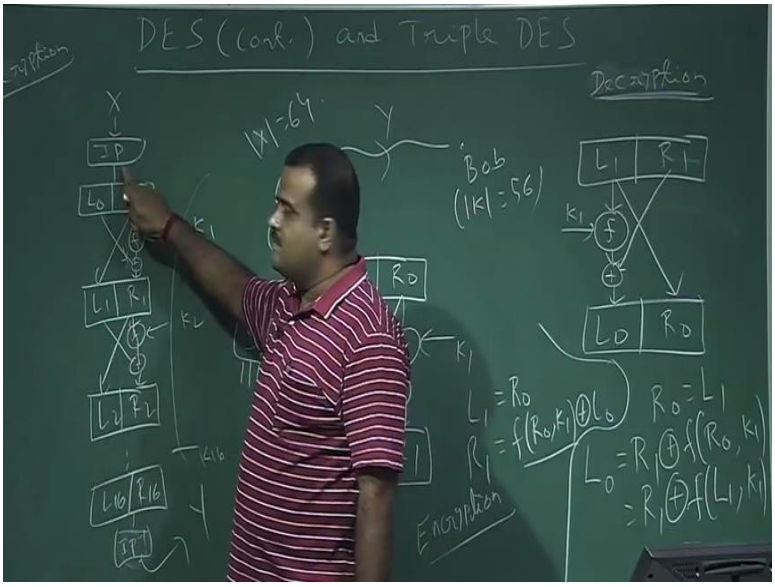
Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 07
Data Encryption Standard (DES)
(Contd.)

So, we talk about the DES decryption. So, we have seen the DES. So, encryption was like this.

(Refer Slide Time: 00:24)



So, you have plaintext x, we apply a IP we apply a formulation on this, then we divide this into two part L 0, R 0 64 bit; 64 bit 32 bit 32 bit then we are having a fiscal operation. So, this is directly coming here, L 1 R 1 then this is the function f, if it is taking k 1 as the first round key, then we are xoring with this bitwise x 1 and this is the R 1. So, this is the first round and then we continue this. So, from here we have L 2 R 2; same crystal structure we are applying with K 2 then we are xoring. So, this one, we will continue up to we got L 16, R 16. So, 16 Feistel cipher we are applying then finally, we are adding the IP inverse, and we got the y with the ciphertext. So, this is the encryption of DES encryption.

Now the question is how the Bob decipher it? So, Alice and Bob; Alice wants to send a message to Bob. So, they agree with the common key k is effective size is 56 bit and Alice has a plaintext m whose size is 64 bit. So, they decided to use the block cipher DES. So, Alice is doing this encryption. So, this is X, Alice is doing this encryption and getting this Y and sending Y to Bob. So, Bob has to decrypt it. So, how Bob can get back the message? Decryption, that is the decryption algorithm or decryption procedure, so from this y Bob has to get back x. So, basically Bob will apply this is IP inverse IP go back here. So, basically we have to invert the Feistel cipher. So, if you can invert the Feistel cipher, if you know how to invert a Feistel cipher then you are done.

So, the question is how we can invert a Feistel cipher? So, suppose we have a one round DES which is basically Feistel cipher. So, this is basically we have L 0, R 0 and the out this is 1 round DES. So, this is L 1, R 1 and this is basically f, this is K 1 for the first round, and we have excluding and this is R 1. So, basically L 1 is basically R 0 and R 1 is basically f of R 0 K 1 XOR with L 0, this is the encryption. Now we want to decrypt, we want to make it reverse I mean. So, for decryption our input will be L 1 R 1. So, this is our input L 1 R 1, now we need to get the L 0 R 0. So, this is the decryption process we want to mount.

So how we can do that? So, from this equation we can say R 0 is basically L 1. So, L 1 is basically R 0. Now we need to get L 0. So, L 0 is basically what? L 0 is basically R 1, if x are both side with f of this quantity then the XOR this and this XOR will cancel out. So, basically we have R 1 XOR with f of R 0 K 1. So, what is R 0? R 0 is nothing, but L 1. So, this is basically R 1 XOR with f of L 1 K 1 that is it.

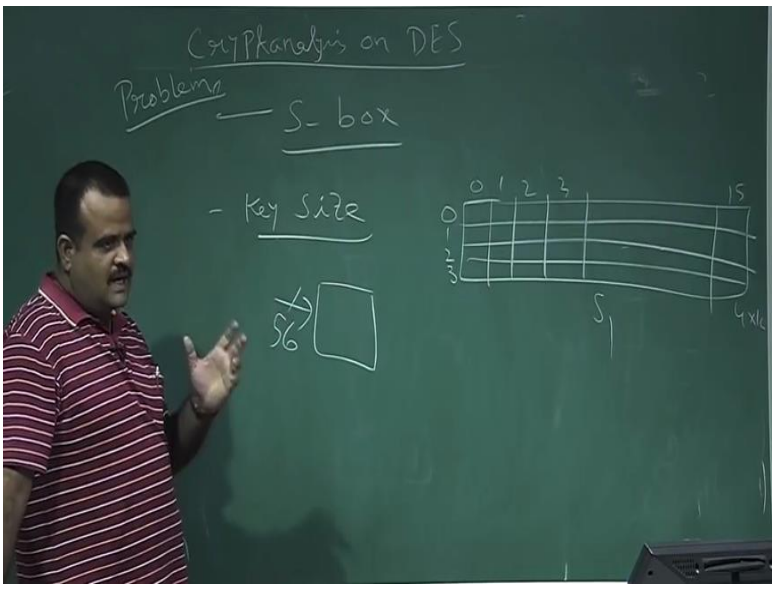
So, that is R 1. So, we just apply f on this with the value K 1 the round key and then we XOR with this with R 1 bitwise XOR and this is our L 0. So, we got both L 0 and R 0 from L 1 and R 1. So, this is a one round decryption method of Feistel cipher and the beauty of this cipher is, we are not inverting this f we are applying same f because sometimes inverse may not be possible because in the f function we have S-box, we have some formulation. So, that S-box is also from 6 bit to 4 bit if you remember is DES iS-box that is a 6 bit to 4 bit. So, that is also difficult to invert; this is one of the S-box in.

If we have to invert f, if you want to find out f inverse then it may not be always possible it may not be injective itself also. So, in that case inverts may not exist then we have a

difficulty; but the beauty of this structure is beauty of this feistel structure is we really do not need to invert f to get the decryption process. So, we just apply f again and we get the ciphertext; we get the plaintext. So, this is the inversion of the Feistel cipher. So, basically for DES we will apply this inversion process and for that we need to have same keys this K 1, K 2, K 16. So, the Bob has to generate the key scheduling algorithm and get the round keys and Bob will do the same process to invert this Feistel cipher and finally, Bob will reach here, after reaching here Bob will apply the IP inverse to get the plaintext X. So, this is the DES decryption.

Now the question is we want to analyze this block cipher DES in the security point of the how secured this DES is whether you should I mean what type of attacks can you think on DES. So, that is called crypt analysis on DES so that is or attacks on DES something like that.

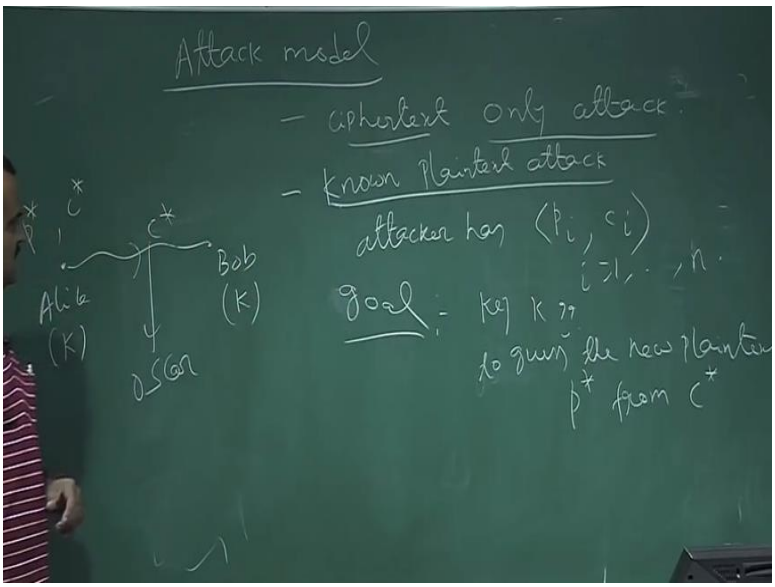
(Refer Slide Time: 08:32)



So, there are some issues with DES, the first issues is it is not well documented, in the sense that the S-box main problem is with the, so this is the problems with DES S-box. So, they have given the just the table; a table and a 4 by 16 table, 4 cross 16 table, 1 2 3; 0 1 2 3 like that 15. So, they have given say this is S 1. So, there are 8 as S-box. So, they have just given S-box in a table and we need to do the table look out, but how these values are coming there is no proper explanation for that. So, that is one of the drawback of this and another issue is with the key size.

So, key size of DES is just 56 bit effective key size. So, that will enable us to mounts the attack like generic attack like exhaustive search attack, time (Refer Time: 10:12) will come to those attacks those are generic attack. So, what do you mean by generic attack non generic attack will discuss that so, but before that let us talk about what are the attack module we have for the cryptographic cipher.

(Refer Slide Time: 10:36)



So, before that we want. So, what are the attack model we can think of a cipher. So, first one is known ciphertext attack or this is called ciphertext only attack ciphertext only attack. So, the point is Alice and Bob they are communicating with each other and the ciphertext are placed into the public channel and Oscar the bad guy I mean the attacker; we should not say bad guy - attacker is sitting here and Oscar has full control on this channel. So, Oscar is hearing all the ciphertext or Oscar is getting all the ciphertext, so that is called ciphertext only attack. Oscar is having only the access of this channel and so Oscar is getting the ciphertext which is between Alice and Bob or all the ciphertext between Alice and Bob.

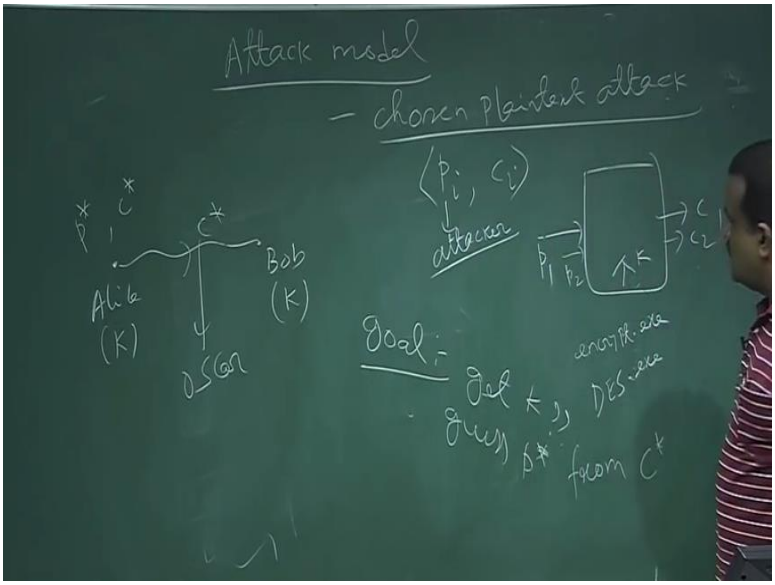
So, that is this model and second model, the next model is known plaintext attack. So, in this attack model Oscar is having some plaintext and the corresponding ciphertext. So, the attacker has or has some plaintext and the corresponding ciphertext or some. So, there are n of such thing. So, attacker has some plaintext; may be some all plaintext and the corresponding ciphertext which Alice and Bob are not currently using that plaintext,

but it was used long tome back so there is no much importance on that. So, they make it public kind of thing. So, they have given this plaintext and ciphertext.

And the goal of this attack is, they are using it common key K, this is the symmetric key set up, they are using a common key K. So, the goal of this attacker is to get the key K or to get the. So, suppose they are now using the message P star the new message and getting the C star. So, or to get, or to guess the new plaintext P star form C star, this is the current plain message they are communicating; current message is P star and the corresponding ciphertext is C star. So, C star Alice is sending to Bob over the public channel, now Oscar is hearing C star and Oscar is having some old messages some PICI some old message and corresponding ciphertext, plaintext corresponding ciphertext.

So, the goal of the attacker is to guess the current message and guess this or get the key that is also a big challenge to get the key. So, this is one model and another model is chosen plaintext attack, this is called this is - I will just rub this.

(Refer Slide Time: 15:07)

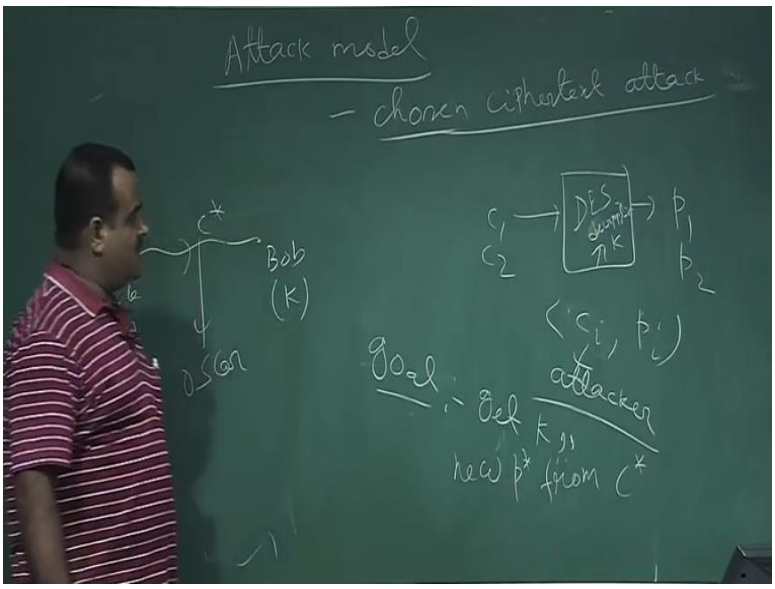


So, this is called chosen plaintext attack; this is the third model chosen plaintext attack. So, here what we are doing? We are giving some more power to the attacker in the sense that, so attacker can choose some plaintext and get some get the corresponding ciphertext; this plaintext can be chosen by the attacker. So, attacker or the Oscar can choose the plaintext and get the corresponding ciphertext. So, as if this encryption machinery, we are giving the temporary access of this encryption machinery to the

attacker, without revealing the key. So, what we are doing? We are inbuilting key over here and we are giving the access in software this could be a encrypt dot exe, I mean DES dot exe, DES encryption dot exe. So, we inbuilt the, we are not revealing the key, key is inside, but we are giving the temporary access of this encryption machinery to the attacker, so that attacker can choose the plaintext P 1 and P 1 get the ciphertext C 1. P 2 can get the ciphertext C 2 like this, for some point of time then we remove this access.

So, we are giving the temporary access of the encryption machinery to the attacker without revealing the key. So, key is inbuilt some sort of. So, attacker can give the plaintext and can get the corresponding ciphertext. So, that is this model and the goal of the attacker is to get the key that is the n or the P star to guess the P star, which is the current plaintext between Alice and Bob, P star form C star. So, this is the goal of the attacker in this attack model; now next one is chosen ciphertext attack.

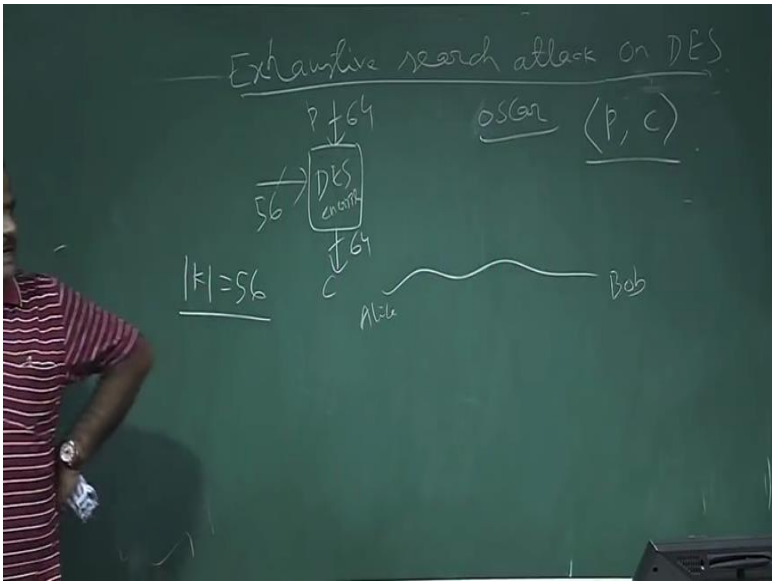
(Refer Slide Time: 17:46)



So, chosen ciphertext attack, so in chosen ciphertext attack we are giving the temporary access of the decryption machinery to the attacker, so like this is say DES decryption function. So, key is inbuilt key were not revealing to the attacker. So, we are giving the temporary access to this machine to the attacker, temporary access to this decryption machinery to the attacker, so that attacker can choose a ciphertext C 1 and get the corresponding plaintext. Attacker can choose another ciphertext P 2 like this. So, attacker can generate this C i, P i, P r. So, this is chosen by the attacker this ciphertext and then

we remove this access from this attacker. So, we are giving the temporary access to this decryption machinery to the attacker and we have removed that access and then after that the goal of the attacker is to; obviously, to get the key or guess the key and to know what is currently going on between Alice and Bob. So, what is the new message or the plaintext from the ciphertext system? So, this is the chosen ciphertext attack.

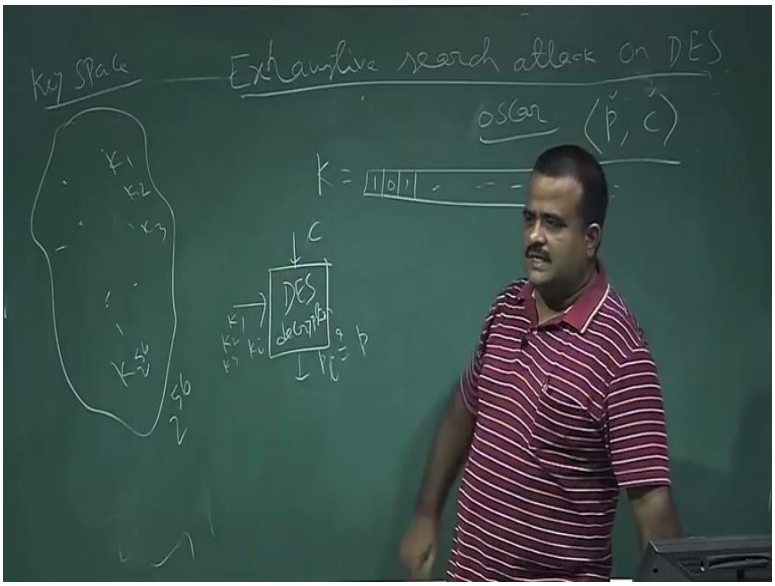
(Refer Slide Time: 19:52)



So, now, we will talk about the exhaustive search attack on DES. So, we talk about exhaustive search attack on DES. So, this is, so DES is a block cipher which is taking 56 bit effective key, this is the encryption of DES, DES encryption. So, Alice encrypt using this at Alice send this, this is P and this is C, Alice send it to Bob. Now key size of the DES is 56 bit, length effective key size is 56 bit and that will mount as this exhaustive search attack on DES.

So, how this is basically a known plaintext attack? Suppose Oscar, the attacker knows this a plaintext and the corresponding ciphertext and attacker wants to guess the key. So, attackers do not know the key, so attacker wants to guess, the attacker does not know the key, attacker wants to guess the key. So, what attacker will do?

(Refer Slide Time: 21:34)



So, attacker knows a plaintext and the corresponding ciphertext, this is kind of known plaintext attacks in attack model (Refer Time: 21:40). So, what Oscar will do? So, Oscar knows the key is 56 bit. So, key is a typically a 56 bit, 0 1 bit space. So, this is the key space. So, what is the size of this key space? 2 to the power 56.

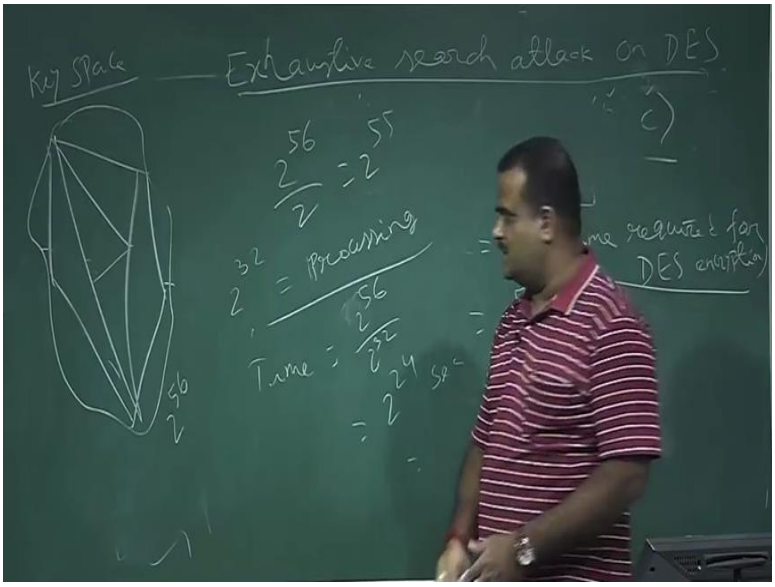
So, if on then we can K 1, K 2, like this. So, these are the keys K 1, K 2, K 3 like this. So, K 2 to the power 56 these are the possible key, this is the key space for DES. Now what Oscar will do? Oscar do not know the key, does not know the key so Oscar will try for all possible key, this is called boot force or existive size. So, Oscar will try for. So, Oscar have this C or then Oscar will do the DES decryption algorithm, this algorithms are public, this block cipher algorithms are public all the secret is the secret key K. So, our encryption algorithm is public, encryption decryption algorithm what we are doing those are public, only secret thing is the secret key K. So, what Oscar will do? Oscar will try for K 1 and decrypt it and C getting a P 1 and check whether this P 1 is P or not - if it is P then fine that is the corresponding key is K 1.

So, this way Oscar will try for all possibilities K 2, K 3, K i and get corresponding P i and check whether P i is matching with P or not. So, this way Oscar will try for all possible keys and once it is matching with this P then it stop, it could be other way also encryption also, Oscar can encrypt P and check whether C i getting C i is matching with C or not because Oscar is having a P C, P r.

So, this is the exhaustive search attack on DES. So, it will search for all possible keys in a key space. So, then what is the time complexity for this? So, time is basically the. So, we have to worst case we are getting the key at the end. So, time is basically 2 to the power 56 size of the key space and time required for DES encryption or decryption; time required for DES encryption or decryption. So, if you assume our machine is fast and this DES encryption decryption time is a 1 second. So, this is basically 2 to the power this many second. 2 to the power 56 second, which is huge, which is may be how many? I mean it is few years. So, that way we cannot do the exhaustive search on DES. So, what is the next step?

Now suppose we have two machines, two computers and we divide the key space into two parts and we ask both the computer search in this part in parallel. So, in that case the time will be reduced by half because they are working in parallel.

(Refer Slide Time: 25:34)

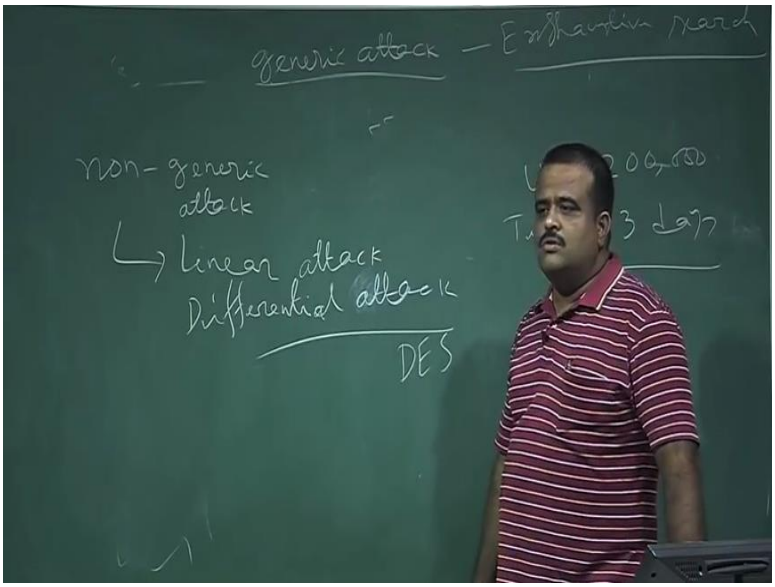


So, time will be reduced by 2 to the power 55 which is not much benefit, but if we have more than two computers if you have many processers, if you have say 2 to the power 32 processers. And then what we do? We partition this key space into that many number of partition and then we ask each of this computer, each of this processer to search in this particular region. So, you are partitioning this key space into this region and will ask the computer will ask the processer. So, this is the parallel computing.

So, processer are running in parallel and they are searching in the respective key space and once somebody got the key, so it will send the signal that hey I have got the key so stop. So, whole system will stop. So, this way if there are 2 to the power 36 or 32 processers, 32 computer or processers which are running in parallel to find the key then the time will be reduced by 2 to the power 56 by 2 to the power 32 which is basically 2 to the power 24.

So, which is this second, which may be less than 2- 3 days or something; so, this is an attack. So, this is an exhaustive search attack on DES. So, this attack was.

(Refer Slide Time: 28:23)



So, electronic founder foundation EFF, they mount this attack in 1996 and they build a hardware for this attack and they have spend around USD 2 lakhs and they can and their time complexity for get the t is just a less than 3 days, I think time is less than 3 days. So, this is an exhaustive search attack on DES and this is a hardware implementation by the electronic founder foundation and there are many softwares implementation on finding this exhaustive search attack on DES. So, DES is broke and this attack this type of attack exhaustive search attack is called generic attack, why? Because here we are really do not bother about the inner design of the DES, would not care how the inside it is the design, we only do care about the key space.

So, this same attack can be mount on another cipher which may be some X block cipher or may be some Sourav block cipher; only thing if the key size is 56 then the same attack

idea will be carried over here. So, we are not really looking at the inside of this cipher, so that sense it is called generic attack and there are some non generic attack on DES. So, those are basically in those attack we want to see, is there any relationship between the plaintext and the ciphertext, linear attack is there any differential between the plaintext and the ciphertext or some after some round, so those are differential attack. So, those are basically non generic attack.

So, non generic attack, so generic attack is basically exhaustive search or the time (Refer Time: 30:01) attack we will discuss the time (Refer Time: 30:02) attack later on. So, non generic attacks are basically linear crypt analysis, linear attack; then the differential attack and then some version of differential attack like boomerang attack, impossible differential attack.

So, in this attack model will really need to see the inner design of the cipher and we are really need to find out some linear relationship between the plaintext and ciphertext so that way these are non generic attack. So, these are cipher specific cipher specific. So, there are some, so there are very well non generic attack available for DES. So, DES is attacked by the linear attack, DES is attacked by the differential attack and there are other non generic attack which are presence in the. So, DES is broke in a sense of generic and also in the sense of non generic. So, we will look out some alternative of the DES, we will talk about triple DES in the next lecture.

Thank you.