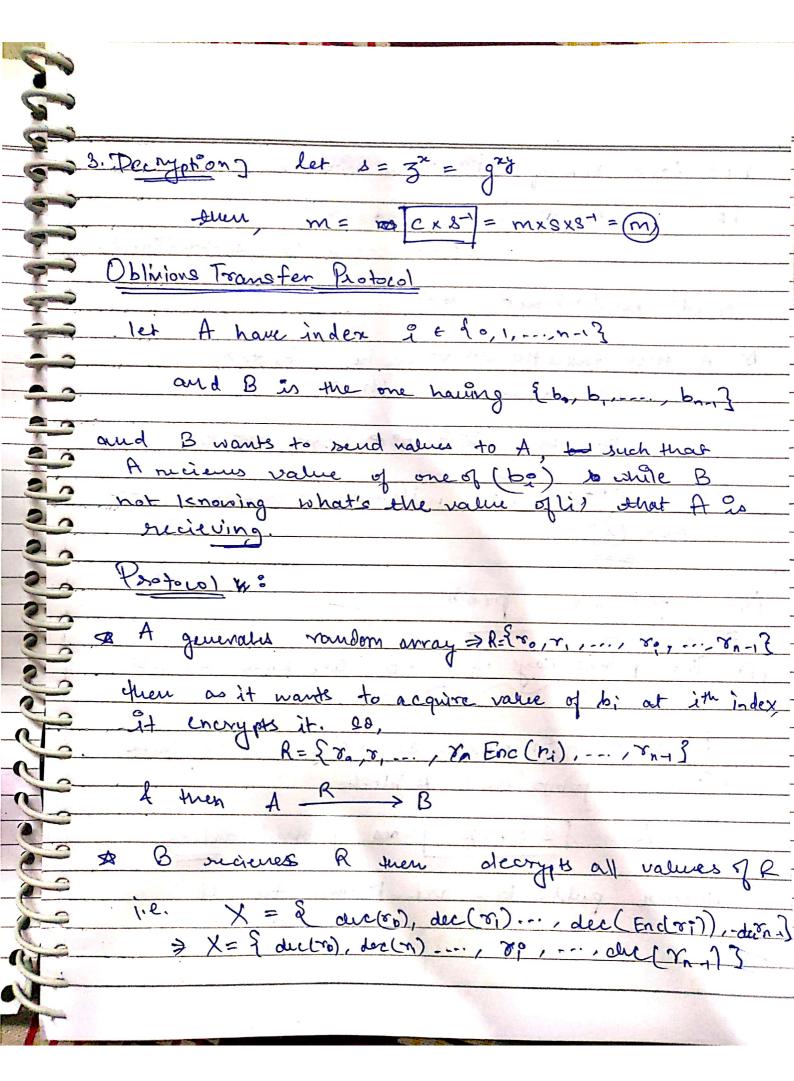
POIS Evaluation 5
Remath Singhal 20171213
20171213
There are a channels to send k blocks of data between A and B.
between A and B.
So, We can we same way as in evaluation 2 by staring k blocks of data as coefficient of a polynomial and generating in points at random values for of this polynomial.
by storing k blocks of data as coefficient of a
polynomial and generating in points at random
values polynomial.
$go = \sum_{i=0}^{\infty} di x^{i}$
21.1 -11. (2002)1/2 (2012)
and points => (1, p(1)), (4P(2)), (n, p(n))
and me only reed k points but of these in
points to reconstouch the polynomial and have
k data points.
No. of the second secon
Also, to heak if the recienced point is un-coroupted"
rather than sending points as it is & points with their digital signatures are sent.
their digital signatures are sent.
377 574
If after reducing, digital signatures are correct. The points are verified and are not corrupted.
the points are verified and are not corrupted.
And minimum roiso non-corrupted blocks required are k to reconstruct polynomial
are k to reconstruct porpromat
Fa 000

hance

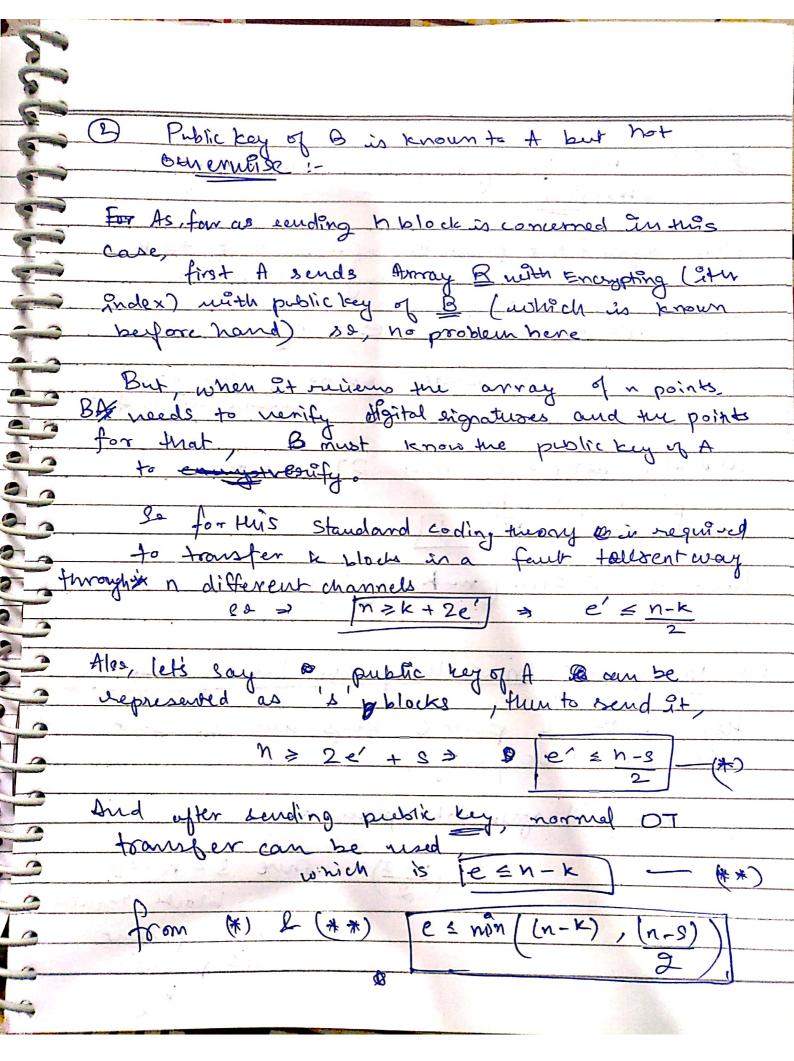
e >n-k

K≥n-e

Elgamel Enouption
The state of the s
A ← → B
1. Generation of public key& private key
a large prime "p" sis generated & a generated
La remevoitor à for La
A Source of
then, a nandom number In ischoren
from Z*
which is me porvate key
t public key = g gx mod p , g , p]
2 Enc Scheme
let m = message,
choose random y E Zp
3 = gt & & = ht & c = (ms) modp
que lignater Encrypted value = 2 3, c3



and takes xor of it value with be
10 X = { bot ducto), both duc (5),,
bj@n:,, bn-, ⊕ duclon-1)}
and sends back to A.
A then takes the ith value i.e. big & si
A men takes the ith value i.e. b; & so; and takes XOR with s;
ie. 为 bi 于 200 bis; 为 9是 bis
hunce obtains (bi) mithour Bicnowing the
Ender (1)
Now for given problem:
The state of the s
1) The public keys of ALB are known to all
For this, ? t is same as using pourous case
with n points and k blocks.
T POINTS OFFICE TO THE PROPERTY OF THE PROPERT
de [e≥n-k ous proved earlier.
I subtic buy are known to all.
becum public kye are known to all.
Ex The second se
becum public kyr are known to all.



\$(111) Public ker of B = known to A not
& (119) Public key of B is known to A, not other rulse.
Here again figure public key of A is sent to B
Here, again fissest public key of A is sent to B via normal coding theory protocol in a
Du balevent way
faut tolevent way e = n-3.
where 82 no. of block for public key of A
public key of A
and also, after then normal DT can take
Large Har which
place for which, [ezn-k]
the state of the s
hure > e smin (n-k, n-s)
27
(IV) Neither party knows the public - key of week other:
(1V) Neither party knows the public - reg of the
Here, both the public keys will be sent
to the other party,
que sorio pario
quis will again take place as
e = (n-e) une e = ha. So
$e \leq (n-2)$ where $s = ha. Sb$
to supresure
A's public
kuy

oregined to represent public ky of B also, after that normal or transfer can take place for which e = (n-12) trune 2 e = nun n-k, n-m, n-s considuit (m=s=1),