Q i) Design a routing protocol that can send k blocks of data successfully even if up to any e of the n connections are corrupt.

ii) Using a public key system design a Robust Oblivious Transfer protocol.

iii) Consider the following 4 cases:

a) PK of both A and B are known to both.

b) PK of A is known to B but not viceversa.

c) PK of B is known to A but not vice versa.

d) Neither A nor B each other's PK.

What is the maximum tolerable e in each of these cases?

A. Routing protocol: Sender.

1. Let K be the no. of blocks to be sent. Divide the blocks into groups of size atmost k such that it satisfies $k + e = n$.
2. Run the protocol for fault tolerant storage described in Evaluation 2 for each of the groups. This step produces an encoding for each group consisting of n blocks. (where $n = k + e$).
3. Let $|g|$ be the no. of groups. Use the above encoding to write $|g|$ in terms of n blocks. Send this encoding to the receiver through the n channels.
4. Send the encoding of each of the groups to the receiver through the n channels.

Fault tolerance: Notice that each group satisfies $k + e \leq n$. We know that the protocol in Evaluation 2 guarantees fault tolerance of upto e blocks. Since only e channels may be corrupt, each group is transmitted with fault tolerance ensured.

Routing Protocol: Receiver

i) Receive n packets from the sender through the n channels.
ii) Using the protocol for decoding described in evaluation 2 recover $|g|$.
iii) Data $= \phi$
iv) Repeat $|g|$ times:
   a) Receive n packets from the sender through the n channels.
   b) Using the protocol for decoding described in evaluation 2 recover a group of k blocks.
   c) Append the k blocks to Data.
v) Return Data.

Unknown Public Key case -

In case the receiver doesn't have the sender's public key, it will be unable to decode as described in evaluation 2. In this case we use some coding scheme from coding theory. For example - we could use Reed-Solomon codes and set $n \geq (k + 2e)$ for each group.

Maximum Tolerable e -

a) PK of both A and B are known to both: Here both A and B can use the protocol involving signatures. Hence $e = n - k$. is the maximum tolerable e.

b) PK of A is known to B but not viceversa. Here only A can use signatures. However, B can use the alternate protocol with Reed - Solomon codes. Thus in the first round B will send over its pk by using the alternate protocol. This round tolerates $e = \frac{n-k}{2}$ errors. Once the key has been sent, they can restart communication using the protocol with signatures and tolerate $e = n-k$ errors.

c) pk of B is known to A but not vice versa: Similar to case b) there is one round with $e = \frac{n-k}{2}$ maximum tolerable errors. Following that the maximum tolerable errors becomes $e = n-k$.

d) Neither A nor B each other's pk: First A sends B its PK as described in b). Then B sends its PK as in c). Thus there are 2 round with max tolerable $e = \frac{n-k}{2}$. After that the max tolerable e becomes $e = n-k$.

El - Gamal Public Key System

<u>Gen</u>

G: Cyclic group of order p, where p is a safe prime.
g: generator of g.
Let $x \in_R \{1, 2, \dots, p-1\}$. compute $h = g^x$.
Now $pk = \langle G, p, g, h \rangle$
$sk = x$.

<u>$enc_e(m)$</u>

Let $y \in_R \{1, p-1\}$
Set $s = h^y$
$c_1 = g^y$
$c_2 = m \cdot s$
Return (c_1, c_2)

<u>$dec_d(c_1, c_2)$</u>

Get $s = c_1^x$
Get $m = c_2 \cdot s^{-1}$
Return m.

Oblivious Transfer Protocol

Client A : has index ind

Server B : has data m of length n.

Public key (e, d) of B is known to A. (cases (a) and (c))

1. B generates an array of random no.s. of length n $r \in_R \{1, 2, \cdots, p-1\}^n$. B sends r to A.
2. A sets $v = r_{ind} \oplus enc_e(k)$ where k is generated randomly from $\{1, 2, \cdots, p-1\}$. i.e. $k \in_R \{1, 2, \cdots, p-1\}$
   A sends v to B.
3. B computes all possible values of k. i.e. $k_i = dec_d(v \oplus r_i)$
4. B computes $m'_i = m_i \oplus k_i$ for all $i \in [n]$.
   B sends m' to A.
5. A recovers $m_{ind} = m'_{ind} \oplus k$.

I B is oblivious to ind.

B receives the following piece of information from A -

$v = r_{ind} \oplus enc_e(k)$: Here B can get ind if it can find r_{ind}. However, without knowing k it cannot recover r_{ind}, assuming it is a PPTM adversary, with better than negl() probability.

II A is oblivious to m_i, $i \neq ind$.

A receives the following pieces of information from B -

i) r : These bits are completely random and convey nothing to A.

ii) m': For each m'_i, $i \neq ind$ $m'_i = m_i \oplus k_i$.
Thus A can recover m_i if it knows k_i. However, $k_i = dec_d(v \oplus r_i)$. Since A does not have B's private key d, it cannot perform this decrypt, assuming PPTM adversary, with better than negl() probability.

OT for cases (b) and (d)

The PK of B must be sent to A. B can use the alternate protocol with Reed - Solomon codes. Thus in the first round B will send over its PK by using the alternate protocol. Once the key has been sent the above OT protocol can be used.