Cryptography and Network Security

Prof. D. Mukhopadhyay

Department of Computer Science and Engineering

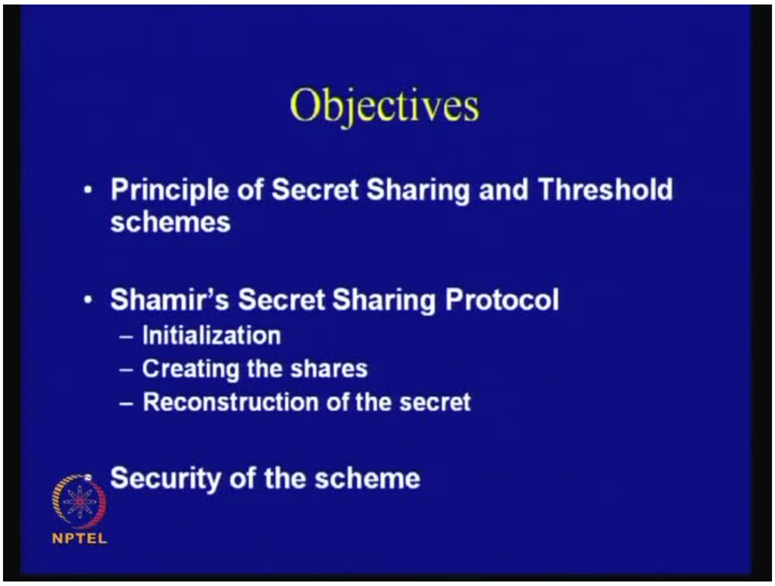
Indian Institute of Technology, Kharagpur

Module No. # 01

Lecture No. # 37

Secret Sharing Schemes

(Refer Slide Time: 00:26)

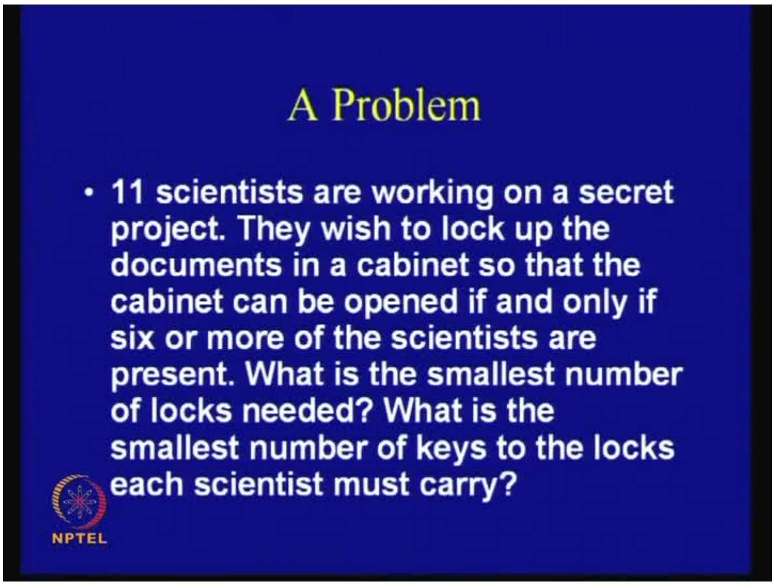


Objectives

- Principle of Secret Sharing and Threshold schemes
- Shamir's Secret Sharing Protocol
  - Initialization
  - Creating the shares
  - Reconstruction of the secret
- Security of the scheme

Welcome to today's class on secret sharing schemes. So, in today's class, we shall essentially discuss about a very interesting technique of sharing secrets. So, it is also commonly referred to as a threshold scheme and it is based on Shamir's secret sharing protocol. And, which actually tells us, how to share the secrets between a set of users. So, and we shall also discuss about, how to initialize this scheme, how to create the shares, how to reconstruct the secret and what is the essential security of the scheme. So, this is the broad aim of today's class.

(Refer Slide Time: 01:08)



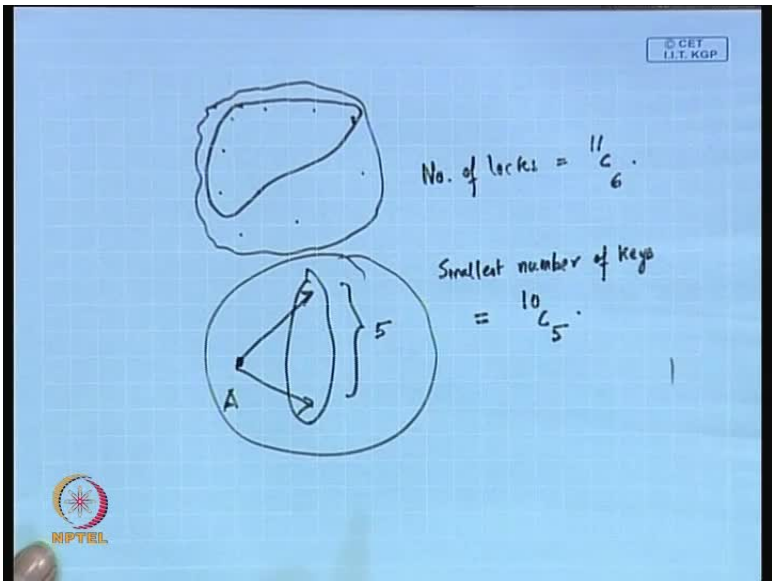
A Problem

- 11 scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry?

So, to start with, let us consider a problem. So, it is a commentarial problem. So, consider that, suppose, there are 11 scientists who are working on a secret project and they wish to lock up the documents in a cabinet, so that, the cabinet can be opened if and only if, 6 or more of the scientists are present.

That means, there are 11 scientists who are working on the problem or on the project and if and only if 6 or more of the scientists combine, then, they should be able to understand the secret project. So, the questions which can come or arise are as follows; like, what is the smallest number of locks needed? So, the, just think that, it is kind of a…We often apply interlocks to our doors; therefore, it is a similar kind of problem. So, the question which can arise is, what is the smallest number of locks which are needed and the other question is, what is the smallest number of keys to the locks, each scientist must carry.

(Refer Slide Time: 02:24)



No. of locks = ${}^{11}C_6$.

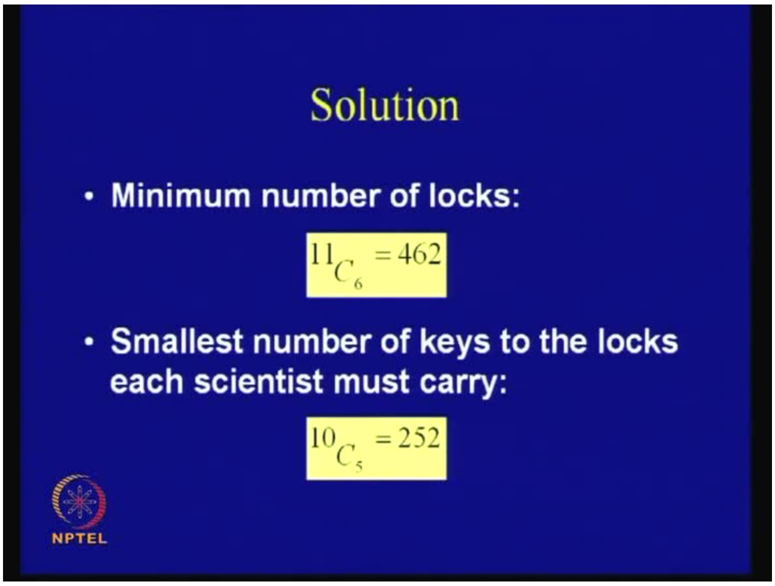
Smallest number of keys = ${}^{10}C_5$.

So, how do we essentially solve this problem? So, you see that, the problem essentially can be visualized like this. So, there is a set like this, and suppose, there are 11 members in this project. So, I am not exactly given it, but is suppose, there are 11 people here; out of them, if 6 people combine, then, they should be able to understand the project, understand the secret.

So, therefore, the question is, what is the smallest number of locks that are needed? So, you can immediately compute that, that means, there, the number of locks means what? That is, if there are 11 people, what a possible solution can be like this. That is, you choose any 6 people and for any chosen 6 people you keep a dedicated lock. So, that means, the number of locks which are needed or the number of ways how you can actually choose 6 from 11. Therefore, the number of locks can be computed to be this, is equal to 11 choose 6. The next question is, what is the smallest number of keys to the locks, each scientist must carry?

So, therefore, for that, you have to understand that, a given scientist can be a member of how many such groups of 6 people. So, that means, you can see that, immediately that, if the group has got 6 people, a particular scientist will form a membership with how many scientists? With 5 scientists. So, there are 5 scientists with whom this particular scientist, say scientist A is can form a membership. So, therefore, if you leave out this particular scientist, there are 10 people apart from this scientist A. And, therefore, the smallest number of keys; obviously, you can keep larger number of, number than that, that at least you need these many number of keys, can be found out by the number of ways; you can actually choose these 5 people from the remaining 10 people. So, that means, it is 10, choose 5.

(Refer Slide Time: 05:03)



Solution

- Minimum number of locks:

$$\boxed{{}^{11}C_6 = 462}$$

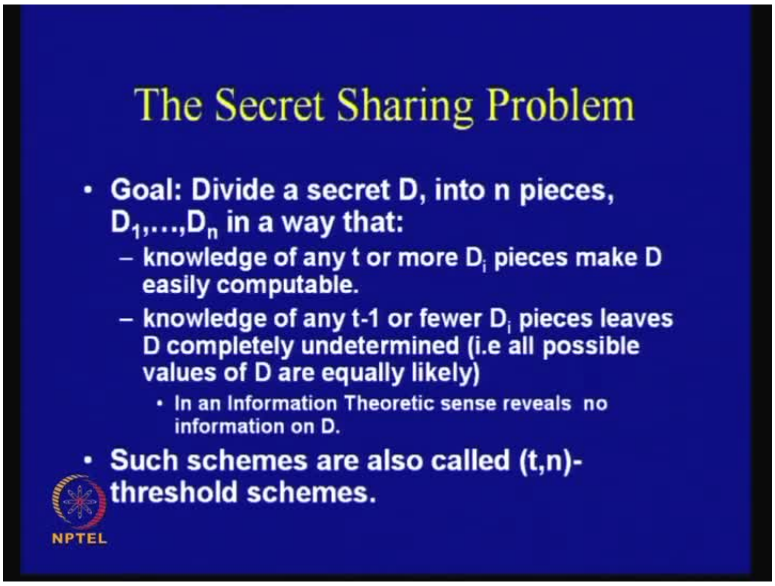
- Smallest number of keys to the locks each scientist must carry:

$$\boxed{{}^{10}C_5 = 252}$$

So, therefore, you can immediately calculate that the number of locks or the minimum number of locks, which are necessary are 462 and the minimum number of or the smallest number of keys to the locks each scientist must carry, is equal to 252. So, therefore, you see that, even for a small problem which has got 11 people and we want a scheme, where 6 people if they combine, they should, they can understand or deduce the secret, then, then a this kind of scheme requires very large number of locks and keys.

So, therefore, the objective of developing an efficient secret sharing scheme, is to find out a mechanism, through which you can actually divide the secret amongst n people, such that, out of them, if t people, where t is less than n, if they combine, they should be able to find out the secret, but the scheme should be efficient, which means that the number of locks or the number of keys should be small; that means, the computational over it should be as minimum as possible.

(Refer Slide Time: 06:07)

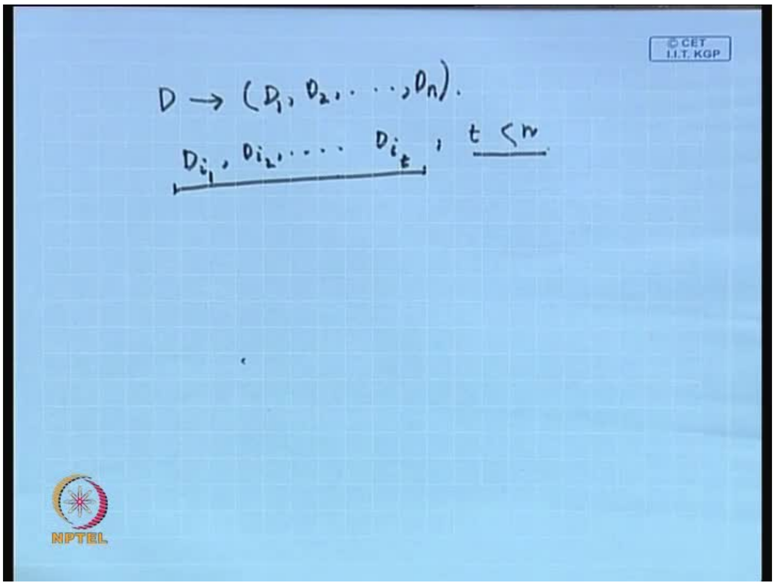


The Secret Sharing Problem

- Goal: Divide a secret D, into n pieces, $D_1, \ldots, D_n$ in a way that:
  - knowledge of any t or more D_i pieces make D easily computable.
  - knowledge of any t-1 or fewer D_i pieces leaves D completely undetermined (i.e all possible values of D are equally likely)
    - In an Information Theoretic sense reveals no information on D.
- Such schemes are also called (t,n)-threshold schemes.

So, therefore, we will formally define the secret sharing scheme. It is as follows: the goal is to divide a secret D into n pieces. So, there is a secret D, which I would like to divide among n pieces.

(Refer Slide Time: 06:25)

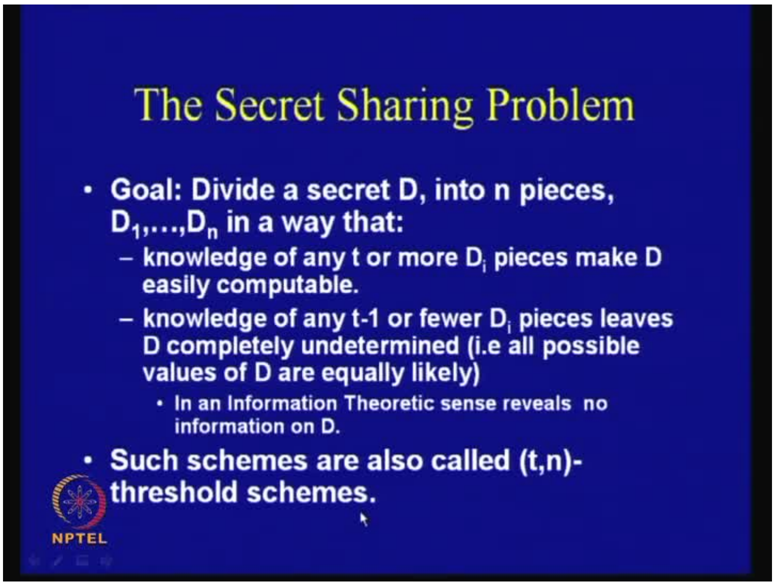


$D \rightarrow (D_1, D_2, \ldots, D_n).$

$\underbrace{D_{i_1}, D_{i_2}, \ldots D_{i_t}}, \ \underline{t < n}$

So, there is a secret D and I want to, and I want to divide that into n such pieces. Then, the idea is that, if out of them, if I can actually find out t such shares, that is, t i D i 1, D i 2 and so on till D i t, if I can find out t such shares, where t is less than n, then, if t is less than n and if you can actually obtain these many shares, then, you should be able to obtain or deduce back the secret; but if the number of shares is less than t, that is, it is, even if it is t minus 1, then, the information which is leaked about D should be ideally 0. That is the adversary or whether the adversaries, if there are t minus 1 people who are combining, they should not be able to recover the secret.

(Refer Slide Time: 07:43)



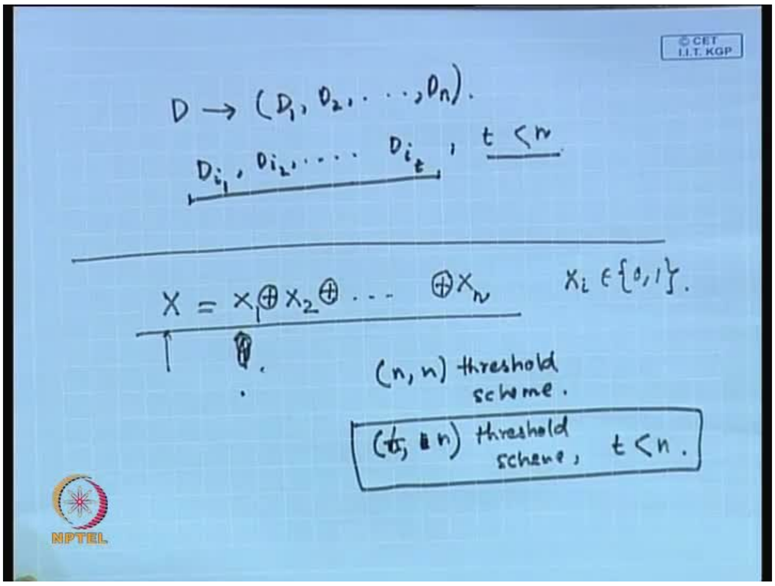
The Secret Sharing Problem

- Goal: Divide a secret D, into n pieces, $D_1,\ldots,D_n$ in a way that:
  - knowledge of any t or more D_i pieces make D easily computable.
  - knowledge of any t-1 or fewer D_i pieces leaves D completely undetermined (i.e all possible values of D are equally likely)
    - In an Information Theoretic sense reveals no information on D.
- Such schemes are also called (t,n)-threshold schemes.

So, therefore, the knowledge of any t or more D i pieces makes D easily computable, but the knowledge of any t minus 1 or fewer D i pieces, leaves D completely undetermined, that is, all possible values of D are equally likely. So, when we are saying that, all possible values of D are equally likely, we are actually saying that in an information theoretic sense; that means, it reveals no information on D.

So, these kind of schemes are commonly referred to as the t comma n threshold schemes; that means, there are t players; if they combine out of these n players, they are able to deduce the secret, but if there are t minus 1 or fewer players, sub shares, then, that does not reveal any information about the secret which is being shared. So, you can immediately understand that, these kind of protocols or these kind of techniques can have varied number of applications; like, one possible applications could be in distributed file systems, where you want to security as well. So, therefore, you know that, if so many people combine, then, you can actually deduce back the secret; that if it is lesser than that, then you are not able to deduce the secret.

(Refer Slide Time: 09:02)



$D \rightarrow (D_1, D_2, \ldots, D_n)$.

$\underline{D_{i_1}, D_{i_2}, \ldots D_{i_t}}$, $\underline{t < n}$

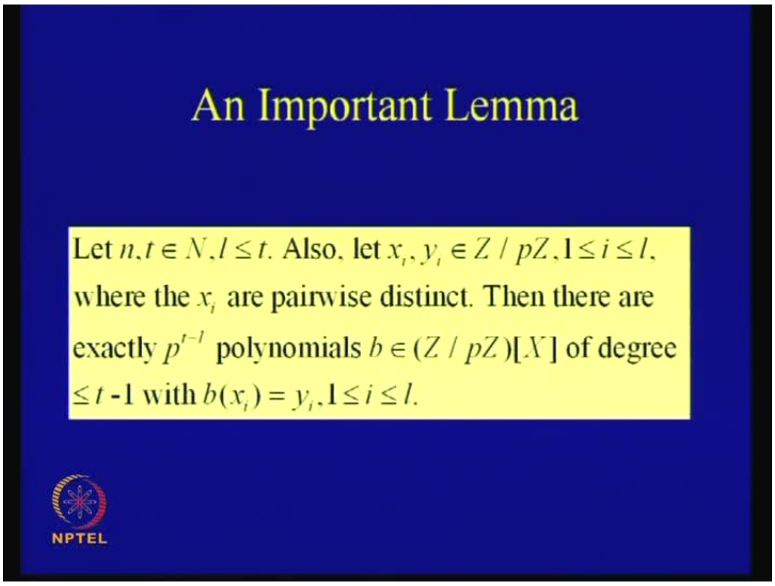
$\underline{X = x_1 \oplus x_2 \oplus \ldots \oplus x_n}$ $x_i \in \{0,1\}$.

(n, n) threshold scheme.

$\boxed{(t, n) \text{ threshold scheme}, \ t < n.}$

See, consider this simple example. That is, suppose, there are, consider some binary or whether vectors like x 1, x 2 and so on till x n. So, consider this function, that is, if I take the, the bitwise xor of these like x 1 xor x 2 xor x n; so, you can consider that all of them are 1 bit values, that is, any x i is a number of 0 or 1. So, consider this xor sum. So, if there is xor sum is x, that is, x is equal to x 1 xor x 2 so on till x n, then, you see that, in order to find out the value of x, we actually require n values, is it not? So, if there are n minus 1 such values, which are being obtained, then, what is the information leakage about x? It is 0, right; because, even if you do not have one such contribution, then, the value of x can be either 0 or 1, with the equal probability. So, therefore, this is an example of an n comma n threshold scheme, right. So, this is an example of an n comma n threshold scheme. Now, more interestingly, we want to, actually find out a technique, which is lesser than that, that is, which is actually a t comma n threshold scheme, where t is less than n. So, how to device a mechanism which is like this?

(Refer Slide Time: 10:48)

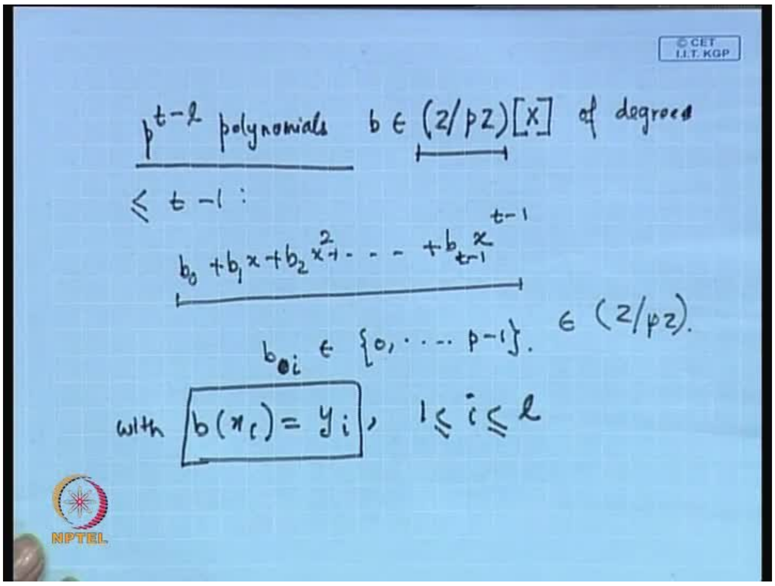


An Important Lemma

Let $n, t \in N, l \le t$. Also, let $x_i, y_i \in Z / pZ, 1 \le i \le l$, where the x_i are pairwise distinct. Then there are exactly p^{t-l} polynomials $b \in (Z / pZ)[X]$ of degree $\le t$ -1 with $b(x_i) = y_i, 1 \le i \le l$.

Do you understand the problem? So, for this, first of all, let us consider an important lemma. It says that, let N comma t, are the members of natural numbers and l is lesser than equal to t. So, that is value l which is lesser than equal to t. Also, let x i y i belong to Z. So, that is, the, basically the congruence set, that is, again it is comprising of Z and z p Z; that means, that, it is the congruence set which is generated by p, that is p is say a pi number; you can actually generate from 0 to p minus 1. So, consider that x i and y y i, which are actually n minus from 0 to p minus 1 and let 1 is less than equal to i is less than equal to l, where the x is are pair-wise distinct. So, the x is are pair-wise distinct and what the theorem says is that, then, there are exactly p to the power of t minus l polynomials and the polynomials are given like this.

(Refer Slide Time: 12:00)



$\underline{p^{t-l} \text{ polynomials}}$ $b \in \underline{(Z/pZ)}[x]$ of degrees

$\leq t-1$:

$$\underline{b_0 + b_1 x + b_2 x^2 + \dots + b_{t-1} x^{t-1}}$$

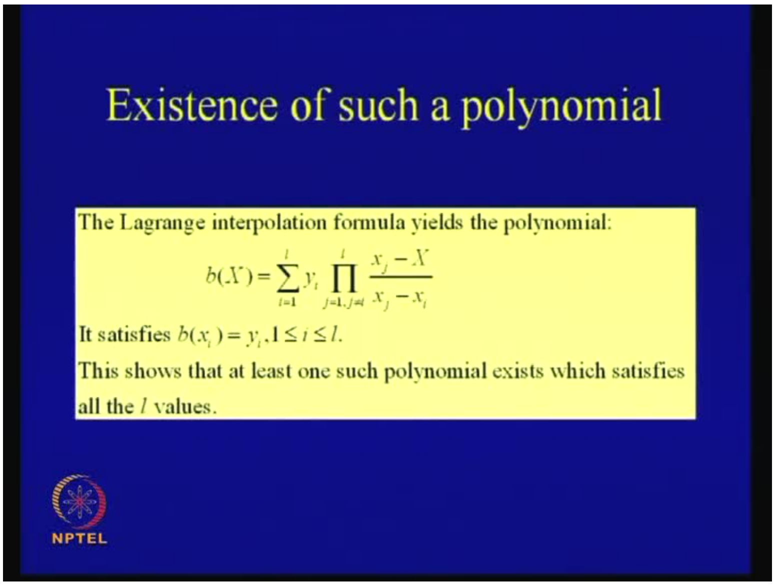
$b_{\bullet i} \in \{0, \dots, p-1\}. \in (Z/pZ).$

with $\boxed{b(x_i) = y_i}$, $1 \leq i \leq l$

So, there are exactly p to the power of t minus l polynomials and the polynomials are given like this; so, which means that, the polynomials are, polynomials when ((integrity)) is x and the coefficients of polynomials are belonging to this set; that is, they are numbers from 0 to p minus 1, ok. And, the degree of this polynomial, of these polynomials is less than or equal to t minus 1. So, what are therefore, what are the possible values of a polynomials? Polynomials could be like b 0 plus b 1 x plus b 2 x plus so on till x to the power of t minus 1, that is, the degree b, is it not? We are going series a square. So, t minus 1.

So, this is a possible polynomial and what are these coefficients? Any b 0 or any b i for that matter, belongs to from 0 to p minus 1; that means, it belongs to this particular set. And it says that, there are exactly p to the power of t minus l polynomials with these degree and etcetera, such that, with b of x i be equal to y i for all i, varying from 1 to l; tThat means, that the polynomial satisfies this equation; that is, if you take x i, if you take x 1, x 2 and so on till x l, then all of them are equal to, I mean, like b of x i b of x 1 is equal to y 1, b of x 2 is equal to y 2 and so on till b of x l equal to y i. And how many such polynomials can we construct? There are exactly p to the power of t minus l such polynomials which we can construct. Now, why so?

(Refer Slide Time: 14:30)



Existence of such a polynomial

The Lagrange interpolation formula yields the polynomial:

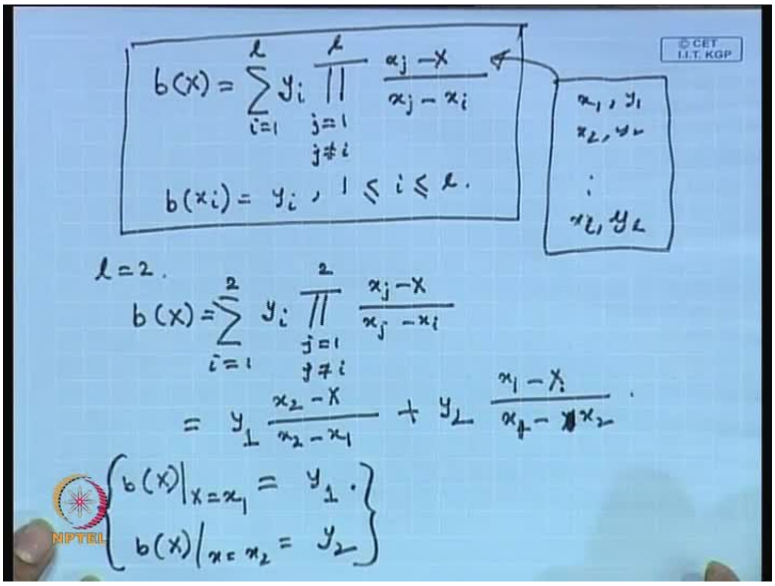
$$b(X)=\sum_{i=1}^{l} y_i \prod_{j=1,j\neq i}^{l} \frac{x_j - X}{x_j - x_i}$$

It satisfies $b(x_i)=y_i, 1\le i\le l$.

This shows that at least one such polynomial exists which satisfies all the l values.

So, in order to understand that, we consider the Lagrange's interpolation formula.

(Refer Slide Time: 14:38)



$$b(X)=\sum_{i=1}^{l} y_i \prod_{\substack{j=1\\ j\neq i}}^{l} \frac{x_j - X}{x_j - x_i}$$

$$b(x_i)=y_i,\quad 1\leqslant i\leqslant l.$$

x_1, y_1

x_2, y_2

$\vdots$

x_l, y_l

$l=2.$

$$b(X)=\sum_{i=1}^{2} y_i \prod_{\substack{j=1\\ j\neq i}}^{2} \frac{x_j - X}{x_j - x_i}$$

$$= y_1 \frac{x_2 - X}{x_2 - x_1} + y_2 \frac{x_1 - X}{x_1 - x_2}.$$

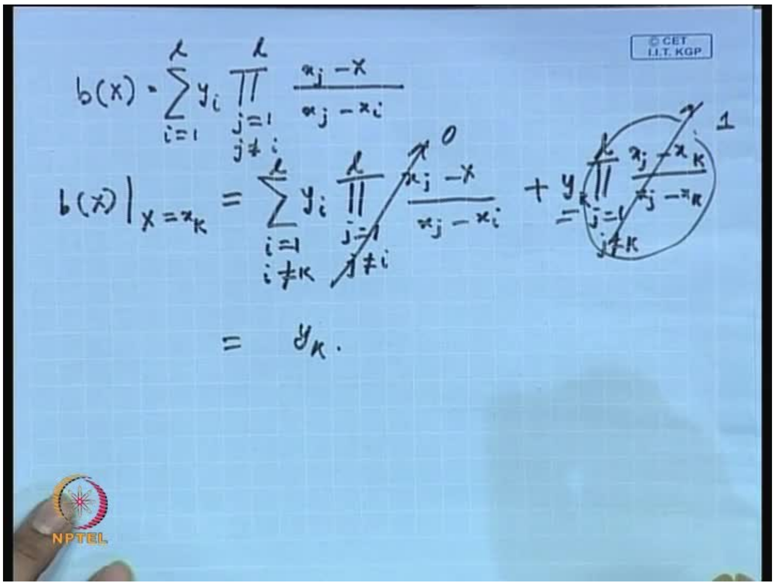
$$\left\{\begin{array}{l} b(X)\big|_{X=x_1} = y_1. \\ b(X)\big|_{x=x_2} = y_2 \end{array}\right\}$$

So, the Lagrange's interpolation formula says that, if you have got a polynomial b X, which is constructed as follows, you take a sigma over y i, where i varies to from 1 to l and then, there is a product from j equal to 1, j not equal to i till l, I will take x j minus X divided by x j minus x i.

So, this polynomial will satisfy b of x i equal to y i for all such is which lies from 1 to l. So, that means, this is what the Lagrange's interpolation formula says; that means, it is kind of like, if I have got points like x 1 y 1, x 2 y 2 and so on till x l y l, then, I can, using the Lagrange's interpolation formula, I can actually calculate or compute this polynomial, for which all these relations are satisfied, at all these l points; which means that, there exists one such polynomial, which satisfies all the l values, right. Then, what we have to show actually is that, there are p to the power of t minus l such polynomials, for which this holds. In order to understand little bit or appreciate this algorithm or rather this interpolation polynomial, you can consider the case where l is equal to 2. So, consider the case where l is equal to 2; so, that means, your b X will be i varies from 1 to 2 and this is y i and this is x j minus X, x j minus x i, j equal to 1, j is not equal to i and it varies till 2. So, what is that; that means, that, this is equal to y 1 and that will be multiplied by x 2 minus X divided by x 2 minus x 1, right; plus y 2 and that is multiplied by x 1 minus x divided by x 2 minus, x 2 minus… So, this is x 1 minus x and that is x 1 minus x 2, right. Is it correct?

So, now we will see that, in this polynomial, if you write b X and you compute it at the value of x b equal to say x 1, then, if you substitute here x 1, then, this x 2 minus x 1 by x 2 minus x 1 this value becomes equal to 1. So, what is this? This is y 1 plus y 2 multiplied by this value goes to, goes to what? Goes to 0. If you plug in here, x equal to x 1, then, this term goes to 0. So, we have got only y 1. Then, what about, if you compute this at the point x equal to x 2, this is similarly, equal to y 2, because that, this goes to 0. So, you see that, this interpolation works for l equal to 2, right. So, similarly, you can actually prove that, this holds for any l actually. So…

(Refer Slide Time: 18:18)



$$b(x) = \sum_{i=1}^{l} y_i \prod_{\substack{j=1\\ j\neq i}}^{l} \frac{x_j - x}{x_j - x_i}$$

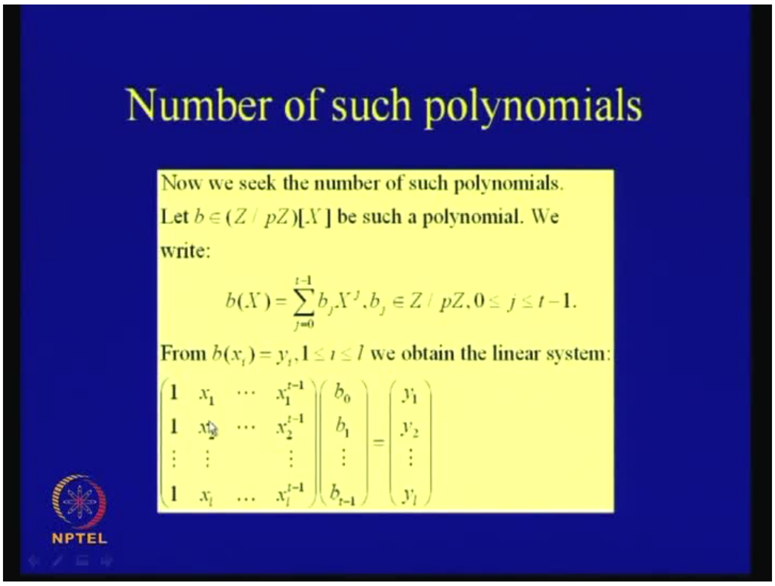
$$b(x)\Big|_{x=x_K} = \sum_{\substack{i=1\\ i\neq K}}^{l} y_i \overset{0}{\cancel{\prod_{\substack{j=1\\ j\neq i}}^{l} \frac{x_j - x}{x_j - x_i}}} + y_K \overset{1}{\cancel{\prod_{\substack{j=1\\ j\neq K}}^{l} \frac{x_j - x_K}{x_j - x_K}}}$$

$$= y_K .$$

So, therefore, you can actually say that, your b x… So, then I am writing down this, b x is equal to y i. So, for the general case, was equal to j equal to 1, j not equal to I, i equal to 1 to l, and this goes to j, this is x j minus X divided by x j minus x I; this was the original formula. So, let us compute this value of b x at the point of x equal to some value, say x k. Let us compute this value of b x at the point of x equal to x k. So, that is equal to, we again take this sigma y i from i equal to 1 to, I mean, this is i, say suppose, i is not equal to k; and this varies from 1 to l and then, you have got y i and then, pi, j equal to 1, j not equal to i, l, x j minus X divided by x j minus x i plus their value when this is equal to k. So, that is y k, then the product term has got x j minus x k divided by x j minus x k, for all the terms.

So, that is j equal to 1, j not equal to k, varying till l, is it correct. So, you see that, for all these things is what, this is 1, right and for all these things, if you see that, one of the terms we will actually have x j. So, which means that, this product will go to, go to 0; because, there really is one such case where x j minus x j will occur, right. And, therefore, this will go to 0; this particular thing will go to 0; this will go to 1 and therefore, you will be remaining with only this point y k. So, therefore, this holds for any k and therefore, for all the l values the Lagrange’s interpolation formula, formula, indeed gives us one such polynomial. Then, what we essentially have to find out, also, I give you that, according to the theorem that, there are p to the power t minus l such polynomials of degree less than equal to t minus 1, where all such, the all are reviles hold.

(Refer Slide Time: 20:51)



Number of such polynomials

Now we seek the number of such polynomials.
Let $b \in (Z / pZ)[X]$ be such a polynomial. We write:

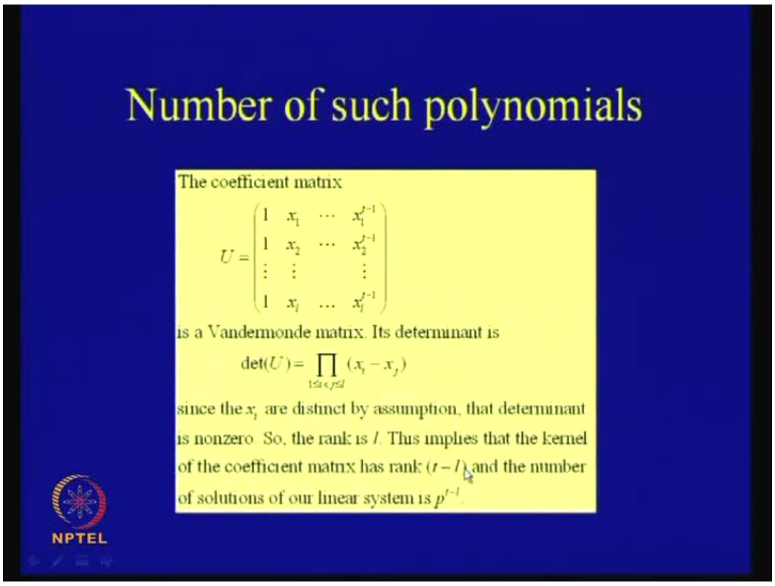
$$b(X) = \sum_{j=0}^{t-1} b_j X^j, b_j \in Z / pZ, 0 \le j \le t-1.$$

From $b(x_i) = y_i, 1 \le i \le l$ we obtain the linear system:

$$\begin{pmatrix} 1 & x_1 & \cdots & x_1^{t-1} \\ 1 & x_2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_l & \cdots & x_l^{t-1} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_l \end{pmatrix}$$

So, for that, we have actually to go little bit into matrix algebra. Now, in, also seek to calculate the number of such polynomials. So, let, gives me such polynomial and we have already seen that, this is the form of the polynomial; that is, sigma j equal to 0 till t minus 1 b j x to the power of j where each b j, that is each coefficient belongs to Z p Z; that means, it is from 0 to p minus 1 and for all j, for all such js from 0 to t minus 1. So, therefore, if I made a b of x i is equal to y i, then, for all these values, we can actually write down in this matrix notation, is it not? That is, we can always write this in this matrix notation, because you know that, all these are essentially polynomials. So, therefore, if you consider the first one, that is, you take x I, you just take b of x 1 is equal to y 1, that is this particular thing; that is 1 into b 0 plus b 1 x plus so on till b t minus 1 x 1 t to the power of minus 1, is equal to y 1, right. So, all these l equations are written in the form a matrix.

(Refer Slide Time: 22:17)



Number of such polynomials

The coefficient matrix

$$U = \begin{pmatrix} 1 & x_1 & \cdots & x_1^{t-1} \\ 1 & x_2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_l & \dots & x_l^{t-1} \end{pmatrix}$$

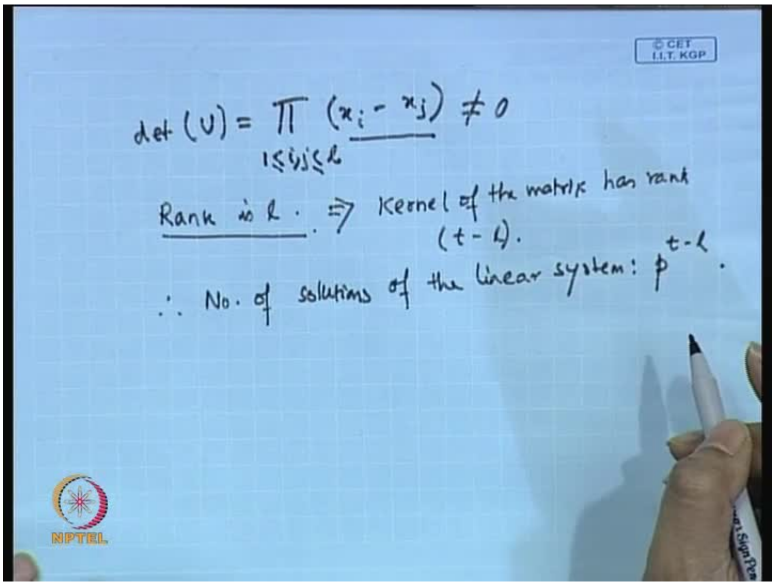
is a Vandermonde matrix. Its determinant is

$$\det(U) = \prod_{1 \le i < j \le l} (x_i - x_j)$$

since the x_i are distinct by assumption, that determinant is nonzero. So, the rank is l. This implies that the kernel of the coefficient matrix has rank $(t - l)$ and the number of solutions of our linear system is p^{t-l}.

So, therefore, now, the question is that, what is the… Therefore, this… Is this matrix notation clear? Right. So, the question is now, that, this is the coefficient matrix and this coefficient matrix we will, we can study a little bit. So, this is actually, commonly known as the Vandermonde’s matrix and its determinant is given by this thing; that is, it is the product of x i minus x j, where i and j ranks from 1 to l.

(Refer Slide Time: 22:42)



$$\det(U) = \prod_{1 \le i,j \le l} \underline{(x_i - x_j)} \ne 0$$

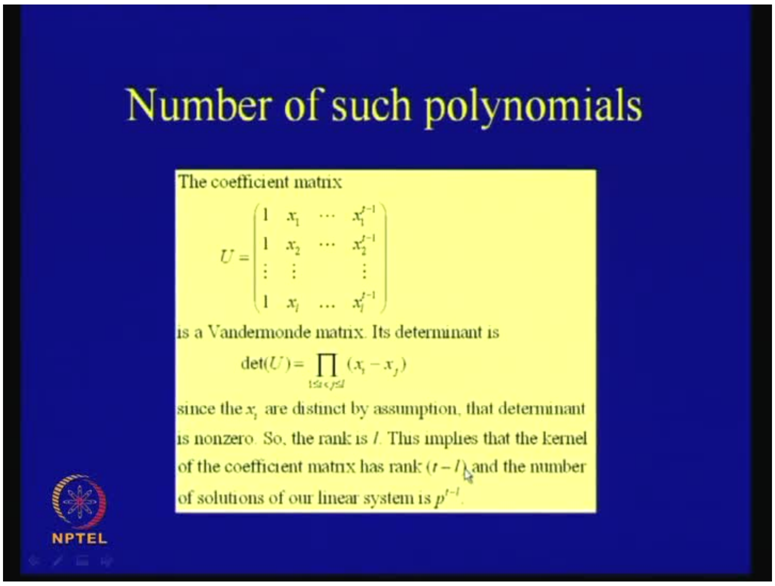
$\underline{\text{Rank is } l}$. $\Rightarrow$ Kernel of the matrix has rank $(t - l)$.

$\therefore$ No. of solutions of the linear system: p^{t-l}.

So, you see that, the determinant of this Vandermonde’s matrix is given by this product, x i minus x j where i and j ranks from 1 to l. So, we note that, if x i and x j are always distinct, that is, they are never same; that is all the x values are distinct, so, that means, that , if that, this, this is a nonzero determinant; and if the determinants are, is a nonzero value, so, the rank of this matrix is actually l.

So, therefore, the rank of the, rank is l, for this matrix the rank is l. and, this implies that, the kernel of the matrix, going back to your matrix algebra classes, kernel of the matrix has rank t minus l. Therefore, the number of solutions of the linear system, that is, a linear matrix system, is actually p to the power of t minus l. So, you can just consider a special case; if your t and l are same, right. Then, how many such solutions are there? There is exactly one solution, right. That is, when your t and l are exactly equal to, equal to each other, then, we have got exactly one solution to the linear system, but as long as your l is, I mean, your t is greater than l, you have got more than one solutions. Is it not so?

(Refer Slide Time: 22:17)



Number of such polynomials

The coefficient matrix

$$U = \begin{pmatrix} 1 & x_1 & \cdots & x_1^{t-1} \\ 1 & x_2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_l & \ldots & x_l^{t-1} \end{pmatrix}$$

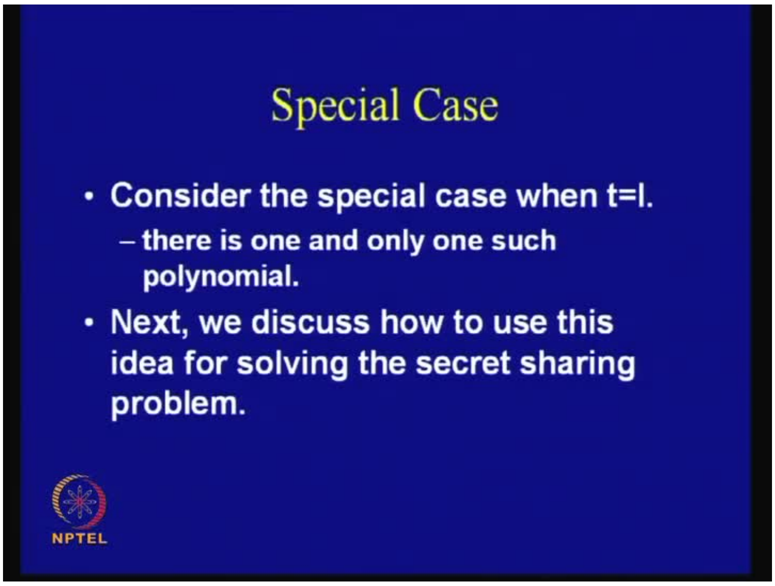
is a Vandermonde matrix. Its determinant is

$$\det(U) = \prod_{1 \le i < j \le l} (x_i - x_j)$$

since the x_i are distinct by assumption, that determinant is nonzero. So, the rank is l. This implies that the kernel of the coefficient matrix has rank $(t-l)$ and the number of solutions of our linear system is p^{t-l}.

So, that means, there are so many matrices; and this is a very important and interesting observation and result, which is used in Shamir’s secret sharing scheme, right. So, this proves the first theorem, that the first lemma, that is, there are exactly p to the power of t minus l polynomials of degree less than equal to t minus 1, which actually satisfies all the relations, all the l relations, all the l pairs x 1 x 2 and so on till x l y l.

(Refer Slide Time: 25:09)

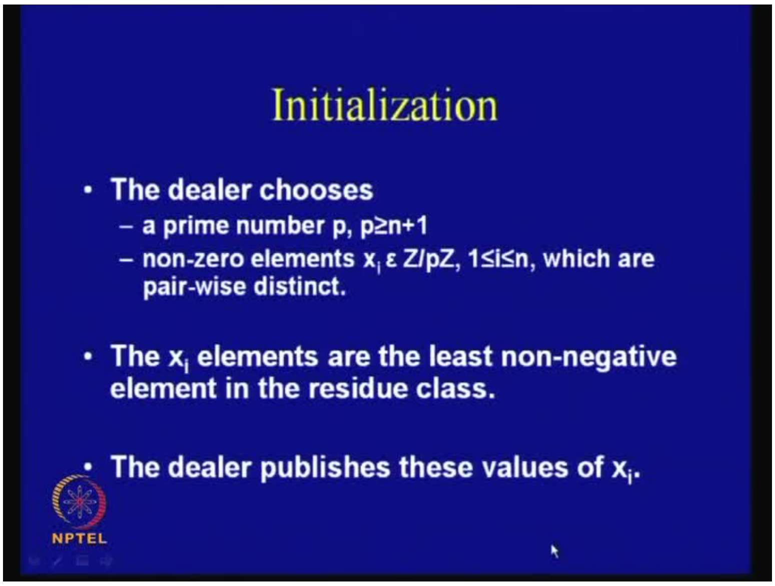


Special Case

- Consider the special case when t=l.
  - there is one and only one such polynomial.
- Next, we discuss how to use this idea for solving the secret sharing problem.

So, therefore, consider a special case, when t is equal to l, there is one and only one such polynomial for this, for which this holds, right. And next, we will discuss, how to use this idea for solving the secret sharing problem.

(Refer Slide Time: 25:29)



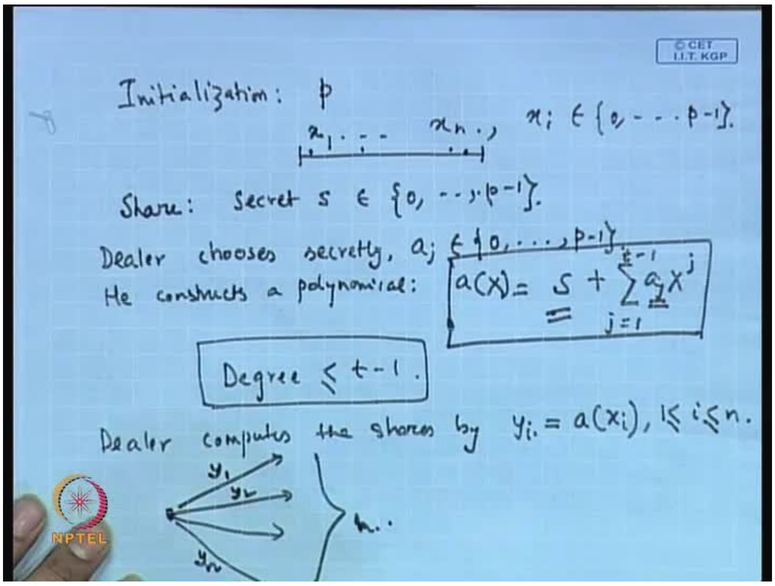
Initialization

- The dealer chooses
  - a prime number p, $p \geq n+1$
  - non-zero elements x_i ε Z/pZ, $1 \leq i \leq n$, which are pair-wise distinct.
- The x_i elements are the least non-negative element in the residue class.
- The dealer publishes these values of x_i.

So, for that, let us consider this initialization. What the dealer does is that, the dealer chooses a prime number p, where p is greater than equal to n plus 1 and non-zero elements x i belonging to again 0 to p minus 1, and i is varied from 1 to n, which are always a load back, all these values of x are actually pair-wise distinct.

So, this pair-wise distinctness is, because we wanted the Vandermonde's matrix to be, to have a non-zero determinant, right. So, therefore, that, all of them are pair-wise distinct and the x i elements are therefore, the least non-negative element in the residue class; there will be, this is a residue class of Z p Z and it is the least non-negative element; so, that means, it varies from 0 to p minus 1. And, the dealer publishes these values of x i. Therefore, these values of x i are actually published by the dealer. So, that is the basic initialization phase, which is being followed.

(Refer Slide Time: 26:35)



Initialization: p

$x_1 \cdots x_n$, $x_i \in \{0 \cdots p-1\}$.

Share: Secret $s \in \{0, \cdots, p-1\}$.

Dealer chooses secretly, $a_j \in \{0, \ldots, p-1\}$.

He constructs a polynomial: $\boxed{a(X) = s + \sum_{j=1}^{t-1} a_j X^j}$

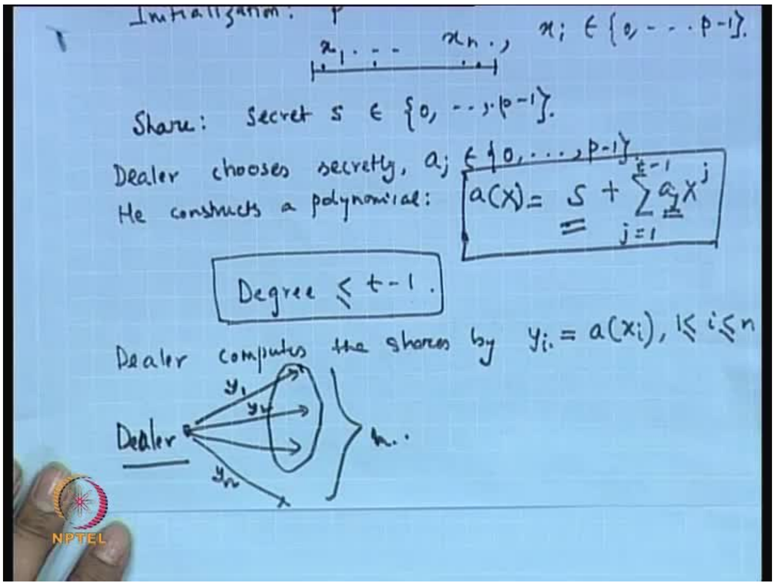
$\boxed{\text{Degree} \leq t-1.}$

Dealer computes the shares by $y_i = a(x_i)$, $1 \leq i \leq n$.

So, therefore, that initialization phase of the secret sharing scheme comprises of generating the values of… So, basically, the first thing is that, you need a prime number p and then, you need to find out values like x 1 till x n, such that all x is are actually from 0 to p minus 1, right. And, these values like x 1 to x n are actually published by the dealer. So, now, we have to prepare the shares. So, what is the share? how is the share prepared? So, let that, there is a secret s, which I want to share; that is, in order to preparing the share, suppose, the secret is some value s, which again lies between 0 to p minus 1. So, what the dealer does is, the dealer secretly chooses some coefficients of a polynomial. So, what the dealer does is that, the dealer chooses secretly a j, where a j varies from 0 to p minus 1 and constructs a polynomial. So, he constructs a polynomial of this nature; that is, a X is given by s, which is the constant, plus sigma of a j X to the power of j and j is being varied from 1 to t minus 1. So, this is the polynomial which the dealer creates secretly.

So, what the dealer does is that, he chooses these coefficients secretly and adds or rather keeps s which is the secret, as the constant of the polynomial, right. And then, what the dealer does? What is the degree of this? The degree of this is lesser than equal to t minus 1, right. Depending upon your a j, because your a js can be 0s also, right. Therefore, the degree is maximum equal to t minus 1. So, the degree of this polynomial is lesser than or equal to t minus 1. So, now, the dealer computes the shares. So, the dealer computes the shares by calculating all the l values, like y i, by calculating that polynomials at i points. Therefore, these could be like i, it is varied from 1 to n; for all n values, it creates n such shares. So, at x 1, x 1, for all these x 1 values, x 2 values and it is, so on till x n values, it creates y, corresponding y i values. So, what may the dealer does is that, to all the share members, right... So, suppose, there are n share members, to the n share members, it communicates y 1, y 2 and so on till y n.

(Refer Slide Time: 29:57)



Initialization: p

$x_1 \ldots x_n$, $x_i \in \{0, \ldots p-1\}$.

Share: Secret $s \in \{0, \ldots, p-1\}$.

Dealer chooses secretly, $a_j \in \{0, \ldots, p-1\}$.

He constructs a polynomial: $\boxed{a(X) = s + \sum_{j=1}^{t-1} a_j X^j}$

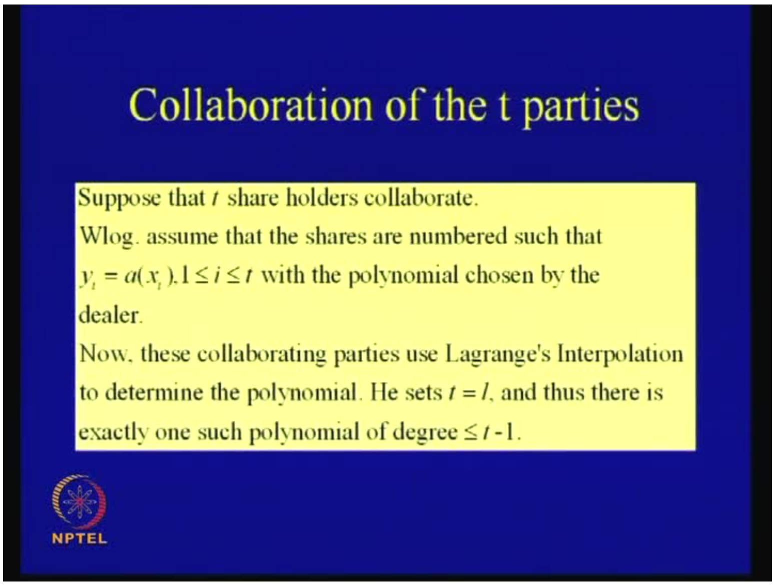
$\boxed{\text{Degree} \leq t-1.}$

Dealer computes the shares by $y_i = a(x_i)$, $1 \leq i \leq n$

Dealer
y_1
y_2
y_n
n.

So, all of, the dealer actually takes this, and communicates these to all the n users, right. So, now you know that, the secret is actually the value of a 0 of the polynomial a X and what we have to understand is that, if t members of this players combined, then, they can actually compute the corresponding constant term; because the constant term is the secret, right. Is it clear?

(Refer Slide Time: 30:35)

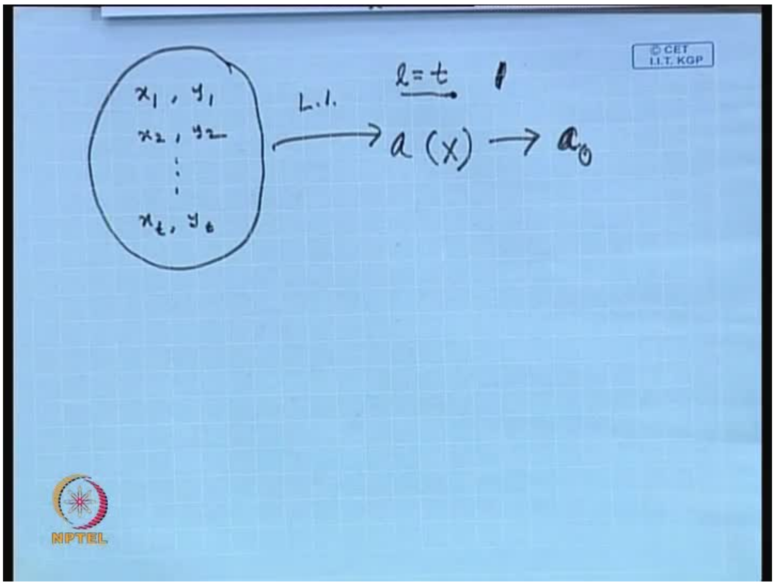


Collaboration of the t parties

Suppose that t share holders collaborate.
Wlog. assume that the shares are numbered such that $y_i = a(x_i), 1 \le i \le t$ with the polynomial chosen by the dealer.
Now, these collaborating parties use Lagrange's Interpolation to determine the polynomial. He sets $t = l$, and thus there is exactly one such polynomial of degree $\le t - 1$.

So, therefore, what the t share-holders do is that, they collaborate, right. So, they basically come together and without less of, or the loss of generality, you can assume that, the shares are numbers like y 1 till y t. So, we have got y 1, y 2, y 3 and so on, till y t and the corresponding x 1, x 2 and so on, until x t. So, what will the, these collaborating parties do? These collaborating parties can apply the Lagrange's interpolation technique, right; and then, try to find out a polynomial, such that, this polynomial should essentially fit all these t points. Now, you see that, if your t is actually equal to l, what we have seen previously, then, there is exactly one such polynomial of degree less than equal to t minus 1. So, that is exactly what the collaborating parties do. They essentially combine, such that, the objective is essentially now, to deduce the constant term of the polynomial; but for that, first of all, we need to compute that, the polynomial; because, what we, what the collaborating parties have, is only the shares.

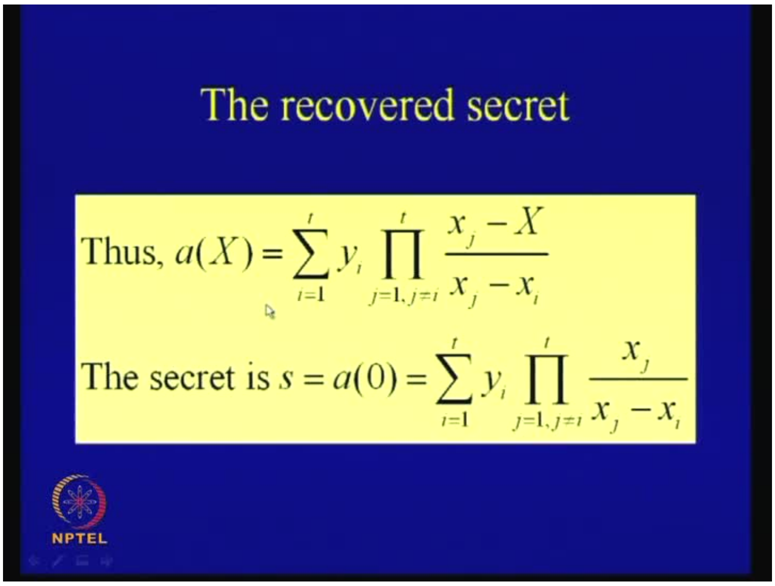
(Refer Slide Time: 32:04)



The collaborating parties… If you see the collaborating parties, they have got x 1 y 1, x 2 y 2 and so on till x t comma y t, right. So, from there, they actually apply the Lagrange’s interpolation technique, Lagrange’s interpolation technique to obtain the value of the polynomial a X.

And, if they know the corresponding polynomial a X, then, they know that, a 0 is the secret of the polynomial, right. Is it not? Right. Therefore, if you know that, the, when a polynomial was constructed by the dealer, right, if the, if the dealer had ensured that, in that polynomial, whatever you say a X or b X, in that polynomial, your t was adjusted or rather l was adjusted, such that, it is exactly equal to t, then, by the first lemma, you know that, they are all exactly, there is exactly one such polynomial for which this holds. And therefore, the Lagrange’s interpolation technique should be an efficient way to compute back the polynomial that holds are secret. So, that is the basic principle of the secret sharing scheme.

(Refer Slide Time: 33:19)

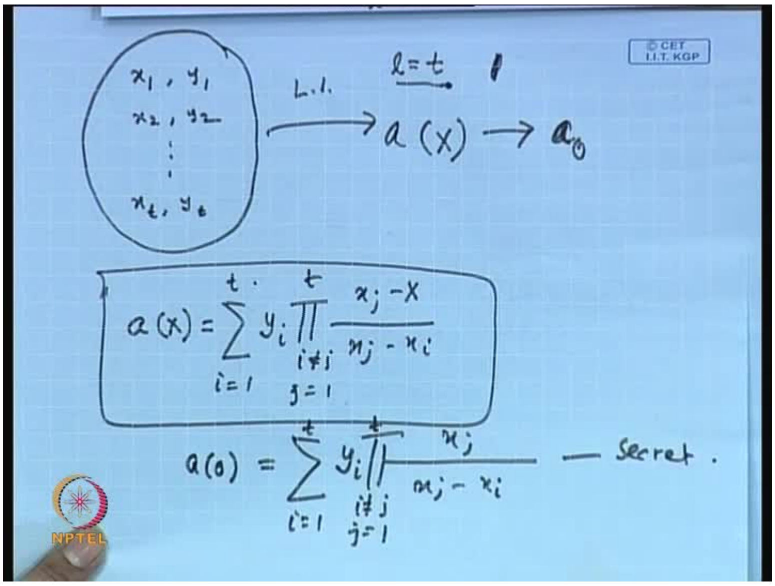


The recovered secret

Thus, $a(X)=\sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x_j - X}{x_j - x_i}$

The secret is $s = a(0) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x_j}{x_j - x_i}$

(Refer Slide Time: 33:24)



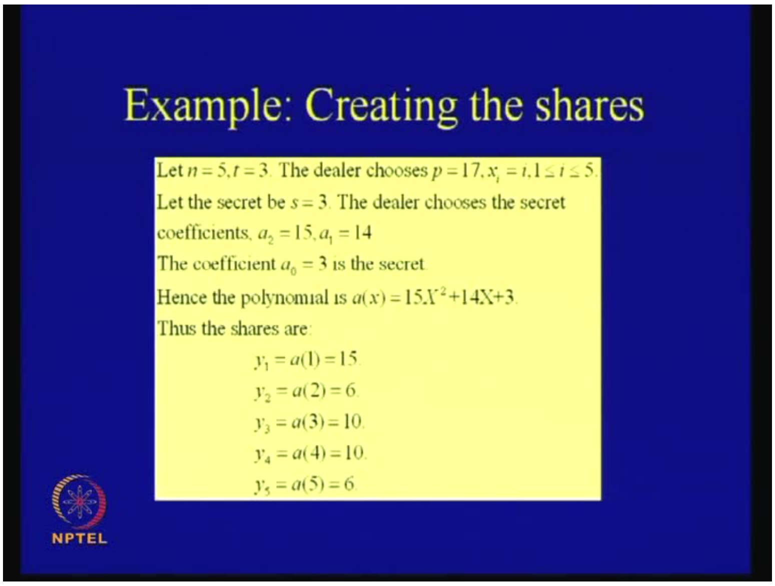
$$\boxed{x_1, y_1 \quad x_2, y_2 \quad \vdots \quad x_t, y_t} \xrightarrow{\text{L.I.}} a(X) \rightarrow a_0 \qquad l = t$$

$$\boxed{a(x) = \sum_{i=1}^{t} y_i \prod_{\substack{i\neq j\\ j=1}}^{t} \frac{x_j - X}{x_j - x_i}}$$

$$a(0) = \sum_{i=1}^{t} y_i \prod_{\substack{i\neq j\\ j=1}}^{t} \frac{x_j}{x_j - x_i} \quad \text{— Secret .}$$

So, therefore, being, I mean, you know that, the, what the users do essentially is, apply the Lagrange’s interpolation technique and compute this; that is, he takes all the y is and compute x j minus X divided by x j minus x i, i not equal to j and j varying from 1 to t and i varying from 1 to t, right. That is what the users can do, right. And you know that, your t was, is actually, I mean, when the dealer had created, this t is equal to l. So, therefore, this is actually, there is only one such polynomial, for which this fitting holds, right. So, actually, the users or the collaborating parties do not need to calculate this, this value; then, what they want is, they only want the secret a 0. So, therefore, what they actually want is only this, y I; you can actually plug 0 here and you know that, it is x j divided by x j minus x i. So, what the collaborating parties want is only this; that is, the corresponding secret. So, are we convinced, that the collaborating parties will be able to calculate back the secret? So, let us consider one example.

(Refer Slide Time: 34:52)



Example: Creating the shares

Let $n = 5, t = 3$. The dealer chooses $p = 17, x_i = i, 1 \le i \le 5$.

Let the secret be $s = 3$. The dealer chooses the secret coefficients, $a_2 = 15, a_1 = 14$

The coefficient $a_0 = 3$ is the secret.

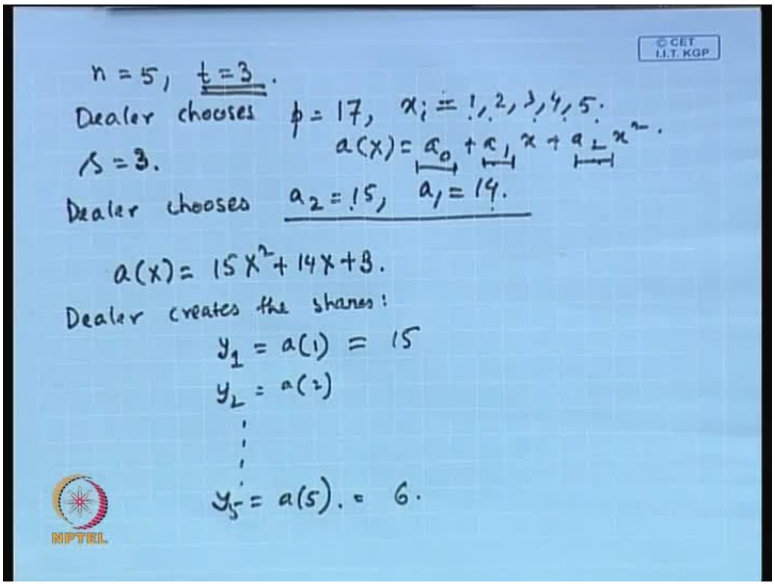
Hence the polynomial is $a(x) = 15X^2 + 14X + 3$.

Thus the shares are:

$$y_1 = a(1) = 15$$
$$y_2 = a(2) = 6$$
$$y_3 = a(3) = 10$$
$$y_4 = a(4) = 10$$
$$y_5 = a(5) = 6$$

So, let us consider a small example. So, you see that, in this example, n is chosen as 5; that means, there are 5 shares which are created and you want to ensure that, if 3 collaborating parties combine, then, they should be able to retrieve the secret.

(Refer Slide Time: 35:16)



$n = 5$, $\underline{t = 3}$.

Dealer chooses $p = 17$, $x_i = 1, 2, 3, 4, 5$.

$s = 3$. $a(x) = a_0 + a_1 x + a_2 x^2$.

Dealer chooses $\underline{a_2 = 15, \ a_1 = 14.}$

$a(x) = 15x^2 + 14x + 3$.

Dealer creates the shares:

$y_1 = a(1) = 15$

$y_2 = a(2)$

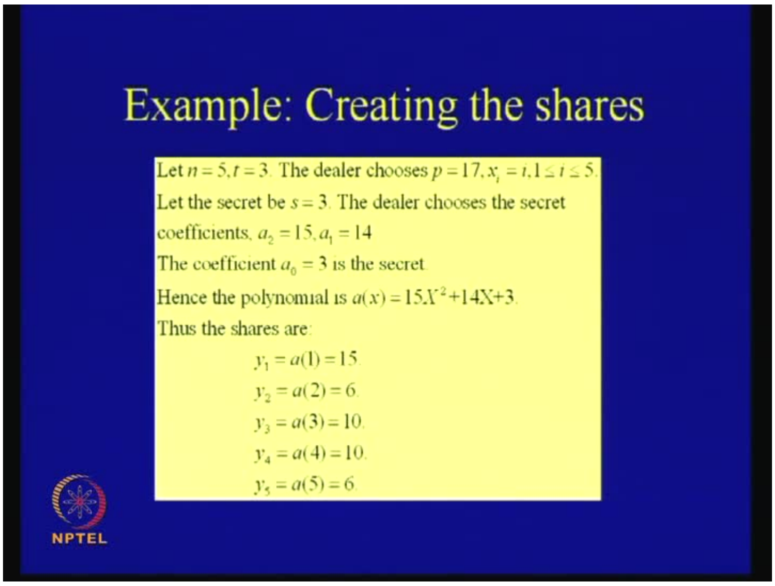
$\vdots$

$y_5 = a(5). = 6.$

So, therefore, consider this example, where there are n is equal to 5 and I want t should be equal to 3 in this special scheme. So, what the dealer does… So, first, the dealer has to create the polynomial, right. So, the dealer chooses a p which is a prime number, such that p equal to 17 and chooses some x is values. So, let us take the x i values are exactly equal to like 1, 2, 3, 4 and 5. So, that is, this x 1, x 2, x 3, x 4 and x 5 is equal to 1, 2, 3, 4 and 5. So, suppose, the secret which I want to share is the value 3. So, what the dealer does is, the dealer chooses secretly, the coefficient, say a 2, is equal to 15 and a 1 is equal 14. So, you note that, since t is equal to 3, what is the degree of the polynomial? It is t minus 1. So, it is 2. So, therefore, the polynomials nature will be like, a 0 plus a 1 x plus a 2 x squared; and I know that, a 0 is what? a 0 is a secret. So, what the dealer needs to do is that, he needs to randomly choose a 1 and a 2.

So, let this be the secret choices for a 2 and a 1. So, let a 2 be equal to 15 and a 1 be equal to 14, right. Therefore, the polynomial, which the dealer chooses is, a X equal to 15 x squared plus 14 x plus 3. And, it needs to create all the shares. Therefore, the dealer actually creates the shares in this fashion. The dealer creates the shares by computing, y 1 equal to a 1, y 2 equal to a 2 and so on; y 5 equal to a 5. So, therefore, if you just plug in these values and you check, it will be equal to like, 15 and this value will be 6; the details are here.

(Refer Slide Time: 34:52)



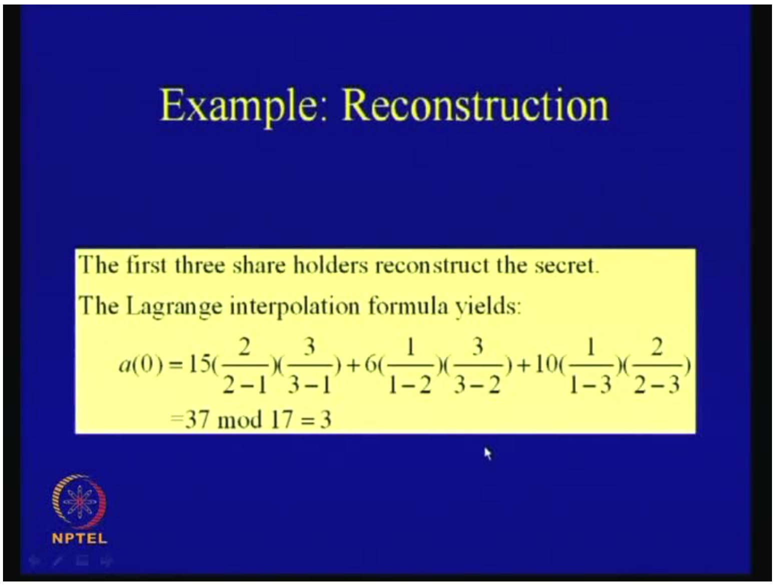
Example: Creating the shares

Let $n = 5, t = 3$. The dealer chooses $p = 17, x_i = i, 1 \le i \le 5$.
Let the secret be $s = 3$. The dealer chooses the secret coefficients, $a_2 = 15, a_1 = 14$
The coefficient $a_0 = 3$ is the secret.
Hence the polynomial is $a(x) = 15X^2 + 14X + 3$.
Thus the shares are:

$$y_1 = a(1) = 15$$
$$y_2 = a(2) = 6$$
$$y_3 = a(3) = 10$$
$$y_4 = a(4) = 10$$
$$y_5 = a(5) = 6$$

So, therefore, you see that, the shares are y 1 equal to a 1 equal to 15; y 2 equal to a 2 equal to 6; y 3 equal to a 3 equal to 10; y 4 equal to a 4 equal to 10; and y 5 equal to a 5 equal to 6. So, these are the corresponding shares which have been created. So, now, what we have to understand is that, you have to see that, if, for example, these three shares are ((revealing)) like 15, 6 and 10, that is, actually gives me this value of 3; or if that, for that values, if any 3 players combine here, they should be able to compute the value of 3. So, how many such 3 players can you choose out of 5? It will choose 3. So, 5 choose 3.

(Refer Slide Time: 38:25)



Example: Reconstruction

The first three share holders reconstruct the secret.

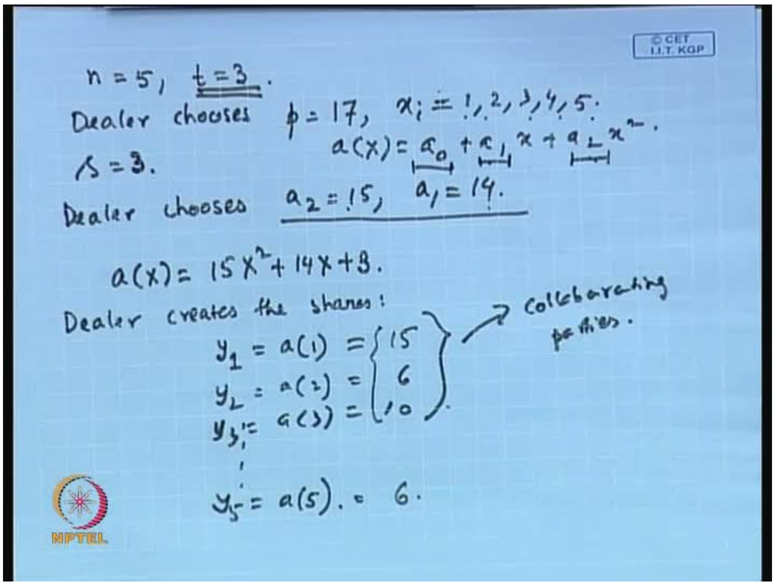
The Lagrange interpolation formula yields:

$$a(0) = 15(\frac{2}{2-1})(\frac{3}{3-1}) + 6(\frac{1}{1-2})(\frac{3}{3-2}) + 10(\frac{1}{1-3})(\frac{2}{2-3})$$

$$= 37 \bmod 17 = 3$$

So, let us see the first three share-holders, for example, combine. So, in that case, they will actually apply the Lagrange's interpolation formula there.

(Refer Slide Time: 38:43)



$n = 5, \underline{\underline{t = 3}}.$

Dealer chooses $p = 17, \; x_i = 1, 2, 3, 4, 5.$

$s = 3.$ $a(x) = a_0 + a_1 x + a_2 x^2.$

Dealer chooses $\underline{a_2 = 15, \; a_1 = 14.}$

$a(x) = 15x^2 + 14x + 3.$

Dealer creates the shares:

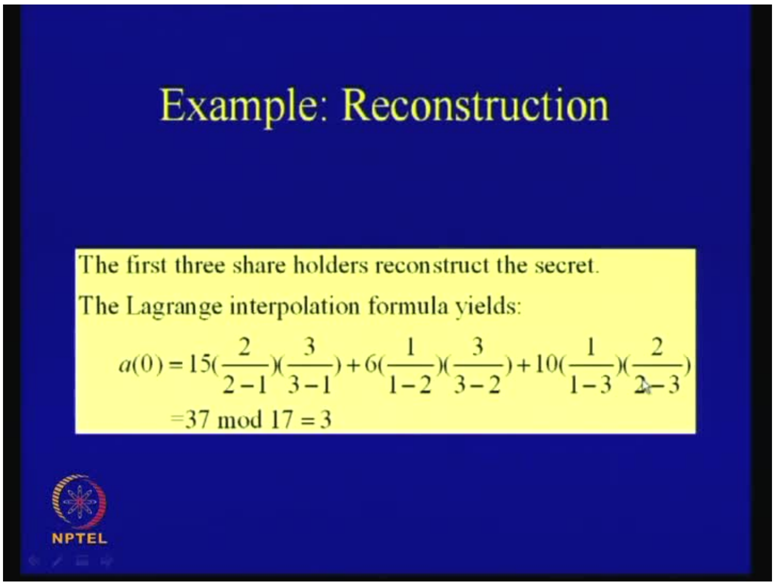
$$\left.\begin{array}{l} y_1 = a(1) = \\ y_2 = a(2) = \\ y_3 = a(3) = \end{array} \left\{\begin{array}{c} 15 \\ 6 \\ 10 \end{array}\right.\right\} \rightarrow \text{collaborating parties.}$$

$\vdots$

$y_5 = a(5) = 6.$

So, you see that, if you see, the first three members were 15 and y 3 was equal to 10. So, there were 15, 6 and 10 which are being revealed; suppose, these are being given to the collaborating parties. So, 15, 6 and 10. So, if this 15, 6 and 10 are revealed, then, what the user will do? Will apply or these collaborating parties will apply Lagrange's interpolation on this 15, 6 and 10, right. Therefore, if you apply Lagrange's interpolation on 15, 6 and 10, the polynomial is as shown here.

(Refer Slide Time: 39:23)



Example: Reconstruction

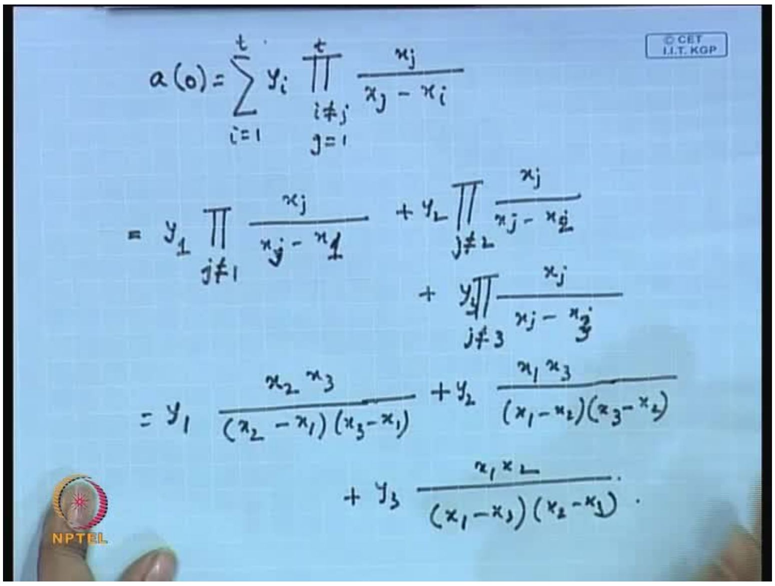
The first three share holders reconstruct the secret.

The Lagrange interpolation formula yields:

$$a(0)=15\left(\frac{2}{2-1}\right)\left(\frac{3}{3-1}\right)+6\left(\frac{1}{1-2}\right)\left(\frac{3}{3-2}\right)+10\left(\frac{1}{1-3}\right)\left(\frac{2}{2-3}\right)$$
$$=37 \bmod 17=3$$

That is, it is 15 into 2 divided by 2 minus 1 into 3 divided by 3 minus 1 plus 6 into… So, 1 by 1 minus 2 plus 3 into 3 minus 2 plus so on.

(Refer Slide Time: 39:40)



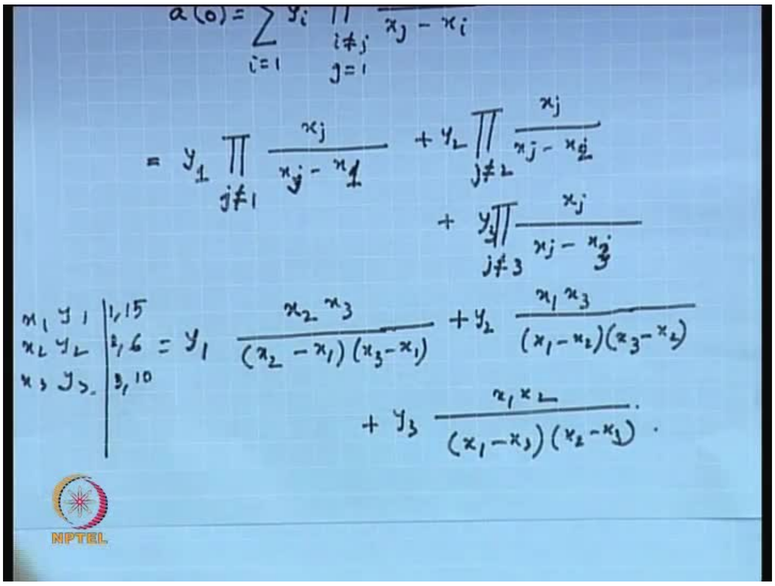
$$a(0)=\sum_{i=1}^{t} y_i \prod_{\substack{i\neq j\\ j=1}}^{t} \frac{x_j}{x_j-x_i}$$

$$= y_1\prod_{j\neq 1}\frac{x_j}{x_j-x_1} + y_2\prod_{j\neq 2}\frac{x_j}{x_j-x_2} + y_3\prod_{j\neq 3}\frac{x_j}{x_j-x_3}$$

$$= y_1\frac{x_2 x_3}{(x_2-x_1)(x_3-x_1)} + y_2\frac{x_1 x_3}{(x_1-x_2)(x_3-x_2)} + y_3\frac{x_1 x_2}{(x_1-x_3)(x_2-x_3)}.$$

So, you see that, this is given by this, right. That is, you know that, for the general case, this was the polynomial, y i x j divided by x j minus x i, i not equal to j and j equal to 1 to t and this is i equal to 1 to t. So, in our case, t is equal to 3, right. So, if t is equal to 3, it is y 1 and then we are doing a product; the product is x j x j minus x i plus y 2, again, this product x j divided by x j minus x i, plus y 3, again this product x j divided by x j minus x i and you note that, this is what, i is 1. So, this is x 1, this is x 2 and this is x 3. And you note that, here j is not equal to i; so, that means, j is not equal to 1 here; j is not equal to 2 here, and j is not equal to 3 here, right. So, that means, this is equal to y 1 into… So, what is the corresponding value of your j here? It is, it can be 2 here, because it is not equal to 1. So, it is x 2 divided by x 2 minus x 1, multiplied by x 3 divided by x 3 minus x 1, plus y 2 and again here, x 1 will come and similarly, x 3 will come. So, it is x 1 minus x 2 into x 3 minus x 2, plus y 3, which is x 1 x 2 and here, x 1 minus x 3 and x 2 minus x 3.

(Refer Slide Time: 41:44)



$$a(0) = \sum_{i=1} y_i \prod_{\substack{i \neq j \\ j=1}} \frac{\quad}{x_j - x_i}$$

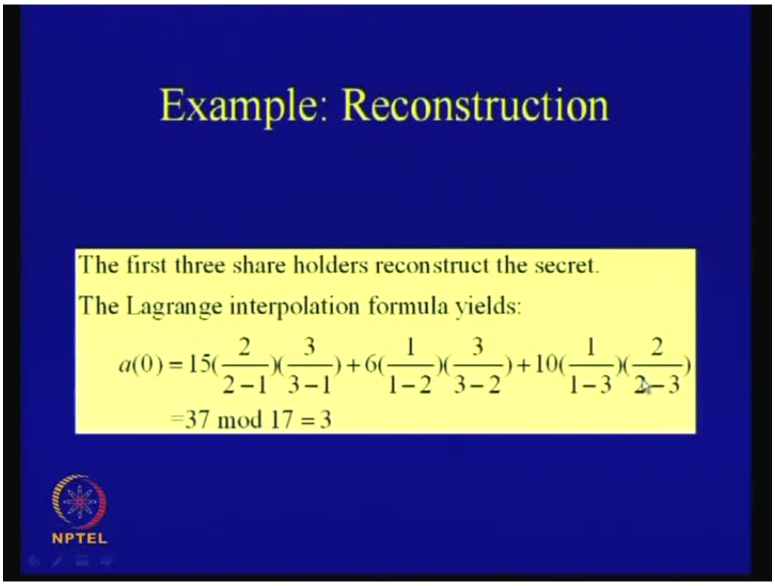
$$= y_1 \prod_{j \neq 1} \frac{x_j}{x_j - x_1} + y_2 \prod_{j \neq 2} \frac{x_j}{x_j - x_2} + y_3 \prod_{j \neq 3} \frac{x_j}{x_j - x_3}$$

$x_1\ y_1$	1, 15
$x_2\ y_2$	2, 6
$x_3\ y_3$	3, 10

$$= y_1 \frac{x_2 x_3}{(x_2 - x_1)(x_3 - x_1)} + y_2 \frac{x_1 x_3}{(x_1 - x_2)(x_3 - x_2)} + y_3 \frac{x_1 x_2}{(x_1 - x_3)(x_2 - x_3)}.$$

So, therefore, if you see, is and you just plug in the corresponding values of, here x 1 y 1, x 2 y 2, x 3 y 3, which are nothing, but what was the values; the values were, this value was 1 comma 15, this value was 2 comma 6 and this value was 3 comma 10.

(Refer Slide Time: 39:23)



Example: Reconstruction

The first three share holders reconstruct the secret.

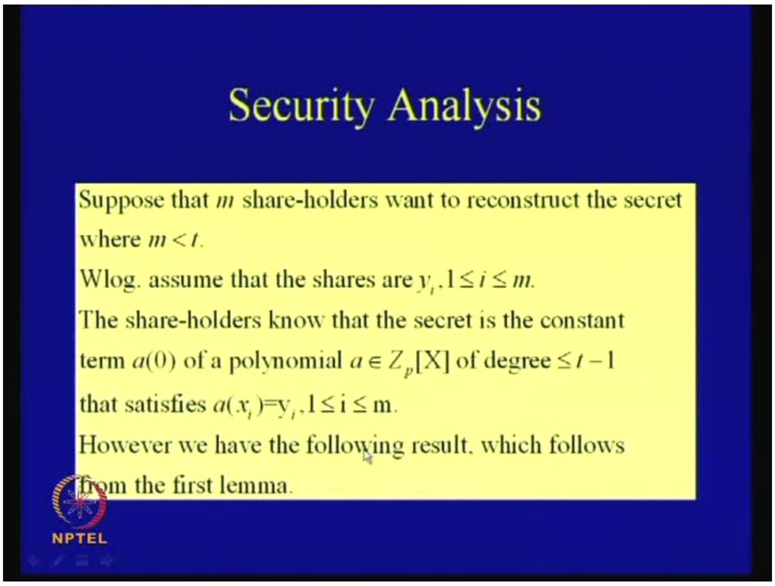
The Lagrange interpolation formula yields:

$$a(0)=15(\frac{2}{2-1})(\frac{3}{3-1})+6(\frac{1}{1-2})(\frac{3}{3-2})+10(\frac{1}{1-3})(\frac{2}{2-3})$$

$=37 \bmod 17=3$

So, if you plug in these values, then, you will get this, right; you get this value, that 15 into 2 by 2 minus 1 into 3 by 3 minus 1 plus so on. So, therefore, you can see, immediately that a 0 is indeed equal to 3, right. The 37 mod 17, therefore, that is equal to 3. So, all these computations are modulus 17; that is modulo of p.

(Refer Slide Time: 42:32)



Security Analysis

Suppose that m share-holders want to reconstruct the secret where $m < t$.

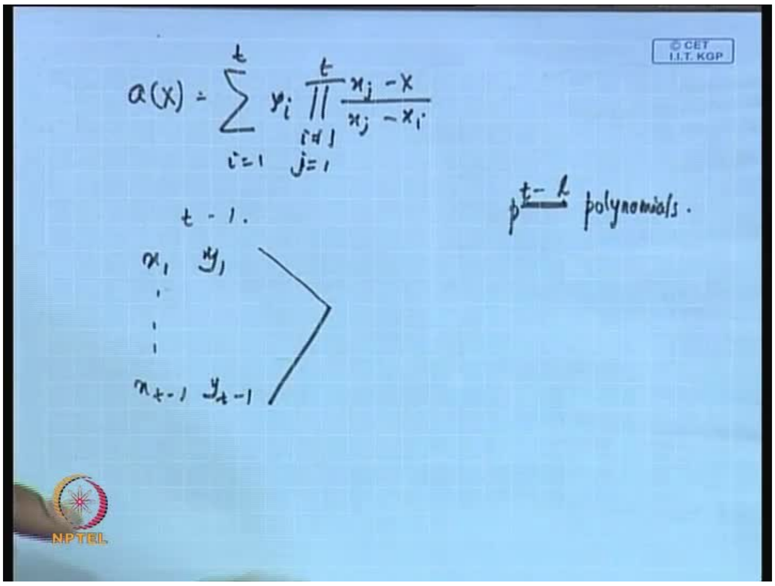
Wlog. assume that the shares are $y_i, 1 \le i \le m$.

The share-holders know that the secret is the constant term $a(0)$ of a polynomial $a \in Z_p[X]$ of degree $\le t-1$ that satisfies $a(x_i)=y_i, 1 \le i \le m$.

However we have the following result, which follows from the first lemma.

So, therefore, you see that, you indeed get the value of the polynomial as it is shown over here. Therefore, now, what we are essentially concerned, is about a security analysis; that is, if suppose, lesser number of people combine than t, then, what is the information leakage? So, what we, have found out that, these are, if out of these t n people, if t people combine, then, they know the secret; but if suppose, if less than that combine, then, what happens?

(Refer Slide Time: 43:13)



$$a(x) = \sum_{i=1}^{t} y_i \prod_{\substack{i \neq j \\ j=1}}^{t} \frac{x_j - x}{x_j - x_i}$$

$t - 1.$

$x_1 \; y_1$

$\vdots$

$x_{t-1} \; y_{t-1}$

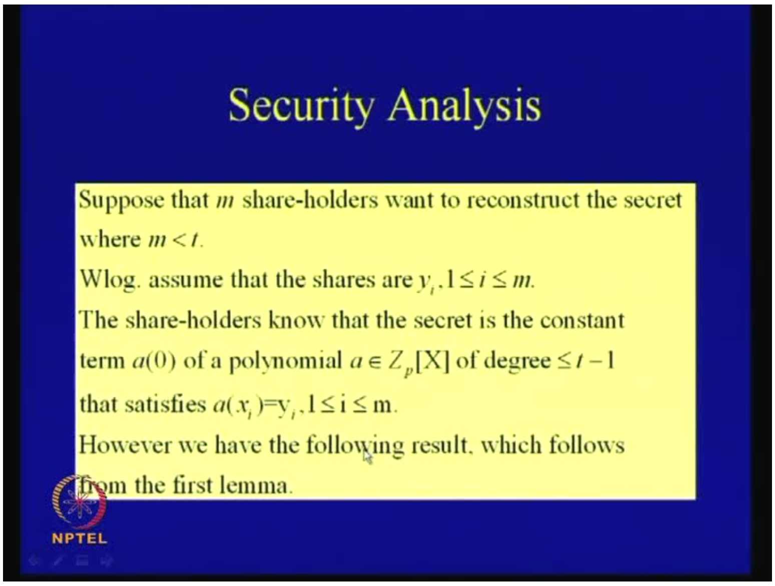
p^{t-l} polynomials.

© CET
I.I.T. KGP
NPTEL

So, for example, if you know that, there are these things, like if there are… So, you know that, the polynomial if there are t members, then, this is the corresponding polynomial, right. y i x j minus X divided by x j minus x i, i not equal to j and j equal to 1 to t, i equal to 1 to t; this is the corresponding polynomial. But suppose, the number of colluding parties is actually, say, suppose t minus 1, even 1 less than that, right. Therefore, the corresponding shares will be x 1 y 1 and so on, till x t minus 1 and y t minus 1.

So, they will apply a Lagrange's interpolation formula on this; but note that, they also know that, the degree is t, t minus 1. So, how many such polynomials will exist? So, you know that, by lemma 1, if there were n such members… So, then the number of polynomials was given as p to the power of t minus l, that was the first lemma. So, there were p to the power t minus l polynomials, which were possible. Therefore, if you have at least this l to be equal to t minus 1, or you know that, if this value, I mean, you know that, if this value is lesser than this, that is, just what you said to be equal to l, then, there is more ambiguity, because there are larger number of polynomials which are possible.

(Refer Slide Time: 42:32)



Security Analysis

Suppose that m share-holders want to reconstruct the secret where $m < t$.

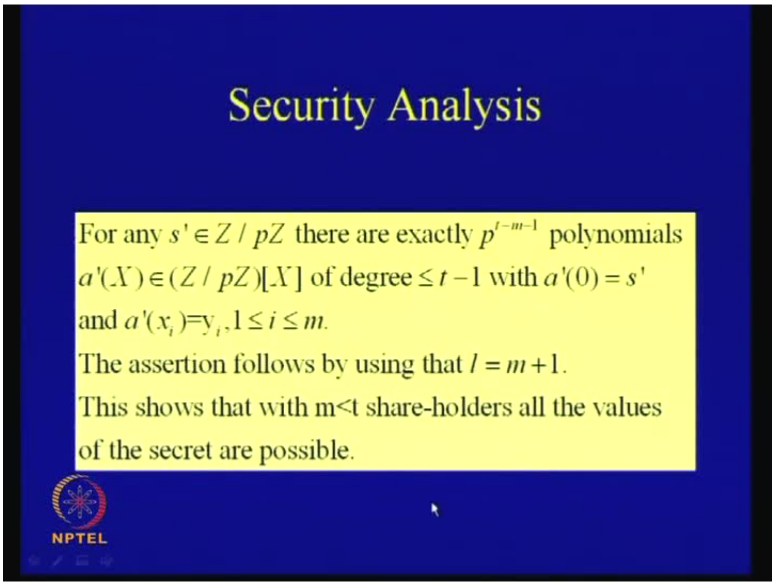
Wlog. assume that the shares are $y_i, 1 \le i \le m$.

The share-holders know that the secret is the constant term $a(0)$ of a polynomial $a \in Z_p[X]$ of degree $\le t-1$ that satisfies $a(x_i)=y_i, 1 \le i \le m$.

However we have the following result, which follows from the first lemma.

So, being more precise, you see that, suppose, there are m share-holders who want to reconstruct the secret, where m is less than t. So, without loss of (( )), assume that, the shares are y, y i, where i varies from 1 to m. So, the share-holders know that, the secret is the constant a 0 of a polynomial of degree less than equal to t minus 1. So, that is known, essentially to the share-holders as well. So, which means, satisfy a of x i equal to y i, but they have, they do not have all the t shares, but they have only m shares; and you know that, m is lesser than t. So, therefore, what is the information leakage and what is the knowledge that is leaked of the constant? That is the question that we are concerned with, right. Therefore, however, we have the following result, which follows actually, from the first lemma.

(Refer Slide Time: 45:52)



Security Analysis

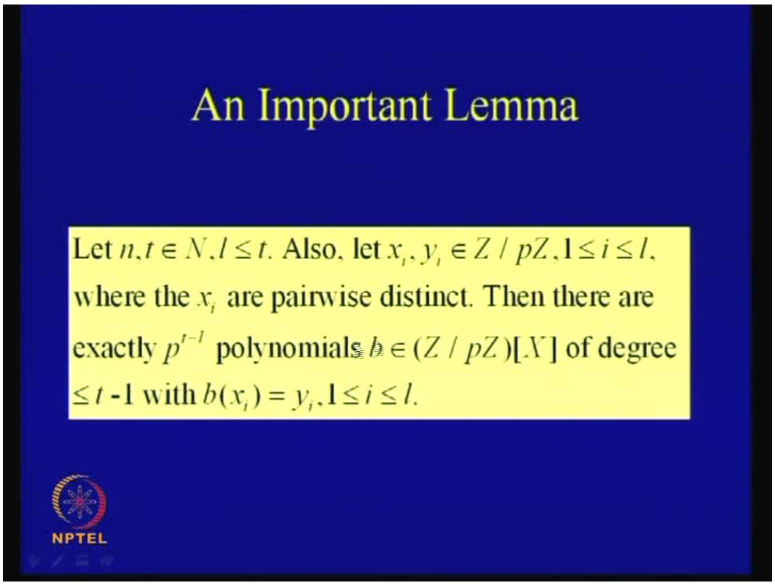
For any $s' \in Z/pZ$ there are exactly p^{t-m-1} polynomials $a'(X) \in (Z/pZ)[X]$ of degree $\leq t-1$ with $a'(0) = s'$ and $a'(x_i)$=y_i, $1 \leq i \leq m$.

The assertion follows by using that $l = m+1$.

This shows that with m<t share-holders all the values of the secret are possible.

The result says that, for any s dash, for any secret for that matter, there are exactly p to the power of t minus m minus 1 polynomials, at these form of degree less than t minus 1, such that, for all these m values this relation is satisfied. Why, because in this, this, this assertion follows by using the fact l is equal to m plus 1, in this case. Why m plus 1? Because, any s dash you choose, right, so, any s dash you choose, you will applying the Lagrange's interpolation formula in this, as well as on this; these m values. So, this m plus 1. So, that is, your l is equal to m plus 1, in this case. So, if you plug in l equal to m plus 1, and you know that, lemma 1 says that, there are p to the power of t minus l such polynomials. So, that means, if you plug in l equal to m plus 1, there are p to the power of t minus m minus l polynomial which are possible.

(Refer Slide Time: 47:06)

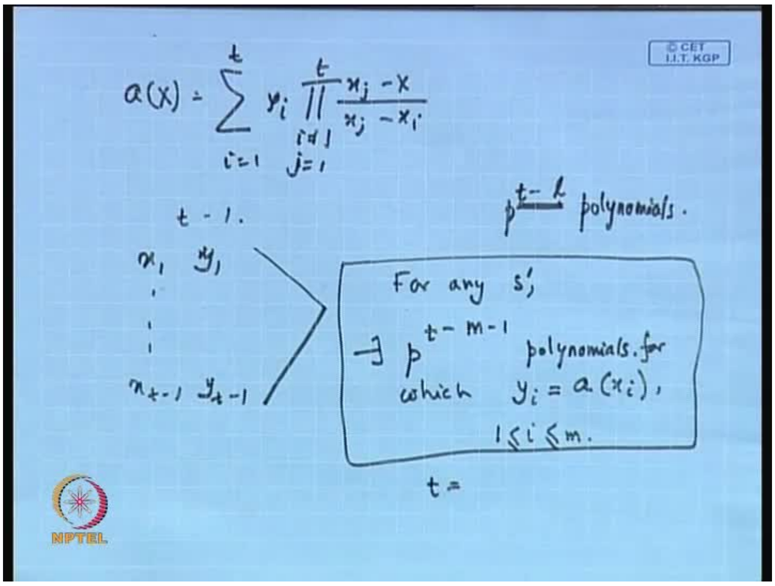


An Important Lemma

Let $n, t \in N, l \leq t$. Also, let $x_i, y_i \in Z/pZ, 1 \leq i \leq l$, where the x_i are pairwise distinct. Then there are exactly p^{t-l} polynomials $b \in (Z/pZ)[X]$ of degree $\leq t$ -1 with $b(x_i) = y_i, 1 \leq i \leq l$.

So, what did the first lemma say? The first lemma said that, there are exactly p to the power of t minus l polynomials; so, for, where all these values are satisfied, for all this l values. So, therefore, now, in our case, this has to satisfy for all these n cases as well as for the constant, which you are choosing for any s dash. So, that means, it is for m plus 1 values. Therefore, the number of such polynomials is exactly equal to p to the power of t minus l and l is equal to m plus 1. So, that is, p to the power of t minus m minus 1 such polynomials.

(Refer Slide Time: 47:55)



$$a(x) = \sum_{i=1}^{t} y_i \prod_{\substack{j=1 \\ i \neq j}}^{t} \frac{x_j - x}{x_j - x_i}$$

$t - 1.$

$x_1 \quad y_1$

$\vdots$

$x_{t-1} \quad y_{t-1}$

p^{t-l} polynomials.

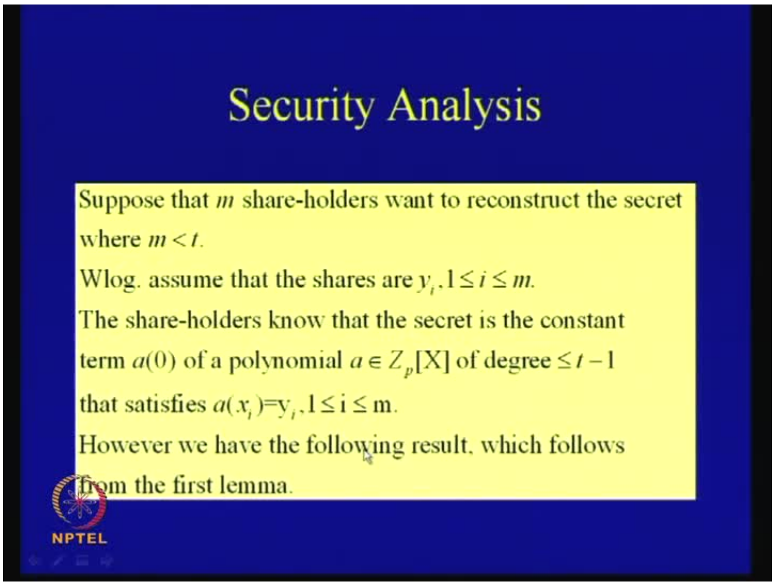
For any s'_j

$\exists\ p^{t-m-1}$ polynomials. for which $y_i = a(x_i)$, $1 \leq i \leq m$.

$t =$

So, therefore, there are exactly p to the power of t minus m minus 1 such polynomials possible; and that is, for the any secret s dash, which you are choosing, there are, there exists p to the power of t minus m minus 1 polynomials, for which y or rather y i is equal to a of that polynomial, you are applying x i for all is varying from 1 to m. So, therefore, you see that, if you set here, t to be equal to… So, there are how many such possible cases here?

(Refer Slide Time: 42:32)



Security Analysis

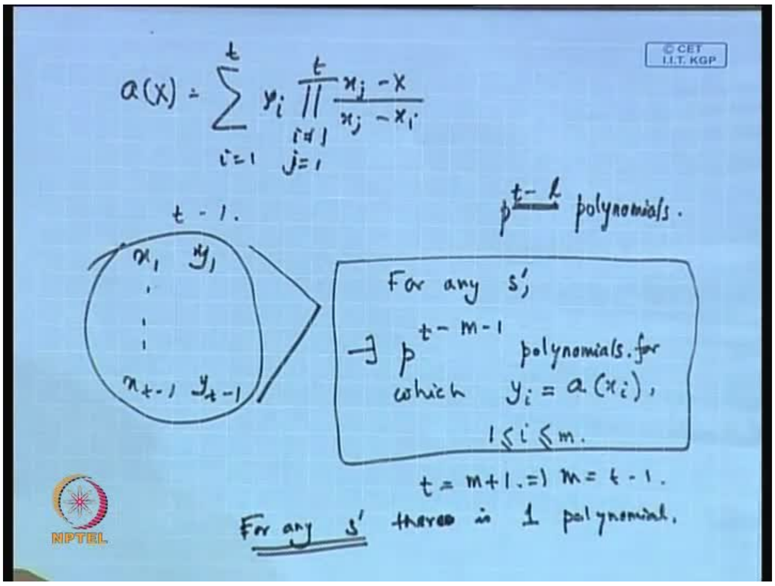
Suppose that m share-holders want to reconstruct the secret where $m < t$.

Wlog. assume that the shares are $y_i, 1 \le i \le m$.

The share-holders know that the secret is the constant term $a(0)$ of a polynomial $a \in Z_p[X]$ of degree $\le t-1$ that satisfies $a(x_i)=y_i, 1 \le i \le m$.

However we have the following result, which follows from the first lemma.

(Refer Slide Time: 48:59)



$$a(x) = \sum_{i=1}^{t} y_i \prod_{\substack{j=1 \\ i \neq j}}^{t} \frac{x_j - x}{x_j - x_i}$$

$t-1.$

p^{t-1} polynomials.

$x_1 \quad y_1$

$\vdots$

$x_{t-1} \quad y_{t-1}$

For any s', $\exists$ p^{t-m-1} polynomials. for which $y_i = a(x_i)$, $1 \le i \le m$.

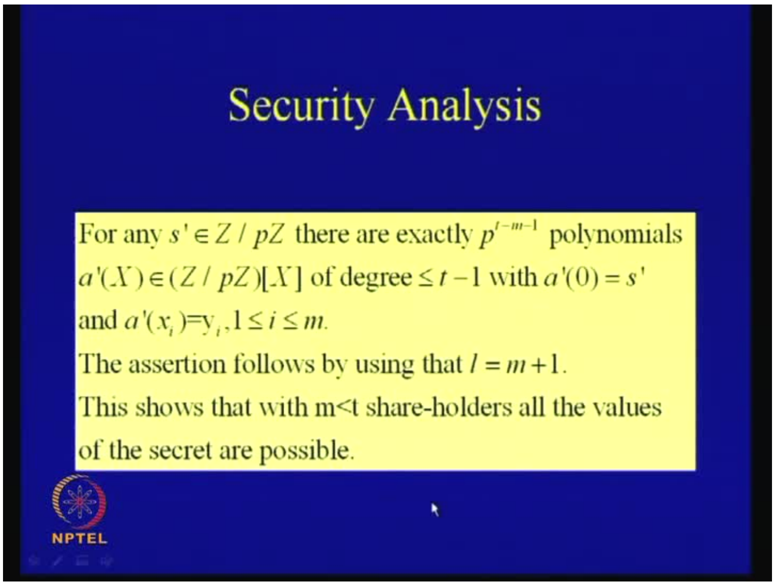
$t = m+1. \Rightarrow m = t-1.$

For any s' there is 1 polynomial.

Say, if you set now, your t to be exactly equal to m plus 1, or rather m is equal to t minus 1. So, then, there are how many polynomials? There is exactly one polynomials; so, that means, in that special case, for any s dash, there is, there is one polynomial for which this result holds. So, which means that, for any s dash, you can select, for any secret which you choose, there is one such polynomial. So, that means, these m shares, where m is equal to t minus 1, is not revealing any information. Do you see that? Because, whatever be the secret value, there exists one polynomial for which, the relation holds for this m points.

So, therefore, since, therefore, these x 1, x 2 and so on till, even this t minus 1 values, or rather these shares, are not leaking any information whatsoever, about the secret, right. Because, whatever secret, you can think of all from 0 to t minus 1, there exists one polynomial, for which this matching holds, for which this directions hold. So, therefore, this is not revealing any information whatsoever about the secret, which is the actual secret; but if you make this t, or rather the, make the value of m to be equal to t, then, there is only one such polynomial for which this relation holds. And therefore, the constant of that, is giving you the secret. So, that is the basic analysis.

(Refer Slide Time: 45:52)



Security Analysis

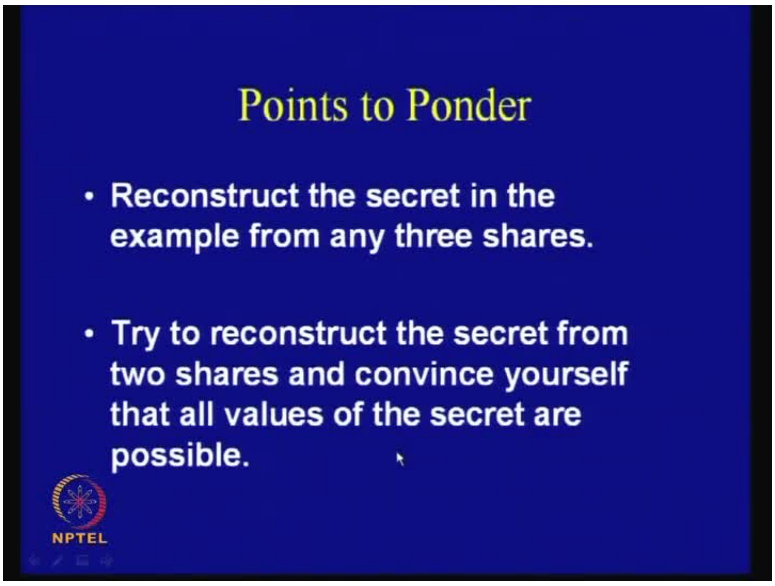
For any $s' \in Z/pZ$ there are exactly p^{t-m-1} polynomials $a'(X) \in (Z/pZ)[X]$ of degree $\leq t-1$ with $a'(0) = s'$ and $a'(x_i)$=y_i, $1 \leq i \leq m$.

The assertion follows by using that $l = m+1$.

This shows that with m<t share-holders all the values of the secret are possible.

So, that means, that, the assertion shows that, with m less than t, so, obviously, if the share, sharing must be even smaller, then, the information leakage is even less and therefore, this shows that, with m less than t share-holders, all the values of the secret are possible.

(Refer Slide Time: 51:18)

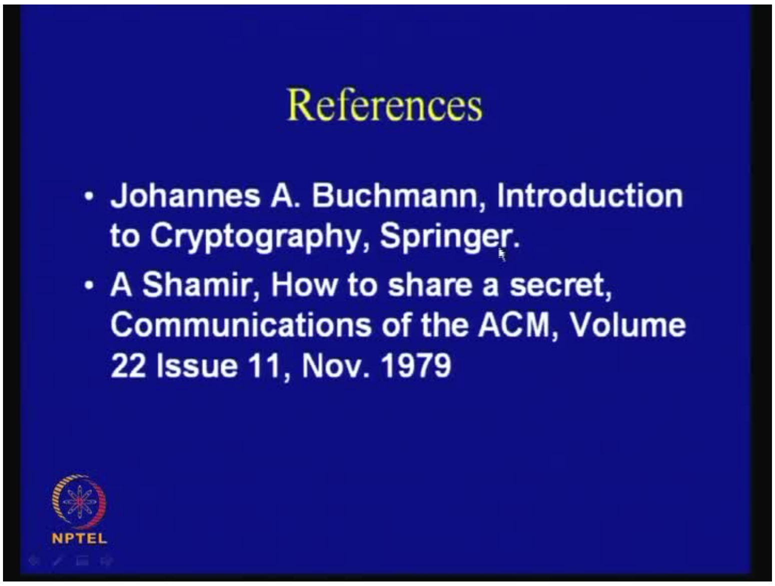


Points to Ponder

- Reconstruct the secret in the example from any three shares.
- Try to reconstruct the secret from two shares and convince yourself that all values of the secret are possible.

So, you can consider some points to think on, for example, you can reconstruct the secret in the example from any of the three shares, that, I mean, I have just considered the first 3 shares, we can choose any 5 choose 3 shares and other thing which you can try is that, to construct or reconstruct the secret from two shares and convince yourself with all values of the secret are indeed possible.

(Refer Slide Time: 51:46)

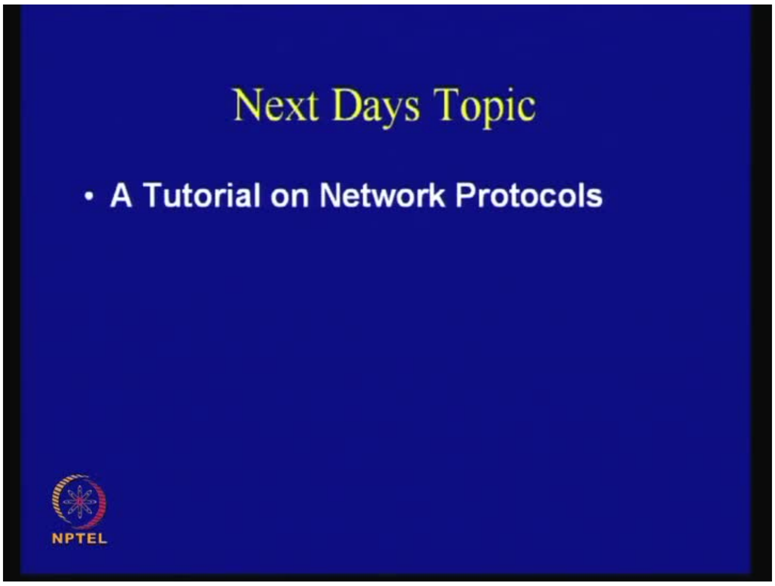


References

- Johannes A. Buchmann, Introduction to Cryptography, Springer.
- A Shamir, How to share a secret, Communications of the ACM, Volume 22 Issue 11, Nov. 1979

So, some of the references which are used is the Buchmann’s book, Introduction to Cryptography and also the actual paper which was written by Shamir in 1979, says that, how to share a secret; it was published in communications of the ACM.

(Refer Slide Time: 52:02)



Next Days Topic

- A Tutorial on Network Protocols

So, in the next day’s class, we will take up the topic on tutorial on network protocols. So, we will, first of all consider that, all of the things what we have learnt together and at least some of them, how to essentially apply them, to develop a secured protocol, secured protocol along the network.