2. Digital signatures are created and verified by using public key / asymmetric key cryptography.
3. The user who is creating digital signature uses his private key to encrypt the signature related document. There is only way to decrypt that document with use of key.



Steps in digital signature :

Step 1 : The sender/signer applies hash function on original message which is to be signed and message digest is computed. The sender uses his signature as his private key.

Step 2 : Now original message along with digital signature is sent to receiver.

Step 3 : The copy of signature is on message, like public key, anyone can use it to verify message.

Receiver decrypts digital signature using public key of sender.

RSA digital signature scheme :

1. The concept of RSA is also used for signing and verifying message which is called as RSA digital signature scheme.
2. Instead of receiver, sender's private and public keys are used. Sender uses his own private key to sign document and receiver uses sender's public key to verify it.

Algorithm- / working :

Step 1 : The sender uses message digest algorithm to calculate the message digest (MD1).

Step 2 : The sender now encrypts message digest with his private key.

Step 3 : Now sender sends original message along with digital signature to receiver.

Step 4 : Once receivers original message and digital signature, it uses same message digest algorithm which was used by sender and calculate message digest (MD2).

Step 5 : Decryption - The receiver now uses the sender's public key to decrypt digital signature.

Step 6 : Verification - Receiver now compares MD@ and MD1 if MD2 = MD1 then receiver accepts original message as correct.

Q.9 Denial of service

1. A denial of service attack occurs when legitimate users are unable to access information systems, devices or other network resources.
2. An attacker, attempt to make it impossible for a service to be delivered by interrupting device's normal functioning.
3. A DOS attack characterized by using single computer to launch the attack.
4. An additional type of dos attack is distributed denial of service (DDOS) attack.
5. In DOS attack, its one system that is sending malicious data or requests, DDOS attack cones from multiple system at once.

* Type of DOS attacks

1. Buffer overflow :
   This is most common DOS attack targeted at application layer. In this attack memory buffer overflow causes machine to consume all hard disk space, memory, CPU.
2. Flood attacks :
   In this DDOS attack, the attacker sends several requests to target server, overloading it with traffic and this resulting in denial of service.
   i. ICMP flood :
      This DOS attack is based on crushing target with ICMP packets. B1 flooding target with more pings than it can respond, denial of service occurs.

   ii. SYN flood :

      SYN flood attack occurs when an attacker sends a request to connect to target server but never completes handshake.

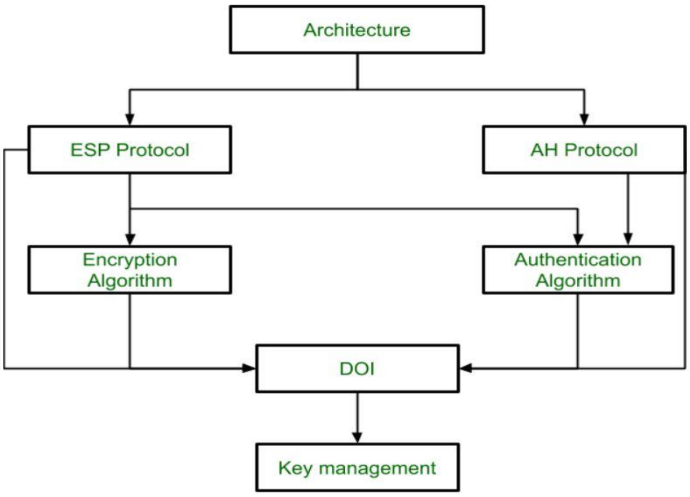
   iii. UDP flood :

      In UDP flood attack, high number of user datagram protocol packets are sent to targeted server with goal of overwhelming that device's ability to process.

Q.10 How does ESP header guarantee to achieve confidentiality and integrity of packet payload? Or IPsec short note.

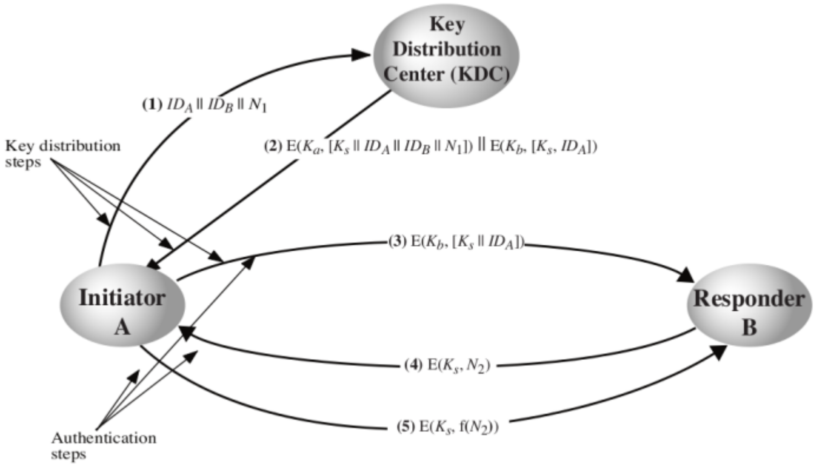
- IPsec (IP security) is suite of protocols developed to ensure the integrity, confidentiality and authentication of data communications over an IP network.

- IPsec may be used in three different security domains : virtual private networks, application- level security and routing security.
- IPsec male use of HMAC authentication code.
- IPsec defines a number of techniques for key management.
- IAB (internet architecture board) included authentication and encryption as necessary security features in next generation IP. Generally issued in IPV6 .
- Capabilities were designed to be usable both with current IPV4 and future IPV6.



Q.11 Needham Schroder Protocol :

- Needham Schroder is a public key protocol based on public key cryptography.
- It uses KDC (key distribution centre). * KDC is third party trusted server can be used for authentication.
- It uses symmetric key encryption.
- KDC shares a symmetric key between all users.
- Purpose of this protocol is to share session key. Session key is ley which is used for particular time slot.
- Three actors : 1. Alice
  2. KDC
  3. Bob


Key Distribution Center (KDC)
(1) $ID_A \| ID_B \| N_1$
Key distribution steps
(2) $E(K_a, [K_s \| ID_A \| ID_B \| N_1]) \| E(K_b, [K_s, ID_A])$
(3) $E(K_b, [K_s \| ID_A])$
Initiator A
Responder B
(4) $E(K_s, N_2)$
(5) $E(K_s, f(N_2))$
Authentication steps

1.

- IDA identifier of Alice
- INB identifier of Bob
- N_1 is nonce which is Random number. It changes every time.

2.

- K_s is session key generated by KDC.
- K_a is secret key shared between Alice & KDC.
- K_b is secret key shared between Bob & KDC.

3.

- N_2 is another nonce.

The purpose of the protocol is to distribute 1>s session key securely to A & B.

Q.12 Digital certificate

- Digital certificate is issued by trusted third party which proves sender's identity to receiver & receiver's identify to sender.
- A digital certificate is issued by certificate authority to verify identify of certificate holder.
- Digital certificate is used to attach public key with particular individual or an entity.
- Digital certificate contains :
  - Name of certificate holder

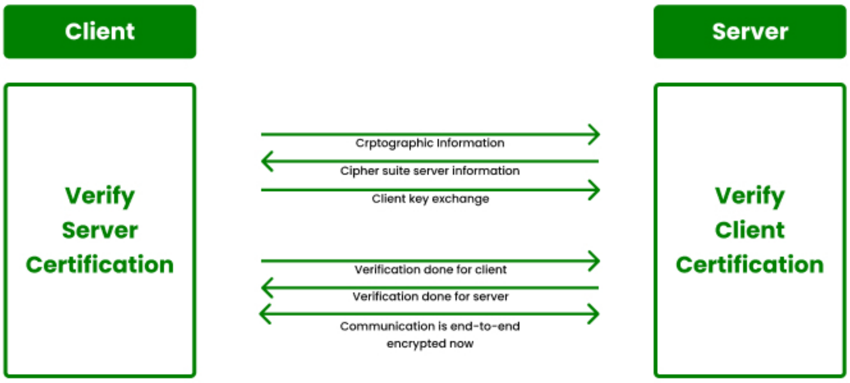
  - ➢ Serial number which is used to uniquely identify a certificate or individual
  - ➢ Explanation dates
  - ➢ Copy of certificate holder's public key
  - ➢ Digital signature of certificate issuing authority.

Q.13 SSL handshake protocol :

- It provides protection to data that is aligned between the web browser and server.
- SSL encrypts the link between web server and browser which ensures that all data passed between them stay private & separate from attacks.
- SSL protocols :
  - ➢ SSL record protocol
  - ➢ Handshake protocol
  - ➢ Change-cipher spec protocol
  - ➢ Alert protocol
- TLS (transport layer securities) :
  - ➢ TLS are aimed to give security at transport layer
  - ➢ TLS was concluded from security protocol called as secured socket layer.
- Handshake protocol is used to establish sessions. This protocol allows client and server to verify each other by transferring series of message to each distance.

  Handshake protocol uses four phases

  - ➢ Phase 1 :
    - ✓ Deciding which version of protocol to use.
    - ✓ The system decides which protocol to use.
    - ✓ Client and server exchange hello-packets with each other.
  - ➢ Phase 2 :
    - ✓ Server sends his certificate.
    - ✓ Server ends phase 2 by exchanging hello-packet.
  - ➢ Phase 3 :
    - ✓ Verification in this phase, client replies to the server by sending his certificate.
  - ➢ Phase 4 :
    - ✓ In this phase, change cipher suite is passed and all verifications are done after this handshake protocol ends.


Client
Server
Verify Server Certification
Crptographic Information
Cipher suite server information
Client key exchange
Verification done for client
Verification done for server
Communication is end-to-end encrypted now
Verify Client Certification

Q.14 Firewall & its types :

- A firewall is network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on set of security rules.
- The purpose of firewall is to establish barrier between your internal network and traffic incoming from external sources (internet) in order to block malicious traffic like viruses and hackers.
- Firewall can be s/w, h/w or both.

Hardware firewall :

- A hardware firewall is a physical device that attaches between computer network and gateway.
- Ex. Broadband router.
- A hardware firewall is also called as appliance firewall.

Software firewall :

- A software firewall is simple program installed on computer that walks through installed software also called as host firewall.
- Some firewalls that can be implemented as s/w or h/w.
  1. Packet filtering firewalls :
     - ✓ Basic type
     - ✓ Acts as management program which monitors network traffic
  2. Cloud firewalls :
     - ✓ Designed using cloud solution
     - ✓ Run on internet by third party vendors

3. Next –generation firewalls :
   - ✓ Latest released firewalls
4. Network address translation (NAT) firewalls :
   - ✓ NAT firewalls are designed to access internet traffic
   - ✓ Works similar to proxy firewalls
5. Unified threat management (UTM) firewalls :
   - ✓ Special type of device

Q.15 Software vulnerabilities :

- ➢ Software vulnerability is defect in software that could allow attacker to gain control of system.
- ➢ These defects can cause because of the way software is designed, or flow in way of its coding.

Vulnerabilities :

- ➢ Buffer overflow
- ➢ SQL injection
- ➢ Malware
- ➢ Trojan horse
- ➢ Viruses
- ➢ Worms
- ➢ Cross site scripting (XSS)

Q.16 Buffer overflow :

- Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another.
- Buffer overflow occurs when the volume of data exceeds storage capacity of buffer.
- This vulnerability can cause system crash or worse any cyber attack.
- For example buffer for log-in credentials may be designed to accept username & password for 8 bytes but if 10 bytes involved in input it may cause overflow.
- Buffer overflows can affect all type of s/w.
- Types of buffer overflow attacks
  - ✓ Stack based

- ✓ Heap based

- Prevention of buffer overflow
  - ✓ Address space randomization (ASLR)
  - ✓ Data execution prevention
  - ✓ Structured exception handler overwrite protection (SEHOP)

Q17 Kerboros protocol:

1. Kerberos provides a centralized authentication server whose function is to authenticate user to servers and to users.
2. In Kerberos authentication server and database is used for client authentication.
3. Kerberos runs a third party trusted server known as key distribution centre (KDC).
4. Main components of Kerberos are

- Authentication server (AS) :

  The authentication server performs the initial authentication and ticket for ticket granting service.

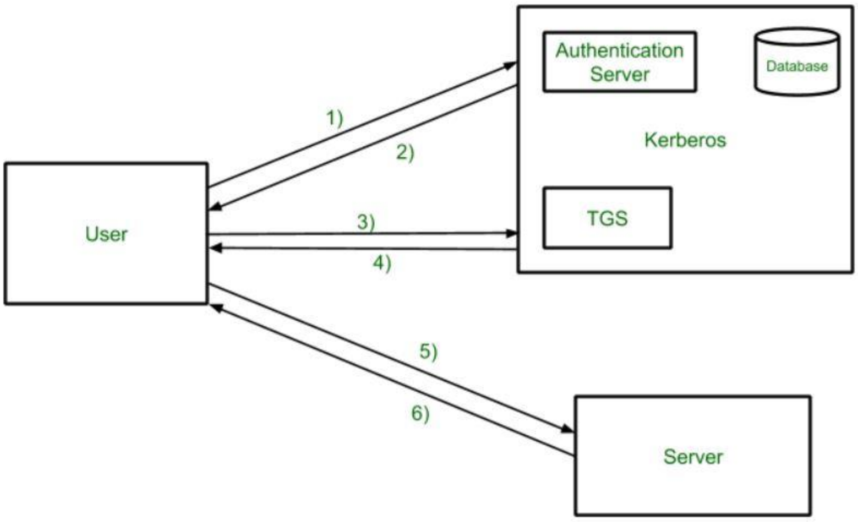
- Database :

  The authentication server verifies the access rights of users in the database.

- Ticket granting server (TGS) :

  The ticket granting server issues ticket for the server.

Diagram :



Step 1 :

User login and request services on the host. Thus user requests for ticket granting service.

Step 2 :

Authentication server verifies user’s access right using database and then gives ticket-granting-ticket and session key. Results are encrypted using password of user.

Step 3 :

The decryption of message is done using password send ticket to TGS.

Step 4 :

Ticket granting server decrypts the ticket sent by user and authenticator verifies the request then creates ticket for services from server.

Step 5 :

The user sends the ticket and authenticator to the server.

Step 6 :

The server verifies ticket and authenticators then generate access to service. After this user can access services.

Q.18 Playfair cipher sum:

THIS IS THE FINAL EXAM KEY – GUIDANCE

TH IS IS TH EF IN AL EX AM

G	U	J	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

TH = PO IN = GF

IS = DR AL = IO

IS = DR EX = LI

TH = PO AM = DO

EF = BN

ANS: PO OR DR PO BN GE IO LI DO

Q.19 RSA sum:

P = 7, Q = 11, E = 17, M = 8

n = p x q = 11 x 7 = 77

Step 1 : p = 7

q = 11

Step 2 : n = p x q = 77

Step 3 : ϕ (n) = (p – 1) x (q - 1)

Step 4 : choose e such that 1 < e < ϕ (n)

gcd (17,60) = 1 gcd (e, ϕ (n) = 1)

Step 5 : d = (k x ϕ (n) + 1)/e

K = 1, 61 is not

K = 2, 121 is not

K = 15, 901 is by 17

D = 53

C = MP^e mod n	C = 8^e mode n	2^4	2^3	2^2	2^1	2^0
	= 8^{17} mode 77	16	8	4	2	1
	= 288 mode 77	1	0	0	0	1
	C = 27					

P= c^n mod n P = 57^{53} mode 77 8^1 mod 77 = 8

$= 3885120 \bmod 77$

$= 8$

$8^2 \bmod 77 = 64$

$8^4 \bmod 77 = 15$

$8^8 \bmod 77 = 71$

$8^{16} \bmod 77 = 36$

$8^{17} = 8^1 \text{ x } 8^{16} = 36 \text{ x } 8 = 288$