Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 48
Differential Cryptanalysis

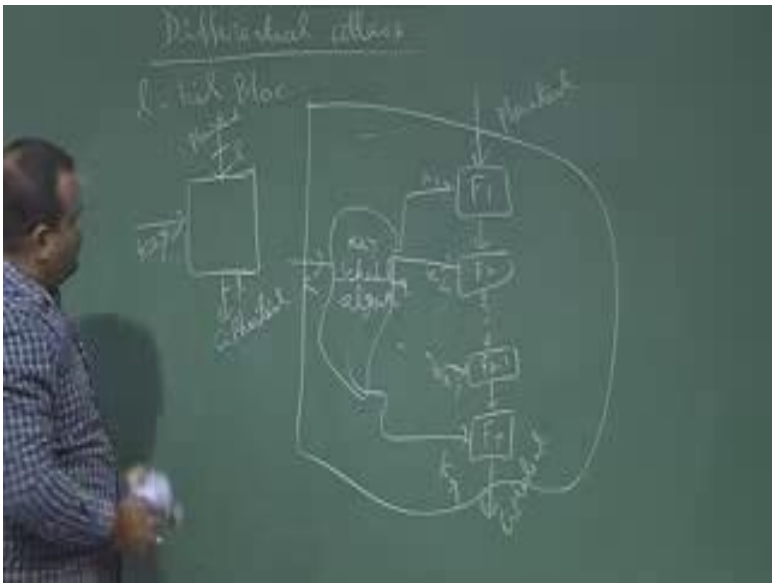
So, we will talk about the generic attack. So, so far we have discussed the non-generic attack where we do not care about the inner design of the cipher, but now here we will really look at the design of the cipher, and we will try to find out some flaw there or anything. So, whether there is a linear attack is linear relationship, so this basically non-generic attack.

(Refer Slide Time: 00:49)

So, this is basically all comes under non-generic attack. So, in the non-generic attack, we will look into the design of the cipher. And then we will try to find out whether there is any flaw or not; if there is any linear relationship between the plaintext and the ciphertext those are linear attack. So, non-generic attack are basically linear attack, linear cryptanalysis, we will talk about those differential cryptanalysis, differential attack and some version of the differential attack like boomerang attack, impossible differential attack, trunked differential attack and also the non-generic attack, slide attack or slide key.

So, these are basically attack some block cipher, but this can be extended to the stream cipher also in some of that attack we can think for then the related key attack. So, this is this related key attack means we want to see whether is there any relation between the round keys. So, this is the attack where we look into the key scheduling algorithm, related key attack like this. So, these are basically non-generic attack that means this attack is particular to that design. So, we are looking into that particular block cipher, we are going into that design and we are checking is there any flaw there or not. So, then if you gets something flaw then we can attack it.

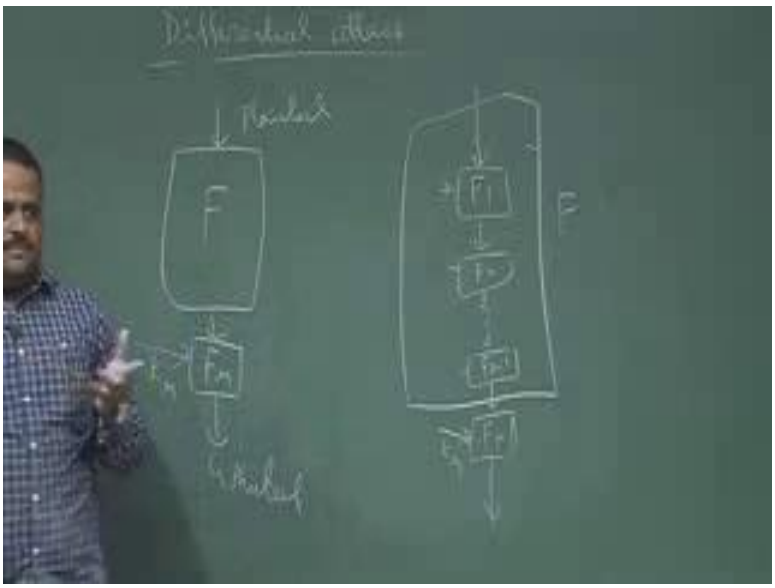
(Refer Slide Time: 02:59)



So let us start with the differential attack, which is a non-generic attack. So, differential attack was introduced for block cipher. So, it is to find out the rth key of the block cipher - differential attack on block cipher. So, let us just recall what is a block cipher. So, l bit block cipher means, so it is basically a function which is taking l bit input plaintext and this is the plaintext, and this is the ciphertext and it is taking the secret key k, this the encryption and decryption is the other way round. So, it is a l bit block cipher. And for r round if it r round then there are r many round function is there. So, suppose we have r round block cipher, r round means we have many r round function F 1, F 2 dot dot dot F r minus 1 and last round is F r. So, this is the plaintext which is the input of the first round. This is l bit, and this is the ciphertext which is the, this is the ciphertext which is the output of the last round or rth round, this the r round block cipher.

And we know this round function each round function we need a round key. So, where from we can get the round key, round keys are coming from the a algorithm which is called key scheduling algorithm, which is a public algorithm which is taking the secret key k which is shared between Alice and Bob. And it is generating the round keys k 1 for each round will need a round keys dot dot dot. So, this is k r minus 1 and for last round this is k r. So, this is basically a typical r round block cipher, this is a typical r round block cipher, I mean l bit if plaintext ciphertext are l bit.

(Refer Slide Time: 05:25)



Now, in the differential attack, this attack will be try to get the rth round key. So, this is the attack where we try to the attacker is attempting to get find out the rth round key. So, for that, we need to have something called differential trials. So, like if we take this say these are the r rounds. So, just let me, this is the r round. So, suppose we denote this up to r minus 1 round as F function capital F function and this is the rth round this is having a k r. So, this is the cipher text. So, basically we have a F function which is taking input as a plaintext and followed by last round F r and we got a ciphertext. And this is the K r. So, this up to this r minus r round, we call this function as a function. So, basically F is consists of F 1, F 2 up to f r minus 1. Now, we want to see some existence of some differential trial in this function or not, F function.

(Refer Slide Time: 07:13)

So, for that, let us define what is the differential trial. So, F is a function. So, suppose it is l bit. So, F is taking l bit input to l bit output, we have the round keys inside that we are not bothering now. So, you are only concerned about this input this output. So, F is a function. So, this is a F function. Now, suppose we defined the difference between this input suppose we take 2 x 1 and x 2 - two input in F and we XORing say this is alpha, these are basically binary bits. So, this XOR be basically is bit wise XOR. So, we just do the bit wise XORing. So, if it is 64 bit say for DES, it is 64 bit. So, x 1 is 64 bit number 11 some 64 bit 01 bit; x 2 is say 1011 like this 011 like this. So, this XOR means bit wise XOR. So, this is basically 0, this is no carry. So, this is 1, this is 1 like this. So, bit wise XOR. So, we take the difference. If the input difference is alpha in F only then we want to see what is the output difference. So, this is basically y 1 is basically F of x 1 and y 2 is basically F of x 2.

And we just do the x 1 if it is beta then we say alpha is going to beta. So, this is call differential tail. We say alpha is going to beta, so that means if the input difference is alpha then we are getting the output difference beta. Now, if this alpha beta exists, that means with high probability that means, if you take input difference alpha then with probability more than half, the output difference should be beta. So, if alpha beta is also 64 bit for DES, so now if such alpha, beta, exist then only we can mount the differential crypt differential attack on this block cipher. So, suppose such alpha beta exists with the

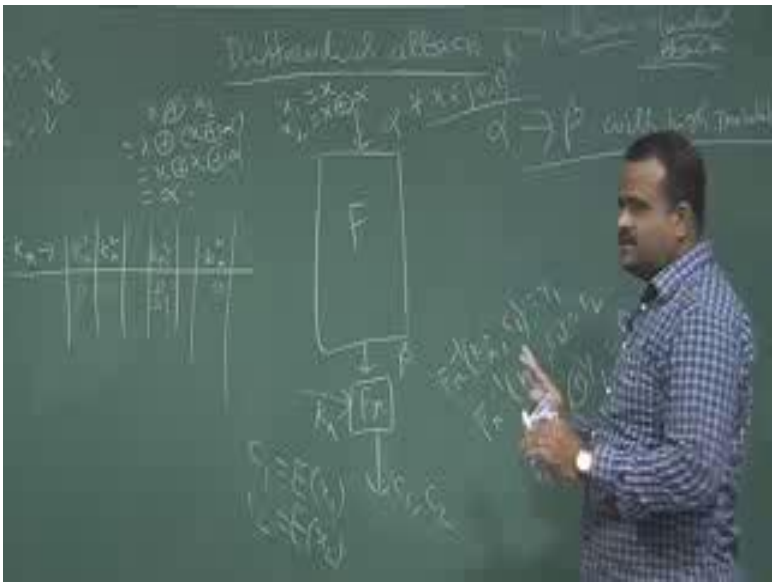
high probability that means, if the input difference is alpha then the output difference will be beta.

(Refer Slide Time: 10:07)

So, for this f, so if the input difference is alpha then the output difference will be beta, so that means, with high probability. How to get this will come to an example with high, high probability means greater than half this is the probabilistic attack high probability. So that means if you take input difference alpha, if you take 2 x 1 x 2 such that x 1 x 2 is alpha then it is expected that they are y 1 y 2; y 1 is basically f of x 1 y 2 is basically will be beta. It is expected that means, with that high probability this will be beta. So, this is basically we can say alpha is going to beta. So, suppose such alpha beta exists then only we can mount the differential attack on this block cipher.

So suppose such alpha beta exists then only one can mount the differential attack on this block cipher how to attack will come to that if such alpha beta exists; otherwise we cannot have the differential attack. If there is no such alpha beta with high probability if we cannot find out alpha beta then sorry boss there is no I mean this cipher is secured under differential cryptanalysis like AES secure full round AES secured under differential cryptanalysis, but DES is broken by the differential attack anyway. So, now suppose we have such alpha beta then how we can have a attack on this block cipher to find out rth round. So, that we have to that is the exact attack on the rth round finding the rth round key.

(Refer Slide Time: 12:21)



So, differential attack, so this is our block cipher F followed by a last round F r, which is taking the rth round key and this is the ciphertext. And we know that alpha beta pair exists, we know this alpha beta, if the input difference is alpha then the output difference of f will be beta with high probability this exist; otherwise we cannot have this attack with high or significant probabilities. So, this is a probabilistic attack; otherwise no sorry boss this cipher is secured under differential cryptanalysis.

So, now how to attack this how to get this clear suppose this alpha beta exists. So, what we do? We take two pair x 1 x 2 which difference is alpha so that means, we choose x 1 equal to x, and x 2 is equal to x XOR alpha. If we choose like this, then x 1 XOR x 2 is basically x XOR x XOR alpha, so this basically x XOR x XOR alpha. So, this is canceling out this is alpha. So, if we choose these two x 1 x 2 this like this, x is a plaintext any plaintext. So, x is if it is l bit x is any l bit. So, there are two to the power l possibilities of x. So, there are 2 to the power l possibilities of x.

So, what we do. So, we got a x we choose a x this choice can be done two to the power l ways and then corresponding x 2 is fixed because we want this difference should be alpha. So, we have to take x XOR alpha as x 2. So, now for this x 1, x 2 this is a chosen plaintext attack, this differential attack is a chosen plaintext attack we are choosing the plaintext, so that we can get the corresponding ciphertext. So, we choose these two plaintext. So, the under this chosen plaintext attack, we should get the corresponding

ciphertext c 1 and c 2. So, c 1 is basically encryption of x 1 and c 2 is basically encryption of x 2 the plaintext x 1, x 2.

So, now we know the input difference is alpha, we know the output difference of f will be beta, but we are here. So, how to go here, so we know this difference is alpha. So, here f of, so basically we know this f of x 1 if you denote by y 1 and f of x 2 if you denote by y 2, we know this y 1 XOR y 2 is beta most likely, because this is a high probability. So, this fact is known to us we want to make use of this fact to guess what is here. So, what we do? We can have the exhaustive boot force attack on this clear exhaustive search. So, k r we can take, so if all the possible values of k r. So, k 1, k r 1, k r 2 like this, so if k r is k r n. So, all possible values if n is if k r is say for DES it is how many bits round keys is 48 bits. So, for DES it is 48 bits k r is 48, so N is 2 to the power 48 for DES. So, this is all possible k rs.

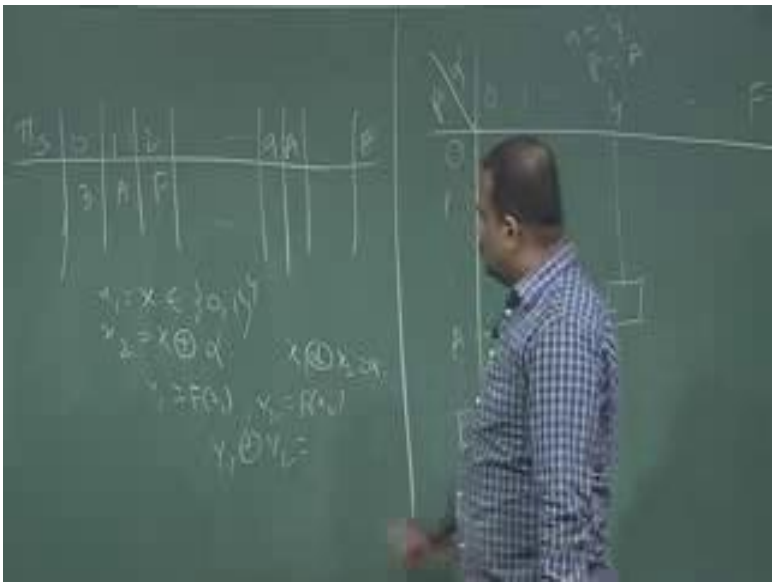
So, now we initialize down this is a counter, we put the counter, initialize the counter by 0. Now, what we do? We choose a plaintext, and we get x 1 we get corresponding x 2 we got c 1, c 2. Now, we choose a candidate we choose a k r i which is initialized by 0 this will try for all possible k i's. Now with this k r i, will convert this. So, with this key k r i will just apply f I inverse k r i with this c 1 we get some y 1. And F r inverse k r i c 2, we got some y 2. Now, we try this with look y 1 XOR y 2, and we check whether this is beta or not. If this is the correct key if k r i is the correct key, then it should give us hear the difference beta, because this is the ciphertext we are just want to we have to reach here in order to get beta because beta is the if the input difference alpha here beta is the output difference on F. So we have to reach here.

To reach here, we need to know this k r. So, we are guessing this we are taking k r is equal to k r I as a candidate key. So, if it is giving as beta, if it is beta, then we increase this k r by counter by plus 1, we increase this counter by plus 1. And these will true for all possible plaintext, we take another plaintext as x 1 then we choose corresponding x 2 and this we are trying for all possible k i's. So, this way we compute this table. And after completing this table whose frequency is more than that is the k r, so that is the attack. So, that is the corresponding rth round key. So, this is the good for (Refer Time: 18:44), but this will give us the rth round key is this set a clear. So, this, we have to try for we choose a x from plaintext that is x 1, x 2 if get as XORing this. Now we are here. Now, we choose all possible k is and we invert this and we increase that this frequency by 1 if

the corresponding the k i's for that corresponding k i we get beta over here because beta is expected because if the input difference is alpha beta will be the output differences in F, so that is expected.

So, if we get beta here then corresponding candidate key will increase the frequency. So, this will do for all possible plaintext, and then finally, after doing this finally, we got this table with many values. So, finally, the put the value which is having more frequency is the rth round key. This is basically the differential cryptanalysis on this block cipher to find the rth round key. So, now, the question is, is this set a clear. So, this is the differential attack. Now, the question is how we can find out such alpha and beta. So, for that let us just look at the some simple block cipher to find the alpha, beta maybe we can try for S-box.

(Refer Slide Time: 20:31)



So, suppose we have a simple block cipher like we have a S-box 4 bit to 4 bit like SPN S-box. So, S-box is this is 4 bit to 4 bit S-box. And we have a round key over here XORing, this is the round key simple block cipher, this is again 4 bit. Now, we this is our s say; now we want to find out alpha beta for this S-box. We want to find out alpha beta; that means, if the input difference is alpha then output different will be beta for this S-box. So, this we want to see how we can how we can get this alpha beta pair for this. This is a simple example to get alpha beta, but as this may not be say simple function it

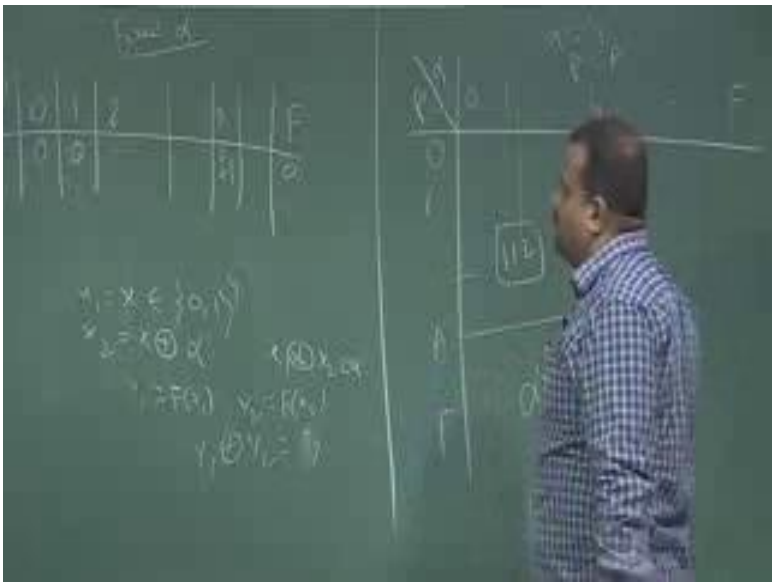
could be any F function. So, only thing we need to have alpha beta in order to attack this block cipher by differential attack.

So, suppose you can take this S-box as the SPN is S-box. So, we have seen the SPN S-box. So, suppose this is a 4 bit-to-4 bit. So, we can just write this S-box function like this. So, 4 bit can be written as hexadecimal form 0 to F. So, like this is the input 0, 1, 2, 3 up to 9, then 10 is basically A, dot dot dot F. So, F is 15. So, 0 to 15 basically then the corresponding output we can have, we can take a standard S-box, SPN S-box from the book. So, I cannot remember the exact form of this suppose this is say 3, A, F like this suppose we have this data. Now, how to get this alpha beta pair, so what we can do? So, this is the S-box. So, input difference will be we want alpha and the output difference will be beta. So, you want such alpha beta pair.

So, what we can do we can have a table like frequency table. So, alpha, beta is also 4 bit-4 bit. So, what we can do we can write this 4 bit as hexadecimal form. So, alpha beta is also starting from 0, 1 to F. So, beta is also starting from 0, 1 to F. So, now, what we do we take a alpha, beta say we are choosing alpha is equal to say 4 and say beta is equal to say we are choosing A. So, this is 4 and this is say A.

Now, we want to fill up this table like this table is a frequency table basically. So, how to fill up this table? So, for this 4 and 4 what we do, we take so the possible beta is basically so the input difference is 4. So, input difference is 4 means we choose x from this, this is our x 1; and we choose x 2 is x 1 XOR alpha for a fix alpha here it is 4. Then their difference is basically alpha. Now, what we do? We compute this S-box. So, we compute y. So, we compute y 1 is basically f of x 1, and y 2 is basically f of x 2. So, here it is f function is just S-box, we will compute x 1 XOR x 2. So, it has some value, say beta.

(Refer Slide Time: 24:53)



So, basically we have a table like this for this alpha. So, we have a beta value for a fixed alpha. So, this is 0, 1, 2 like f. So, we initialize this by all by 0 count, this is just a count. So, this beta, so suppose this is say we are getting say B. So, say here is B. So, it was A, so we are add just plus 1 here if we are getting B. So, like this we change another plaintext x. So, alpha is fixed. So, this is for a fixed alpha. So, alpha is fixed. So, for a fixed alpha, we compute all these betas and we just add the count if we get that beta. So, we are varying this over the plaintext. So, this way we can fill this table frequency table. So, after getting this table, whose is having the maximum value, so that count we are putting here, so that is the frequency having maximum value this is F alpha, beta. So, like this, we compute this table for all possible alphas.

So, if we take another alpha will do having same technique, we will choose a plaintext x 1 then x 2, we will compute this and the maximum frequency, we store it here. So, this table we can compute. So, in this table, if all the values are almost same then there is no differential tail exists, but if there is a value say all are set in and if there is a value say 112 frequency then the corresponding alpha beta is our differential tail, then we can mount the attack. If such exists this is the frequency table so that means, there is a significant probability that if you take input difference alpha then the output difference will be beta.

So, this is the way we can find alpha beta, but if such alpha beta exists then also we can mount the differential attack, otherwise not. So, this table can give us such alpha, beta, if all the values of this tables are similar then there is no such alpha beta exist in the F. So, this then this block cipher is cannot be attacked by the differential cryptanalysis.

So, I suggest you, you can just have a try to get this alpha beta for the SPN network, which we have discussed in our block cipher. So, just try to get some alpha, beta for that without such alpha beta exists or not.

Thank you.