NPTEL

NATIONAL PROGRAMME ON TECHNOLOGY ENHANCED LEARNING

IIT BOMBAY

CDEEPIIT IIT BOMBAY

Quantum Information and Computing

Prof. D.K. Ghosh
Department of Physics IIT Bombay

Modul No.08

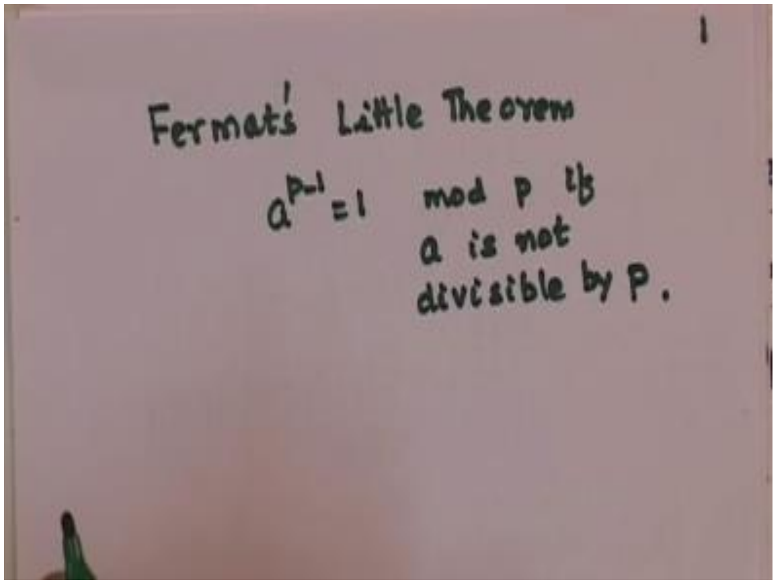
Lecture No.42

Cryptography- RSA Algorithm- II

In the last lecture we introduced you new two elements of RSA algorithm and I pointed out that RSA algorithm uses what is known as a trapdoor function we defined a trapdoor function to be one where the function is easy to calculate in one direction but is a hard problem to compute it is universe and I pointed out as an example that multiplication of two large prime is a polynomial time or an easy problem whereas given a composite number which is known to be a product of two large prime numbers to find it is integer factors is what is known as a hard problem.

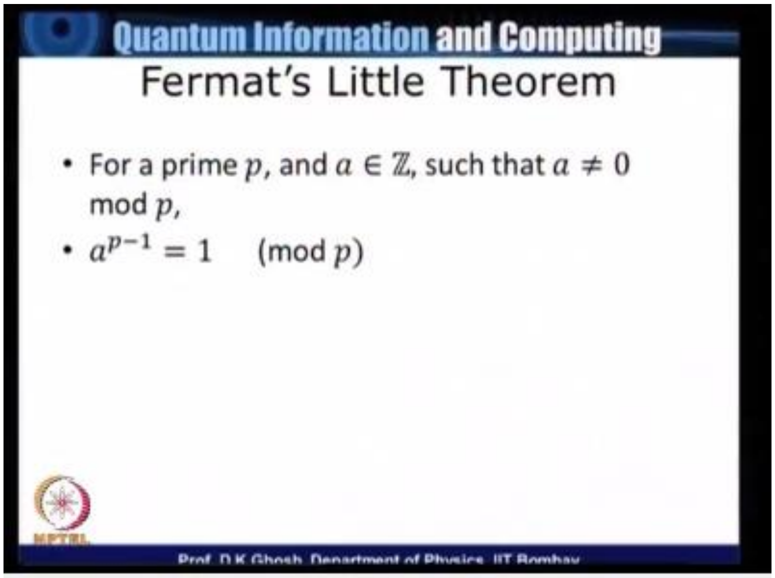
At least till source algorithm of quantum computing we have absolutely no way of factorizing a number a composite number in a polynomial time now in order to see how RSA use this fact to develop a an unbreakable code we were looking at certain elements which are required for establishment of RSA algorithm and last time I proved what is known as a Fermat's little theorem as is shown in the slide we said that for a prime number p and a belonging to any set in the integer such that a is not divisible by p we have $a^{p-1} = 1$ mod p. So this was Fermat's little theorem.

(Refer Slide Time: 02:15)



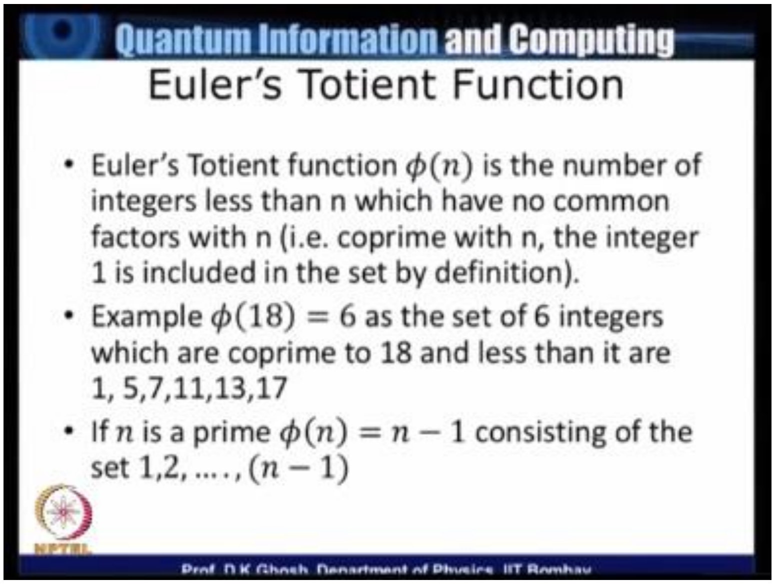
$a^{p-1} = 1$ mod p if a is not divisible by p the next thing that we started talking about as is shown in the slide is.

(Refer Slide Time: 02:52)



Euler's Totient function.

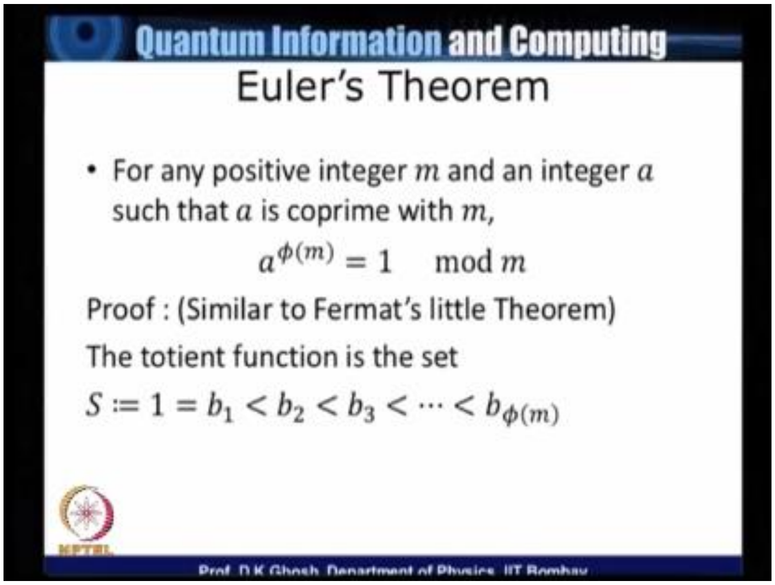
(Refer Slide Time: 02:58)



As we explained last time Euler's Totient function $\phi(n)$ is the number of integers which are less than the argument of the function namely n which have no common factors with n this is one use as phrase say which are coprime with n and as an example I showed you how $\phi(18)$ happens to be equal to 6 because there are a set of six integers which have no common factors with the number 18 and these are 1 which by definition is the number of the set 5, 7, 11, 13 and 17 now I have already told you these numbers themselves do not have to be prime because two numbers may not have a common factor and they live themselves need not prime.

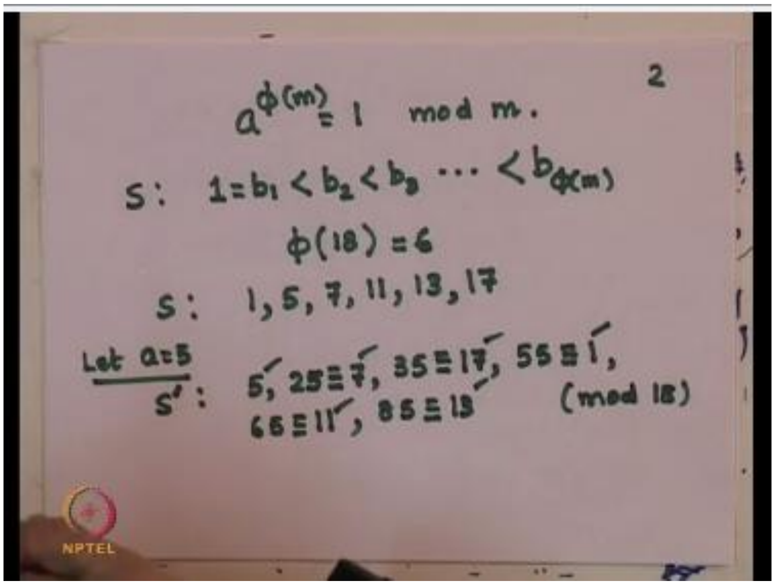
However if it happens that the argument of the Totient function is a prime then the value of the Totient function is one less than the prime number itself that is because all the numbers below it have no common factors with the argument of n.

(Refer Slide Time: 04:12)



Based on this let me illustrate another theorem which is known as the Euler's theorem the Euler's theorem states that for any integer m and an integer S such that a and m are coprime I must have $a^{Ø(m)}$ = 1mod m.

(Refer Slide Time: 04:34)

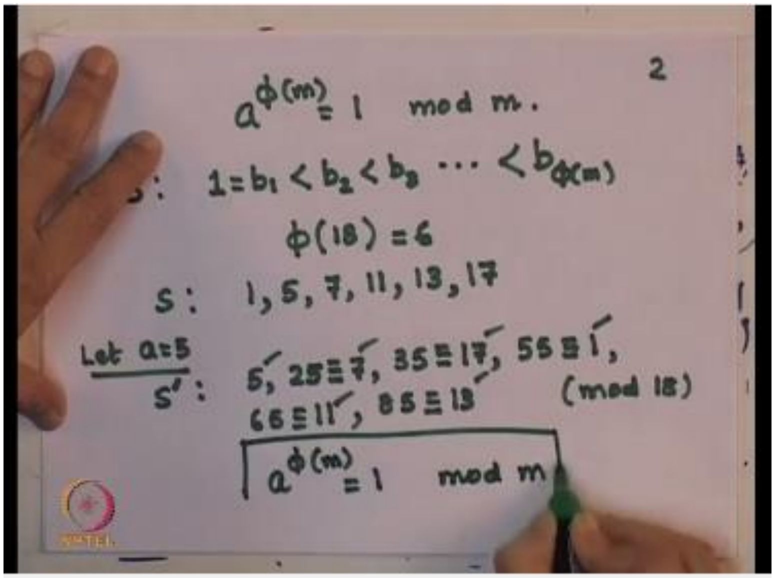


The proof is very similar to the way we have proved the Fermat's little theorem but let me do the following let me define the set S as all numbers which are less than Ø(m) starting with one of course by definition let us call it 1 is equal to $b_1 < b_2 < b_3$ and there are Ø(m) of them so less than $b_{Ø(m)}$ now what do we do is this we say that if we multiply each element of this set by a getting thereby a ab2 ab3etc… I would get the same set s modular m in the way we have proved this while proving Fermat's little theorem because we can easily show if ab_i is equal to ab_j then i must be equal to j b_i must be equal to b_j just to illustrate.

What I mean by that let us take our old example of the number 18 we had said that Ø(18) consists of digits which are numbers which are 1 by definition 5, 7, 11, 13 and 17. So $\phi(18) = 6$, now I am multiplying with a, let me take a to be equal to 5. Now if I do that I get the set s' now let us see what this S' is, so I get 1x 5 = 5, 5 x 5 is 25 but since I am doing my arithmetic modulo 18 this is equal to7, 7 x 5 is 35 modular 18 this number is same as 17, 11 x 5 is 55 which is equal to 1.

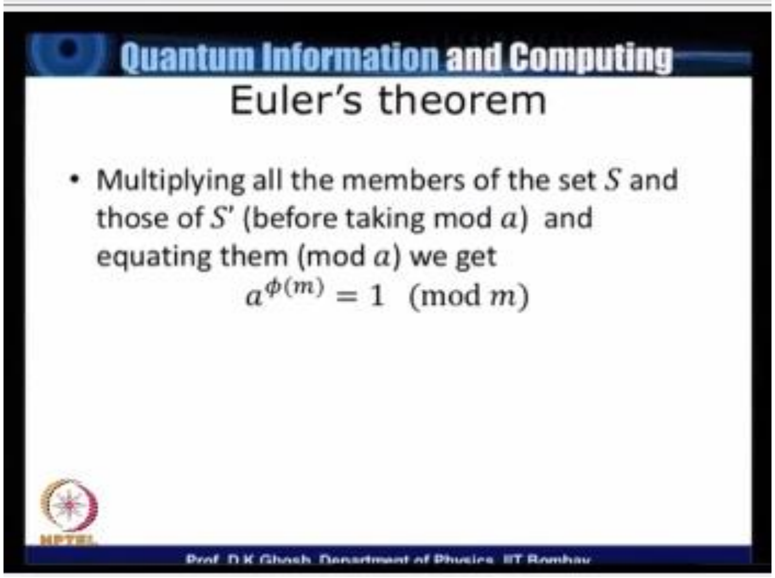
Because 54 is divisible by18, 39 x 5 is 65 which is equal to 11 and finally 17 x 5 is 85 which is equal to13 all these are mod 18, you can check immediately I have 1, 5, 7, 11,13 and 17 this sensor, as I did in the case of form as little theorem supposing I multiply the elements of s with a.

(Refer Slide Time: 07:32)



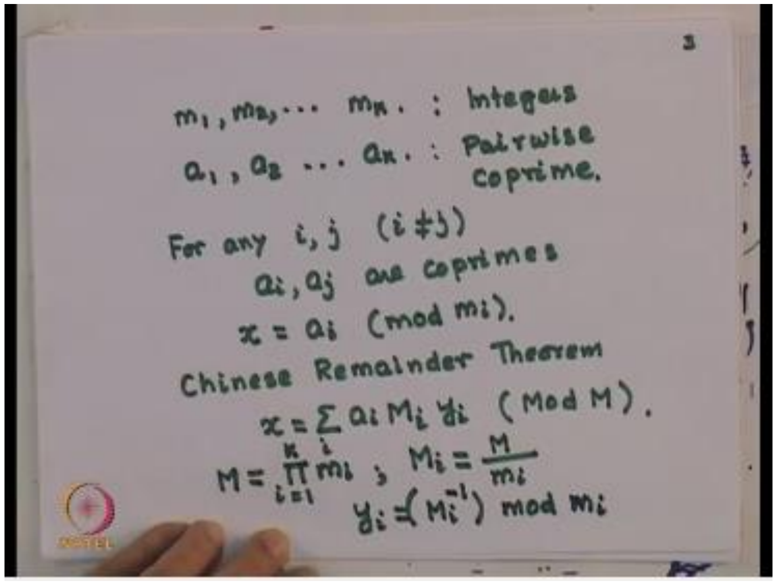
I would get this set on the right hand side which other than for a^{5n} factor is identical to the sentence, so that tells me that $a^{5(m)}$ must be equal to 1 of course mod m. So this is my Euler's theorem.

(Refer Slide Time: 07:54)



The third element that I need I will illustrate it but will not go for proving it the proof is not difficult I will in fact put it in the notes accompanying the lectures, but I will just illustrate this.

(Refer Slide Time: 08:15)

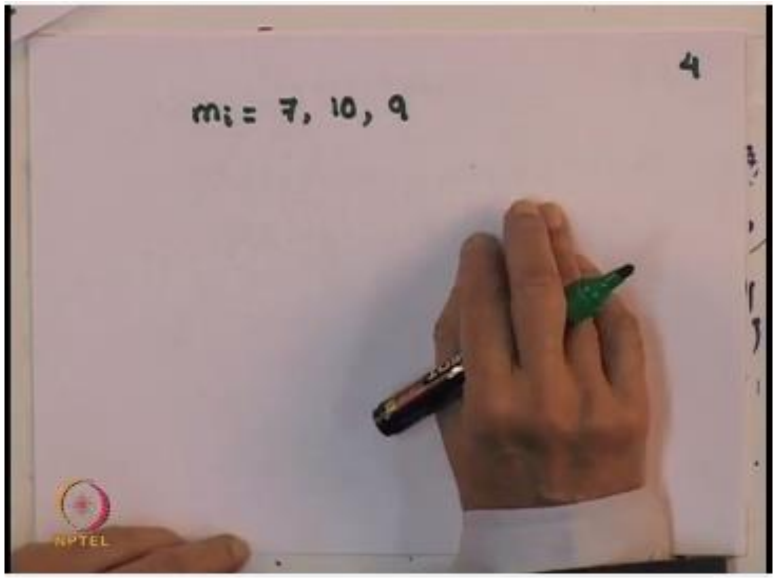


Suppose I have a set of integers which are m1, m2 up to m_k and I have another set of k numbers which I will write as a_1, a_2 -…a_k. So these are sets of integers and another set of integers a_k the condition on these ak's are that their pair wise co-prime, what it means is, that for any I and J, I_0 = J of course, a_i and a_j do not have any common factors. So a_j and a_j are co-primes, that is what is meant by pair wise co-prime.

Now with this if you look at the following set of equations x = a_i (mod m_i) now these are actually a set of K equations because for every i, I have this, now what the Chinese remainder theorem says, is that this set of equations has a unique solutions and this solution is given by X is equal to sum over i a_i, I will explain the new quantities I am introducing M_i y_i(Mod M). So a_i of course we have already said what they are.

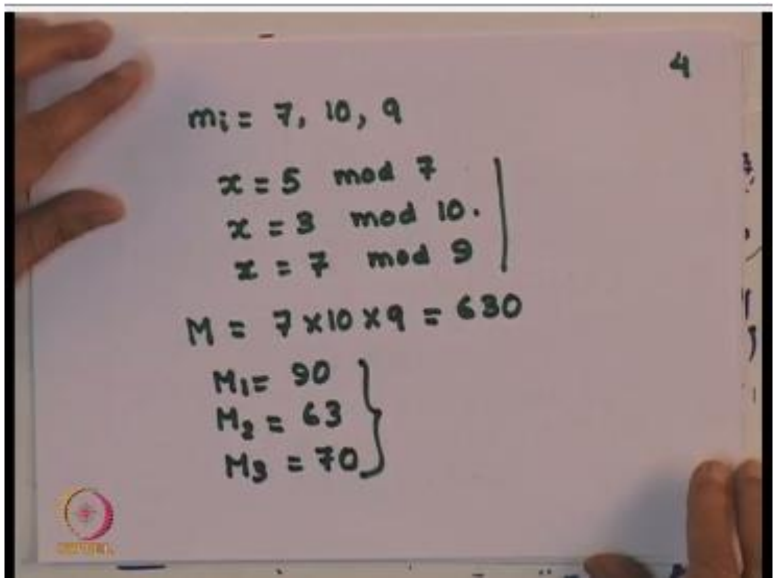
We define Capital M as equal to the product of all the K M_i and M_i is the product of all m_i's other than the i^{th} one, what it means is capital Mi is simply M/mi and finally I need to define what is Y_i and Y_i is $(M_i)^{-1}$ mod M, okay. Let my set M_i be.

(Refer Slide Time: 11:29)



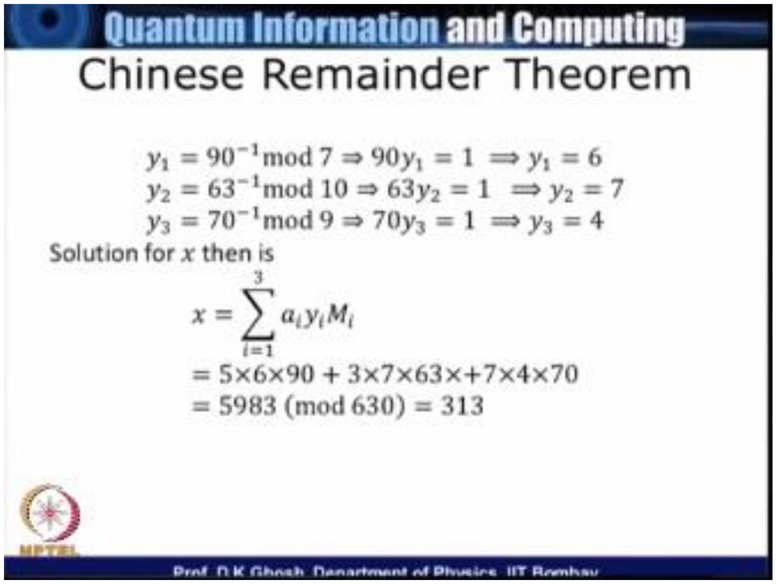
7, 10 and 9, no common factors in Mi’s. Now look at this.

(Refer Slide Time: 11:42)



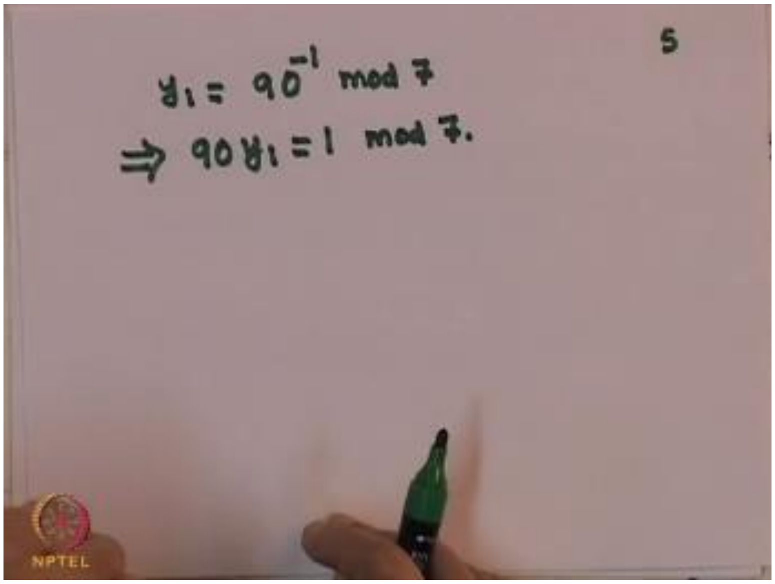
I am looking at, the following equation supposing I am looking at X = 5 mod 7, x = 3 mod 10 and X= 7 mod 9 these are the three equations I am looking for. Now my M becomes 7x10x9 now multiply this with the calculator 630 M_1 leave out the 7 so 10x9 is 90 M_2 is 7x 9 is 63and M_3 =7x10 is 70. Now we defined y_1.

(Refer Slide Time: 12:51)



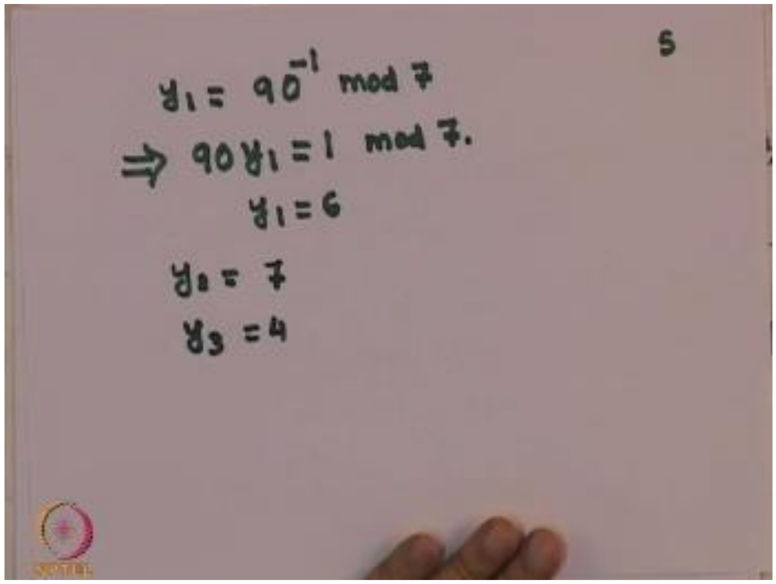
We said y_1=M_1 inverse.

(Refer Slide Time: 13:03)



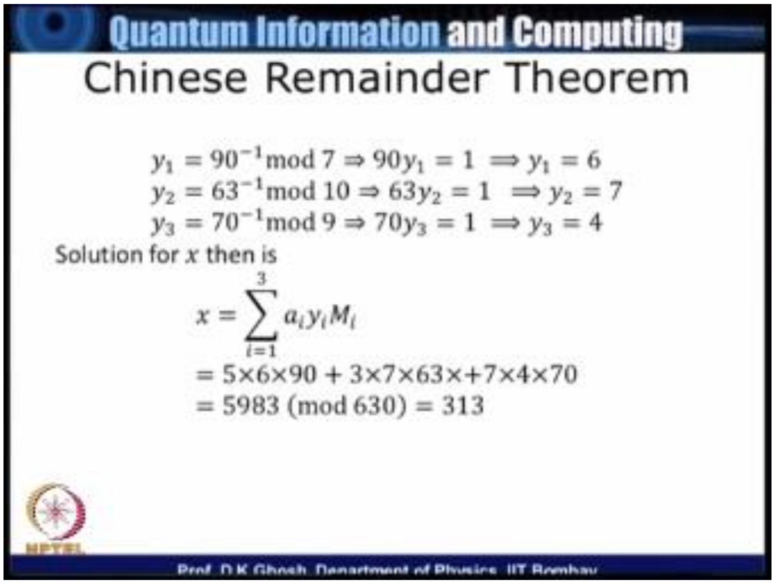
So M_1 will be 90, so 90 inverse mod 7, how do I solve it this simply implies $90y_1=1$ mod 7 this very easy by inspection because I have given you small numbers otherwise even if you have to do it computation it is not all that difficult to find out what this is, actually you know that 91 y_1 would have been divisible by 7. So therefore it turns out that this y_1 is actually equal to 6.

(Refer Slide Time: 13:48)



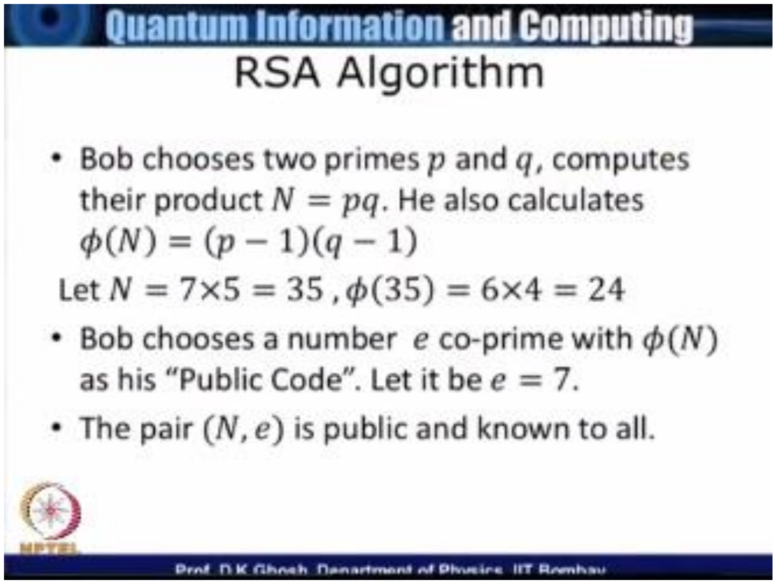
And that is very easy to understand because 90 y_1 we have 84 is divisible by 7 so I am left with another 6 y_1 so 6 y_1=1 I was 6 x 6= 36 which is which leaves 1 when you divided by 7 and likewise my y_2 will turn out to be equal to 7 and y_3 turns out to be equal to 4. Look at the slide gives you the result.

(Refer Slide Time: 14:31)

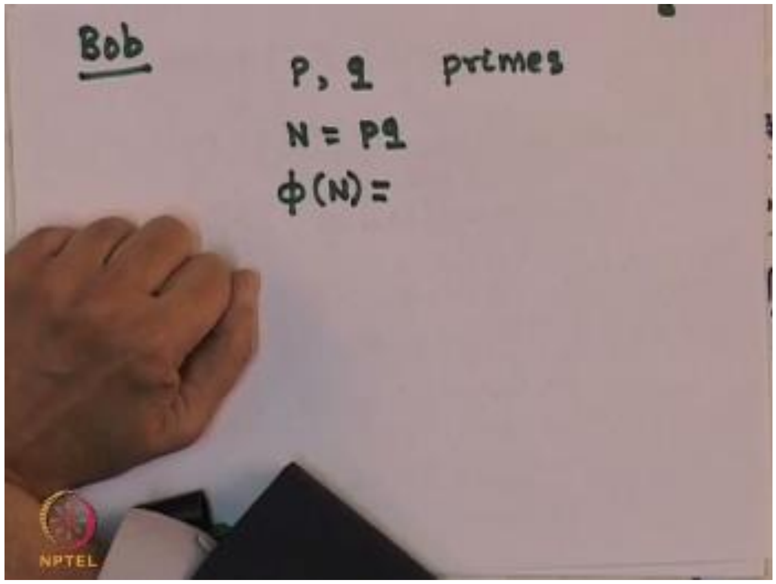


You just add up now you have y_1 $a_i y_i M_i$ add this up you get a number 5983 but our calculation is modulo M so therefore it works out to 313. I leave it to you to check that this does indeed satisfy all the three equations that we wrote down. So then that we are in place for discussing what is RSA algorithm, so let me explain what is RSA algorithm. So I have two people as usual Bob and Alice, Bob chooses to arbitrarily large prime numbers, now this is Bob's private job he chooses p and q.

(Refer Slide Time: 15:23)

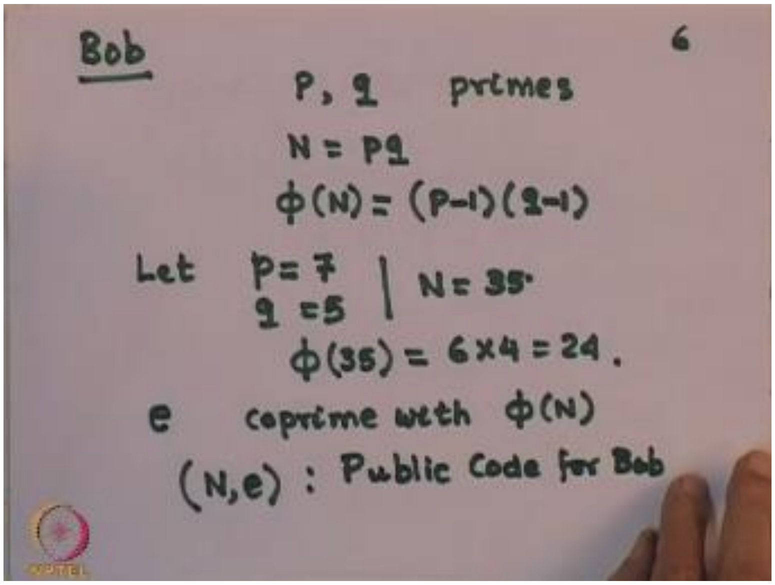


(Refer Slide Time: 15:27)



Which are both primes can be taken to be large and he computes the number N=pq now this is what Bob is doing, he also calculates the number which is ϕ(N). Now remember N is the factor of two primes and you have already stated that if an argument of the quotient function is a prime then the number ϕ(N) is nothing more other than 1 less than that number, so in other words.

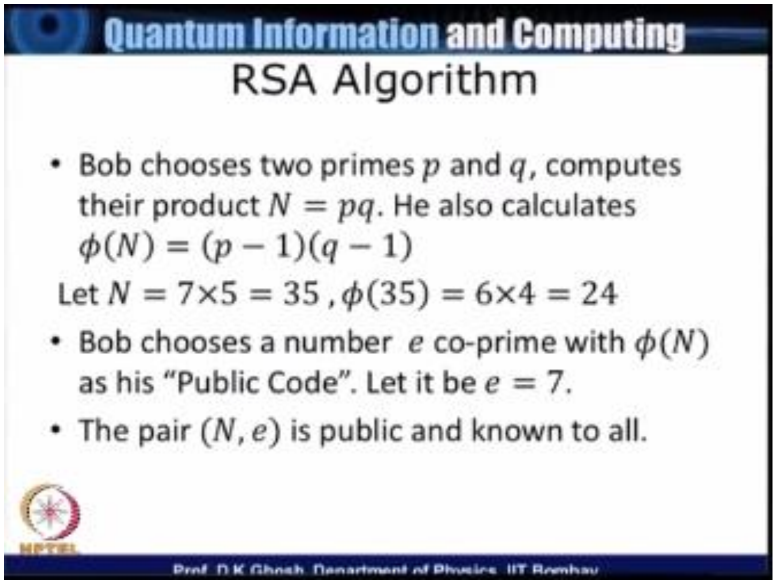
(Refer Slide Time: 16:12)



$\phi(N)$ is simply (p-1)(q-1) as an example which I will take small numbers obviously because I want you to calculate be able to calculate using a calculator, let a p be equal to let us say 7x5, so let p be equal to 7, q be equal to 5, so that N=35. Next job of bob is to end and let us also write down what is ϕ of this number $\phi(35)$ which is (p-1)(q-1) which is 6x4=24, so these are things which Bob calculates because he is the person who has chosen the two prime numbers.

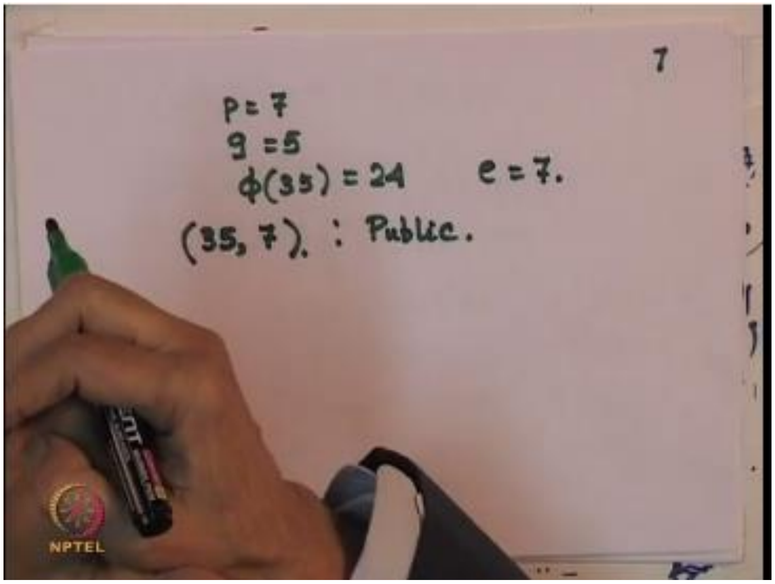
Bob chooses a number e which is co-prime with this $\phi(35)$ $\phi(N)$ the set N and e they are called the public code for Bob, what it means is anyone has an access to these two numbers which are probably published in a directory under Bob's entry. So now what Bob does is this.

(Refer Slide Time: 17:57)



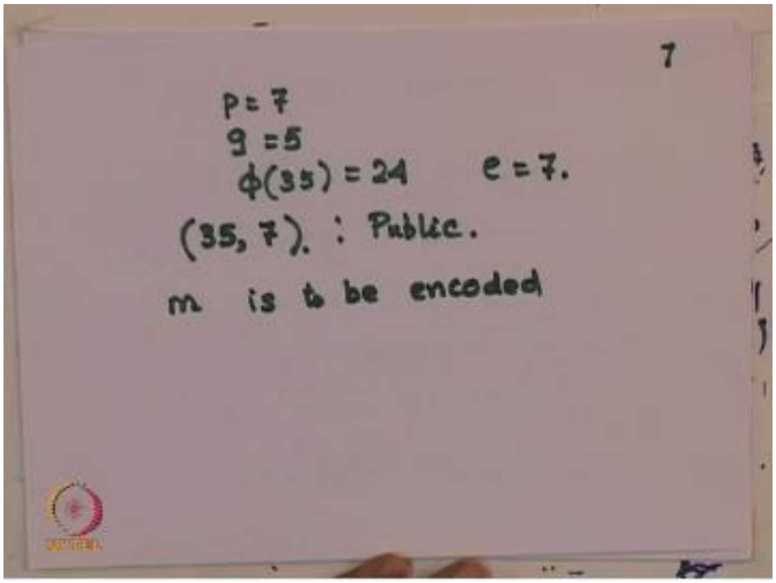
So let me give as an illustration what Bob has done now so far so bob has chosen p=7

(Refer Slide Time: 18:04)



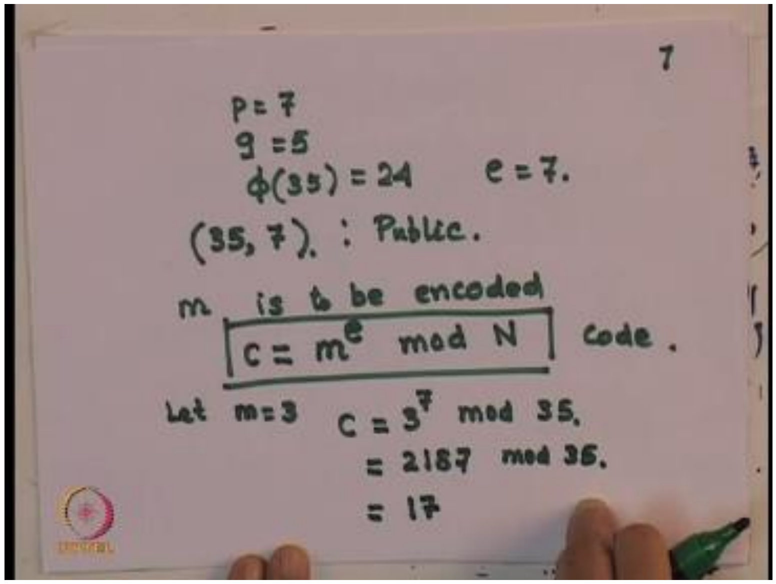
g = 5 ϕ = 24 and I am looking for a number which is co-prime with 24 let me choose this number to be equal to 7 so he is equal to 7 I will take so this is my public good what the public code means is supposing I one to encode a number m m is message.

(Refer Slide Time: 18:43)



m is to be encoded the algorithm that I am talking to you about is the coding done by anyone who is interested in sending a message to Bob and Bob has given his public key algorithm Bob public key to be the number n Andy.

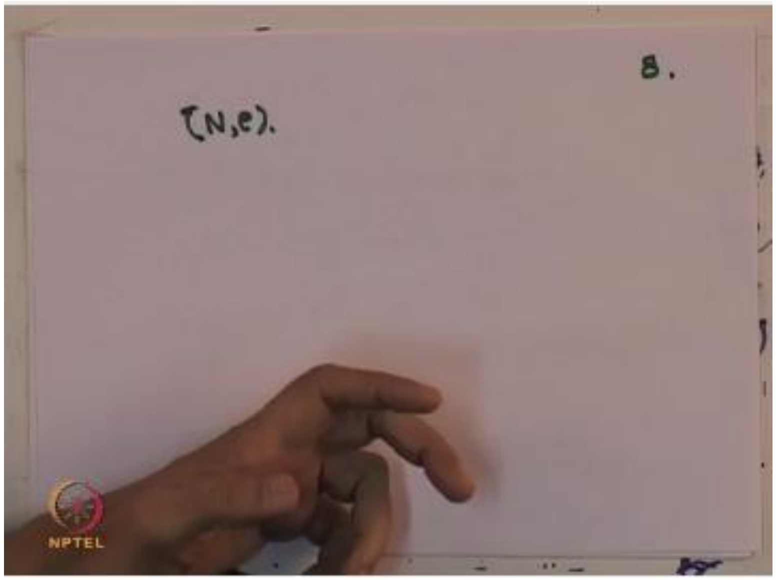
(Refer Slide Time: 19:15)



So what a person does the person who intends to send a message to Bob he us as m to be coded by a letter c and that is simply done by m^e mod N and he sends it through a public channel to Bob just to give it an illustration let m = 3 we had said e = 7so my see in this case will be 3 to the power 7mod 35 you can use this number you can calculate this number in a calculator you will find this number is given by 2187 mod 35 and this will work out to 17 so very trivial division and the remainder will turn out to be 17 so therefore instead of using three.

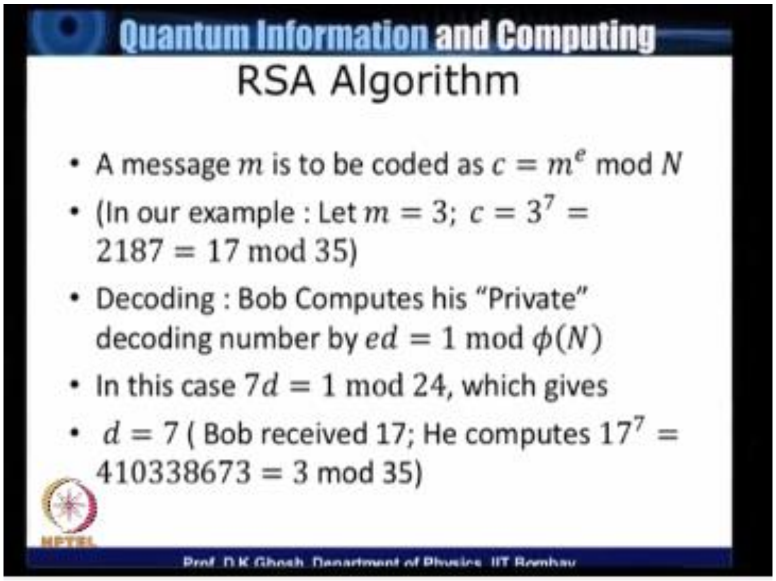
Person who is sending a message to Bob our name for this person now we so we Yves uses this code and sends a message using.

(Refer Slide Time: 20:43)



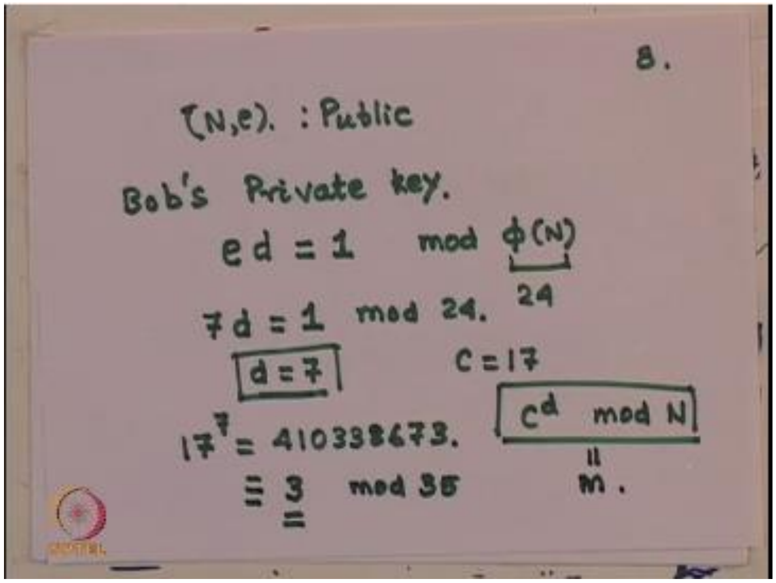
This n E now Bob receives here Bob's drawn. Is to decode it but you remember bob has lot more information given capital N even cannot factorize them so in other words Eve has no knowledge of the prime factors of M which Bob had said to be P and Q now of course in this case in the example I am giving N is 35 you can but on the other hand if it is a very large number typically128-bit number this is an impossible task because by definition of trap door function the factorization is not possible within polynomial.

(Refer Slide Time: 21:41)



So Bob now has to some or other decode this number with ABC.

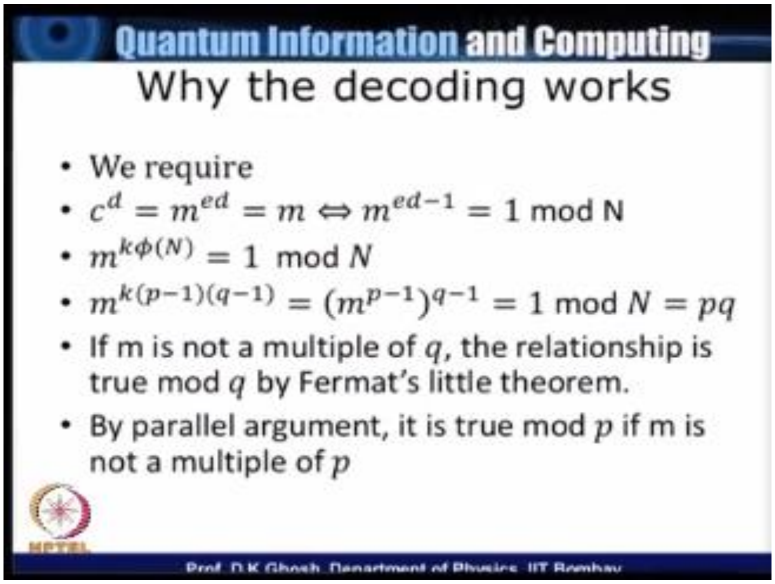
(Refer Slide Time: 21:49)



So this was public now Bob's private code bob has e he multiplies that with the d and determines d such ed is = 1 but modify n so in this particular case my ϕn was 24 which of course Bob knows now they think is this that this means since II was equal to 7 I am looking for 7 d = 1 mod 24 it just incidentally turns out though it is not necessary that d also happens to be = 7 you can check y 7 x 7 is 49, 49 is 48 + 1 and 24 of course is a factor of 40 so this is what Bob computers and the message that he has got see was = 17 he now computes 17 to the power actually he compute C^d which is 17^7 which turns out to be a fairly large number.

In fact I will write it down it is 410338673 and it computes it modulo n if you do this modulo n modulo 35 this will turn out with 3 mod 35 and 3 was the message itself. So this is equal to M you can check it for any other pair of numbers that if you like. Now what that we do is this, my next job is to simply find out why does this decoding work so let us look at the slide again.

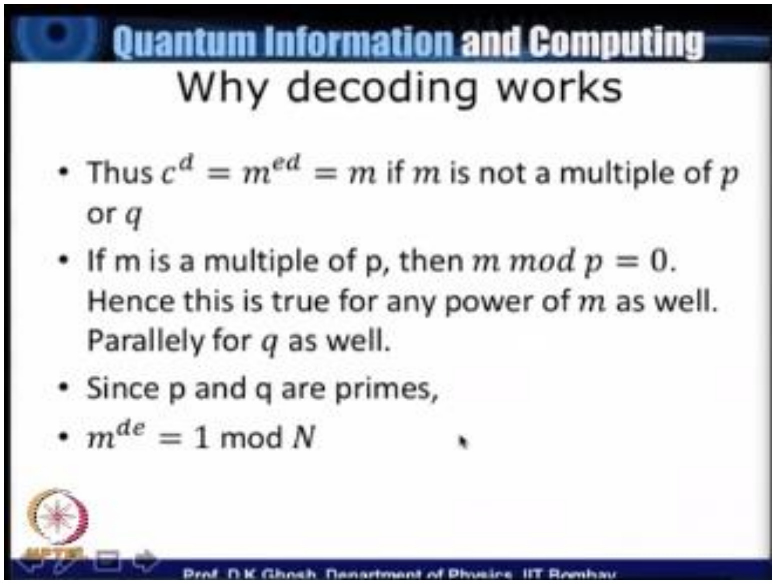
(Refer Slide Time: 24:21)



So we are looking for $C^d = m^{ed}$ and I want it to be equal to M, so what it means is m^{ed-1} is equal to 1 mod N. So let us look at the following. Now I am aware of the following result by Euler's theorem $m^{k\phi N} = 1$mod N this we have proved in this particular case since M is a product of P and Q I have $m^{kxp-1 \text{ x } q-1}$ now let us write it in this fashion $(m^{p-1})^{q-1} = 1$ okay. And so if m is not a multiple of Q then this relationship is true by Format's Little theorem and if I wrote this M as $(M^{q-1})^{p-1.}$

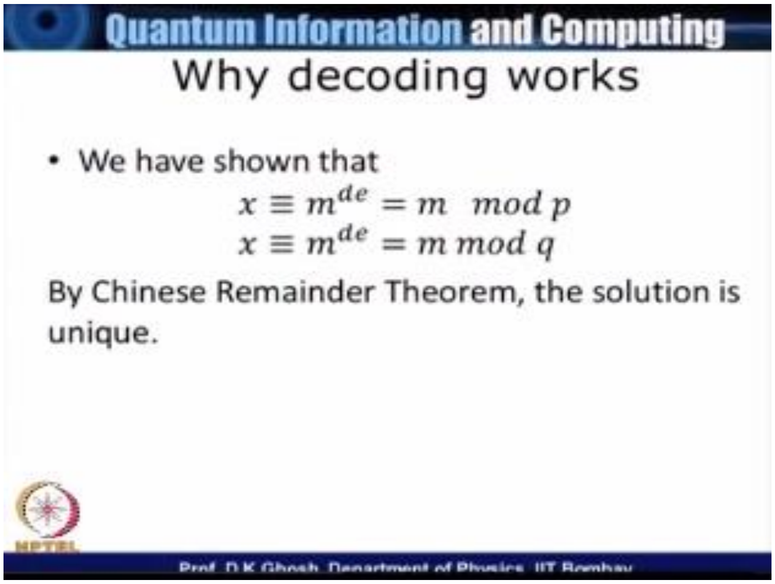
Then by parallel argument I can prove that this is also true by Format's Little theorem for the other integer pl, so only problem now is.

(Refer Slide Time: 25:53)



That $C^d = m^{ed} = m$ is true if M is not a multiple of P or Q now suppose M is indeed a multiple of P then n mod p is 0 by definition, so if it is true for m it is true for any other power as well and this argument would also be valid for key. So therefore we have $m^d = m$ mod n, so now what we have done is this.

(Refer Slide Time: 26:31)



We have shown that X = M^{de} = M mod p and another equation is M^{de} = m mod q these are pre equation but we have already said that such pairs of equation where M^{de} has been replaced by X has a unique solution by Chinese Remainder Theorem. So therefore, the solution that Bob has worked out s unique and hence the decoding works. So what we have done today is to establish the validity of public key algorithm, the key is calculated using a trap door function by Bob which is to take two prime numbers find their product n and then determine a number E which acts as the code and N and E are public.

He has a private key which only he knows how to calculate and that is d and then if he receives a message he can easily decode it. As we pointed out earlier that we may have to relook at the RS algorithm if the trapdoor function which was crucial to our argument does not remain valid for the factorization case, that is if I can use the quantum computer and if I can actually use Shor's algorithm successfully then of course we are unique to have second cabinet for that RSA algorithm is valid or not.

NATIONAL PROGRAMME ON TECHNOLOGY ENHANCED LEARNING

(NPTEL)

NPTEL
Principal Investigator
IIT Bombay

Prof. R.K. Shevgaonkar

Head CDEEP

Prof. V.M. Gadre

Producer

Arun kalwankar

Online Editor
& Digital Video Editor

Tushar Deshpande

Digital Video Cameraman
& Graphic Designer

Amin B Shaikh

Jr. Technical Assistant

Vijay Kedare

Teaching Assistants

Pratik Sathe
Bhargav Sri Venkatesh M.

Sr. Web Designer

Bharati Sakpal

Research Assistant

Riya Surange

Sr. Web Designer

Bharati M. Sarang

Web Designer

Nisha Thakur

Project Attendant

Ravi Paswan
Vinayak Raut

NATIONAL PROGRAMME ON TECHNOLOGY ENHANCED LEARNING (NPTEL)