Name :- Akash Santosh katkar
Roll No.:- 35
GI No.:- 5895 Signature :- Akash.

INS Assignment 2

Q.1. Explain Diffie-Hellman key Algorithm with an example.

→ Diffie-Hellman key :-

i) The DH key exchange algorithm produces a session key.

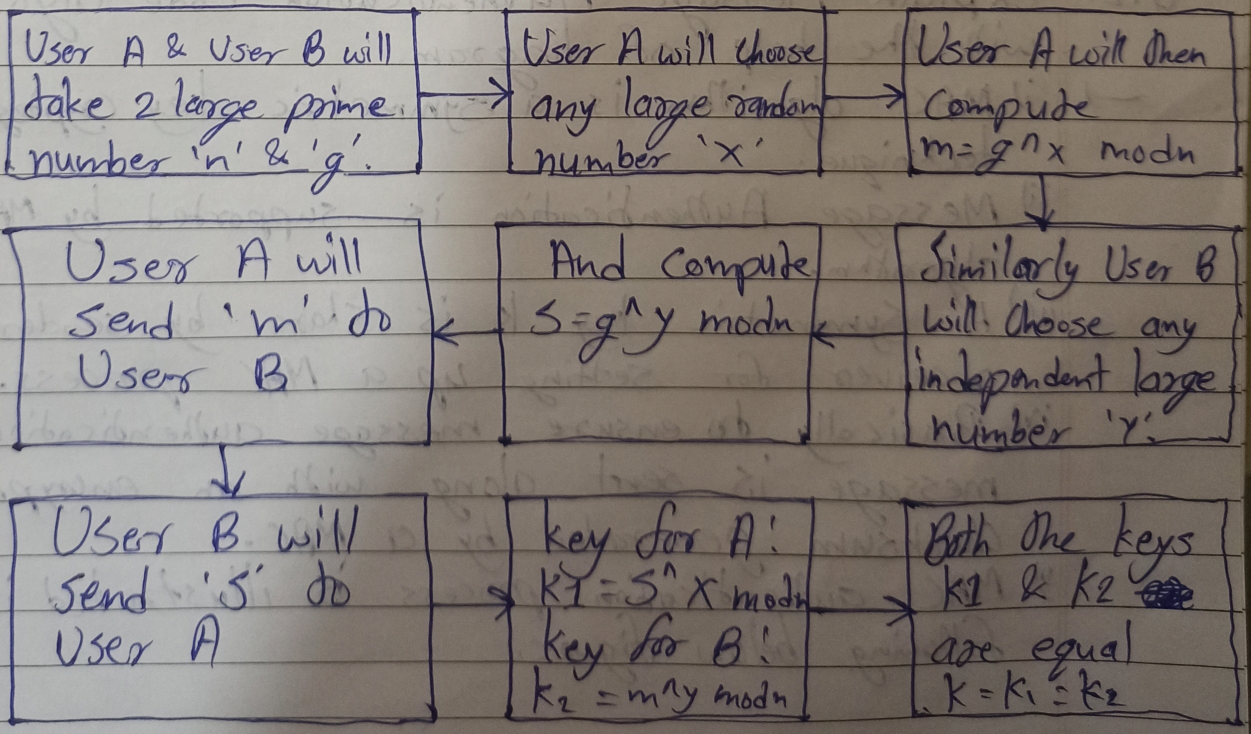
ii) This algorithm solves the problem of key agreement between sender & receiver or exchange of keys between communication parties.

iii) In this method cryptographic key are securely exchanged over a public channel.

iv) This method is used for two parties who are unknown to each other, jointly create a secret key over an insecure medium.

v) Symmetric key is generated which is agreed by both the parties, taking part in communication.

vi) The generated key is used for encryption & decryption mechanism.

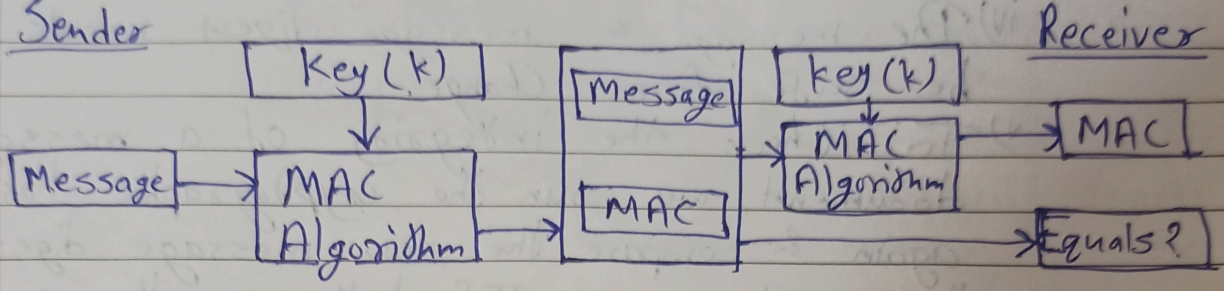


Name:- Akash Santosh Kalkar
Roll No.:- 35
GI No.:- 5895
Signature:- Akash.

User A	User B
A chooses $x = 3$ ($g = 7$ & $n = 11$)	B chooses $y = 6$ ($g = 7$ & $n = 11$)
$m = g^x \bmod n$	$S = g^y \bmod n$
$m = 7^3 \bmod 11$	$S = 7^6 \bmod 11$
$m = 343 \bmod 11$	$S = 117649 \bmod 11$
$\boxed{m = 2}$	$\boxed{S = 4}$
A sends $\boxed{m = 2}$ to B	B sends $\boxed{S = 4}$ to A
key for A	key for B
$k_1 = S^x \bmod n$	$k_2 = m^y \bmod n$
$k_1 = 4^3 \bmod 11$	$k_2 = 2^6 \bmod 11$
$k_1 = 64 \bmod 11$	$k_2 = 64 \bmod 11$
$\boxed{k_1 = 9}$	$\boxed{k_2 = 9}$

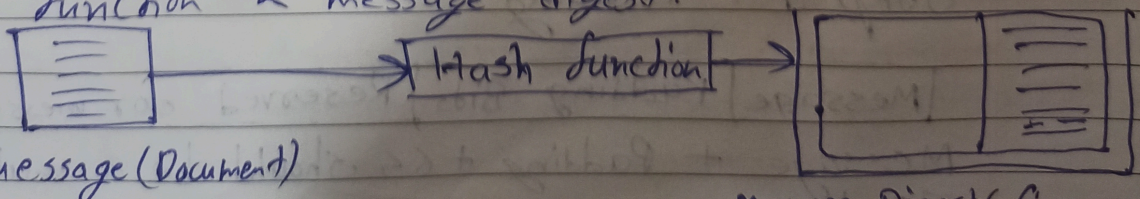
Q.2. Explain Message Authentication code algorithm with the help of diagram.

→ i) MAC algorithm is a symmetric key cryptographic technique.
ii) Message Authentication is supported by MAC algorithm.
iii) A Symmetric key K is share by sender & receiver for setting up a MAC process.
iv) Basically to ensure message authentication a message is sent along with an encrypted checksum generated by a MAC.
v) MAC authentication process is illustrated in the following below figure.



vi) A MAC value is generated by a sender, who uses commonly used MAC algorithm & by inputting some message & secret key k.
vii) Like hash, MAC function also reduces random generated long input into a ~~final~~ fixed size output
viii) For Compression, MAC uses secret key.
ix) Along with the MAC, uses sender sends message.
x) Message needs to be encrypted in case of confidentiality.
xi) A receiver assumes that the message is not authentic.

Q.3 Explain Hash function with the help of diagram
→ i) To preserve the integrity of the message it is passed through an algorithm called cryptographic ~~it is passed through an algorithm~~ hash function.
ii) The function creates a compressed image of the message that can be used like a fingerprint
iii) figure below shows the message cryptographic hash function & message digest.

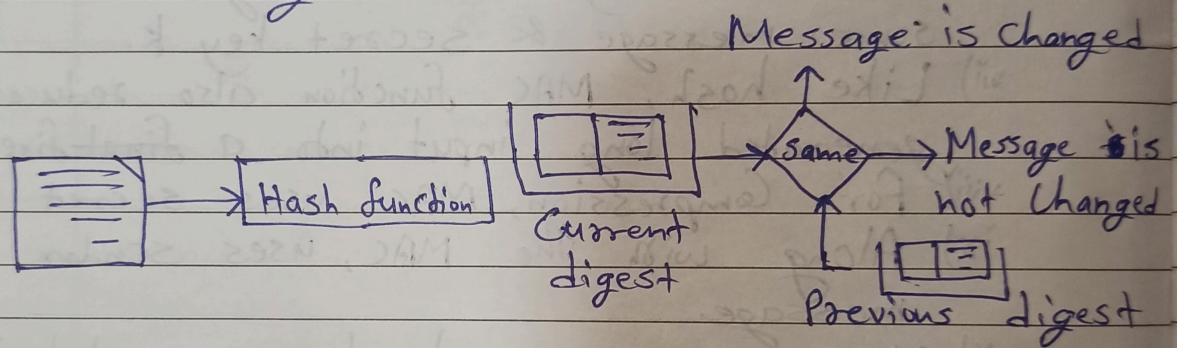


Message (Document)
Message Digest (fingerprint)

Name :- Akash Santosh kartkar
Roll No. :- 35
GI No. :- 5895
Signature :- Akash

iv) The message & message digest needs to be safe from change.

v) To check the integrity of a message or document, we run the cryptographic hash function again & compare the new message digest with the previous one. If both are the same, we are sure that the original message has not been changed.



Q.4. Explain working of MD5 algorithm with the help of diagram.

→ i) MD5 is ~~quite~~ quiet fast & produces 128-bit message digest.

ii) After same initial processing, the input text is processed in 512-bit blocks (which further divided into sixteen 32-bit sub blocks).

iii) The output of the algorithm is a set of four 32-bit blocks, which ~~make~~ makes up the 128-bit message digest.

Step 1 : Padding

Message	Padding Bits	Reserved for message length

- Message + Padding + 64 should be a multiple of 512 bits.

Name :- Akash Santosh Katkar
Roll No :- 35
GI No :- 5695
Signature :- Akash

PAGE No. 5
DATE / /

If message is 400 bits in length
400 + 64 = 464 Nearest multiple of 512, 512
Hence, padding = 512 - 464 = 48 bits

400	48	Reserved for message length

Step 2 :- Append length

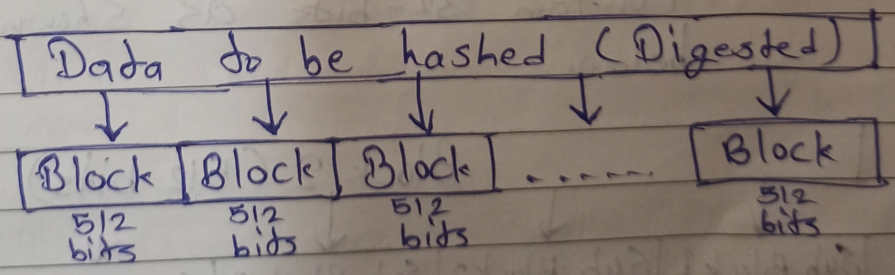
Message	Padding Bits	Reserved for message length

Message + Padding + 64 should be a multiple of 512 bits.

If message is 400 bits in length
400 + 64 = 464 Nearest multiple of 512, 512
Hence padding = 512 - 464 = 48 bits.

400	48	64

Step 3 :- Divide the input into 512 bits block.



Step 4 :- Initialize Chaining variables
i) four variables (called as Chaining variables) are initialized.
ii) They are called as A, B, C & D. Each of these is

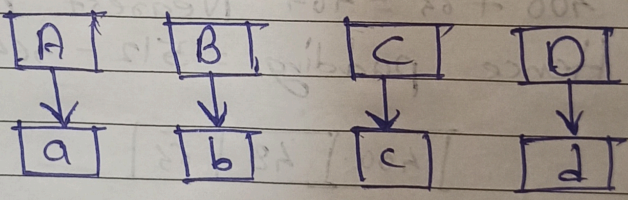
a 32-bit number.

iii) The initial hexadecimal value of these chaining variables are as shown below.

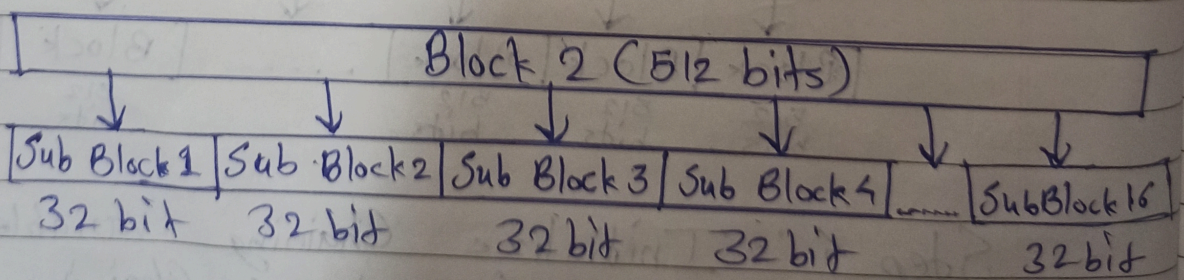
32			8	8	8	8
	A	Hex	01	23	45	67
128	B	Hex	89	AB	CD	EF
Bits	C	Hex	FE	DC	BA	98
	D	Hex	76	54	32	10

Step 5 :- Process block

Step 5.1 :- Copy the changing variables into four corresponding variables a, b, c, d.



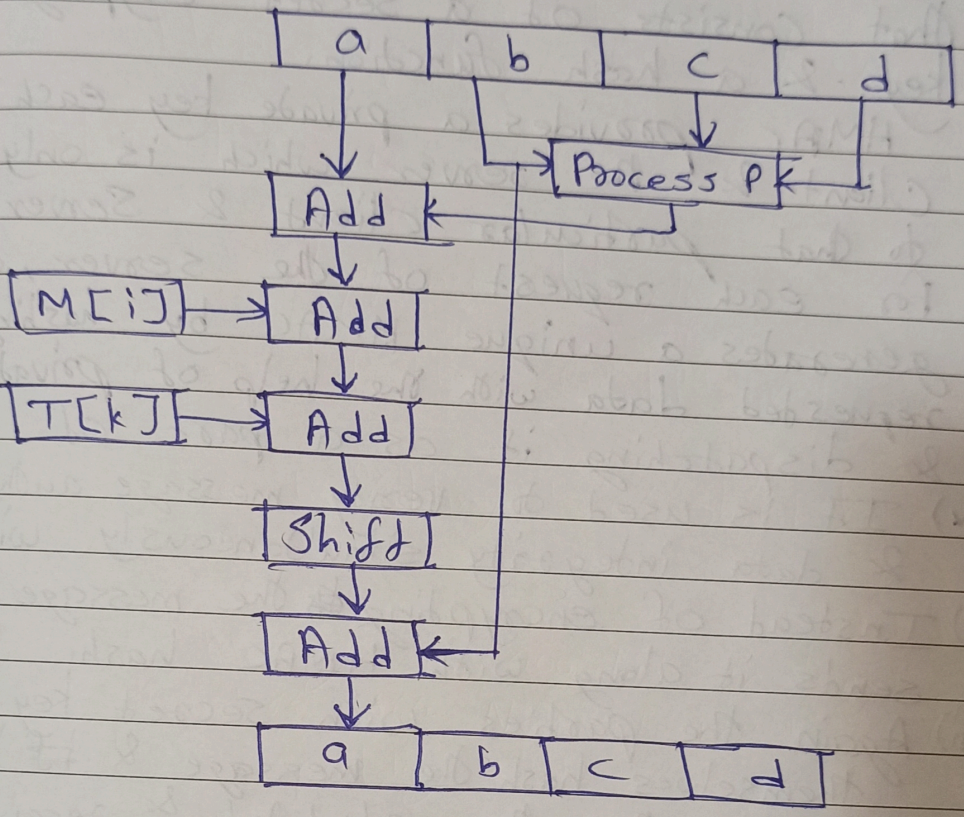
Step 5.2 :- Divide the current 512-bits block into 16 sub-blocks. Thus, each block contain 32-bits as shown in figure below.



Step 5.3 :- Now, we have four rounds. In each round we will process all the 16 sub blocks

Name :- Akash Santosh Katkar
GI No.:- 5895
Roll No.:- 35
Signature :- Akash.

belonging to a block.



Step 5.4 :- Process Block

Round	Process
1	(b AND c) OR ((NOT b) AND (d))
2	(b AND d) OR ((c) AND (NOT d))
3	b XOR c XOR d
4	c XOR ((b) OR (NOT d))

Q.5. Explain working of HMAC algorithm with the help of diagram.

Name :- Akash Santosh kadkar
Roll No. :- 35
GI No. :- 5895
Signature :- Akash.

PAGE No. 8
DATE / /

→ i) HMAC is a particular type of MAC that consists of a secret cryptographic key & a hash function.
ii) HMAC provides a private key each for client & the server which is only known to that particular client & server.
iii) For each request of the server, client generates a unique HMAC by hashing the requested data with the help of private keys & dispatching it as a part of request.
iv) It is used to verify message authentication & data integrity simultaneously with MAC.
v) Instead of encrypting the message, HMAC sends it along with HMAC hash.
vi) Again the parties with secret key will themselves hash the message & if it is authorized then the calculated & received hashes will match.
vii) Once the request is received by the server & regenerate regenerate its unique HMAC, comparison of two HMAC takes place. If they are equal, the client is trust worthy & executes its request.

• Working of HMAC :-
Consider the following variables :-
MD :- Message Digest or Hash function which is used (Ex. MD5, SHA1)
M :- Input Message whose MAC is to be computed.
L :- Number of blocks in the message.

Name :- Akash Santosh Kathar
GR No :- 5895 / Roll No :- 35
Signature :- Akash.

Date : / /
Page No. : 9

b :- Number of bits in each blocks.
K :- Shared symmetric key which is to be used for HMAC.

Ipad :- A string 00110110 repeated b/8 times.
Opad :- A string 01011010 repeated b/8 times.

Step 1 :-
Make the key length k equal to b.
- If key length k < b.
- The size of key length k is increased so that its size & total number of bits b in the initial message blocks are total number of bits b in the initial message blocks are equal to make this, left of k are appended with 0 bits.
- Example :- If the original key length k = 150 bits & b 256 bits then append 106 bits to the left, all with a value 0.

Make the key length k equal to b
- If key length k > b
- Reduce the key size k to make its size & total numbers of bits b in the initial message blocks are equal.

Make the key length k equal to b.
- If key length k = b.
- None of the action will be performed & it will processed towards Step 2.

Step 2 :-
XOR operation between k & Ipad to get the value of S1. XOR operation is performed between any k generated in step 1 & Ipad to get the value of variable S1.

Step 3 :-
S1 is appended by message M.
End of S1 is appended by original message (M) generated in Step 2.

Step 4 :-
Message digest algorithm.
Ex. SHA1, MD5 etc is selected & applied on the Step 3 output which operation is further known as H.

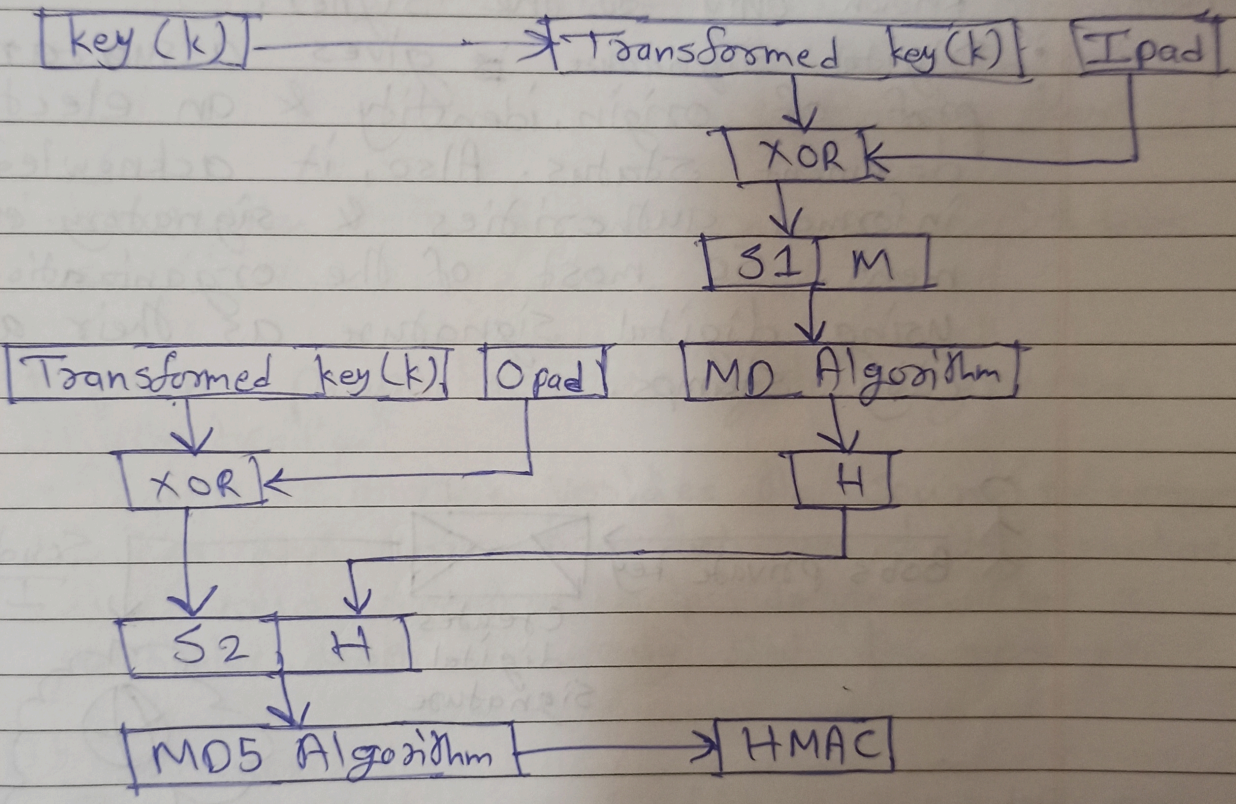
Step 5 :-
XOR operation between key length K & Opad to know the value of S2.
XOR operation is performed between key K generated in Step 1 & Opad to get the value of the variable S2.

Step 6 :-
End of S2 produced in Step 5 is appended by message digest H generated in Step 4.

Name :- Akash Santosh kadkar
GI No.:- 5895
Roll No.:- 35
Signature :- Akash.

classmate
Date
Page 11

Step 7:-
Message digest algorithm
Ex. SHA1, MD5, etc is selected & applied on the step6 output which is further Consider to the final MAC.

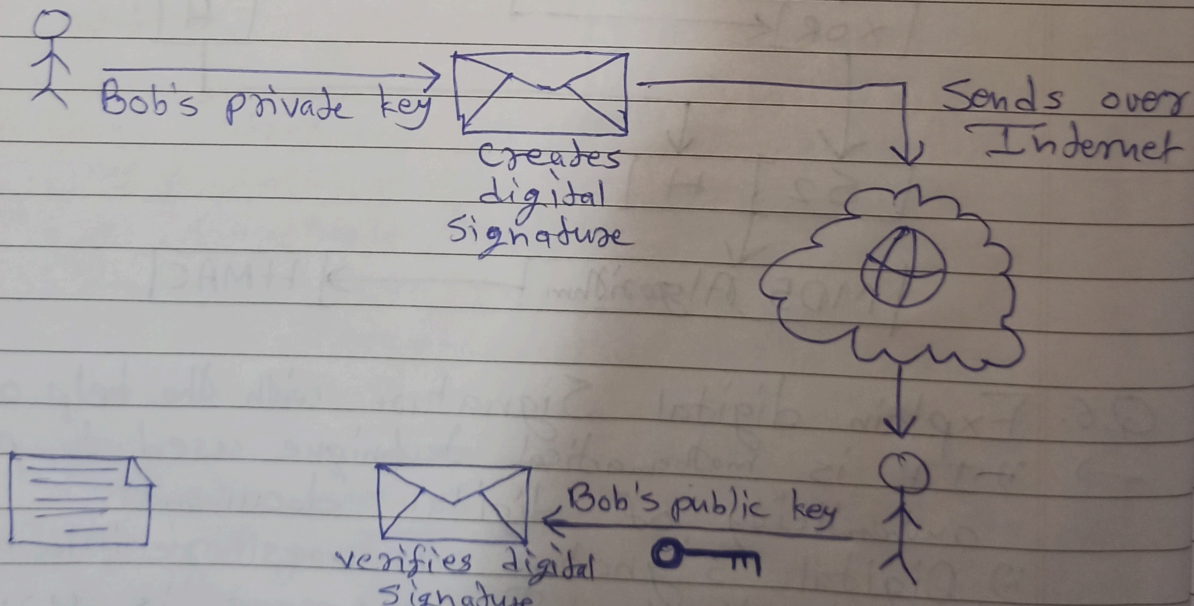


Q.6. Explain digital Signature with the help of diagram.
→ i) It is mathematical technique used to produce authenticity of digital documents.
ii) Digital signature assures recipients :-
- Authentication :- The message is send by the known sender.
- Non-~~Repudi~~ Repudiation :- The sender cannot deny that he has not sent the message.
- Integrity :- While transmitting the message it has not altered.

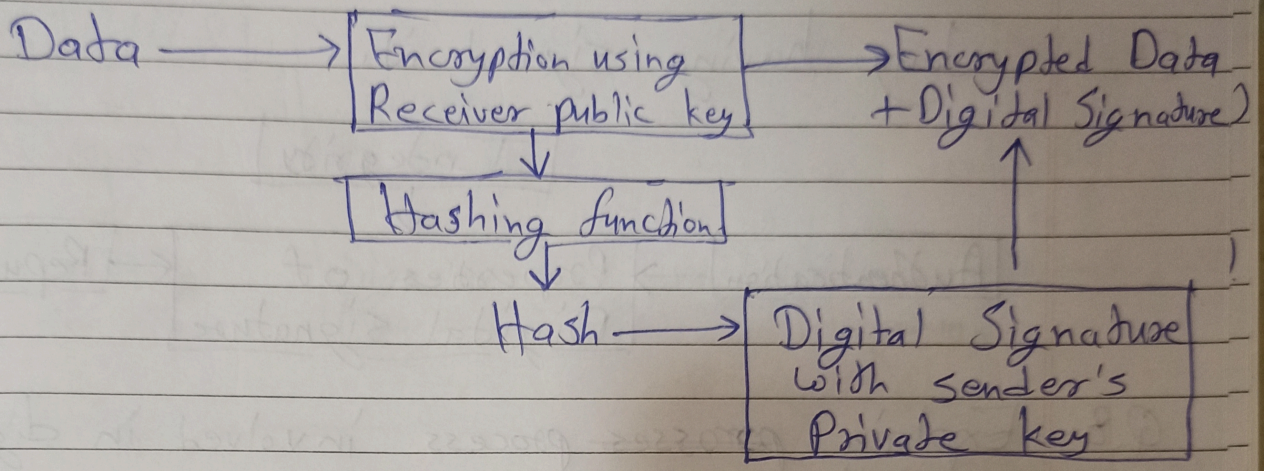
Name :- Akash Santosh kakkar
GI No.:- 5855
Roll No:- 35
Signature :- Akash.

classmate
Date
Page 12

- Integrity of message & the original source of the document are ensured by attaching code like signature.
- Digital signature is a cryptographic value computed from secret key & data & is known only to the signer.
- Digital Signature ~~is~~ gives assurance of proof of origin, identity & an electronic document status. Also, it acknowledges informed authorities & signatory endorsement. So most of the organizations are using digital signature as their authenticity stamps.



Name :- Akash Santosh Kadkar
GI No.:- 5895
Roll No.:- 35
Signature :- Akash



∴ Encryption with digital Signature of Sender's side.

Q.7. Explain properties of digital signature.

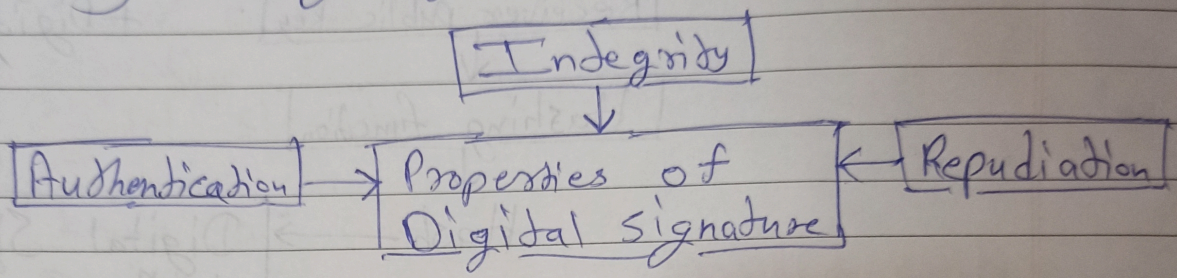
→ i) Authentication :-
- Digital signature verifies the source of message.
- When each user has their own digital signature then valid signature helps to proves that a particular user has only sent the message.

ii) Integrity :-
- The sender & receiver of a message are sure about during transmission, the message has not altered, originality of the message is intact.
- Even the contents of encrypted message can be altered sometimes. But when the document is digitally signed, any alteration in the message after signature will cause in invalidating the signature.

iii) Repudiation :-
- After signing on the documents, the entity cannot

Name :- Akash Santosh kadkar
Roll No.:- 35
GI No.:- 5895
Signature :- Akash.

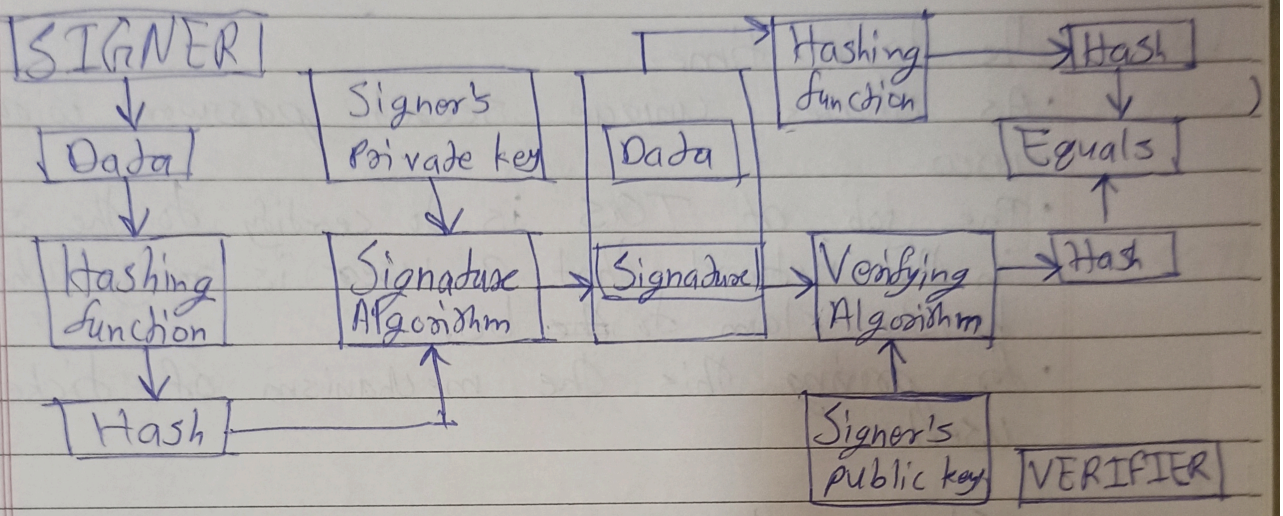
deny having signed it.



Q.8. Explain ~~processes~~ process involved in digital signature.

→ i) Every party involved in the process should have public & private key pair.
ii) Basically, different key pairs are used for process of verifying / signing & encryption / decryption.
iii) Signature key is private key used for signing & the verification key is public key.
iv) Hash function data is provided to the signer & & produce hash of data.
v) Signature algorithm is then fed by the signature key & hash value.
vi) It generates the digital signature on that particular hash.
vii) Data is appended by the signature.
viii) Both signature & data are sent to the verifier
ix) Verification algorithm is fed by the digital signature & the verification key by the verifier
x) Output is generated by the verification algorithm.
xi) To produce the hash value, verifier executes same hash function on the data which is received.

Name :- Akash Santosh Kalkar
Roll No :- 35
GI No :- 5895
Signature :- Akash.



Q.9. Explain the working of kerberas with the help of diagram.

→ i) Kerberos is an authendication protocol that has become very popular.
ii) Several systems including ~~AT&T~~ Windows 2000 uses kerberas which is designed for smaller scale use such as an a LAN.
iii) It is named after the three-headed dog in Greek mythology that guards the gates of Hades.

Working of Kerberos :-
- User A :- The client workstation.
- Authendication Server (AS) :- Verifies (authendicate) the user during login.
- Ticked Granding Server (TGS) :- Issues tickets to certify proof of identity.
- User B :- The server offering services such as network printing, file sharing or an application program.
- The job of AS is to authendicate every user at

Name :- Akash Santosh kadlag
GI No.:- 5895
Roll No.:- 35
Signature :- Akash.

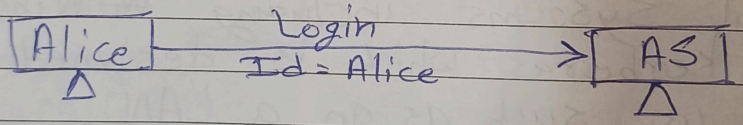
classmate
Date
Page 16

The login time.

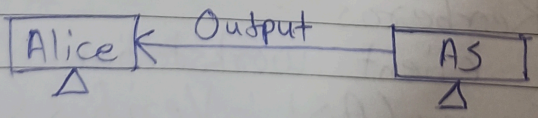
- As shares unique secret password with every user.
- The job of TGS is to certify to the servers in the network that a user is really what he/she claim to ~~the~~ be.
- for proving this, the mechanism of tickets used.

- Step 1 : Login
- Step 2 : Obtaining service Granting Ticket (SGT)
- Step 3 : User communicates for accessing server.

Step 1 : Login



- User A (Alice) sits down at an arbitary public workstation & enter his/her name.
- The workstation sends her name in plain text to the AS.



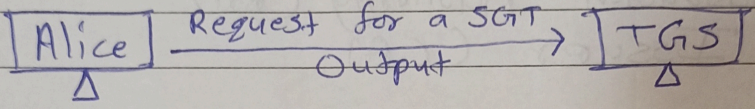
- AS produces a package of user A(Alice) & randomly generate a session key (KS).
- The encryption of this package & symmetric key takes place which is send to Ticket Granting Service (TGS) by AS.
- The output of the above step is called Ticket Granting Ticket (TGT).

Name :- Akash Santosh kadkar
GI No.:- 5895
Roll No.:- 35
Signature :- Akash.

classmate
Date
Page 17

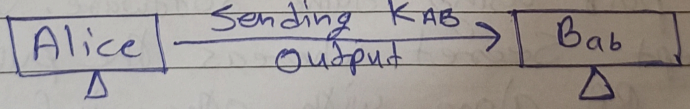
- TGT is combined with KS & then encrypted by symmetric key generated from user A(Alice) password & send to user A (Alice).

Step 2 :- Obtaining Service Granting Ticket (SGT)

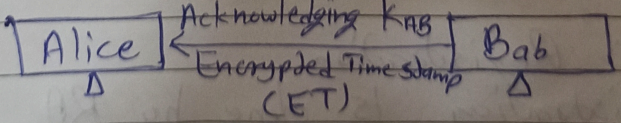


- When TGS satisfies authorization of user A (Alice), it produces session key K_{AB}.
- Key is sent twice to User A(Alice) by TGS. First time, it is combined with user B's Id & encrypted with KS & next time, it is combined with A's Id & encrypted with User B key KB.

Step 3 :- User communicates for accessing server



- User A(Alice) transmits K_{AB} encrypted with secret key as well as timestamp to User B (Bab) to enter into a session with him.



- User B (Bab) appends 1 to timestamp than with K_{AB} it encrypts the result & sends it to User A(Alice) again.

Name :- Akash Santosh kadkar
GI No.:- 5895
Roll No.:- 35
Signature :- Akash.

classmate
Date
Page 18

Q.10 Explain the steps of creation of digital Certificate in details.

→ i) The parties involved in creating digital certificates are :
- The subject (End User)
- Registration Authority (RA)
- The Issuer (CA)

ii) Steps of creation of Digital Certificate :-
1) Key generation
2) Registeration
3) Verification
4) Certificate Creation.

Step 1 :- Key Generation
Key can be generated in two ways
1) The subject can create a private key & public key pair using same software. The private key is kept Secret, whereas the public key is sent to the RA along with other information.
2) In case, if user does not know about creating pair then on behalf of subject, RA can generate a key pair.

Step 2 :- Registration
1) Registration is done by RA, if key is generated by RA.
2) If user generates the key he/she reads the public key, its associated registration information & also all facts about him/her to RA.

Name :- Akash Santosh kadkar
GI No.:- 5895
Roll No.:- 35
Signature :- Akash.

Date : / /
Page No.: 19

Step 3 :- Verification

1) After completing the registration process, RA has to verify the user's credentials.
2) The second check is to ensure that the user who is requesting for the certificate does indeed passess the private key corresponding to the public key.
3) • RA can demand that the user must digitally sign the certificate signing Request (CSR) with his/her own private key.
   • RA can create random number challenge, encrypt it with user's public key & ask the user to decrypt it using her private key.
   • RA can create a dumy certificate for the user, encrypt it & sends it to user. The user can decrypt it only if he/she has valid private key.

Step 4 : Certificate Creation

1) If all the above steps are successfully created, the RA forwards all the details of the user to CA.
2) The CA does it own verification & creates a digital certificate for the user.
3) The CA sends the certificate to the user & saves one copy of it for its own records. The CA then sends the certificate to the user.