Unit -4

1) Authentication Requirment:

*Disclosure - Appropriate Cryptographic key

*Traffic Analysis - Discovery of the pattern of traffic between parties

*Masqueriade - Insertion spurious file or msg

*Content Modification - Modification of content

*Sequence Modification - Modification of sequence in msg

*Timing Modification - Modification of Msg time

*Source repudation - denial of msg service from src

*Destination repudation - Denial of msg service from destin

2.) Authentication functions:

Msg encryption:

The process of converting cipher text to plain text.

Msg Authentecation code: MAC

A public function of the msg and a secret key that produces a fexed length value serves as a Authenticator.

eg: OTP, System generated emails.

Hash function:

A public function that uses maps msg and values, which serves as the authenticator.

3) SHA - 512 Algorithm:

* The Secure hash algorithm (SHA) was developed by the National institute of standards and Technology in 1993.

* SHA is based on the hash function MD4.

* This algorithm takes as input a message with a maximum length of less than 2^{128} bits and output as 512 bit message bit

* The values return by hash function is called hash values, hash codes

Use of hashing:

1.) Data verifaction

2) password Storage

3) Digital signatures

4) MAC

SHA - 512

Working :

1) padding

2) Appending

3) Divide the i/p into 512 bit block

Padding :

* The msg is padded, so that its length is congruent to 896 modulo 1024.

* Even if the msg is already desired length, padding is added.

* padding length ranges from 01 to 1024

Appending :

* A block of 128 bits is appended to the msg.

* so that total length can be calculated.

Divide the I/p into 512 bit blocks.

According to the length, the input is block into 512 bit blocks

Step 4:

Intialize hash buffer.

* A 512 bit buffer is used to hold the resutts of hash function.

* The buffer can be represented as eight 64-bit registers (a,b,c,d,e,f,g,h).

$a = \underbrace{6A09}_{1}\underbrace{E667}_{2}\underbrace{FF87}_{3}\underbrace{C908}_{4}$

b = 8EFK69WK12f

c =

d =

e =

f =

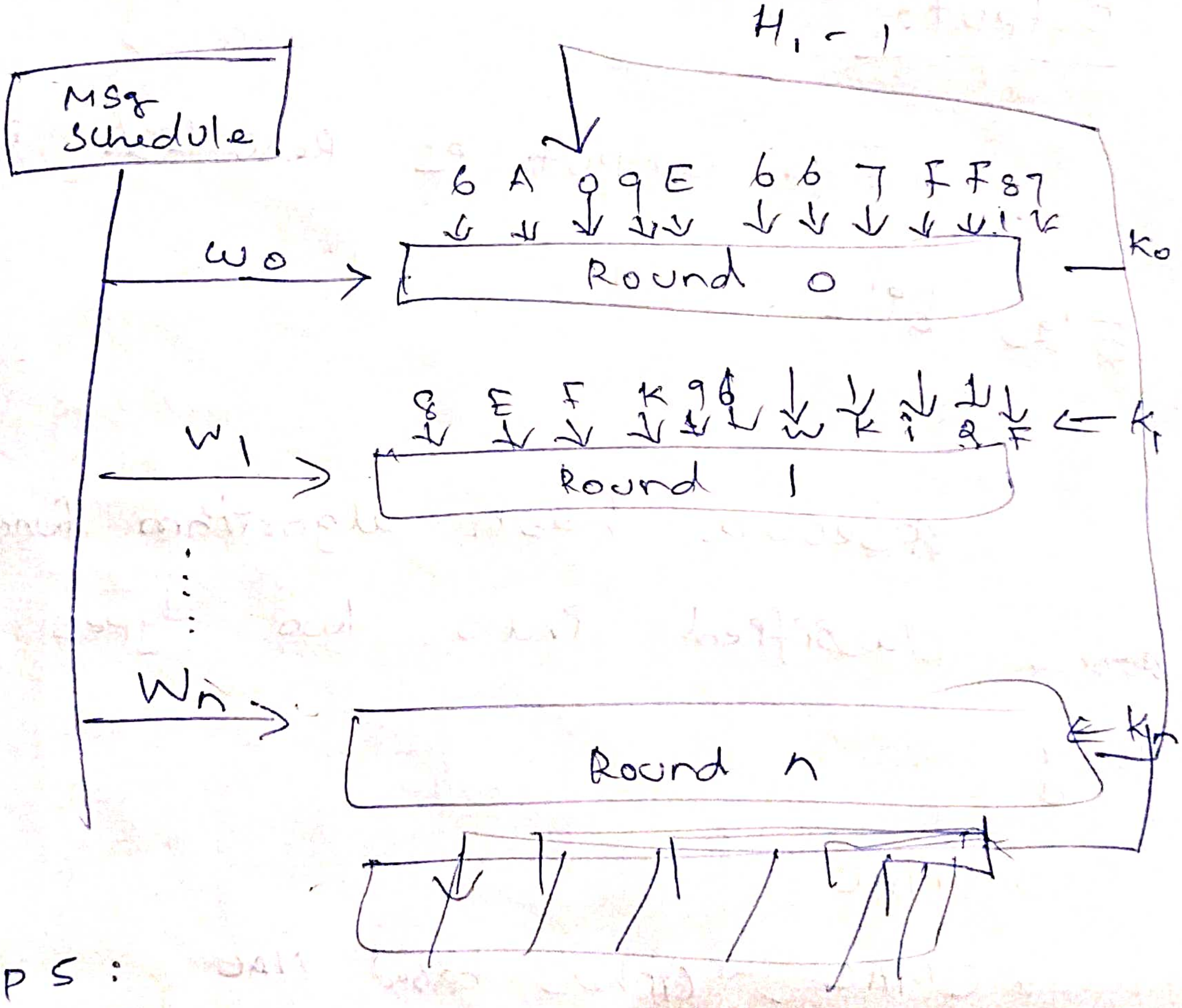
g =

h =

* These values are stored in big endian format, which is the most significant byte of word in low address byte position

Step 4 :

process blocks



Step 5 :

* Msg is blocked into 128 bit blocks.

* The heart of the algorithm is module that consist of 80 rounds

*Each round takes as input of 512 - bit buffer values.

* The output of the eightieth round is added to the input to first round.

Step6:
Output:

The output is Resulted in 512 bits.

*Secure hash algorithm functions are classified into two types they

* HMAC
* CMAC → Cipher based MAC

HMAC

* It is an cryptographic hash function.

*It is more faster than MD5 and SHA.

*Library code for cryptographic hash functions are widely available

4) Digital Signature:

*A digital signature is an authentication mechanism, that enables the creator of a Msg to attach a code that acts as a signature.

*Message authentication protects two parties who exchange msg from any third party.

*A digitial signature is a analogous to the handwritten signature.

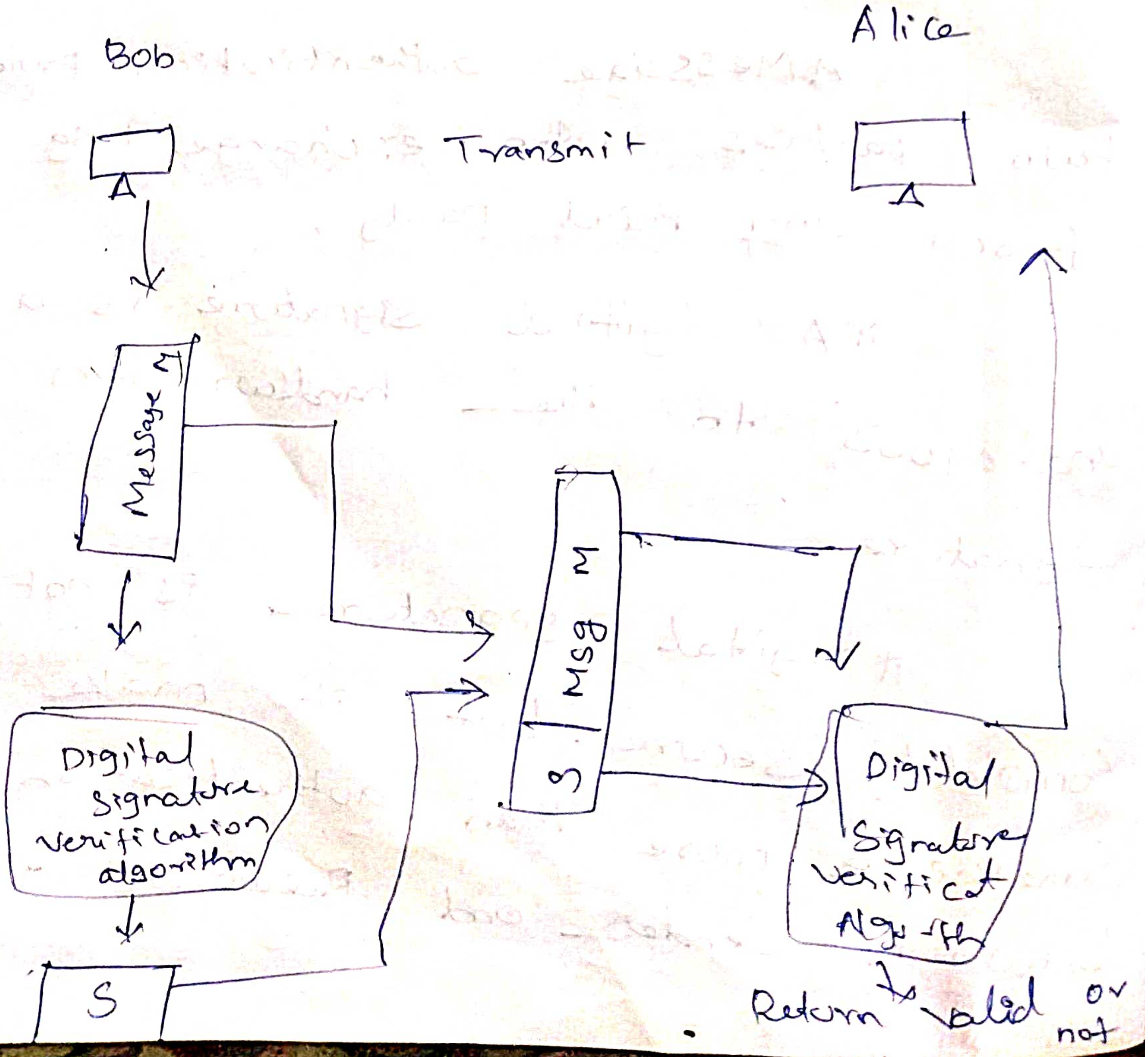
*Digital signature is not completely secure. but it make something more than authentication between Sender and Receiver

*A digital signature must verify the following condition

1) It must verify the author, date and time

2) It must to authenticate the contents.

3) It must be verifable by third parties to solve disputes


Bob
Alice
Transmit
Message M
Msg M
S
Digital signature verification algorithm
S
Digital Signature Verificat Algo-rth
Return to valid or not

* The general schema for Digital signature is classified into two types they are

1) Aritibrated

2) Direct.

Aritibrated:

* Every msg signed communicated between sender and receiver is sent to arbiter.

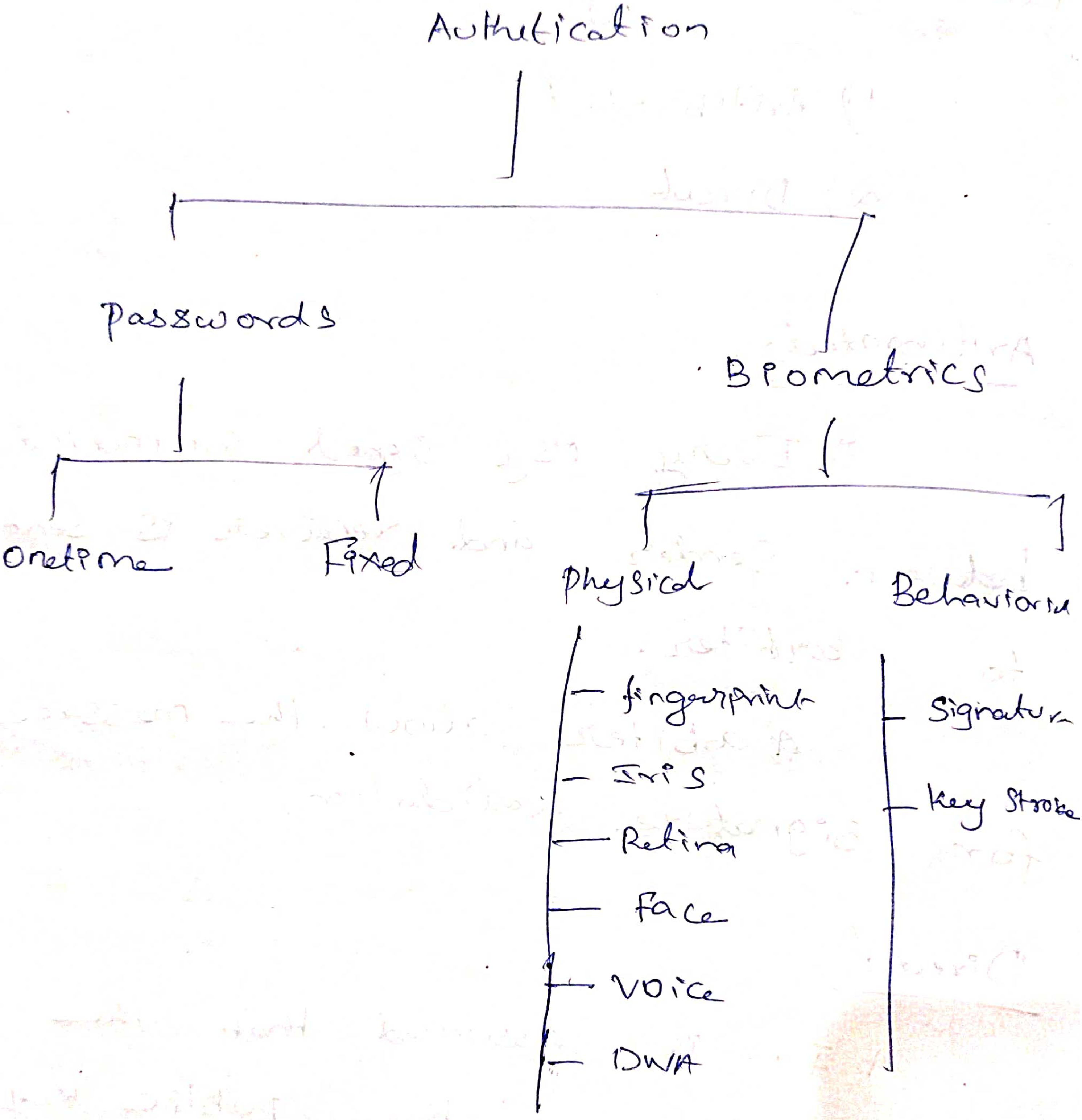
* arbiter allow the message for signature validation.

Direct:

* It is assumed that the destination knows the public key of source.

* Sender's code is private key

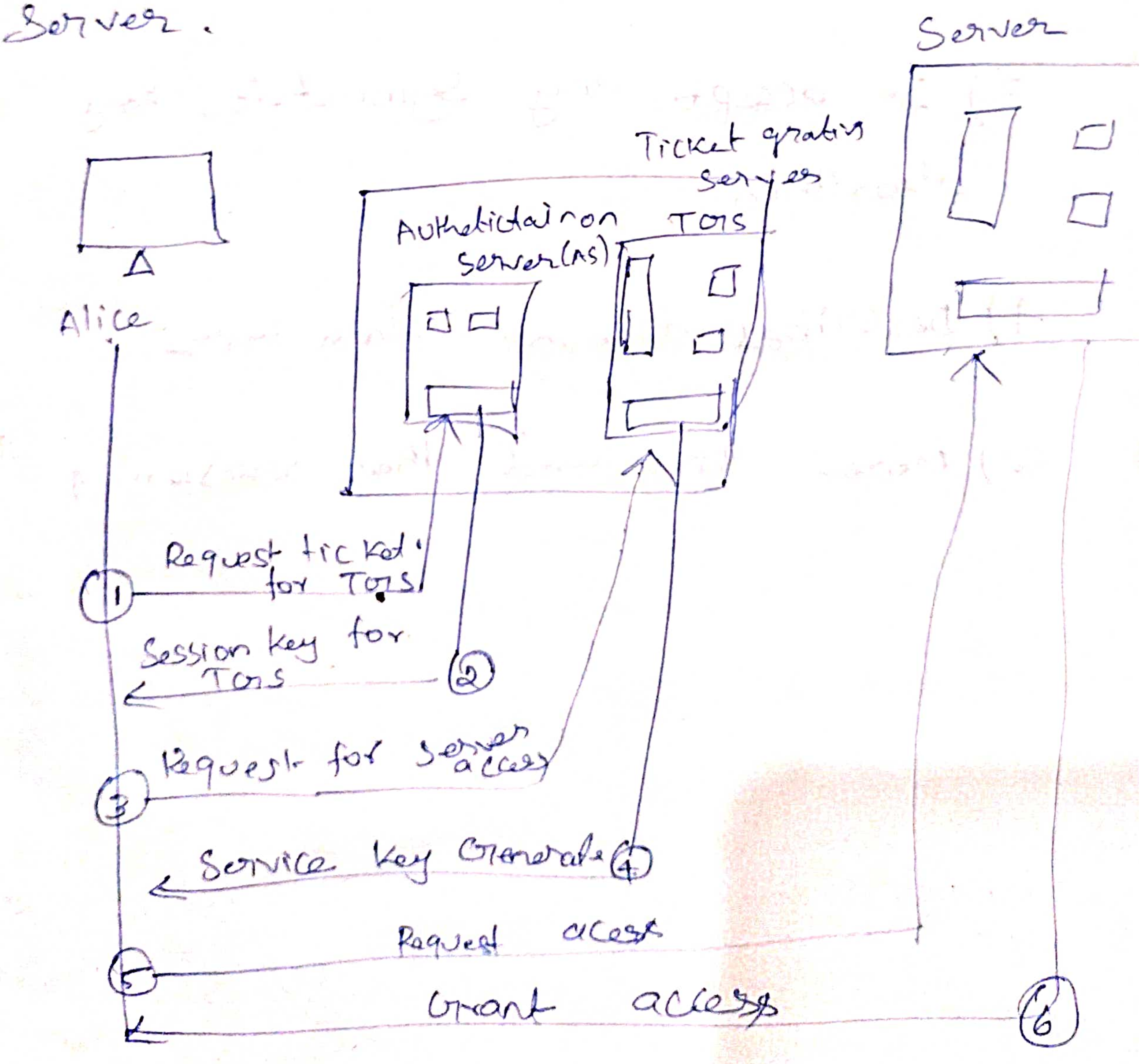
5) Entity Authentication



6) kerberos - Authentication.

* Kerberos is an Authentication protocol used for client Server communication using trusted third party.

* Kerberos makes a secure connection between client and Server.



keyboros Version 5

* The minor differences between version 4 and version 5 are listed here.

1) Tickets generated by version 5 ~~of~~ are lifetime accessible.

2) It allows ticket to be renewed

3) It accept any symmetric key algorithm

4) Describes different data types

5) More overhead than version 4