Cryptography and Network Security

Prof. D. Mukhopadhyay

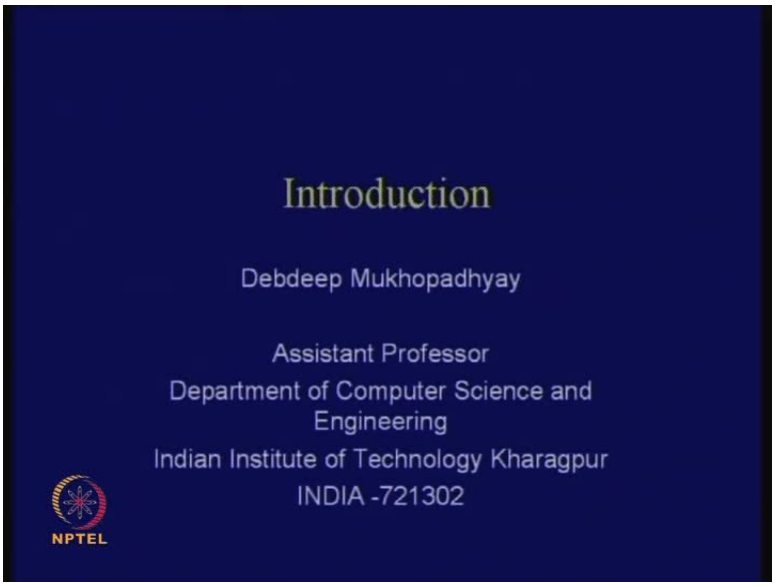
Department of Computer Science and Engineering

Indian Institute of Technology, Kharagpur

Lecture No. # 01

Introduction

(Refer Slide Time: 00:25)



Welcome to this course of cryptography and network security. So, I shall be, in today's class, I shall be introducing this topic and I shall be trying to address about certain issues which are important in crypto and network security.

This course, essentially deals with the, deals with the, communication of data between two, I mean a sender and a receiver. And the idea is that the sender and the receiver are communicating information over an insecure channel, and there is an eavesdropper who is trying to essentially understand, what information is being transferred from the sender to the receiver.

So, the objective of the sender and the receiver would be to use cryptography or principles of cryptography and to ensure that certain properties of the data are not compromised. For example, the integrity of the data, that is whether the data has been

modified or not, the secrecy of the data, that is what information has been transferred, and there are similar certain other objectives which needs to be satisfied.

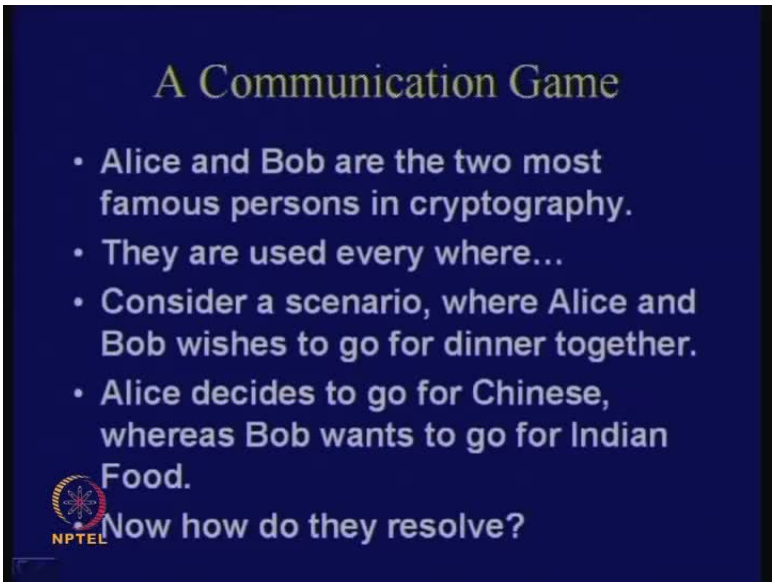
So, essentially cryptography or the principles of cryptography gives you certain mechanisms or certain principles of how you can carry these operations forward, how you can satisfy these properties when you transfer data, transfer information over an insecure channel. So, that is the objectives of essentially studying this subject of cryptography and network security.

(Refer Slide Time: 01:53)

In order to understand that, we will see a communication game, and we will see essentially, what are the issues which are involved in such a particular, such a game; then, we shall define the concept of protocols as opposed to something which we know as algorithms. And then we shall define some, some, magic function which will be used to solve this simple protocol or simple game that we considered.

This magic function is something, which we will try to understand and essentially throughout the course, throughout this entire course, we shall be studying various techniques, various methods, how you can realize this magic function. So, these magic functions are realized in a form of cryptographic functions. So, in today's class we shall end with this particular note.

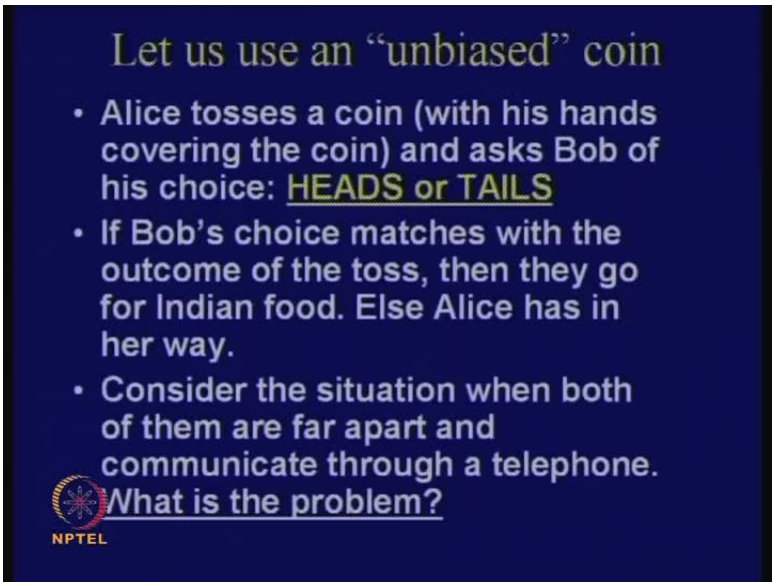
(Refer Slide Time: 02:46)



So, going into the communication game, let us consider, let us consider a game where Alice and Bob, who are essentially, you will be seeing in the literature, this Alice and Bob, you can imagine, they are the most famous persons in cryptography, that is, they are the most widely popularly known, I mean, known names for the sender and the receiver. So, Alice and Bob are the two most famous persons in cryptography and they are used everywhere.

So, Alice and Bob essentially are just two names to denote the sender and the receiver; we can understand like, we can take Alice to be the sender and Bob to be the receiver of the information. And just let us consider a scenario where Alice and Bob wishes to go for a dinner together and they want to, and Alice would like to go for a Chinese food whereas Bob intends to go for an Indian food.

(Refer Slide Time: 03:55)



So, the question is that if Alice and Bob want to dine together, then how do they resolve this problem of not concurring at what they want to have for dinner? So, how do they resolve this problem? Very simple, they can use an unbiased coin; so, this can be one example, that is, if I believe that both of them are not ready to compromise and they have got, I mean, very strong desires either to go for a Chinese food or an Indian food, then what Alice will do is that Alice will toss an unbiased coin.

By the term unbiased coin, we mean that the probability, of the coin, when we toss the coin, the probability that the outcome is a head is half and is equal to the probability that the outcome is a tail. So, Alice what she does is that she tosses a coin, with her hands covering the coin and asks Bob of his choice; so, essentially, Bob has to say that head or tail. And if Bob's choice matches with the outcome of the toss, then they go for an Indian food, that is Bob wins the game; else, Alice has in her way, which means, Alice says that we have to go for the Chinese food. This is a very, quite an acceptable solution, assuming that the coin is an unbiased coin and the coin has got only two possibilities, that is it can either result in a head or it can either result in a tail; so, considering this situation, this is quite an easy problem, which can be solved.

But imagine that is what happens in real life, is that most of us are quite distant apart; that is, for example, imagine that Alice and Bob are two friends who stay a far distance apart and for them, they want to meet at one place and have the dinner, but where do

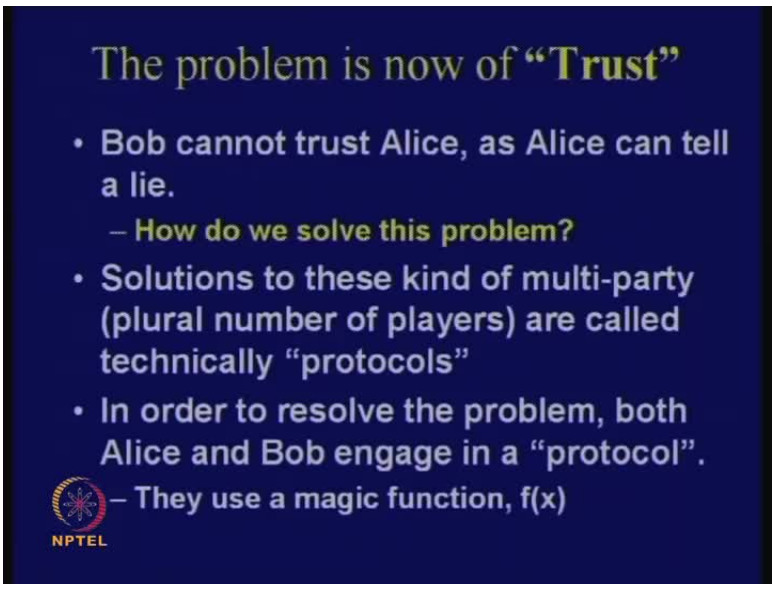
they meet? That is a problem. Therefore, they cannot have an unbiased coin and they cannot toss that at the same place.

So, consider the situation when both of them are far apart and communicate through a telephone; and so, therefore, what is the essential difference when we are separating out Alice and Bob over a large distance, from this particular problem? What is the essential problem?

The problem is essentially of something which we call trust; that is, when Alice and Bob are quite a distance apart, then, for example, if Alice tosses the coin, so imagine that they engage the same technique, that is, both of them use the unbiased coin and even when they are distant apart, then Bob cannot see the outcome of the toss.

Therefore, when Alice takes a coin and tosses, since Bob is at a distance apart, Bob is unable to see the outcome of what happens at Alice's end. So, therefore Bob does not trust Alice; so, Alice can claim Alice; that is the point. Therefore, they have to do something better, they have to do something different.

(Refer Slide Time: 06:50)



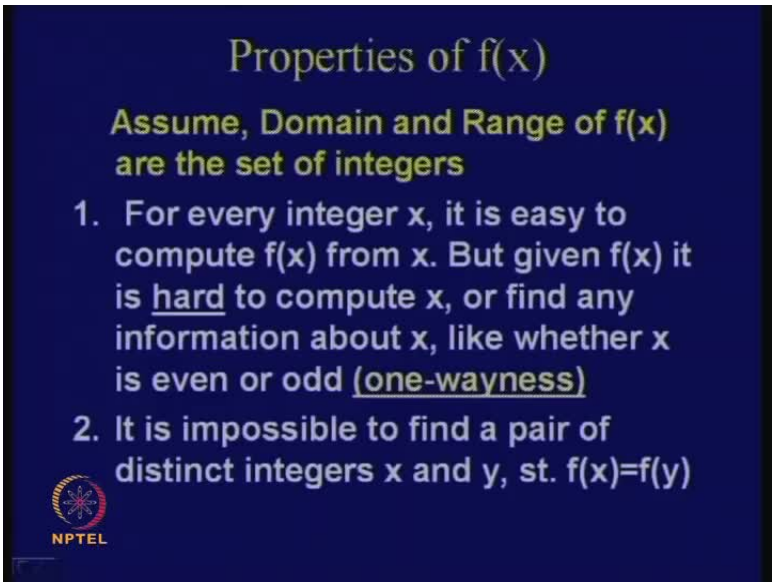
So, in order to do that, what they do is that, therefore, the problem is that in this case of trust, and Bob cannot trust Alice as Alice can tell a lie. So, the question is, how do we solve this problem?

These kinds of problems are very popular in our network security domain and often involve not only two parties, but actually multi-party scenario; therefore, there is more than one party who are playing this game. So, these types of, these types of scenarios are very commonly or technically known as protocols.

So, therefore, in order to resolve the problem, both Alice and Bob have to engage in a protocol and they have to solve this problem. So, therefore, they have to engage in a protocol. Therefore, protocol is something which is similar to an algorithm; so it is basically a sequence of steps in order to solve a problem, but the thing is that, in case of protocols we have got more than peoples, more than one parties who are involved in a game; so, that is the idea. So, in this case, we have got two parties like we have got Alice and Bob, who want to solve the problem and they need to concur upon agreement, but they are not at the same place geographically.

In order to do that, they use a magic function, and I call that as f x or denote that as f x. Let us see what these properties of this magic function should satisfy, so that this problem of trust can essentially be resolved.

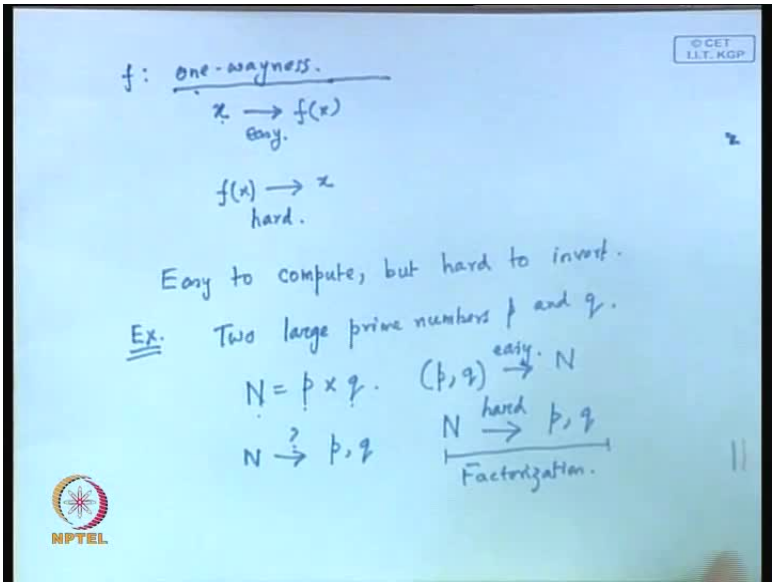
(Refer Slide Time: 08:27)



Let us consider some properties of the function f x. So, you assume that the domain and the range of f x are the set of integers; so, therefore, you understand what is meant by domain and range. Imagine, that x is chosen from a pool of values and I call that to be the domain of f x and all the possible values that f x can result to, is called a range of f x.

So, therefore, imagine that x is chosen from the set of integers and it also results in the set of integers. So, therefore, f x has got a domain and range, both of which are the set of integers. So, for every integer x, it is easy… So, therefore, the property of f x are as follows, so the property of f x: the first property, something which we call as one-wayness; it means, very simply that this function f x is easy to compute. So, let us just try. Let us not go into what is meant by easy and what is meant by not easy or hard; let us just take it as two terms; so, let us not go into the technical details, right now. So, therefore, what I am trying to say is that for every integer x, it is easy to compute f x from x, but it is easy in one way; but given f x, it is hard to compute x.

(Refer Slide Time: 09:53)



Therefore, the problem is as follows like if you take x, the property of this function f is something we have called as one-wayness. So, if I give you x, then to compute f x, is easy. So, therefore, for example, you can just take x and very easily compute the value of f x, but if I give you the value f x and I ask you what is the value of x - then this should be a relatively difficult problem.

So, that is what is meant by the one-wayness property of f. And actually in literature we will see that inspite of lot of research, we have got several, we have got few candidates for one-way functions. But there are no concrete proofs, which says that whether the function can be prove to be a one-way function or not. But this is the notion; so, the

notion is what? The notion is of something which I call as one-wayness, which means, a function which is easy to compute, but hard to invert.

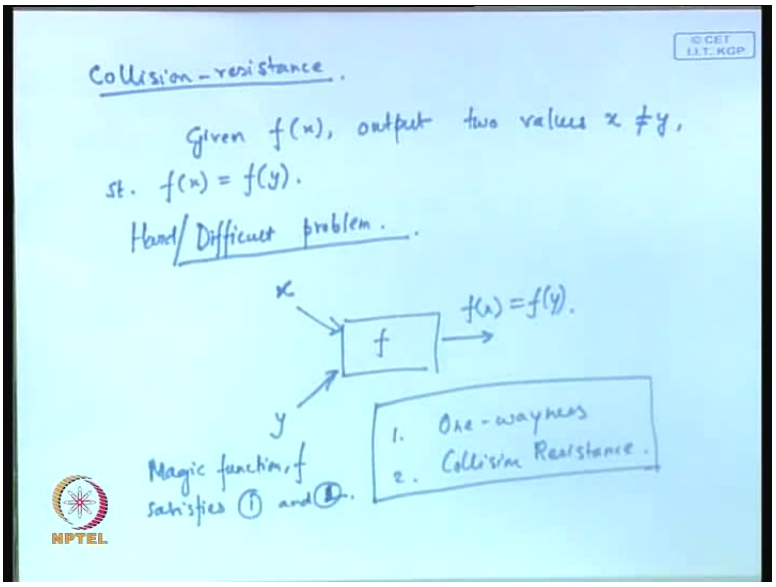
So, I give an example, which is believed to be correct, like you take two prime numbers or two large prime numbers p and q, so if I tell you that N is equal to p into q, then given p and q, computing N is an easy problem; it is quite relatively an easy problem.

So, I give you p and if I give you q, from there computing the value of N is an easy problem; but if I give you N and I ask you - what is the value of p and q, it is believed to be a hard problem; so, if I give you N and I ask you what are the corresponding values of p and q, it is believed to be a relatively hard problem. So, this problem is commonly known as the factorization problem.

So, this is a probable candidate for a one-way function; this is one property which the function f needs to satisfy. The other property is that, when I say impossible, I mean to say, it is difficult to find a pair of distinct integers x and y, such that f x and f y are the same; so this is also sometimes called collision resistance.

So, therefore, if I give you a function f and I tell you that, report two values of x and y which are not the same, but which results in a same values of f x and f y, then this should be a relatively hard problem. So, therefore it says that, therefore, collision resistance means this that is…

(Refer Slide Time: 13:02)



So, next property is of collision resistance, which says that, if I give you, or given a function f x, output two values: x not equal to y, such that f x and f y are same; so, this should be a difficult problem.

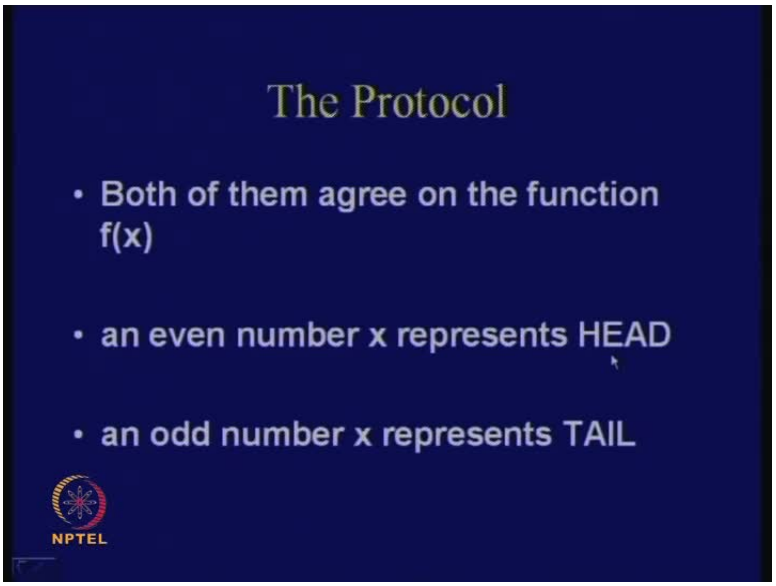
I will come to at the end of the class, to explain a little bit about what I mean by an easy problem or what I mean by a hard or difficult problem; this is, a hard or a difficult problem. So, therefore, it is not easy to report two values x and y which will essentially result in the same values of f x and I mean, which will result in the same values of the output of f.

So, if I take a function f and to take or report two values of x and y which are different, but which results in same values of f x and f y, should be hard or impossible; so, therefore, the property essentially satisfy these two properties: the first property is of one-wayness and the second property is of collision resistance.

Let us assume that the magic function f essentially satisfies these two properties. Now, let us see if Alice and Bob engage such a magic function, then does their problem of resolution get solved. So, therefore, the magic function f satisfies these properties of one and two, and now the question is that - if it does so, then does the problem of resolution get solved?

So, therefore, in order to solve this problem, Alice and Bob essentially have to engage the function f in something, which I called as a protocol.

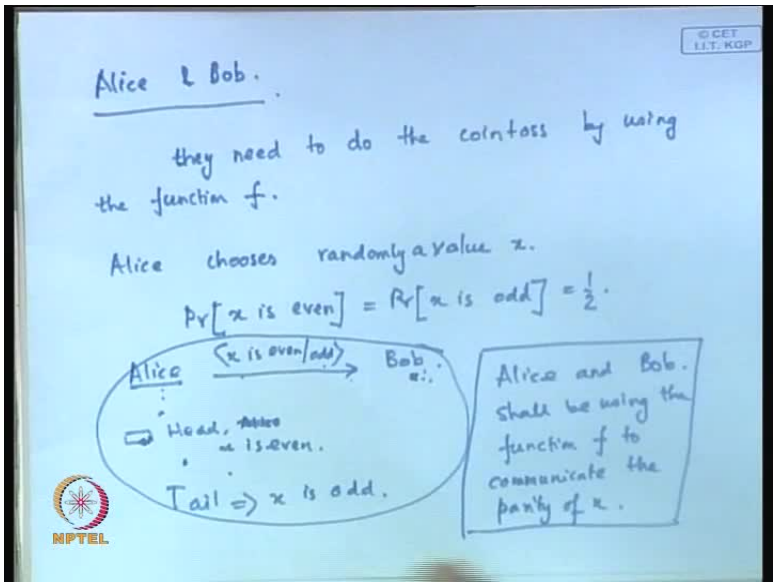
(Refer Slide Time: 15:24)



Let us see what could be the protocol. So, both of them agree on the function f x; so, therefore, they decide upon a function f x and which they believe is, which they believe should satisfy these two properties of one-wayness and collision resistance. And they assume that head will be represented by an even number x and tail or the outcome of tail will be represented by an odd number of x.

So, see what Alice and Bob are trying to do? Essentially, Alice and Bob are trying to do the same thing, like tossing an unbiased coin when both of them were together, but now since they are apart from each other, they cannot really do it straightaway; so, what they do is that they use this magic function f, and essentially try to, which satisfies these two properties and try to do the same thing. So, essentially they have to decide whether a head is resulting.

(Refer Slide Time: 16:53)



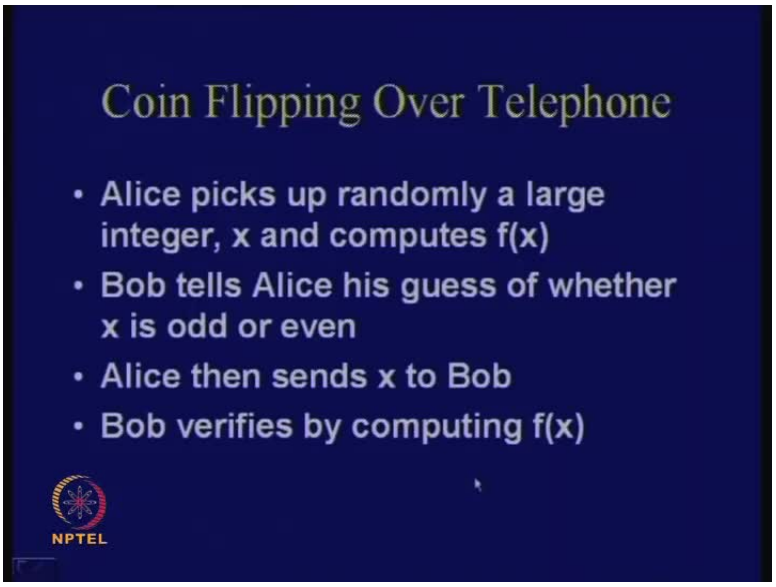
I mean, so, what they will do is that they will try to replace the function, they will try to replace the function, if by, they will try to replace the unbiased coin by the function f, and will try to see that whether a head results or whether a tail results by the computation of the function f x. So, what Alice and Bob does is as follows - so, Alice and Bob essentially does the same thing; that is, now they need to do the coin toss by using the function f. So, they need to use the coin toss by using the function f and in order to do that, there are two possibilities. The possibilities are whether…

So, what they essentially try to do here is that, Alice chooses randomly a value x, chooses randomly a value x; so, this x, if it is randomly chosen from the set of integers, the probability that x is even is the same as the probability that x is odd and that is equal to half, but till this part there is no problem. The problem happens or the problem of trust happens, when Alice communicates this information, that is, whether x is even or odd to Bob; so, we try to understand the problem and is as follows - if Bob predicts that x is even or so therefore imagine that Alice essentially does a coin toss at its end, and depending upon the coin toss, that is whether the toss results in head or a tail, it chooses the value of x to be even or odd. So, therefore, if this coin toss results in head, Alice chooses, I mean x is even, but if this coin toss is a tail, then x is odd. So, remember what was the game? The game was that Bob initially has to guess, what was the parity of x, that is, whether the value of x was even or odd?

But the point is, since they are doing over a communication channel, why Bob is not believing Alice or does not have trust in Alice is that, after the result of the coin toss, Alice can essentially say or communicate a wrong information to Bob; that is, even if Bob is correct, like, for example, coin toss at Alice's end was actually head, and when Bob also had said that head would have been the resultant, head would have been the outcome, so what Alice can do is that Alice can pass on a wrong information, that the result was a tail.

In order to prevent such a scenario, Alice and Bob shall be using the function f; so, in order to solve this problem of trust, Alice and Bob shall be using the function f to communicate the parity of x; that is, whether x is even or whether x is odd - that information now Alice will not pass just on the clear, but instead will compute the value of f x and will pass on that information to Bob.

(Refer Slide Time: 21:16)



I believe that even if this is not clear till now, it will be clear, I will try to make it more clear. So, at this point, at least try to understand, that a head event or a head outcome is being represented by even number x; whereas, a tail is being represented by an odd number x. So, what Alice does is as follows. Therefore, I call this as a coin flipping over the telephone; so, essentially, they are flipping the coin as we have done when both Alice and Bob were together, but only in this case, we have to solve this problem over the telephone.

So, what Alice does is that Alice picks up randomly a large integer x; so, therefore, when I say randomly, it is just like they are based upon the outcome of a toss at which Alice does. So Alice takes an unbiased coin and it does not really matter at Bob's end whether it is an unbiased or biased, because Alice does not have an advantage right now about that. So that just imagine, that Alice picks up randomly a large integer x and computes the value of f x; so, Bob tells Alice his guess of whether x is odd or even; so what Bob does is Bob predicts - what was the guess of Alice.

So, in this case, Alice picks up randomly a large integer x and computes the value of f x and this value of f x is now passed to Bob; so, Bob now has the value f x. And Bob, based on the value of f x, so Bob essentially has got the information of f x, but now what Bob needs to do, is that Bob needs to tell Alice his guess of whether x is odd or even.

I will come to the properties, but first of all just try to understand the protocol. Then Alice what she does is that Alice then sends x to Bob and Bob verifies by computing the value of f x. So, here, there are two important things to be noticed. The first important thing to be noticed is that - Bob has got an information of f x and when it is trying to guess, that is, whether x is odd or even, in order to see that Bob does not have an advantage of guessing, means what? Means that the function f x should not reveal any information about the oddity or even parity of x, which means that f x, which means that f x should not reveal any information about x and that property is satisfied by the one-wayness guarantee of the magic function f.

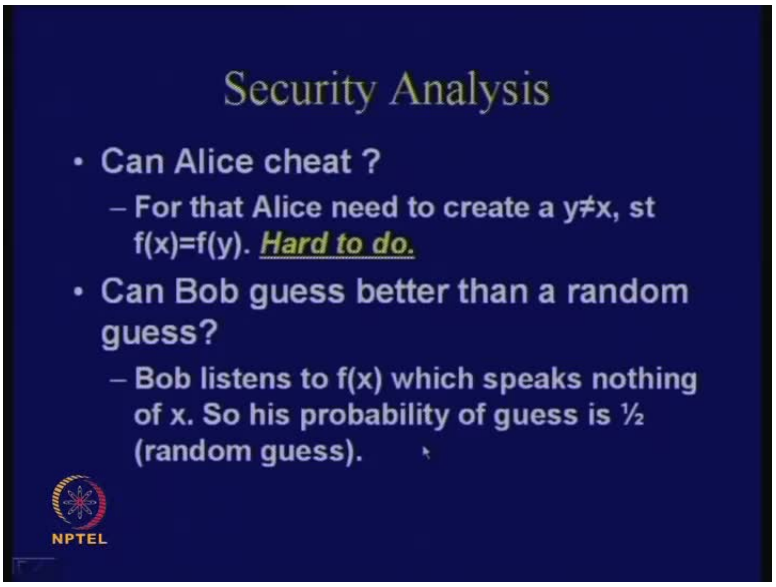
So, how we will do it, we are not really bothered at this point, we are just trying to understand the properties. The other important thing is that, when I am considering the end of Alice, when Alice is computing the value of f x and sending this value of f x - why is Alice doing so? Alice is doing so, because if Bob's guess is correct, then later on Alice should not be able to change the value of x, that is, change the parity of x, such that the value of f x which she has previously committed will remain the same. So, what does that mean? So, what Alice will try to do, if she wants to cheat? She will try to change x to x dash, such that the parity of x and the parity of x dash are different. And what is the other property? The thing is that, the value of f x and the value of f x dash will collide.

So, that is how Alice will try to cheat Bob, because then it can say, that see actually what you have guessed is wrong, because what is you have guessed is, you have guessed x,

but whereas the correct value is x dash, and you see that you can calculate the value of f x dash and it will be the same as that of f x. But this is also hindered and Alice also does not have this advantage because of the collision resistance guarantee or collision resistance property of the magic function f x.

So, therefore, therefore, that is the reason why we say that the magic function f x needs to have the one-wayness property and also the collision resistance property. I hope it is clear till this point.

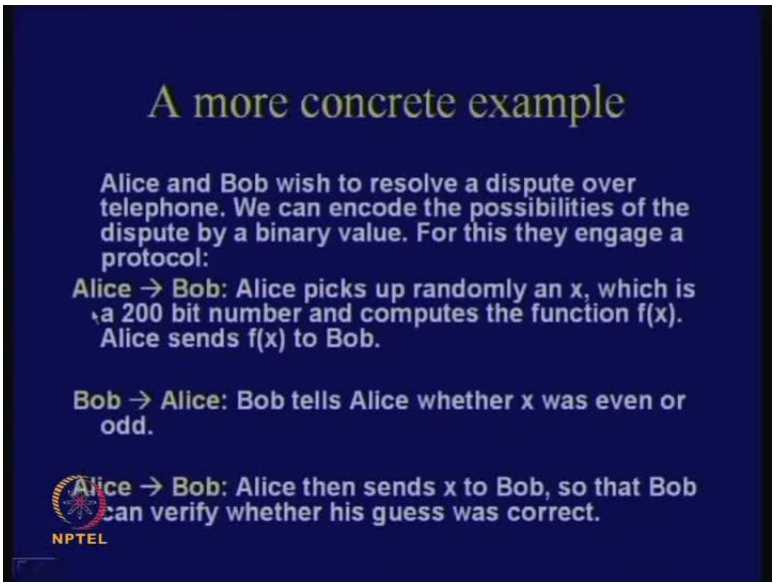
(Refer Slide Time: 25:56)



So, therefore, if I do a security analysis, so the question is can Alice cheat? For that Alice needs to create a y, which is not equal to x, such that f x and f y are the same. When I say that y is not equal to x, which means in this case, the important information is the parity of y and the parity of x are different, such that f x and f y are same and this is believed to be hard. The other important thing is that - can Bob guess better than a random guess - so Bob listens to f x. Can Bob guess better than a random guess, means initially, if Bob has not been provided with the information of f x, what should be the probability of Bob guessing correct - it is half, right? So, even when the information of f x is provided to Bob, the probability should still remain half; so, his probability of guess is half.

Therefore, it should be still like a random guess, which means that the value of f x does not leak any information about the value or parity of x; so, these two are being guaranteed by the properties of the magic function f.

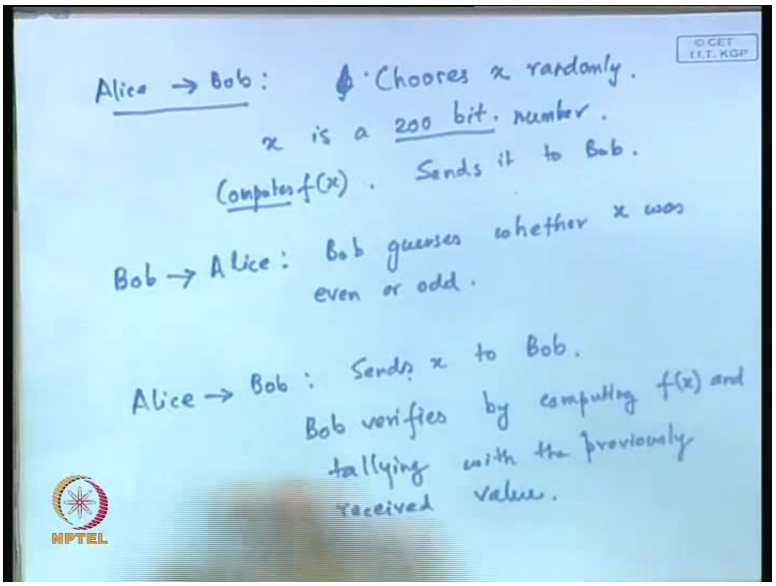
(Refer Slide Time: 26:40)



So, we will consider a little bit more concrete example; so, this is a similar scenario where Alice and Bob wish to resolve a dispute over the telephone. We can encode the possibility of the dispute by a binary value; so for this they engage a protocol. So what we've just now seen.

So, Alice and Bob, essentially what both of them do is like this – so, Alice picks up randomly an x, which is a 200 bit number and computes a function of f x as follows; so, it computes the value of some f x value, which I will discuss just now. So what Alice does is that…So, let us consider this particular example, little bit minutely.

(Refer Slide Time: 27:25)



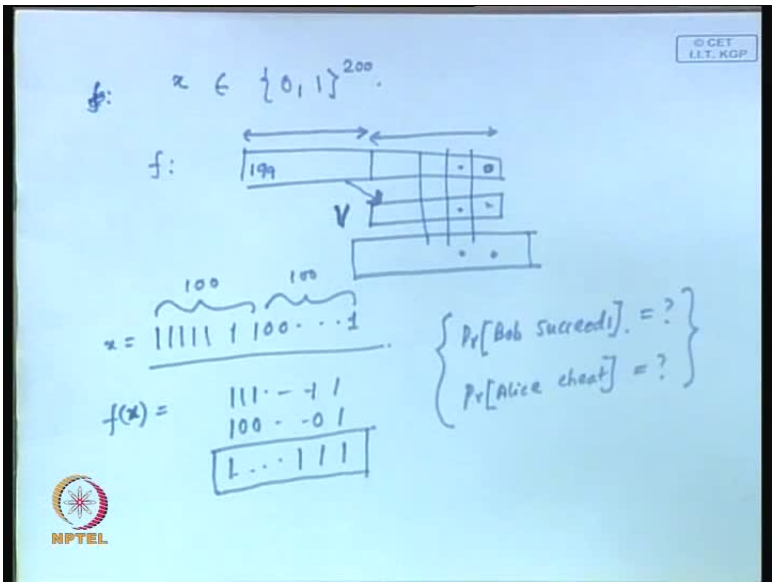
So, what Alice does is, Alice sends to Bob the outcome of a function f x. So, it chooses x at random, it chooses x randomly and x is a 200 bit number; it is a 200 bit, it means, 200 number of 0-1 values; so, it chooses a 200 bit number, a 200 bit value and computes the value of f x and sends it to Bob. So, computes the value of f x and sends it to Bob. So, what Bob does is that, so Bob now sends to Alice, the guess; so, Bob now guesses whether x was even or odd and sends this information back to Alice. Alice, now what she does it…

Bob needs to verify, therefore, what Alice does is that Alice now sends x to Bob; so, what will Bob do? Bob will verify, Bob verifies by computing f x and tallying with the previously received value; so this is the basic protocol, right?

Now, what do we need to do? We need to think of such a function f x. We have seen that if this f x function satisfies the collision resistance and the one-wayness, then this protocol should give a fair evaluation and do something which is similar to when Alice and Bob did simultaneously; when both of them were together, they just did a random coin tossing; so, therefore, both of them do not have any additional advantage in the game.

In order to do that, we will consider a concrete example of the function f. So just consider the following function.

(Refer Slide Time: 30:12)



So, imagine that f is essentially…So, you know that x has been chosen to be a 200 bit number, right? So, I denote that as a 0-1 string of 200 bit values, and what f does, is that it takes in the values of x, so, therefore x is something like from 0 to 199; so, it takes the first 100 bit values and it takes the next 100 bit values and I call this part... Therefore, it takes this part and does a bitwise OR between these values; so, therefore, it does a bitwise OR. So, all these bits are getting odd, therefore, this is odd bit, this and you get this; you odd this bit, with this and you get this. So, this is nothing but the MSB part; therefore, you just take the MSB part, bring it here, you take this part and do a bitwise OR between the bits and you get the resultant output.

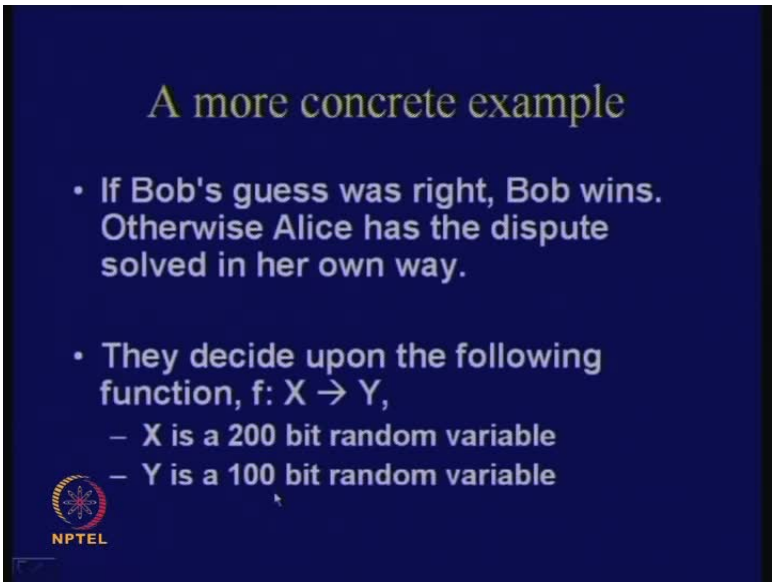
So, let us consider a simple example, like, for example, if there is the string like 1111 and so on, there are 100 bits, 100 values here and similarly, the next 100 values are say 0000 and say 1. So, what will be the corresponding…So, this is x, so what is the corresponding value of f x? It is 111 and so on, and you odd that with 100 and 1; therefore, if you do a bitwise OR, you get 1 here and this is again a 0, so we have got a 1 here, and so you will get a 1 for all the values; so, this your corresponding value of f x.

So, let us just imagine a function f which looks like this and try to compute the success probability of Alice and Bob. So, for example, here in this function…So this function can also be replaced by other possible candidate; this is just a simple example. So for example, we could have replaced this OR by a XOR and we could have computed the

similar properties, but I am trying to find out this particular… I am just taking this as an example and trying to compute what is the probability that Bob succeeds; that is, Bob is correct in his guess, and what is the probability that Alice can cheat.

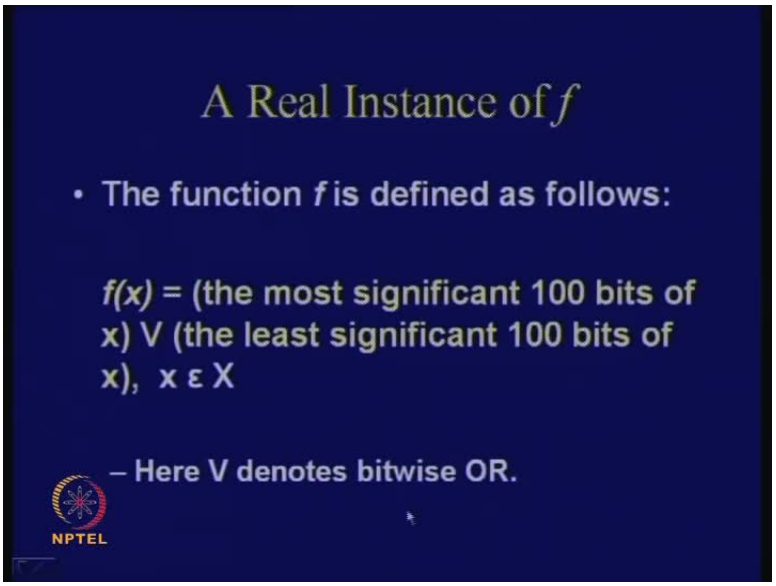
So, we are interested in these two probabilities and what we have to see is that whether there is an additional advantage over a random coin toss? Therefore, typically we will try to compare this with a random coin toss and based upon that we will see whether this function f is really a candidate for a magic function or not?

(Refer Slide Time: 33:37)



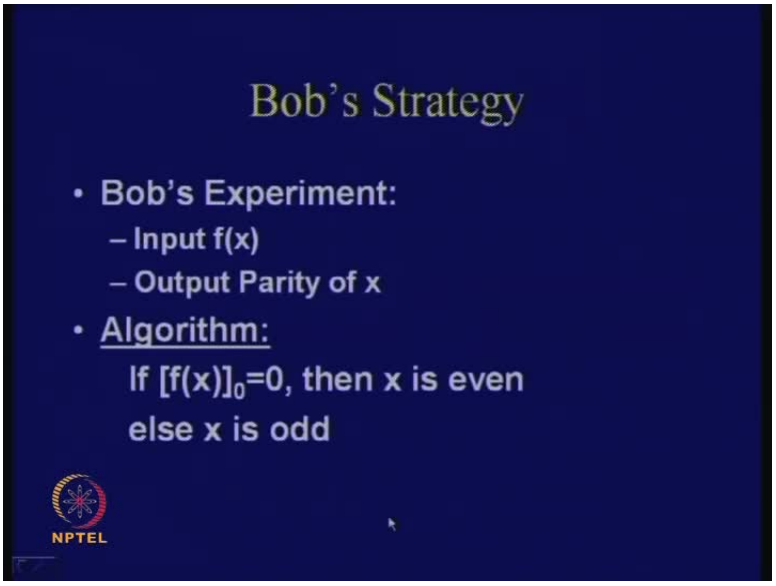
So, how do we calculate these values, that is, the probability of Bob will succeed or probability of Alice will cheat? So, for that, we have to observe the properties of this OR function. What I have said to you, that is a more concrete example is this: that if Bob's guess was right, Bob wins; so, this was a game - if Bob's guess was right Bob wins, otherwise Alice has the dispute solved in her own way. So, what they do is that they decide upon a function like this; so f is essentially a map from x to y, where x is a 200 bit random variable and y is a 100 bit random variable.

(Refer Slide Time: 33:56)



So, the function is just as I have told you now, that you take the most significant 100 bits of x and you odd that with the least significant 100 bits of x. So, x is just a 200 bit string and you odd or you do a bitwise OR between the first 100 bits of x and the least 100 bits of x; so here, OR denotes a bitwise OR operation.

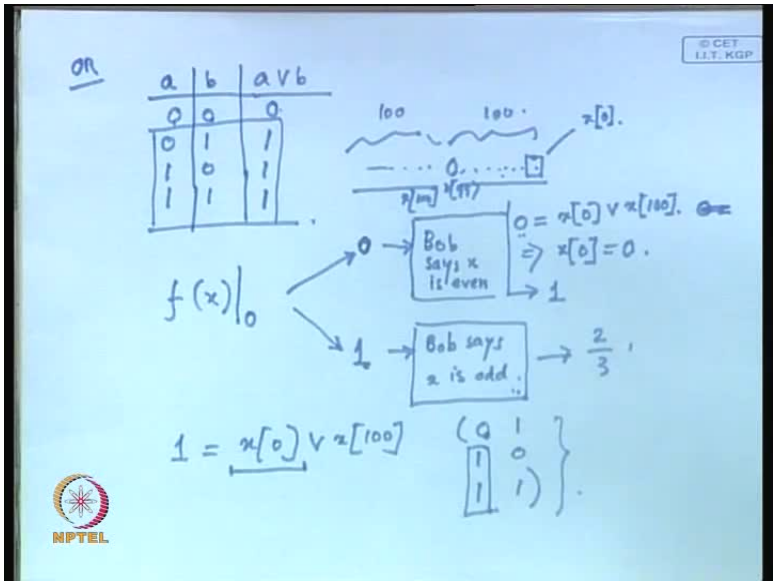
(Refer Slide Time: 34:24)



What we are interested now in doing is, that we are interesting in calculating the success probability of Bob and the probability that Alice can cheat. In order to do that, we have to first of all think of an algorithm or a strategy for Bob; so, Bob essentially has to adapt

the principle or adapt an algorithm or something which we commonly call as an experiment of Bob. What is Bob's objective? Bob has been provided the value of f x and Bob has to guess the parity of x; so, therefore, Bob needs to do something good.

(Refer Slide Time: 35:07)



Now see, that this property or rather if you see the property of this OR function; you know that if I just do a simple truth table of this OR function, you know that if there are two inputs like a and b and this is a OR b, so if you just consider the binary truth table, you see here, there is only one value which is 0 here, but the rest of the things in it reports in a 1. So, therefore, this property or rather this observation, Bob will exploit to make his guess more favorable, I mean, to enhance its probability of success. In order to do that, you see that Bob essentially has got the value of f x; so, Bob has got the value of f x and what it will observe is, what is the least significant bit of f x?

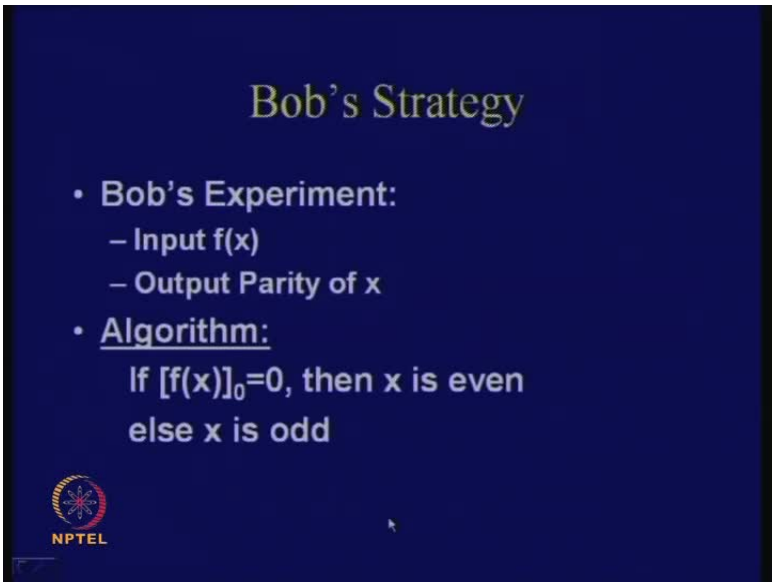
You see, there can be two possibilities here - it can either be 0 or it can either be 1. If it is a 0, what does it mean? Just think of the function f x, just think of the function f x; therefore, if you just think of the first 100 bits here, so f x means what? This is the first 100 bits, so you just consider that this is some value and I call that to be the x 0 value; so that is the least significant bit of x, and there are other values here; so there are 100 more bits here.

So, therefore, how do I compute f x? I just take this and I odd with this. If the resultant value or the least significant bit of the result is a 0, which means that 0 is the OR of x 0

and we have got x 0 to x 99 here, and this is your x hundredth bit; therefore, this is the OR of x 0 and x 100. So, if this value is 0, you see that in the truth table of a OR b there is only one possibility; that is, both a and both b are odd; so, therefore, you can say with the probability of 1 that x 0 is 0. What does it mean? It means that x was an even value; therefore, immediately the parity of x gets ascertained; so, therefore, if this be so, then Bob has got, I mean with a probability of 1, Bob can say, Bob says, x is even; otherwise Bob says x is odd. So, you see, that in this particular case, Bob has a probability of success of 1, but in this case, the success probability of Bob is not exactly 1, but it is slightly different.

Can you say what is the probability here? You see that if this be 1, so what are the possible cases? It means that it belongs to this case; therefore, it means that 1 is equal to x 0 or x 100 and we are interested in the value of x 0. In how many possible ways you can get a 1 here? It could be either be a 0 1, it could be either be a 1 0 or it could either be a 1 1; so you see that in these three cases, there are two cases for which this x 0 value was actually 1, which means the x was odd and that is what Bob is saying. But in the other case and there is one case out of these three cases, where Bob will fail; therefore, the probability of success here is actually 2 by 3, because in two cases Bob is correct out of three cases. So, here in this case the probability of success is 1 but here it is 2 by 3; so, Bob can use this particular observation to develop a strategy.

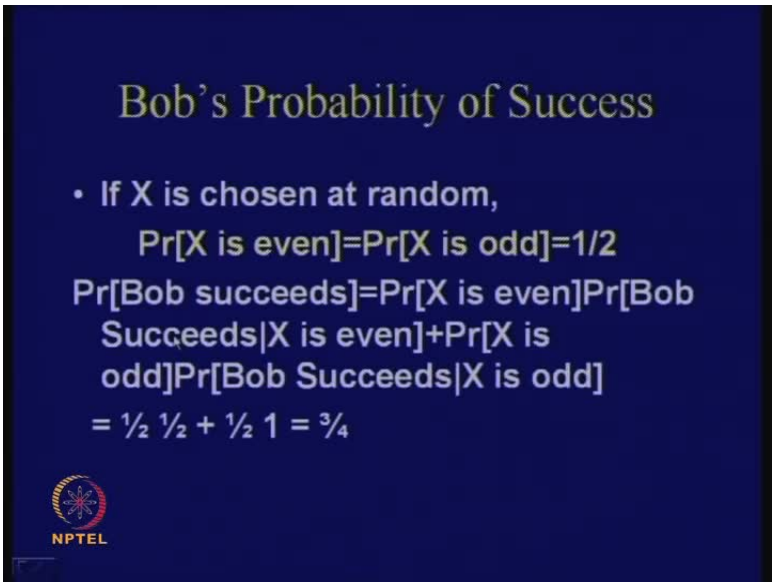
(Refer Slide Time: 39:35)



The strategy is very simple, the strategy is like this - if the zeroth bit of f x is 0, then x is even, otherwise x is odd; so, this is a simple algorithm or simple strategy which Bob can adopt. In this case, the probability of success of Bob will be 1, but in this case the probability of success of Bob will be 2 by 3.

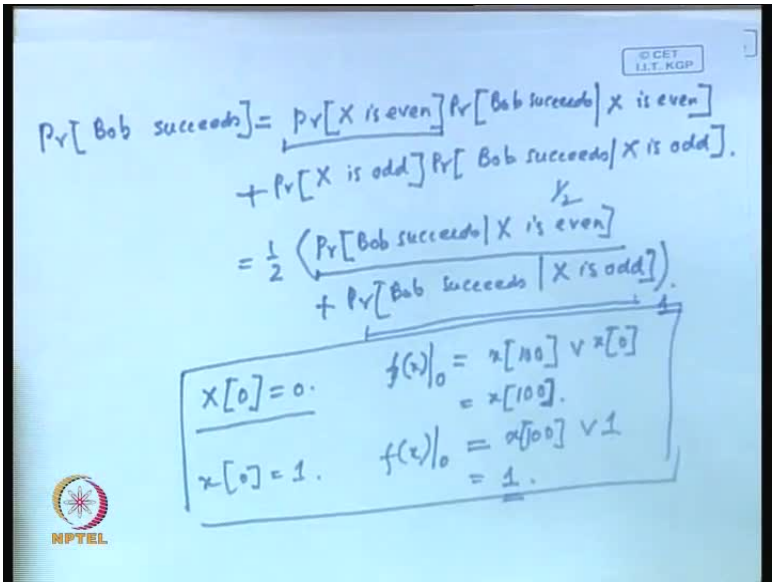
You note one thing, that is, x was randomly chosen, but the value of f x is actually not randomly chosen. Therefore, if I say, what is Bob's probability of success, you cannot straightaway assume that the value of f x 0 be being equal to 0 is half and compute the value of f x; you have to do slightly different thing, that is what I will come to next. But this is correct that is if it says, x is even - so in this case the probability of success of Bob is 1, but in this case - the probability of success of Bob is 2 by 3, as we have just worked out.

(Refer Slide Time: 40:37)



Next, we are interested in calculating what is Bob's probability of success? How do we calculate Bob's probability of success? So, you know that there are two possible ways - since x is randomly chosen, x can either be even or x can either be odd, and therefore the probability that x is even is equal to probability that x is odd and that is equal to half. So, now, the probability that Bob succeeds can easily be found out or can be written in this fashion.

(Refer Slide Time: 41:18)



Therefore, if I want to calculate this particular probability that Bob will succeed, I can do this in this fashion - probability of Bob succeeds is equal to probability that x is even multiplied by probability that Bob succeeds; conditional probability, so, it is a conditional probability and here the condition is that x is even. And basically, what I am trying to do is that I am trying to split the possibilities into two mutually exclusive cases - one is when x is even and the other one is when probability of when x is odd. Therefore, I write the other part as probability of x is odd multiplied by the probability that Bob will succeed, given x is odd.

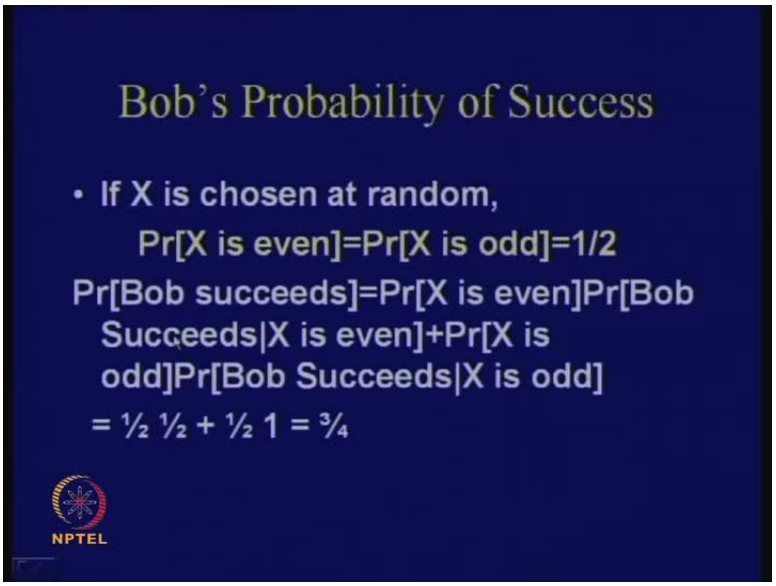
So, we split this into two mutually exclusive cases and what is the probability that x is even? I know that is half and I also know that the probability that x is odd is also half; so, I can take this half common, and I have got probability that Bob succeeds, given x is even, plus the probability that Bob succeeds, given that x is odd. So, now you see, that we have got two cases - one is that when x is even; so when x is even, then what is the probability that Bob will succeed?

So, x is even means, what? x is even means x 0 is 0. What is the corresponding value of f x 0? It is x 100 or with x 0; in this case, it is equal to x of 100; so, depending upon the value of x 100, Bob will say it to be 0 or 1; so, Bob did not predict its value. So, you see that if, x of 100 is also 0, in that case, the result is 0 and therefore, what Bob guesses is correct; that is, Bob guesses x to be even and that is correct. But if x 100 is 1 then this result is 1; so, therefore Bob will see this 1 and using its strategy Bob will guess that x is odd, but actually x in this case is even, therefore Bob fails.

Therefore, when x 100 is 0, then Bob is successful, but when x 100 is 1, then Bob fails. And what is the probability of x 100 is 0 or 1? It is half, because x is randomly chosen, therefore anywhere the bits being equal to 0 or 1 is actually equal to half.

Therefore, this particular value, that is, probability that Bob succeeds when x is even is actually equal to half. What about this case - when x is odd? If x is odd means x of 0 is 1 and therefore, x of this value is equal to x of 100 or with 1 and this is always 1. Therefore seeing this 1, Bob using its strategy will always guess that x of 0 is 1, and therefore, its probability of success is actually equal to 1, when x is odd.

(Refer Slide Time: 45:09)

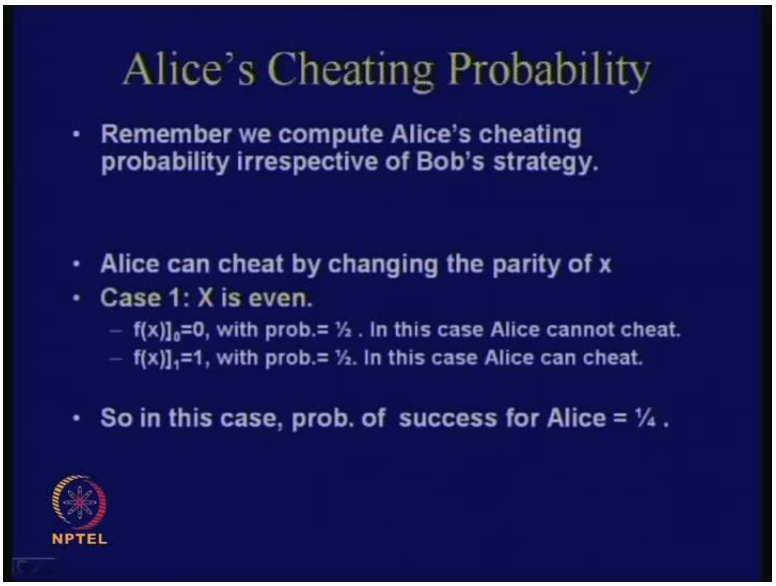


Now, we combine these two things and we obtain what we have written out in this slide; we obtain that, here write, half into half that is plus half into 1 and therefore, we get a probability that Bob is successful is equal to 3 by 4.

So, what should have been the ideal probability of Bob's success actually? It would have been half; therefore, we see that there is a significant excess over half and that excess is over 1 by 4; that means, that the magic function f which we have instantiated by this OR function is not correct.

Therefore, this is not a very good candidate for such a function, but this is an example. We are just seeing that example in order to appreciate the problem and motivate the study of this present course, that is - why at all we are studying cryptography? What is the purpose? That is why we are trying to see a simple game and we are trying to see a possible candidate of the function f.

(Refer Slide Time: 46:27)



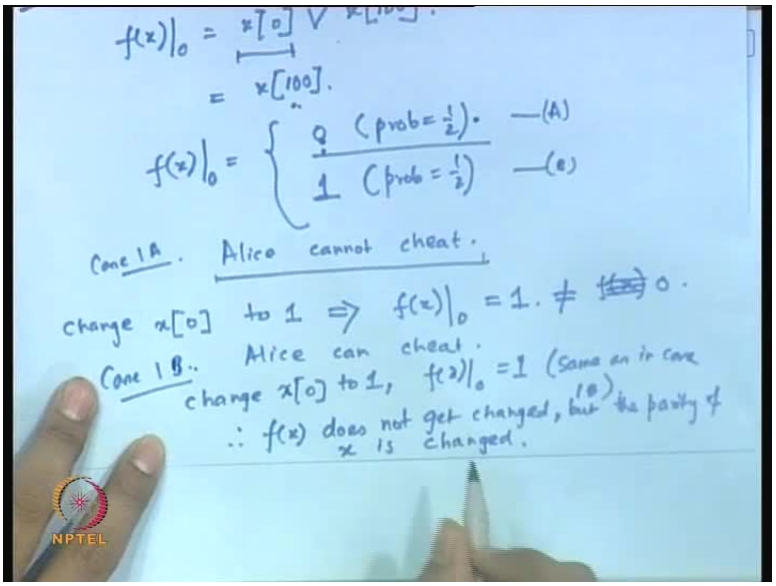
But you just try to understand first, that this particular function f which we have chosen is not actually an ideal candidate, because here, in this case, the probability that Bob succeeds is not actually equal to half, but it is quite greater than half; so, it is significantly larger than half and therefore Alice and Bob should not be satisfied with the function f. What is the probability that Alice will cheat? That is, Alice's cheating probability? So you see that in this case, remember that we will compute Alice's cheating probability irrespective of Bob's strategy.

Alice really does not know what strategy Bob has taken and Alice still wants to cheat; so, therefore, in order to cheat, what does Alice need to do? You see, that Alice has communicated the value of f x and therefore, when Bob guesses, that is what is the parity of x. In order to cheat, what Alice will do is that Alice will change the value of x or change the parity of x, keeping the value of f x intact; therefore, Alice can cheat by changing the parity of x.

So, therefore, Alice needs to change the parity of x such that here - there should be additional certain few words - the value of f x should be intact, the value of f x should not change. So, in order to compute the probability, let us divide this again into two cases, like what we have done in the previous case. Let us divide this, the first case is - x is even; so when f x is even…; so when x is even, therefore, x 0 is 0; so what is the value of f x? There can be only two possible cases - f x 0 equal to 0 and f x 1, this should be

actually 0; therefore, the f x 0 can either be 0 or it can be either equal to 1; so there can be two possible cases here also. That is, if you see the case one - x is even; so if x is even the value of f x 0 is again equal to x 0 OR with x of 100; so what is the value of f x 0 here? It is equal to 0 because x is even, so x of 0 is 0.

(Refer Slide Time: 48:09)



So, therefore, what is a probability that therefore This is actually equal to x of 100; so, therefore, depending upon the value of x 100, whether its 0 or 1, f x 0 is 0 or 1. Therefore, the f x 0 being equal to 0 or being equal to 1, both has got a probability of half because that depends upon whether the 100 bit is, x 100 is 0 or 1; therefore, this also has a probability of half and this also has a probability of half. Note that in this case, when f x 0 is 0, then Alice cannot cheat, why? Because in order to cheat, Alice needs to make the value of x odd and still see, whether function f x results in a 0, which cannot be the case.

If x 0 is changed from 0 to 1, therefore in order to cheat in this particular case - if I call this as a case a and I call this as a case b - so in this case one a, Alice cannot cheat, why? Because in order to cheat, Alice needs to do, what? She needs to change the value of x 0 to 1, but this implies that f x 0 computes to 1, which means that this is not the same as the previous case. Therefore, this is not the same as what was initially reported; that is, initially f x 0 was 0, therefore this is not equal to 0; since this is not equal to 0, so Alice

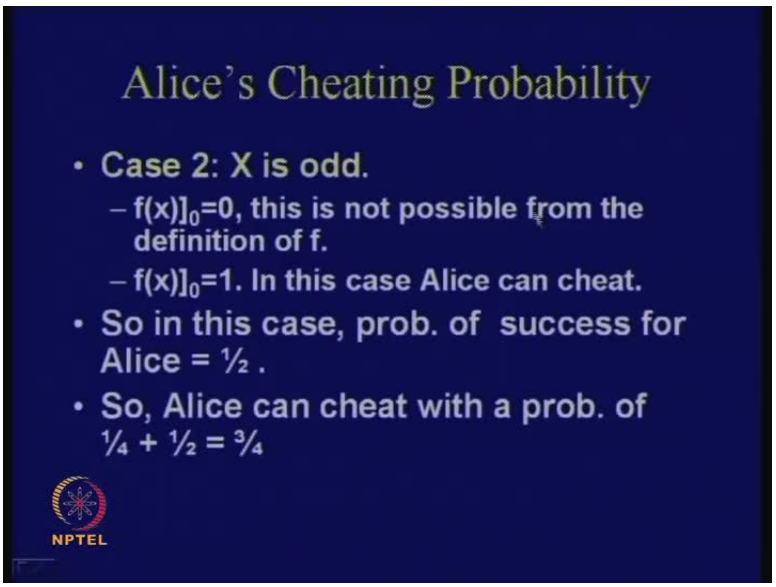
cannot essentially change the value of x 0 to some other, I mean, cannot change the parity of x, but still keep the same value of f x.

So, therefore, in this case, Alice is unable to cheat, but what about case one b? Alice can cheat, why? Because in this case f x 0 is actually equal to 1; so when f x 0 is equal to 1 then - and we know that in this case x is even - so, even if Alice changes x 0 to 1, this particular f x 0 value does not get affected; therefore, the f x value is, f x 0 is still 1 and this is the same as in case one b; therefore, f x does not get changed, but the parity of x is changed.

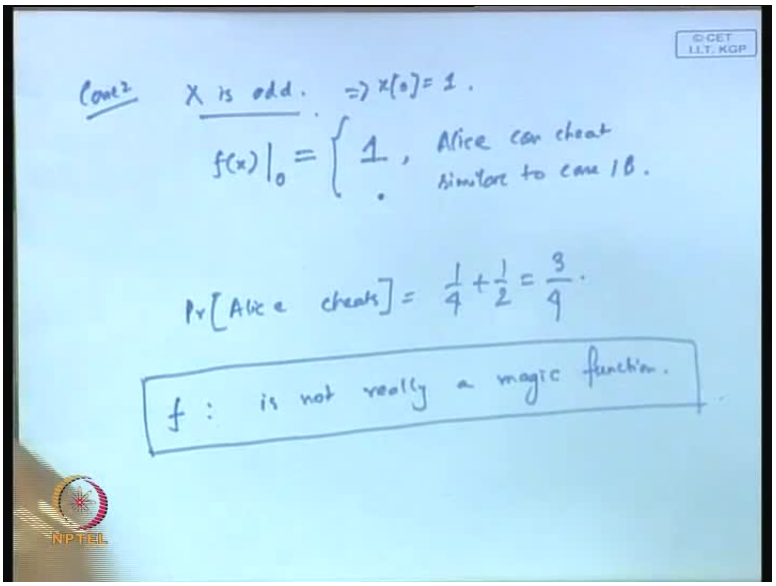
So, therefore, Alice, what she has done in this case one b is that although x was even, can actually change this x even to an odd value by just flipping the last bit, but the value of f x 0, which she has committed does not get changed. Therefore, Bob does not have any other way to understand that Alice has done this malice; therefore Alice is able to cheat; therefore, Alice is successful to cheat.

So, therefore, what is the probability that Alice is able to cheat, comes from this particular case and what is the probability of this? It is half; so the probability of this is half and the probability that x is even is also half and therefore the resultant probability in this case is actually equal to 1 by 4.

(Refer Slide Time: 52:35)



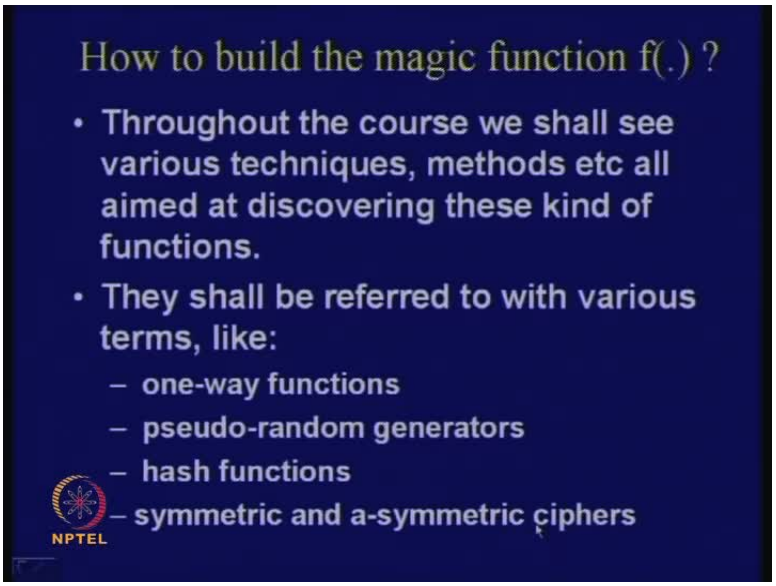
(Refer Slide Time: 52:40)



So what about the next case, that is, case two? In case two, x is odd and therefore f x 0, what are the possible values of f x 0? If x is odd, it means that x of 0 is 1. Now, in this case, can f x 0 be equal to 0? That is not possible, because if I OR with 1, I will definitely get a 1, so the only possibility is here in this case is 1. In this case, also, Alice can cheat by a similar logic as we have done for case one b.

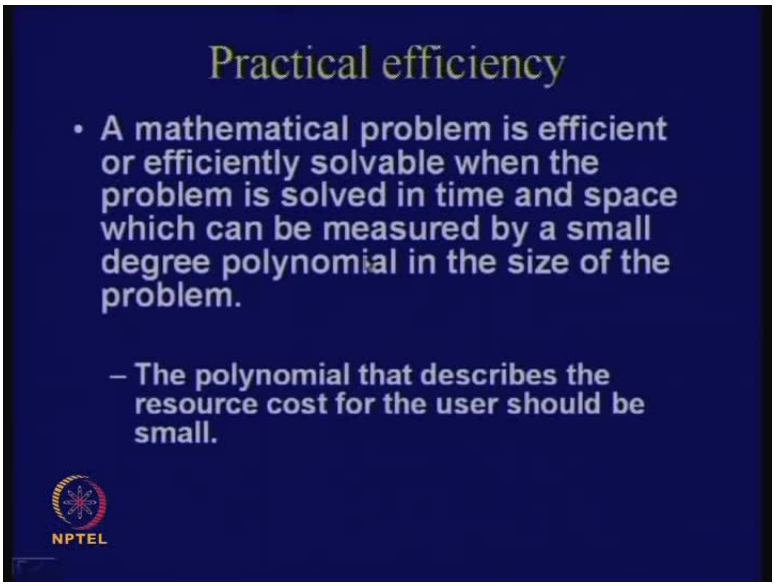
So, Alice can cheat similar to case one b; so, therefore, in this case the probability that Alice is able to cheat is actually equal to half into one, because that is the only outcome here. Therefore, the total probability that Alice can cheat is actually, probability that Alice cheats or Alice can cheat, is actually equal to 1 by 4 plus half and that is equal to 3 by 4.

(Refer Slide Time: 54:18)



So, you see that here also Alice has got a significant probability of being able to cheat; therefore, this function f, I conclude from here, this f as we have defined, is not really a magic function. So, which means what? Which means that we need to find out such values of f which are really possible candidates of magic function and that is the objective of this course. That is, throughout this course, we shall try or see various techniques or methods which will aim at discovering these kinds of functions and they will be referred with various names like one-way functions, pseudo-random generators, hash functions, symmetric and asymmetric ciphers and so on.

(Refer Slide Time: 54:38)



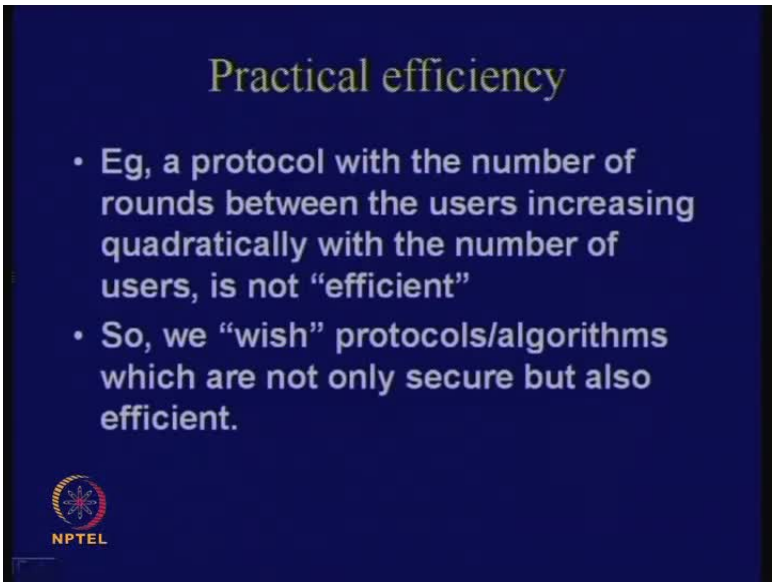
So, I will just conclude; so that is the objective of this course, but I will conclude with this class with just few words on what I meant by easy and hard. Actually, I will be talking about this in more details in throughout the course and it will be more clear as we proceed in the course, but I mean, just to understand what is meant by practical efficiency - a mathematical problem is efficiently solvable when the problem is solved in time and space, which can be measured by a small degree polynomial in the size of the problem. So, the problem that describes the resource cost for the user should be small.

Therefore, what I mean by this is that when I am saying an easy problem is that with respect to the input size of the problem, the cost of your time or the cost of your space in solving the problem should be, as can be expressible in a polynomial, with a polynomial of its input size and the degree of the polynomial should be small.

For example, if I have got an algorithm which solves in a linear time complexity, say something like o n, something which we defined as o n, which means it is linearly dependent upon the input size. As opposed to that, if I take a quadratic problem, that is, if some problem like the time and cost of some time and space of some problem is proportional to the square of its input size, then I say, that to be a quadratic problem; therefore, the quadratic solution to the problem and therefore the time and space of such a solution is obviously known, then what we get by a linear time problem, linear time solution.

Therefore, the idea here is that a mathematical problem, I call that to be easy or I call that to be an easily solvable, is when the problem which is solved in time and space can be measured by a small degree polynomial in the size of the problem. And, therefore, as opposed to that when I have called some problem is really a hard problem or a difficult problem, I mean to say, that the best algorithm that I know to solve this problem has got a time or space complexity, or space which is proportional or which cannot be really expressable in a polynomial with respect to the input size, and the degree of the polynomial is small.

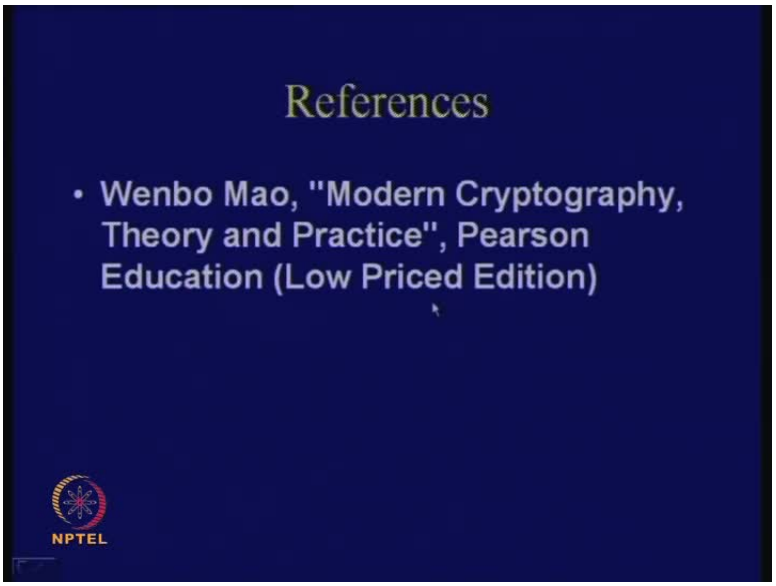
(Refer Slide Time: 57:25)



For example, if I have got a solution which is, say, an exponential with respect to the input size, for example, for example if I, suppose the input size is n and if I have to do two power of n amount of storage is required to solve that problem, then I call the problem to be a relatively difficult problem or a hard problem. So that is the measure behind easy and a difficult.

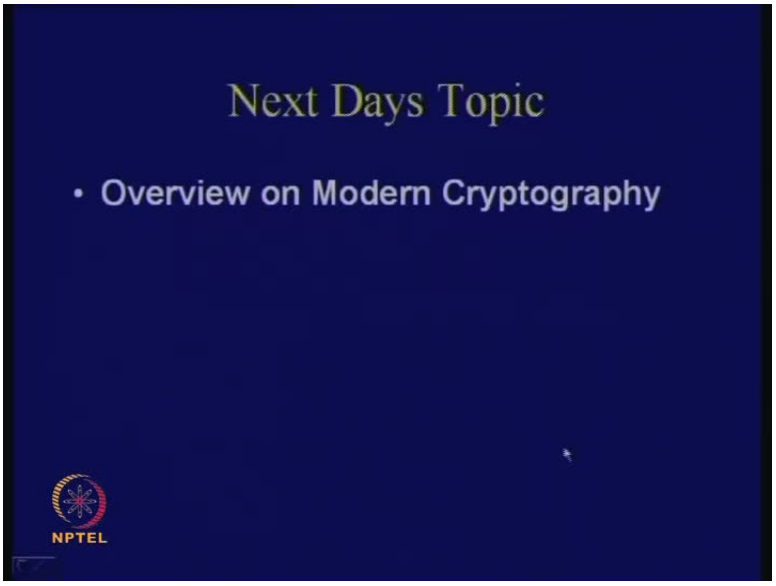
We also have to keep our practical efficiency in mind, for example, a protocol with the number of rounds between the users, if it increases quadratically with the number of users, then I say that not to be efficient, but it may be the best possible way to do it; but the researches throughout the world will try to make that protocol better or more efficient. So, what does it mean? I mean to say that, I will try to increase or rather reduce the number of users and make it more and more efficient; therefore, you should not increase quadratically, I mean, may be it will increase linearly.

(Refer Slide Time: 58:14)



Therefore, we wish to make protocols or algorithms which are not only secure, but at the same time they are also efficient; therefore, efficiency is also another thing which we will always keep in mind in developing cryptographic algorithms. So, I conclude this topic ((part)) with reference which I have followed.

(Refer Slide Time: 58:29)



I have followed the book of Wenbo Mao for this part, it is Modern Cryptography and Theory and Practice - that is a low priced edition from Pearson Education. In the next

day’s class, we will have an overview on modern cryptography. We will see various cryptographic algorithms, various objectives of modern day ciphers.

So, we conclude this course.

Thank you.