

**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

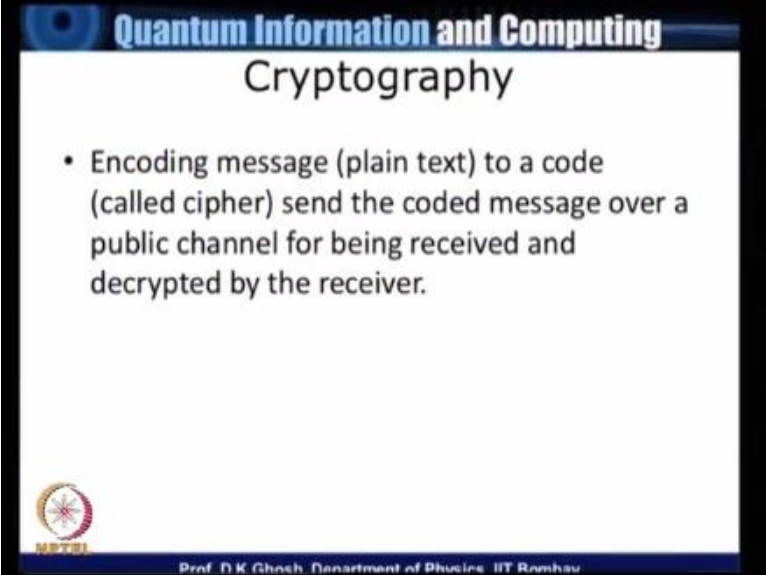
Lecture No.41

Cryptography- RSA Algorithm - I

During the last three lectures also we have been discussing about competing theories namely quantum mechanics and hidden variables and we talked about the objections that Einstein and co-workers they had which is known as Einstein Podolsky and Rosen paradox then we introduced certain inequalities original EPR due to John Bell and there are many variants thereof which provided a conclusive test for quantum mechanics over the competing theory of hidden variables.


What we will do now is to discuss a possible application of the principles of quantum computing to what we will call as the cryptography now that what is cryptography so cryptography is basically.

(Refer Slide Time: 01:15)



Quantum Information and Computing
Cryptography

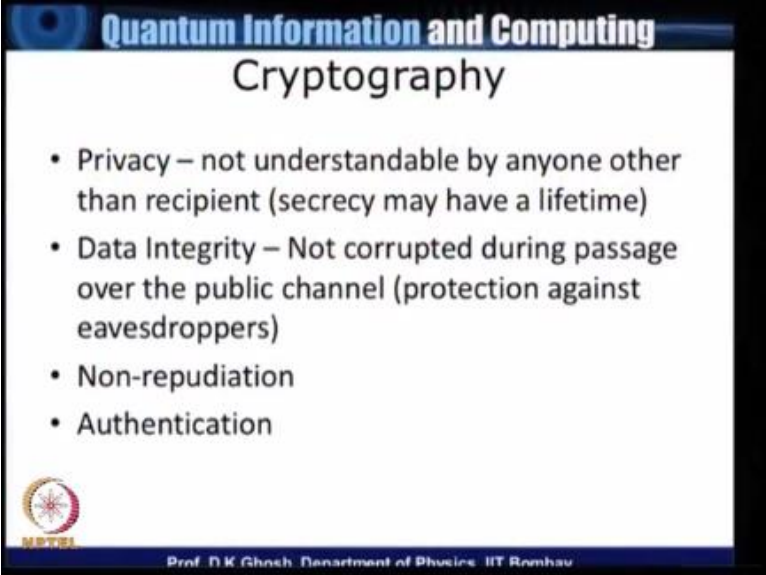
- Encoding message (plain text) to a code (called cipher) send the coded message over a public channel for being received and decrypted by the receiver.

 NPTEL
Prof. D.K. Ghosh, Department of Physics, IIT Roorkee

The subject of sending encoding a message which we will call as a plain text to a code which will be called as the cipher and send this coded message to a receiver over a public channel by public channel I mean it could be a fiber optic channel for instance and but basically a channel which is open for any outsiders and in principle it should be possible for somebody to eavesdrop on your conversation of course the conversation does not really mean oral conversation in this case it means a coded message is being sent over the internet and to a receiver.

Now at the other end when a receiver receives it since the message was coded he will need to decode it and finally convert the cipher text back into the message in the form in which it was sent so this is the principle of cryptography so let us look at what are the elements of cryptography what do you want from a the subject of cryptography so there are four or five challenging things about cryptography.

(Refer Slide Time: 02:37)



Quantum Information and Computing
Cryptography

- Privacy – not understandable by anyone other than recipient (secrecy may have a lifetime)
- Data Integrity – Not corrupted during passage over the public channel (protection against eavesdroppers)
- Non-repudiation
- Authentication

Prof. D.K. Ghosh, Department of Physics, IIT Roorkee

So first is privacy that is whatever you are sending should not be understandable by anyone other than the recipient now what I mean it by it is very simple you see when two people who are not familiar with the third language for instance if you do not understand French you want both you and your friend they understand only English then even if you happen to hear a conversation which is going on in French it would not mean anything to you, so in other words there is a privacy element in the conversation.

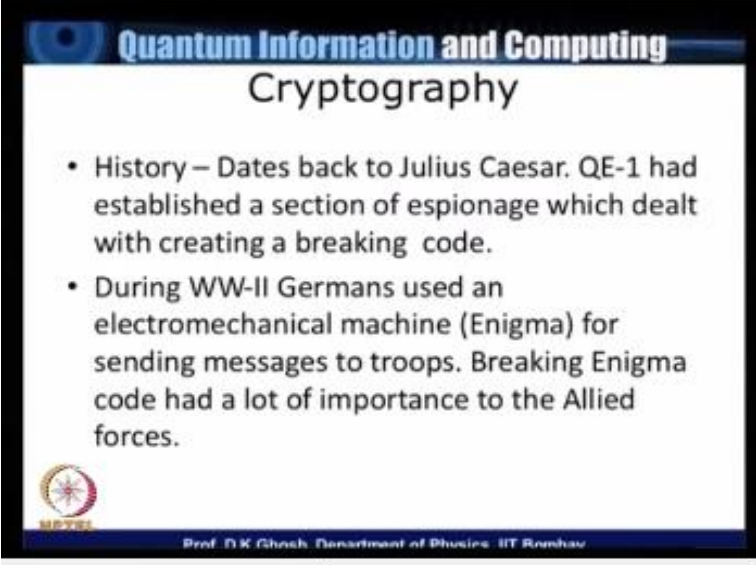
So it should be understandable to the person for whom it was meant this second thing about the secrecy is that this secrecy should not be taken to far most messages have a lifetime what I mean by that is this that supposing you are doing a banking transaction on the internet during the time it takes for you to send the message to your bank let us say to transfer certain amount of money to another account and the bank executes that transaction the text remains confidential so therefore after that somebody cannot tamper with that message for instance you cannot send say send 500 rupees to somebody and somebody cannot alter that message and say send 5,000 rupees instead.

So there is a duration for which this secrecy need for secrecy may be valid the second point is data integrity and this is a very important point that it should not be corrupted during the passage over a public channel and this is of course a very big problem there our noses in the channel but even if you assume there are no stray noses in the channel you do not want a third person whom we will call eavesdropper to be listening in to the conversation I have already explained I mean the word use the word listen in a general context of tapping the conversation the third point is what we will call it a non-repudiation.

Supposing you have sent a message and later neither you should be in a position to say or decline that you had sent that message nor the receiver should be in a position to say that he did not receive that message so this is the element which will call as the non-repudiation and finally the authentication the authentication works like this the sender again let me comeback to the example of you talking to your bank.

Now the bank should be in some way certain that the instruction that is given to it is being given by it is client that is you and that is how the bank's use various types of protection the simplest one being use of a password it could be one-time passwords so many other things that you could be familiar with. So authentication of the sender and the receiver these are very useful elements of cryptography. Incidentally cryptography as a subject has a very long history in fact it the earliest known cryptographic protocol.


(Refer Slide Time: 06:34)



Quantum Information and Computing

Cryptography

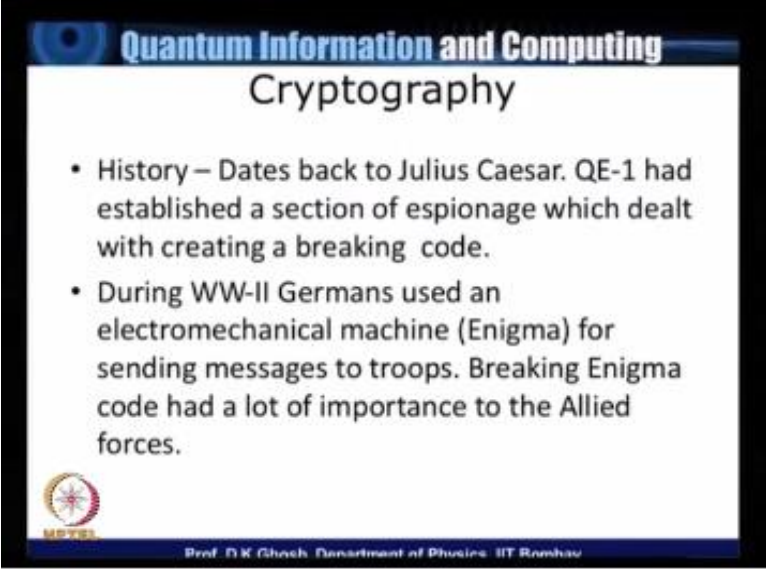
- History – Dates back to Julius Caesar. QE-1 had established a section of espionage which dealt with creating a breaking code.
- During WW-II Germans used an electromechanical machine (Enigma) for sending messages to troops. Breaking Enigma code had a lot of importance to the Allied forces.

 IIT Bombay

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


Was used by Julius Caesar and Julius Caesar used to send cryptic messages to his soldiers in their fight against the Gauls and of course that was a very trivial cryptography what he used to do, is to advance every letter by three for example the letter A would become D letter B would become E and so on so far, coming back to not exactly modern era but Queen Elizabeth I had established a section of espionage.

(Refer Slide Time: 07:09)



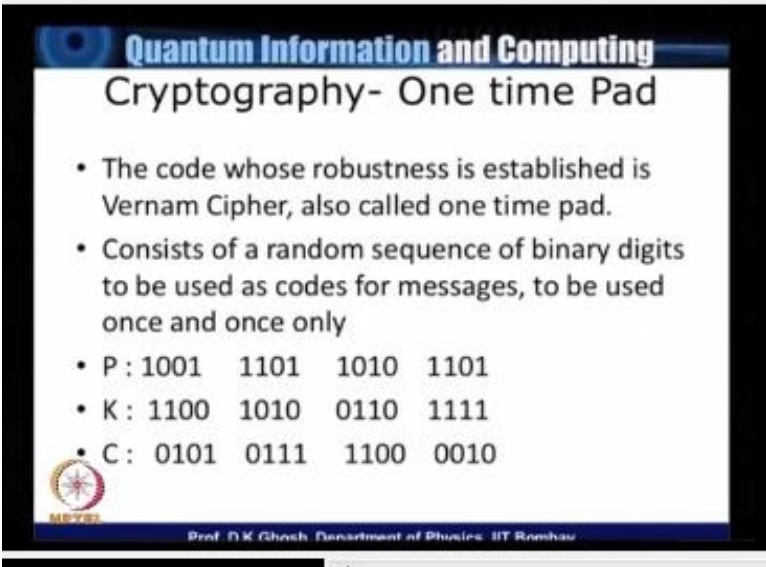
Quantum Information and Computing
Cryptography

- History – Dates back to Julius Caesar. QE-1 had established a section of espionage which dealt with creating a breaking code.
- During WW-II Germans used an electromechanical machine (Enigma) for sending messages to troops. Breaking Enigma code had a lot of importance to the Allied forces.

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

And where it dealt with creating and breaking a code, then we make a big jump on time during the World War-II Germans use an electromechanical machine known as enigma for sending messages to its troops, in fact breaking of the Enigma code had a great deal of influence on the result of the Second World War particularly in the naval battles. So let us look at what is a secured communication. Is there any communication which in principle is secure?

(Refer Slide Time: 07:53)



Quantum Information and Computing
Cryptography- One time Pad

- The code whose robustness is established is Vernam Cipher, also called one time pad.
- Consists of a random sequence of binary digits to be used as codes for messages, to be used once and once only

• P : 1001 1101 1010 1101
• K : 1100 1010 0110 1111
• C : 0101 0111 1100 0010

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

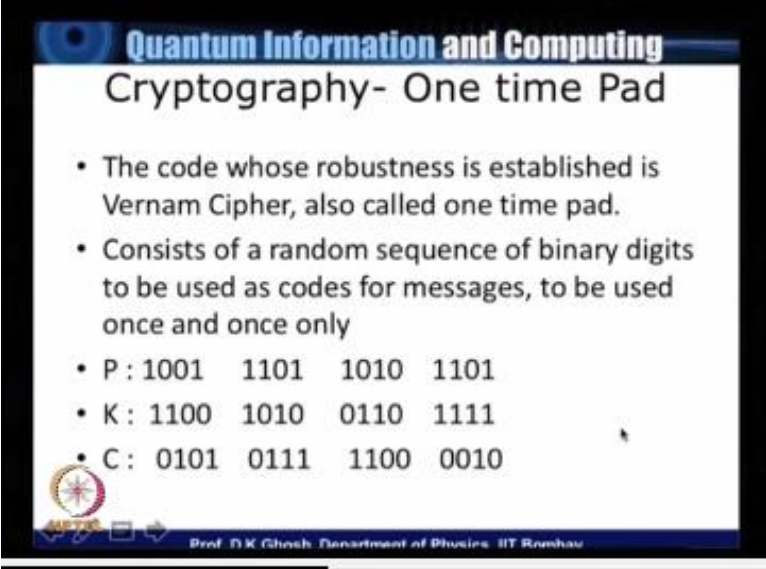
Now it turns out that most of the codes may be given, may be broken given enough time, a code which is known to be robust it is called one-time pad or it also goes by the name of Vernam cipher. Now let me explain the principle of this one-time pad, so one time-pad could be a code which is agreed between two friends to be used once and once only. Now for instance if you decide that I will send a return message.

And in that written message every word will be picked up, let us say from a particular dictionary say oxford English dictionary. Now what I do is this, I pick up a word find out on which page this word appear which column which line, so I will instead of that word which I want to send I will code it by page number, column number, line number. Now my friend who should be in the possession of an identical copy of the dictionary.

All that in needs to do is to look up that what is this code what does this code translate to. So in the way he can find out and this could be any other book on as well, it does not have to be restricted to a dictionary, the advantage of such a code is, that if you use it once and once only it can never be broken because if you repeat there is a possibility of people trying to find out what

is this document that you are using or relying on for Senegal. So basically the way I would describe it is this that suppose I have a random sequence of binary digits.

(Refer Slide Time: 10:04)



The slide is titled "Quantum Information and Computing" and "Cryptography- One time Pad". It contains the following text:

- The code whose robustness is established is Vernam Cipher, also called one time pad.
- Consists of a random sequence of binary digits to be used as codes for messages, to be used once and once only
- P : 1001 1101 1010 1101
- K : 1100 1010 0110 1111
- C : 0101 0111 1100 0010

At the bottom, it says "Prof. D.K. Ghosh, Department of Physics, IIT Roorkee".

Which will be used as codes for messages and I will be using it once and once only, so what happens here is this, look at this line here. So this is the code that I want to sign 1001 1101 1010 1101 this may stand for some letters or whatever you have. But this is this is a plain text that is why P, that is what I want to say, the plain text is the name given to the message that you want to actually sent.

Now what I do is, I generate a random key this random key is basically a sequence of random binary digits which the sender has and an identical copy of it the receiver has, no matter how far the receiver is located. Now what happens is this, that the cipher code is simply addition modulo 2 of P&K you can see this here, 1+0 is 1, 0+0 is 0, 0+1 is 1, 1+1 is 0. So this is the plain text this is the key of which both sender and the receivers have the copy. And this is C that is the coded or the cipher message which is sent over a public channel.

(Refer Slide Time: 11:39)

Quantum Information and Computing

RSA

- $C_i = P_i \oplus K_i$
- $P_i = C_i \oplus K_i$
- RSA Cryptosystem (1977) Rivest, Shamir and Adleman used a public key encryption for encoding and sending data over internet. It enables one to establish the identity of sender and receiver.

Prof. D.K. Ghosh, Department of Physics, IIT Roorkee


So basically every sequence C_i is obtained by addition modulo 2 of P_i with k_i and I can recover the p_i back at the receivers end by writing.

(Refer Slide Time: 11:56)

Quantum Information and Computing

RSA

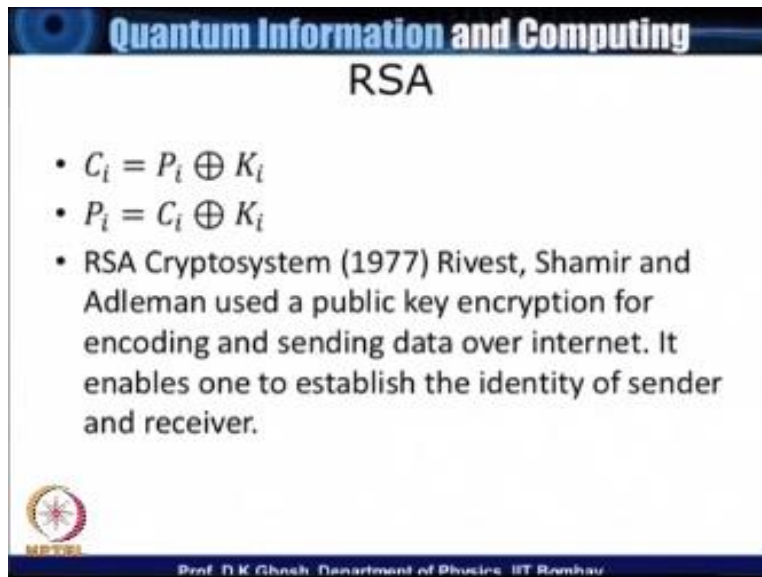
- $C_i = P_i \oplus K_i$
- $P_i = C_i \oplus K_i$
- RSA Cryptosystem (1977) Rivest, Shamir and Adleman used a public key encryption for encoding and sending data over internet. It enables one to establish the identity of sender and receiver.

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

$P_i = C_i$ addition modulo 2 of K . Now as long as this k_i is used once and once only, no one can ever break this. So this is a onetime pad, now the point is this how do you generate one-time pad we will be discussing today on the existing ways in which the one-time pads are generated. Now this obviously cannot be an agreement between two friends that I will be using an oxford English dictionary or some novel that each one of us have taken fancy too.

So this is the existing code which is being used extensively both in military communication and financial transaction is known as RSA cryptosystem.


(Refer Slide Time: 12:59)



Quantum Information and Computing

RSA

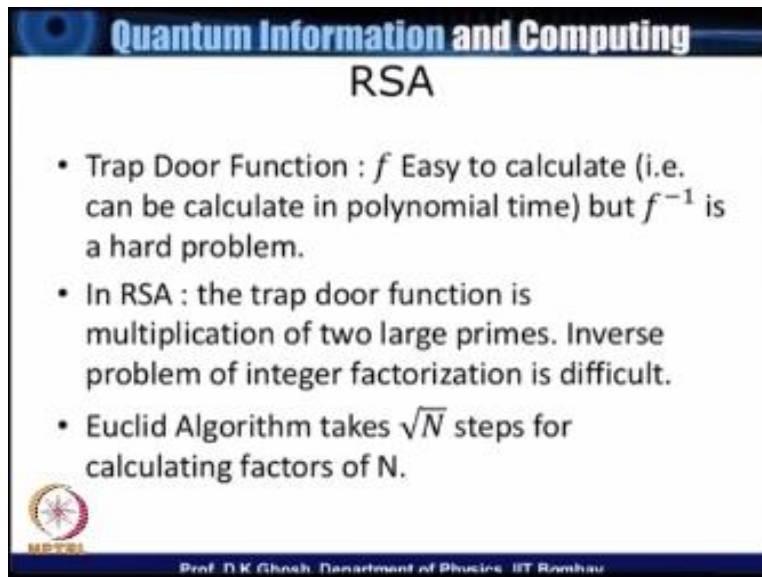
- $C_i = P_i \oplus K_i$
- $P_i = C_i \oplus K_i$
- RSA Cryptosystem (1977) Rivest, Shamir and Adleman used a public key encryption for encoding and sending data over internet. It enables one to establish the identity of sender and receiver.



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

RSA which was invented by three scientists in MIT in 1977 named Rivest, Shamir and Adleman they use what is called as a public key encryption for encoding and sending data over the Internet. Now it enables want to establish the identity of the sender and the receiver and the data remains absolutely confidential and let me explain how to works. So what RSA uses is what is known as a trap door function.


(Refer Slide Time: 13:42)



Quantum Information and Computing

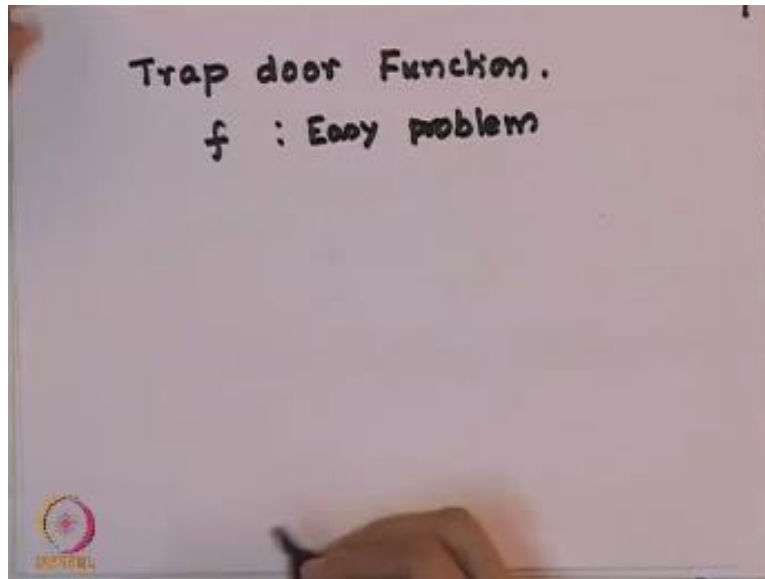
RSA

- Trap Door Function : f Easy to calculate (i.e. can be calculate in polynomial time) but f^{-1} is a hard problem.
- In RSA : the trap door function is multiplication of two large primes. Inverse problem of integer factorization is difficult.
- Euclid Algorithm takes \sqrt{N} steps for calculating factors of N .

 Prof. D.K. Ghosh, Department of Physics, IIT Roorkee

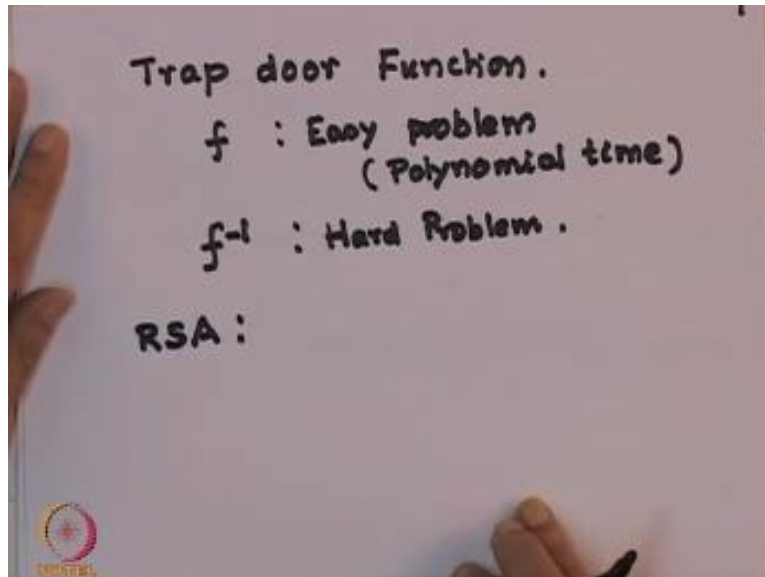
A trap door as you know is a door which opens one way but is difficult to open the other way one of the most common examples of a trap door function is the valve that exists in our heart between the oracle and the ventricle. The, it is a one-way valve which allows the blood to flow only in one direction, so that the blood does not flow back from ventricle on to the Oracles. It is a trapdoor function one-way valve. So in mathematical language I would call a function as a trap door function.

(Refer Slide Time: 14:26)



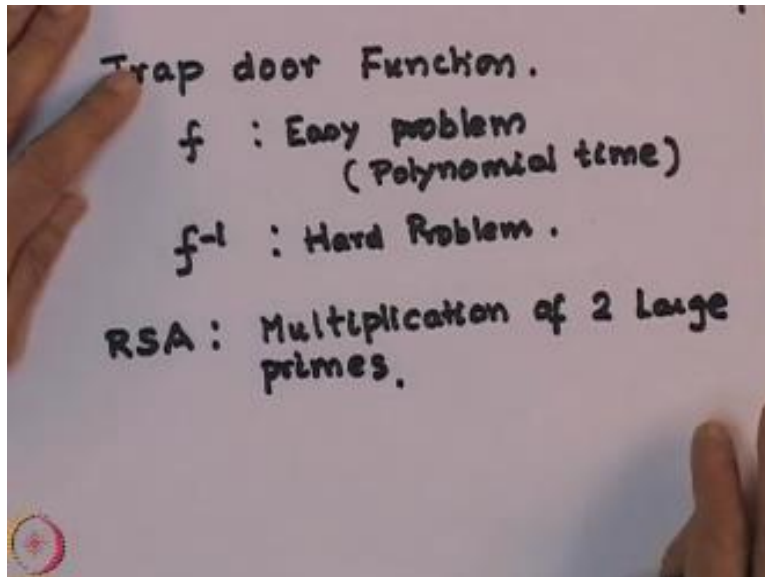
Where f is an easy problem, in the language of computer science an easy problem is one which can be computed in polynomial time.

(Refer Slide Time: 14:53)



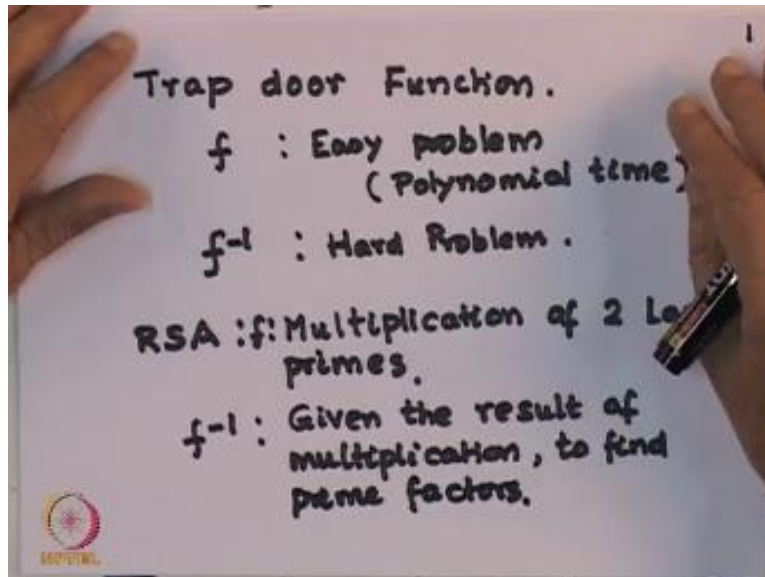
We have seen this and discussed it several times, but however its inverse that is coming back from that trap door to the other side is a hard problem usually a non polynomial time or an exponential problem. Now what RSA does is to choose the following as examples of the trap door function that we use. The easy problem is multiplying two large primes.

(Refer Slide Time: 15:41)



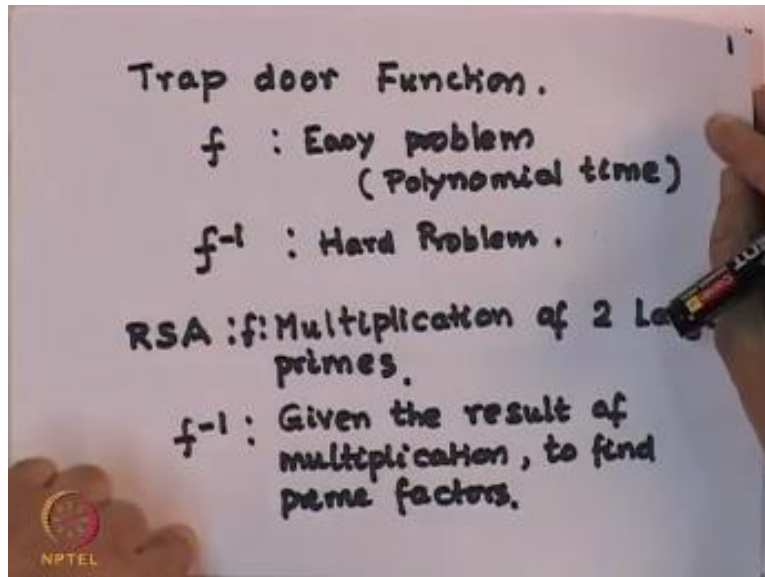
So multiplication of two large primes is my one-way function, this is multiplication as we all know is an easy problem, but given the result of multiplication the inverse problem.

(Refer Slide Time: 16:13)



So this is my f , the inverse problem is given the result of multiplication to find out the factors prime factors we have discussed this in detail when we were talking about source algorithm and we had pointed this out as one of the possible successes of the quantum computers whenever it comes into play, that there are now quantum algorithms which probably make it possible for computing what are known as integer factorization. But we are discussing still the classical regime where.

(Refer Slide Time: 17:17)



f is easy multiplication is easy factorization is difficult.

(Refer Slide Time: 17:25)

Quantum Information and Computing

RSA

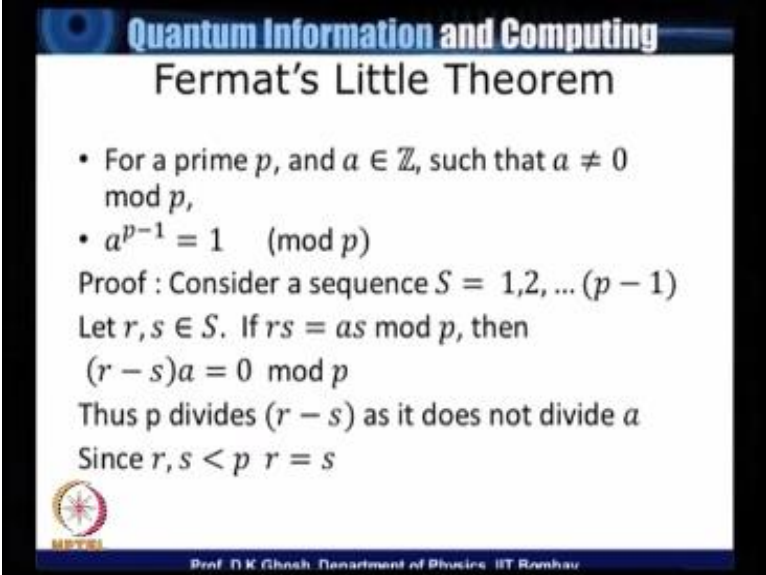
- Trap Door Function : f Easy to calculate (i.e. can calculate in polynomial time) but f^{-1} is a hard problem.
- In RSA : the trap door function is multiplication of two large primes. Inverse problem of integer factorization is difficult.
- Euclid Algorithm takes \sqrt{N} steps for calculating factors of N .

Prof. D.K. Ghosh, Department of Physics, IIT Roorkee

Just to go back to our school days we used to use what is known as the Euclid algorithm for calculation of factors as you know what we use to do in Euclid algorithm is to try to do a repeated division. Now so what we do basically is this start with whether the number is divisible by 2 number 3, 4 extra, extra and of course you could reduce it because if it is divisible by 2 you need not check go further but basically it requires of the order of \sqrt{N} attempts before you have found a factor.

If there is any the reason is that if a number is known to have two factors then one of the factors has to be less than or equal to the \sqrt{N} and the other factor of course is greater than or equal to the square root of n now but as we know square root of n is a hydrometer now we will now be talking about the RSA algorithm but before we can discuss what are the elements of RSA algorithm I need three major components and these three major components are the following so the first one if.

(Refer Slide Time: 19:04)




Quantum Information and Computing

Fermat's Little Theorem

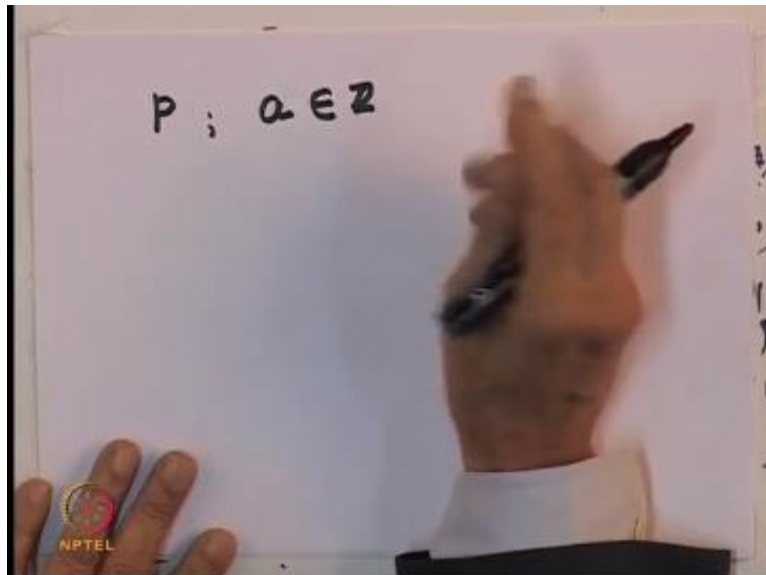
- For a prime p , and $a \in \mathbb{Z}$, such that $a \not\equiv 0 \pmod{p}$,
- $a^{p-1} \equiv 1 \pmod{p}$

Proof : Consider a sequence $S = 1, 2, \dots, (p-1)$
Let $r, s \in S$. If $rs \equiv as \pmod{p}$, then
 $(r-s)a \equiv 0 \pmod{p}$
Thus p divides $(r-s)$ as it does not divide a
Since $r, s < p$ $r = s$

 Prof. D.K. Ghosh, Department of Physics, IIT Roorkee

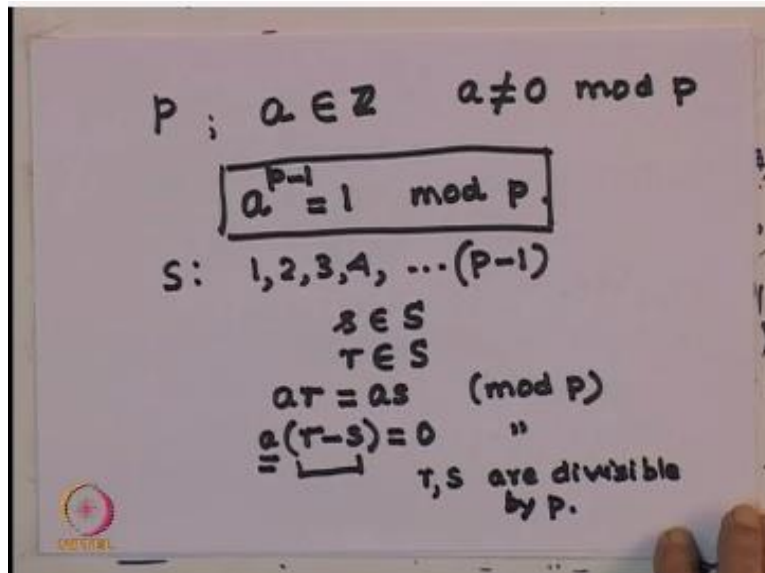
I can look at the slide is what is known as the Fermat's little theorem not to be confused with the more famous form as last theorem regarding existence of things parallel to Pythagoras theorem for other integers this is a different theorem much used in discrete mathematics but not as well-known now basically what we are trying to say is this that supposing have a prime number P .

(Refer Slide Time: 19:32)



And consider any number a belonging to the set of integers Z now the number a .

(Refer Slide Time: 19:49)



Is not divisible by so in other words a is not $\equiv 0 \pmod{p}$ in that case the former's little theorem states that $a^{p-1} = 1 \pmod{p}$ so this is for mass little theorem let me give you a quick proof of this now first consider a set of numbers 1 2 3 4 like this up to $P-1$ remember P is a prime number so there are no factors now having done that suppose I take any element out of this set let me choose an element small s belonging to S and another element are also belonging to S now suppose I multiply both s and R with a so I get ar and as is now under what conditionally is $ar = as$.

Of course everything is \pmod{p} now you can bring display that side and you can immediately say this means $a \times r - s = 0 \pmod{p}$ but have already started by saying is not divisible by P so if a is not divisible by P it means $r - s$ are divisible by P so r and s are divisible by P but we have already said.

(Refer Slide Time: 21:58)

$P; a \in \mathbb{Z} \quad a \not\equiv 0 \pmod{p}$

$a^{p-1} = 1 \pmod{p}$

$S: 1, 2, 3, 4, \dots, (p-1)$

$s \in S$
 $t \in S$

$$at = as \pmod{p}$$
$$\underbrace{a}_{\neq 0} (t-s) = 0$$

"
 $t-s$ are divisible by p .

r sorry I, I did not mean r and s I said $r - s$ is divisible by P okay but I have already said that r and s are less than P sure it therefore this statement has no solution unless of course.

(Refer Slide Time: 22:16)

$P; a \in \mathbb{Z} \quad a \not\equiv 0 \pmod{p}$

$a^{p-1} = 1 \pmod{p}$

$S: 1, 2, 3, 4, \dots, (p-1)$

$s \in S$
 $t \in S$

$at = as \pmod{p}$

$\underbrace{a}_{\neq 0} (t-s) = 0$ "
 $\underbrace{\quad}_{\neq 0}$ are divisible by p .

r happens to be equal to s so therefore if you multiply each of these members of this set s by a number a which is not divisible by P .

(Refer Slide Time: 22:40)

$P ; a \in \mathbb{Z} \quad a \neq 0 \pmod{P}$

$a^{P-1} = 1 \pmod{P}$

$S : 1, 2, 3, 4, \dots, (P-1)$

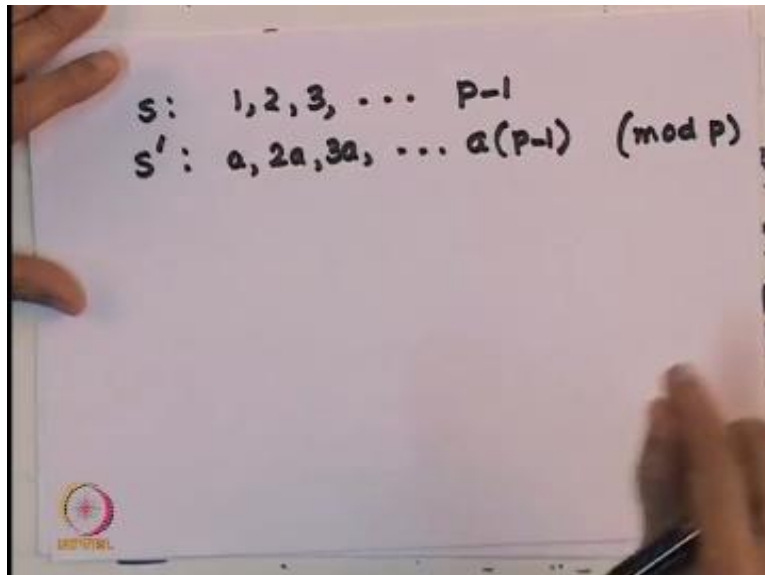
$s \in S$
 $t \in S$

$$at = as \pmod{P}$$
$$a(t-s) = 0$$

$\frac{t-s}{1} \overset{a \neq 0}{\neq} 0$ " is divisible by P .

Then a are equal to $s \pmod{p}$ implies that r is equal to s so what am I doing is this when I multiply each of these numbers by a modulo P I am generating the same sequence of number in a different order because no two numbers can be identical is what we have proved that the if you have a are equal to a s then it means our must be good so therefore the set s and they said that I obtained by multiplying each element with a so original set is.

(Refer Slide Time: 23:13)



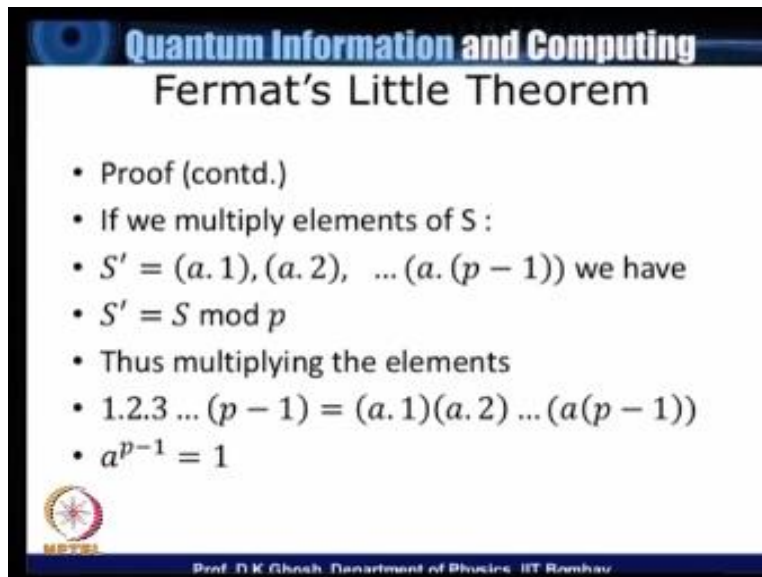
A photograph of a whiteboard with handwritten mathematical expressions. The expressions are:

$$S: 1, 2, 3, \dots, p-1$$
$$S': a, 2a, 3a, \dots, a(p-1) \pmod{p}$$

The whiteboard has a small logo in the bottom left corner. A hand is visible on the left side, and another hand is visible on the right side, holding a pen.

1 2 3 4 up to $P - 1$ and the set s prime is obtained by multiplying each number with a so I have got a $2a$ $3a$ etc. a times $P - 1$ so these two sets are identical sets mind you I am talking about modulo P they are identical set but in arranged in a different order so let us look at this.


(Refer Slide Time: 23:52)



Quantum Information and Computing

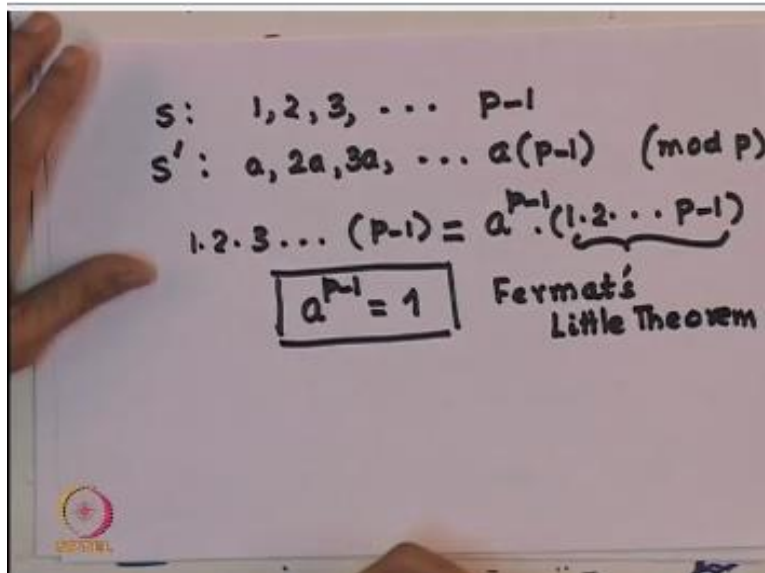
Fermat's Little Theorem

- Proof (contd.)
- If we multiply elements of S :
- $S' = (a. 1), (a. 2), \dots (a. (p - 1))$ we have
- $S' = S \pmod{p}$
- Thus multiplying the elements
- $1.2.3 \dots (p - 1) = (a. 1)(a. 2) \dots (a(p - 1))$
- $a^{p-1} = 1$


Prof. D.K. Ghosh, Department of Physics, IIT Roorkee

So what we are saying is this that if I do this then I get the same set supposing I now multiply them throughout.

(Refer Slide Time: 24:00)

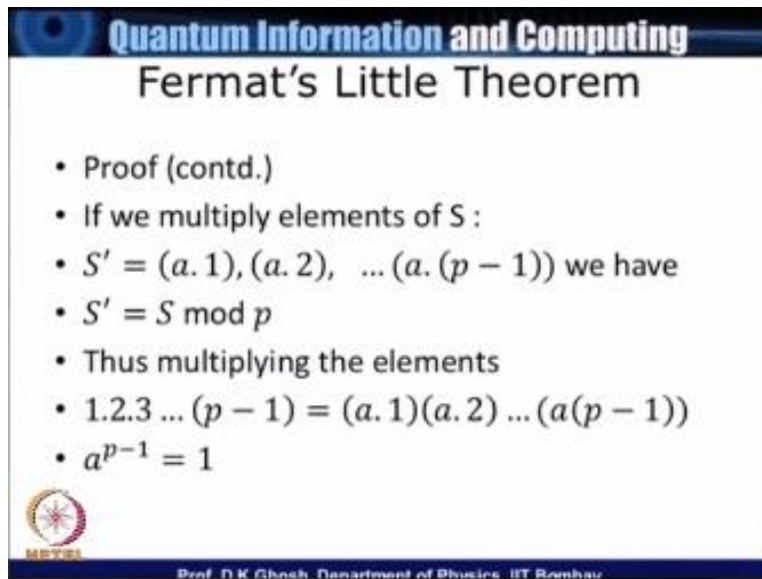


The image shows a whiteboard with handwritten mathematical derivations. At the top, two sets are defined: $S: 1, 2, 3, \dots, p-1$ and $S': a, 2a, 3a, \dots, a(p-1) \pmod{p}$. Below this, the product of the elements in S is equated to the product of the elements in S' , resulting in $1 \cdot 2 \cdot 3 \dots (p-1) = a^{p-1} \cdot (1 \cdot 2 \cdot \dots \cdot p-1)$. The term a^{p-1} is boxed, and the text "Fermat's Little Theorem" is written to its right. A small logo is visible in the bottom left corner of the whiteboard.

$$S: 1, 2, 3, \dots, p-1$$
$$S': a, 2a, 3a, \dots, a(p-1) \pmod{p}$$
$$1 \cdot 2 \cdot 3 \dots (p-1) = a^{p-1} \cdot (1 \cdot 2 \cdot \dots \cdot p-1)$$
$$\boxed{a^{p-1} = 1} \quad \text{Fermat's Little Theorem}$$

So I get $1 \times 2 \times 3 \dots p-1$, is equal to there are $P - 1$ terms so a appears $p - 1$ times so I get $a^{p-1} \times 1 \times 2 \times 3^{p-1}$ though in the second set they will appear in a different order. So comparing the two sides I get $a^{p-1} = 1$ so this is Fermat's Little Theorem.


(Refer Slide Time: 24:50)



Quantum Information and Computing

Fermat's Little Theorem

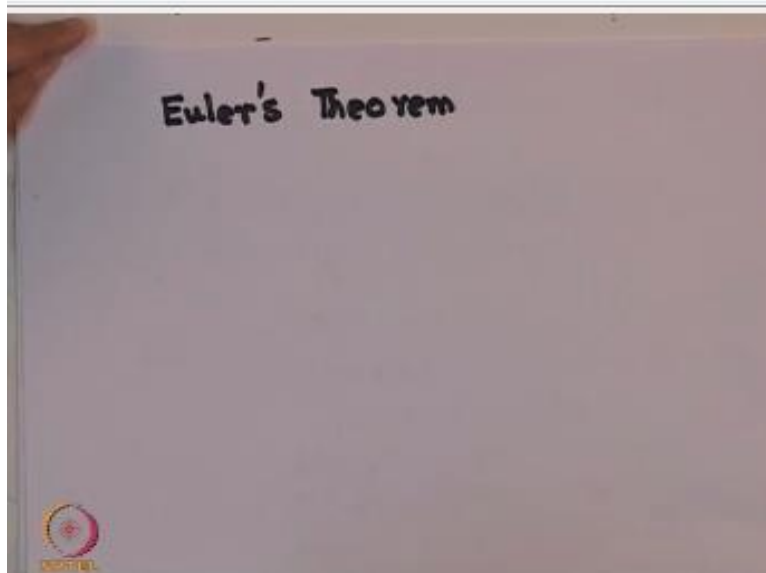
- Proof (contd.)
- If we multiply elements of S :
- $S' = (a. 1), (a. 2), \dots (a. (p - 1))$ we have
- $S' = S \text{ mod } p$
- Thus multiplying the elements
- $1.2.3 \dots (p - 1) = (a. 1)(a. 2) \dots (a(p - 1))$
- $a^{p-1} = 1$



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

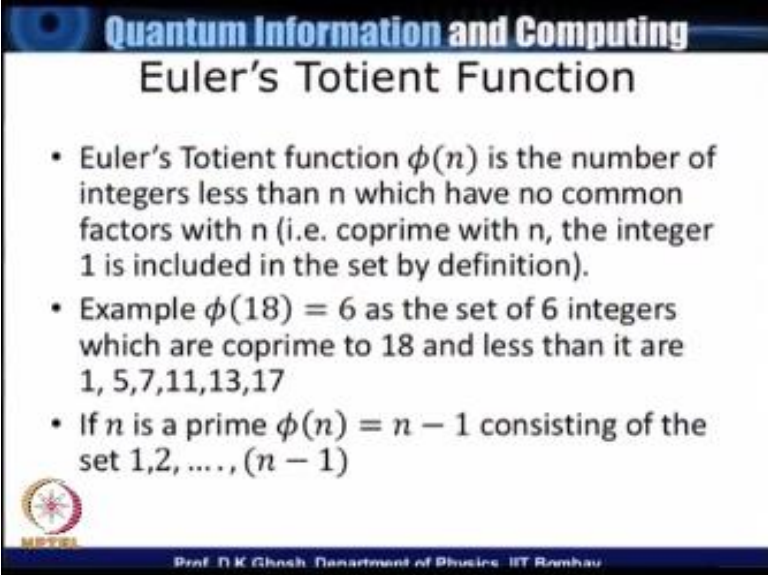
The second theorem or element of proof that I require goes by the name of Euler's theorem.

(Refer Slide Time: 25:04)



The same Euler whose algorithm we wanted to use for factorizing but we are not successful, but before we do that let me define what is known as Euler's Totient function it is shown in the slide.


(Refer Slide Time: 25:24)



Quantum Information and Computing

Euler's Totient Function

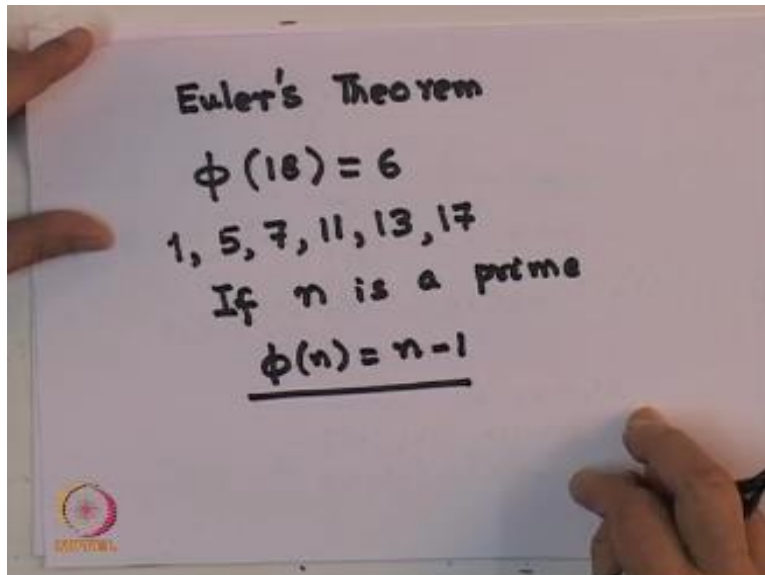
- Euler's Totient function $\phi(n)$ is the number of integers less than n which have no common factors with n (i.e. coprime with n , the integer 1 is included in the set by definition).
- Example $\phi(18) = 6$ as the set of 6 integers which are coprime to 18 and less than it are 1, 5, 7, 11, 13, 17
- If n is a prime $\phi(n) = n - 1$ consisting of the set 1, 2, ..., $(n - 1)$

 Prof. D.K. Ghosh, Department of Physics, IIT Roorkee

So Euler's Totient function corresponding to a number n integer n is the number of integers which are less than n which have no common factors within I will illustrate what I mean by an example. Now when we say two numbers have no common factors one also uses a phrase that these two numbers are co-prime remember we are not talking about two numbers being primes we are simply saying that two numbers are co-prime it means there is no common factor between them.

For example a number 15 and a number let us say 16 they are co-prime to each other because 15 has only factors 3 and 5 and the only factors of 16 are two, so therefore there are no factor, this Totient function is essentially the, if you count the number of integers less than n which do not have a common factor with the argument of five just to give you example consider $\phi(18)$.

(Refer Slide Time: 26:46)



So $\phi(18)$ is equal to 6 all that I do is to count how many numbers less than 18 have no factors common with 18 and we use one as a part of the set by definition 2 is a factor of 18 3s 4s I mean it is not a factor but they are co common factors between them 5 does not have a factor, 7 does not have a factor, 11 does not have a factor, 13 and 17 clearly if n is a prime if n is a prime then $\phi(n)$ must be equal to $n - 1$ because all numbers below and are co-prime with n . In the next lecture we will continue this discussion and try to come up with what the RSA algorithm is all about.

**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)

Copyright NPTEL CDEEP IIT Bombay