Information Security.

GoodLuck | Page No.
Date

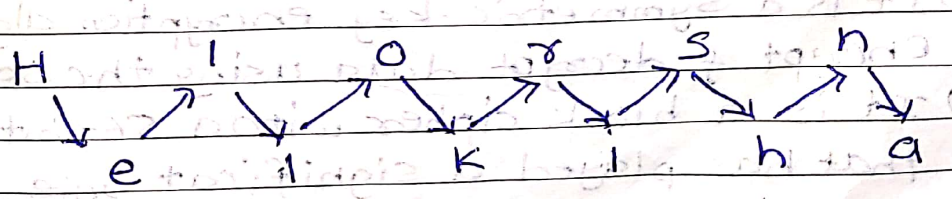
What is Transposition Technique? Explain its two types with examples in detail.

→ ① A transposition Cipher Technique is an encryption method used to encrypt a message.
② This encryption method is done by playing with the position of letters of the plain text.
③ The positions of characters present in the plaintext are rearranged or shifted to form the ciphertext.
④ It makes use of some kind of permutation function to achieve the encryption purpose.
⑤ It is very easy to use & so simple to implement.

- Types
1). Rail fence technique.
2) Message - Rectangle technique.

① Rail fence Technique:
① It is simplest trans position cipher technique.
② It is also called as zigzag cipher.
③ It gets its name from the way through which it performs encryption of plaintext.

e.g. Plain text = "Hello Krishna"
Now, we will write this plain text in the diagonal form:



Now, following the 2nd step we get our cipher-text.

Cipher Text = "Hlorshelkina"

(2) Message Rectangle Technique:

(1) It is a another form of Transposition cipher technique which is used to encrypt the msg or info.
(2) In this technique, first we write a msg or plaintext in rows.
(3) After that, we read the msg column by column.
(4) In this technique we use a key to determine the no. of rows.

step1: First we write the msg in the form of rows & columns & read the msg column by column.
step2: Given a key, which we will use to fix the no. of rows.
step3: If any space is empty then it is filled with null(-) or left blank.
step4: The msg is read in the order as specified by the key.

e.g. plaintext: 'attack postponed until two am'.
Key: 4312567

Key	4	3	1	2	5	6	7
plaintext	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	-	-	-

Ciphertext: ttnaaptmtsuoaodwcoi-knl-pet

Q.2 Describe the DES in detail.

→ DES - Data encryption standard.

(1) It is a symmetric key encryption algo. used to encrypt & decrypt data using the same key.
(2) It is a block cipher with a 56-bit key length that has played a significant role in data security.
(3) DES is a block ciphe & encrypts data in blocks of size of 64 bits.
(4) It means 64 bit of plain text go as the i/p to DES which produces 64 bits of ciphertext.

• How DES works?

① Initial permutation (IP):
- plaintext is divided into 64-bit blocks
- IP is applied to shuffle bits according to a fixed table

② Key Generation:
- 64 bit key is reduced to a 56-bit key
- 56 bit key divided into 2 halves
- Key scheduling generates 16 subkeys th^r. left shifts

③ 16 Rounds of Feistel Cipher.
1) Divide: 64-bit block divided into right & left halves.
2) Expansion: Right half expanded to 48 bits using expansion table.
3) XOR with subkeys: The expanded right half is XORed with a round-specific subkey.
4) XOR with Left half: left half is XORed with the O/P from the permutation step.
5) Swap: The left & right halves are swapped.

④ Final permutation: (FP)
- After 16 rounds left & right halves are combined.
- FP is applied which is the inverse of IP.

⑤ Ciphertext.
- The final 64-bit block is the encrypted ciphertext.

⑥ Decryption
- Decryption follows the same steps as encryption, but the subkeys are applied in reverse order.

• Advantages:
- Simple & fast due to feistel structure.
- Suitable for H/w implementation.

• Disadvantages:
- Key size is too small.
- Replaced by more secure algo. like AES.

Q.3. Explain active & Passive attack with example.

→ An attack is when the security of a system is compromised by some action.
Two types of attacks,
1) Active
2) passive.

1) Active attack:
- Active attacks are unauthorized actions that alter the system or data.
- In this, the attacker will directly interfere with the target to gain unauthorized access to comp. systems & n/w.
- This may include the injection of hostile code into communications, alteration of data, & masquerading as another person to get unauthorized access.
- It is very difficult to prevent active attack because of wide variety of potential physical s/w.
- Types:
  1) masquerade.
  2) replay
  3) Modification of msg.
  4) Denial of service.

2) Passive attack:
- It is very difficult to detect.
- The msg traffic is sent & received in an normal fashion.
- Neither the sender nor the receiver is aware that a third party has read the msg or observed the traffic pattern.
- Types:
  1) Release of msg content
  2) Traffic Analysis.

9. Diff. betn Symmetric & Asymmetric cipher model.

Symmetric Cipher model.	Asymmetric cipher model.
1) Uses a single key for both encryption & decryption.	(1) Uses two keys private key, & public key one to encrypt & other to decrypt.
2) Size of ciphertext is the same or smaller than original plaintext.	(2) Size of ciphertext is the same or larger than original plaintext.
3) Encryption process is very fast.	(3) Slow.
4) Secret key must be securely shared betn. sender & receiver.	(4) Public key can be shared openly but private key kept secret.
5) Provides confidentiality.	(5) Confidentiality, authenticity & non-repudiation.
6) Efficient as it is used for handling large amount of data.	(6) Less efficient as it can handle small amount of data.
7) less secure.	(7) More secure.
e.g. DES	(8) Diffie-Hellman.
	(9) It is used for secure data transmission, encryption & digital signatures.

10. RSA algorithm.

(1) It is a Asymmetric or public-key cryptography algo.
(2) It works on two diff. keys: Public & private key.
(3) Public key is used for encryption & is known to everyone
(4) Private key is used for decryption & must be kept secret by the receiver.

e.g.

If Person A wants to send a message to Person B.
- Person A encrypts the msg using Person B's Public key.
- person B decrypts msg using ~~Person A's~~ their private key.

• Algo.

- Key Generation by Person A.

Select p, q. p ≠ q both prime p ≠ q.

Calculate $n = p \times q$.

calculate $\Phi(n) = (p-1)(q-1)$

Select integer e $\gcd(\Phi(n), e) = 1$; $1 < e < \Phi(n)$

Calculate d. (Private key) $d = e^{-1} \pmod{\Phi(n)}$.

Public key $PU = \{e, n\}$.

private key $PR = \{d, n\}$.

- Encryption by person B with person A's PU key.

Plaintext $M < n$

Ciphertext $C = M^e \bmod n$.

- Decryption by: A with A's PR key.

Ciphertext C

Plaintext $M = C^d \bmod n$

e.g. $p = 3, q = 11, M = e = 7$.

$n = p \times q = 3 \times 11 = 33$

$\Phi(n) = (3-1)(11-1) = 20$

$ed = 1 + k\Phi(n)$.

$7d = 1 + k\Phi(n)$

$d = \frac{1 + 0 \times 20}{7} = \frac{20}{7}$

$d = \frac{1 + 1 \times 20}{7} = \frac{21}{7}$

$d = \frac{1 + 2 \times 20}{7} = 3$

25/03/2025 Unit No. 02 - 28/03/25
Tuesday

Principles of Public-key Crypto Systems.

Good Luck | Page No. | Date

RSA algorithm — e = Public key & d = private key

- As like before.

e.g. p = 13, q = 17, Public key A = 35, PR(A) = ?

$n = p \times q = 13 \times 17 = 221$

$\phi(n) = (p-1)(q-1) = 12 \times 16 = 192$

$e = 35$

$\gcd(35, 192) = 1$

$de = 1 + k \bmod \phi(n)$

~~$35d = 1 \bmod 192$~~

$d = \frac{1 + k \bmod \phi(n)}{e}$ $\quad d = \frac{1+1 \times 192}{35}$

$d = \frac{1+0 \times 192}{35}$ $\quad = \frac{193}{35}$

~~$d =$~~ $\quad = 5.5$

$d = \frac{1+2 \times 192}{35} = \frac{385}{35} = 11$

Flow.

p & q → Prime nos. } given
e → Public key
d → private key (or)

$n = p \times q$

$\phi(n) = (p-1)(q-1)$

If we have given e then

$d = \frac{1 + k\phi(n)}{e}$

OR

If we have given d then

$e = \frac{1 + k\phi(n)}{d}$

GoodLuck | Page No.
Date

Key Management

- Key management is a technique which supports key generation, storage & maintenance of the key between authorized users.
- It plays an IMP role in cryptography as the basis for securing cryptographic goals like confidentiality, authentication, data integrity & digital signatures.
- The basic purpose of key management is key generation, key distribution, controlling the use of keys updating, destruction of keys & key backup/recovery.
- It is the process & procedures involved in generating, storing, distributing & managing cryptographic keys used in cryptographic algorithms to protect the sensitive data
- The keys used to protect sensitive data are kept safe from unauthorized access or loss.

- Key management Lifecycle:-

1. **Key Generation**: keys must be generated using strong cryptographic random no. generators
2. **Key Distribution**: securely sharing keys is essential, especially in symmetric encryption
3. **Key storage**: Keys must be stored securely to prevent unauthorized access.
4. **Key usage**: Keys should be used only for their planned purpose.
5. **Key Rotation**: old keys should be archived or securely destroyed after expiration.
6. **Key revocation & destruction**: If a key is compromised, it must be revoked & replaced immediately.

GoodLuck | Page No.
Date

Diffie-Hellman Key Exchange Algo.

- It is not an encryption or decryption algorithm.
- It is an key exchange algorithm
- Used to exchange keys between sender & Receiver.
- It follows Asymmetric key cryptography. (Two separate keys for encryption & decryption)

• Procedure:

① Consider a prime no. q.
Let $q = 7$.

② Select α such that $\alpha < q$ & α is primitive root of q.
$\alpha^1 \bmod q$ ---- $\alpha^{q-1} \bmod q$ shd have value $\{1, 2, \ldots, q-1\}$
Let $\alpha = 5$

③ Assume X_A (Private key of A) & $X_A < q$.
Calculate, $Y_A = \alpha^{X_A} \bmod q$
Y_A = Public key of A.
X: Private
Y: Public

e.g. $q = 7$, $\alpha = 5$, $X_A = 3$.

$Y_A = 5^3 \bmod 7$

$Y_A = 6$

④ Assume X_B & $X_B < q$.
Calculate $Y_B = \alpha^{X_B} \bmod q$.

e.g. Let $X_B = 4$.

$Y_B = 5^4 \bmod 7$

$Y_B = 2$

$X_A = 3$, $Y_A = 6$
$X_B = 4$, $Y_B = 2$

⑤ Calculate secret keys K_1 & K_2
(Y_A) K_1 → person A (Y_B) K_2 → person B.

$K_1 = (Y_B)^{X_A} \bmod q$. $K_2 = (Y_A)^{X_B} \bmod q$

If $K_1 = K_2$ then key exchanged is successful

GoodLuck | Page No. | Date

$K_1 = 2^3 \bmod 7 = 1$

$K_2 = 6^4 \bmod 7 = 1$

$K = K_2$

∴ success

∴ key exchanged successfully.

Authentication Requirements.

- Message authentication is concerned with
  - Protecting the integrity of a message
  - Validating identity of originator
  - non-repudiation of origin
- There are three alternative functions are used:
  - hash function
  - Message encryption
  - Message authentication code (MAC)
- Following are the Message security requirement
  1) Disclosure
  2) Traffic analysis
  3) Masquerade
  4) content modification
  5) sequence modification
  6) Timing modification
  7) source repudiation
  8) Destination repudiation

① ~~Disclouser~~ Disclosure

Release of message contents to any person or process not possessing the appropriate cryptographic key.

② Traffic Analysis:

- Discovery of the pattern of traffic bet^n parties
- In a connection oriented application, the frequency

& duration of connections could be determined.
- In either a connection-oriented or connectionless environment, the no. & length of messages bet^n parties could be determined.

(3) Masquerade:
- Insertion of messages into the n/w from a fraudulent source
- This includes the creation of messages by an opponent that are purported to come from an authorized entity.
- Also included are fraudulent acknowledgements of msg receipt or nonreceipt by someone other than the message recipient.

(4) Content modification:
Changes to the contents of a message, including insertion, deletion, transposition or modification.

(5) Sequence modification:
Any modification to a sequence of messages bet^n parties, including insertion, deletion & reordering.

(6) Timing modification:
- Delay & replay of messages.
- In a connection-oriented application, an entire sequence of messages could be replay of some previous valid session.

GoodLuck | Page No.
Date

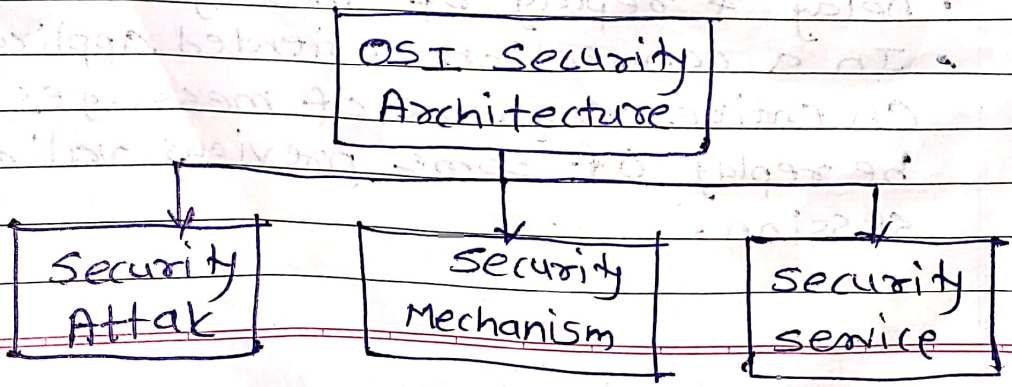
(7) Destination Repudiation:
Denial of receipt of message by destination of transmission of message by source.

- Message authentication is a procedure to verify that received messages come from the alleged source & have not been altered.
- Message authentication may also verify sequencing & timeliness.

Unit No. 01

The OSI security Architecture:

- Open system interconnection (OSI) security refers to a set of protocols, standards & techniques used to ensure the security of data, & to
- These security services & mechanisms help to ensure the confidentiality, integrity & availability of the data.
- The OSI security Architecture focuses on these concepts:
  - security attack
  - security mechanism
  - security service



(1) Security Attack:
- An attack is when the security of a system is compromised by some action.
- Two types of attack : Active & Passive.

(2) Security Mechanism:
- A ~~mechasi~~ mechanism that is designed to detect, prevent or recover from a security attack.

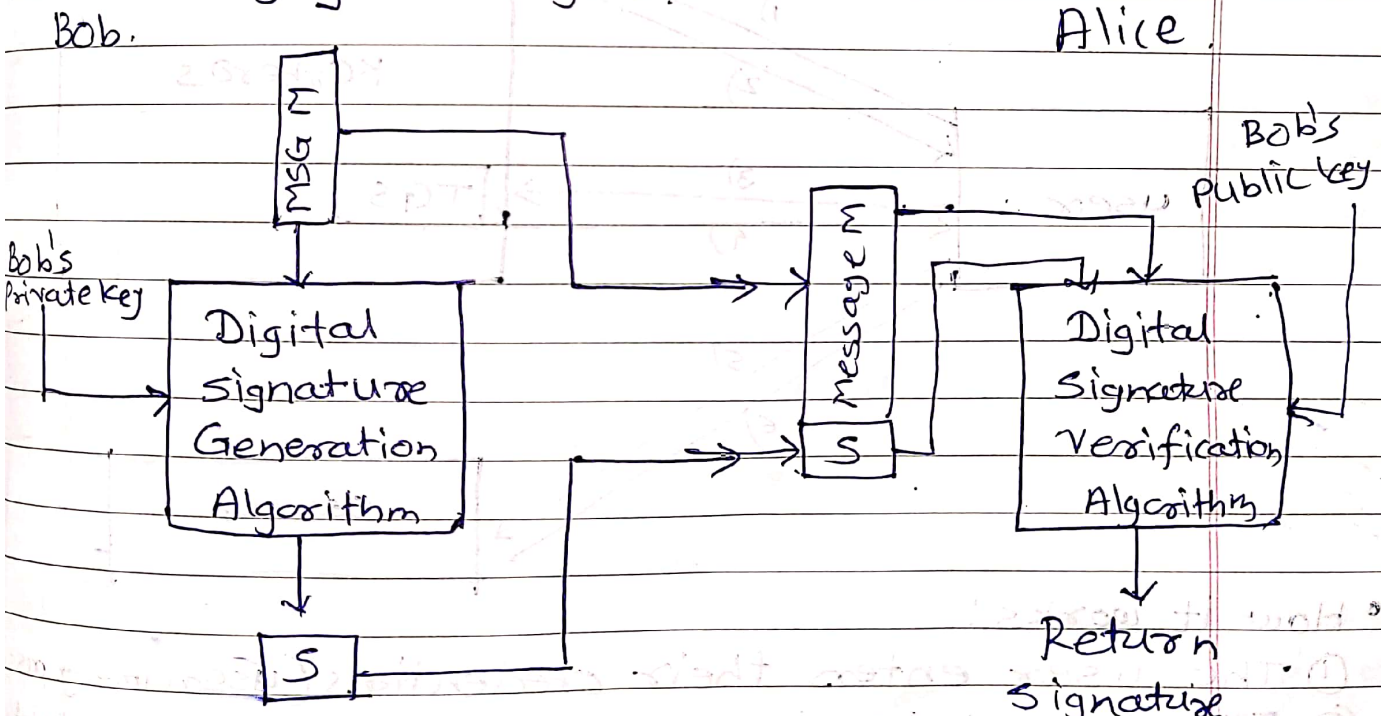
(3) Security service:
- A service that enhances the security of the data processing system.
- The services make use of one or more security mechanisms to provide the service.

29/03/2023

Unit No. 03 Digital Signature

Digital signature standard.

- It is an asymmetric key cryptographic algorithm.
- Private key is used for encryption.
- Public key is used for Decryption.
- It is used for authentication & Non-Repudiation
- It is a way of authenticating a digital data coming from a trusted source.
- It defines the algorithms that are used to generate digital signatures with the help of Secure Hash Algorithms (SHA) for the authentication of electronic documents.
- It only provides us with the digital signature function & not with any encryption or key exchanging Strategies.



Advs-

- Confirms the sender's identity.
- Uses strong encryption for protection.

Dis:

- Managing key pairs across multiple devices & systems can be challenging.
- User must securely store their Private key

Kerberos Authentication service.

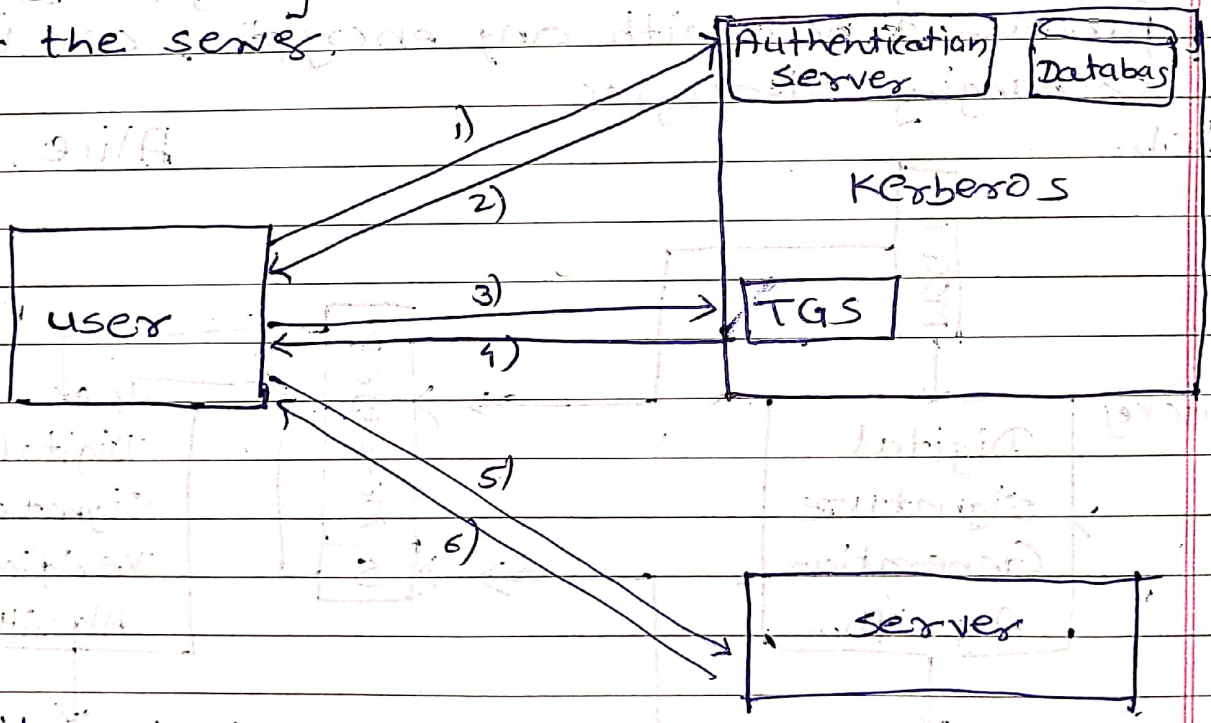
- Kerberos is an Centralized Authentication service.
- It depends on symmetric Encryption.
- In this authentication server & database is used for client authentication.
- It runs as a third-party trusted server known as the Key distribution center.

- Components of Kerberos

① Authentication server (AS): Performs the initial authentication & ticket for Ticket Granting service.

② Database: A authentication server verifies the access rights of users in the database.

③ Ticket Granting server (TGS): Issues the ticket for the server.



- How it works:

① The user enters their credentials (username & passwo

② The authentication server verifies the credentials & issues a ticket Granting Ticket (TGT), which is encrypted using a secret key derived from the user's password.

③ when the user wants to access a servie, they present the TGT to the Ticket Granting serve.

④ The TGS issues a service Ticket, encrypted with the servie's secret key

⑤ The user presents the service Ticket to the requested service.

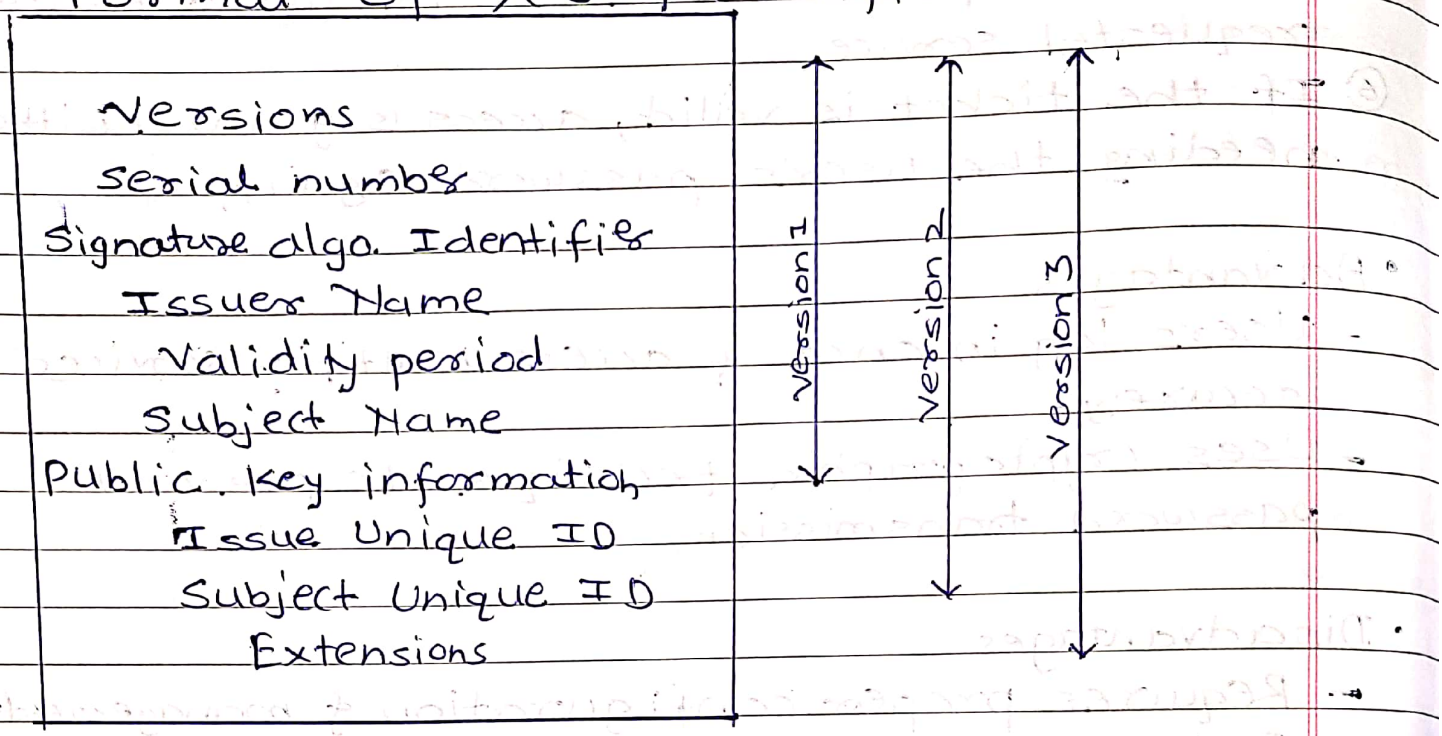
⑥ If the ticket is valid, access is granted without needing the user's password again.

Advantages
- Users log in once & access multiple services securely.
- Uses cryptographic techniques to prevent password transmission.

Disadvantages
- Requires proper configuration & management.
- Relies on timestamps, so clocks must be synchronized.

X.509 Authentication Service.
- It is a digital certificate accepted internationally
- ~~we~~ It does not generate any keys but it provides a way to access public keys.
- These user ~~certif~~ certificates are assumed to be produced by some trusted certification authority.
- Once a X.509 certificate is provided to a user by certified authority, that certificate is attached to it like an identity card.
- The chances of someone stealing it or loosing it are less, unlike other unsecured passwords
- With the help of this analogy, it is easier to imagine how this authentication works. → The certificate is basically presented like an identity at the resource that requires authentication.

- Format of X.509 certificate.



1) Versions: Defines the X.509 version that concerns the certificate.
2) Serial number: Unique no. / serial no. of a certificate.
3) Sign. algo. identifier: It states the algorithm which is used by the issuer.
4) Issuer Name: The person who issued the certificate.
5) Validity period: Defines the period up to which certificate is valid.
6) Subject Name: Name of the person to whom ~~we~~ are giving the certificate.
7) Public Key information: It defines the subject's public key & the info. about that public key.
8) Issue Unique ID: Unique ID of issuer.
9) Subject Unique ID: ——u——u——u— Subject.
10) Extensions: Contains additional standard info.

Digital signature : Requirements.

IMP

① - The signature must be a bit pattern that depends on the msg being signed.

GoodLuck | Page No. | Date

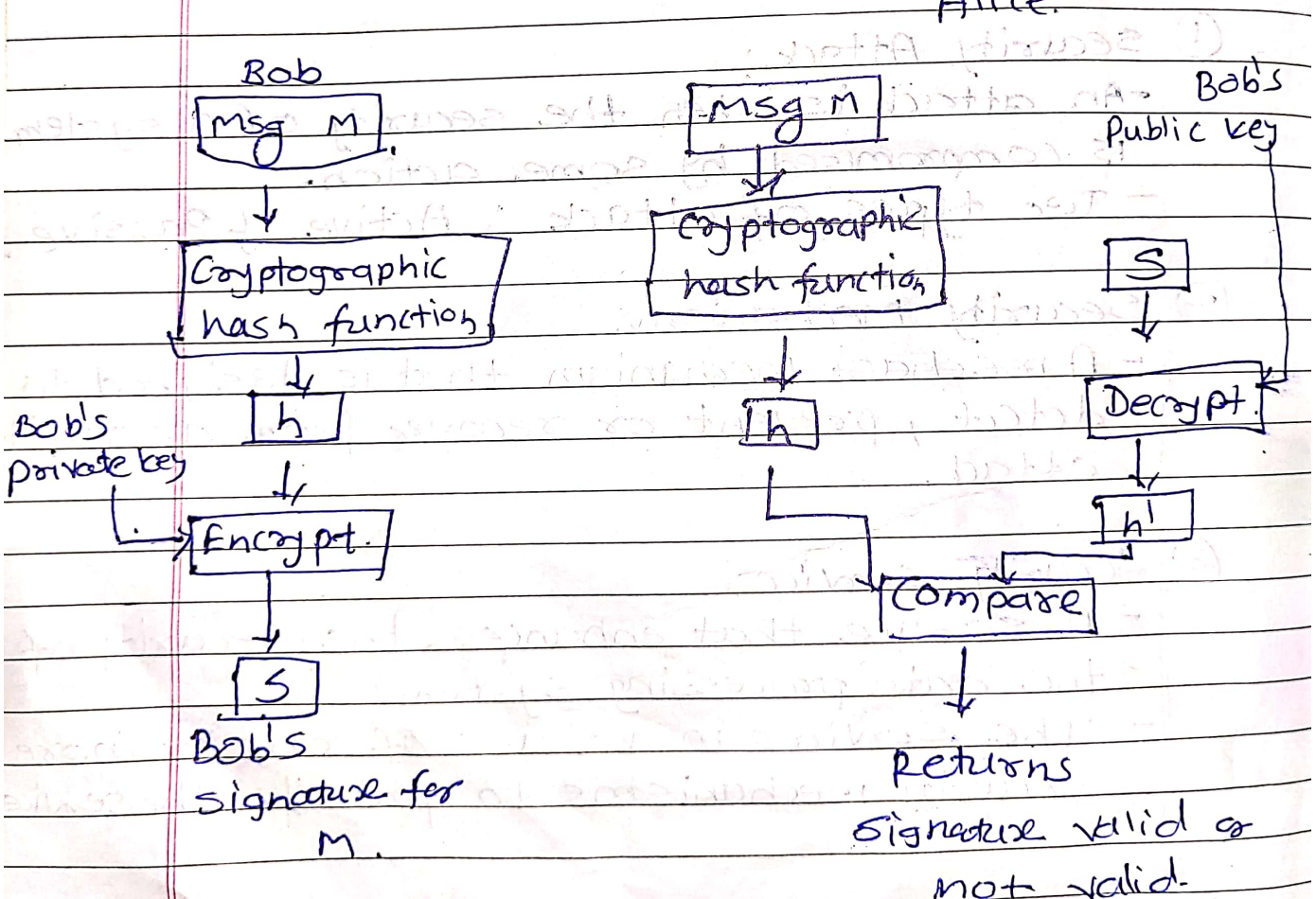
② - The signature must use some information unique to the sender to prevent both forgery & denial.

③ - It must be relatively easy to produce the digital signature.

④ - It must be relatively easy to recognize & verify the digital signature.

⑤ - It must be computationally infeasible to forge a digital signature.

⑥ - It must be practical to retain a copy of the digital signature in storage.



Format of

Properties of Digital signature.

GoodLuck | Page No.
Date

1. It must verify the author, the date & time of the signature.

2. It must authenticate the contents at the time of the signature.

3. It must be verifiable by third parties, to resolve disputes.