G2020 Rebecca CSS
SEM:06

BARFI Page No. Date

1/12

Q2]

A]

Security services

(1) ITU-T provides some security services and some mechanisms to implement those services to avoid the various active and passive attacks

(2) Security and mechanism are very closely related

(3) A security service makes use of one or more security mechanisms.

(4) There are various types of security services such as

1. Data confidentiality
2. Data Integrity
3. Authentication
4. Non-Repudiation
5. Access-control

(5) Data-confidentiality
The protection of data from a unauthorized disclosure

(6) Data Integrity
The assurance that data is received is as sent by an authorized entity

(7) Authentication
Assurance that the communicating entity is the one claimed

(8) Non-Repudiation-
protection against denial by one of the parties in a communication.

(9) Access control
Prevention of the o unauthorized use of a resource.

Security Mechanism

(1) A mechanism that is designed to detect, prevent or recover from a security attack
(2) There are various types of security mechanisms. like
i) Encipherment
ii) Data Integrity
iii) Digital Signature
iv) Authentication exchange
v) Traffic padding
vi) Routing control
vii) Notarization
viii) Access control.
(3) Encipherment
This security mechanism deals with hiding and covering of data which helps data to become confidential
(4) Data Integrity
This security mechanism is used by appending value to data to which is created by the data itself
(5) Digital signature
It is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically
(6) Authentication exchange
Two entities exchange some messages to prove their identity to each other.

3/12

(7) Traffic padding
Means inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis

(8) Routing control
means selecting and continiously changing different available route between sender and receiver to prevent the opponent from eavesdropping on a particular route.

(9) Notarization
This security mechanism involves use of trusted third party in communication. It acts as a mediator in the exchange

(10) Access control
This mechanism is used to stop unattended access to data which you are sending.

Relationship between security service and mechanism
(1) In security servile, there is data confidentiality in mechanism encipherment and routing control is being used
(2) Data integrity is in security service where as in security mechanism there is encipherment, digital signature and data integrity
(3) In authentication in security services is used where as encipherment, digital signature & authentication exchanges are used in security mechanism
(4) Non-repudiation is used in services where as digital-signature, data integrity and notarization is used in mechanism
(5) Acess control mechanism is used in both security and mechanism.

62020 Rebecca CSS
SEM:06

BARFI Page No. Date

4/12

Q2]

B] Diffe - Hellman Key exchange algorithm.

① DH Key exchange algorithm is a method for securely exchanging cryptographic keys over a public communications channel
② Keys are not actually exchanged but they are jointly derived by both.
③ The purpose of the algorithm is to enable two users to securely exchange keys that can then be used for subsequent symmetric encryption of messages
④ The algorithm itself is limited to the exchange of secret values
⑤ The DH algorithm depends for it effectiveness on the difficulty of computing discrete logarithms.

Example :-

Suppose Alicia and Brinn agree on $q = 7$ and $q = 7$. Alicia chooses secret key as 3 and Brinn chooses as 6. Their public and private keys will be calculated ie Y_A and Y_B

$p = 11$, $q = 7$, $Xa = 3$, $Xb = 6$

$Y_A = 7^3 \bmod 11 = 2$

$Y_B = 7^6 \bmod 11 = 4$

Y_B is gone to Alicia

Y_A is gone to Brinn

They calculate the shared secret key

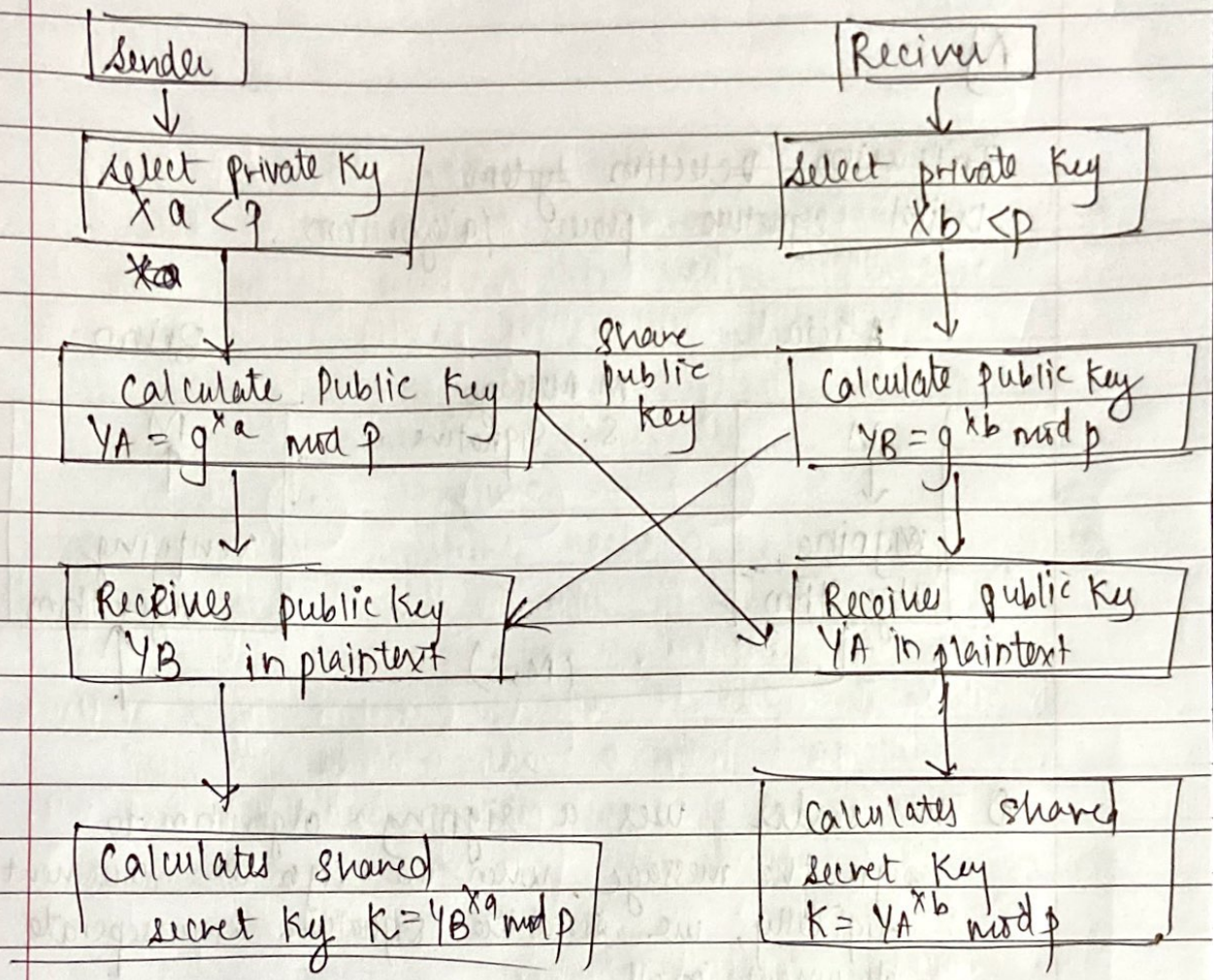
$Y_B^{Xa} \bmod p = 4^3 \bmod 11 = 2^6 \bmod 11 = 9$

62020
SEM: 06

CSS

BARFI Page No. Date

5 / 12



Common elements prime number p
g is a primitive root of p. g < p.

① Ramesh and suresh agree on p = 17 & q = 7

② Ramesh selects another secret large random number and calculates $q^a \bmod p = 7^5 \bmod 17 = 11$ a = 5

③ Ramesh sends it to suresh

④ Suresh selects another number 3 i.e b = 3 such that $S = q^b \bmod p = 7^3 \bmod 17 = 3$

Q2020
SEM:06 CSS

BARFI Page No.
Date

Rebecca

6/12

(5) Suresh sends number to Ramesh
(6) Ramesh now calculates secret key

$$R_k = S^2 \bmod p$$
$$= 3^5 \bmod 17$$
$$= 5$$

(7) Suresh now calculates

$$S_k = R^b \bmod p$$
$$= 11^3 \bmod 17$$
$$= 5$$

(8) If both the secret keys are same Ramesh & Suresh can agree for future communication
(9) We know that both the keys are the same (i.e 5) is same for both hence proved.