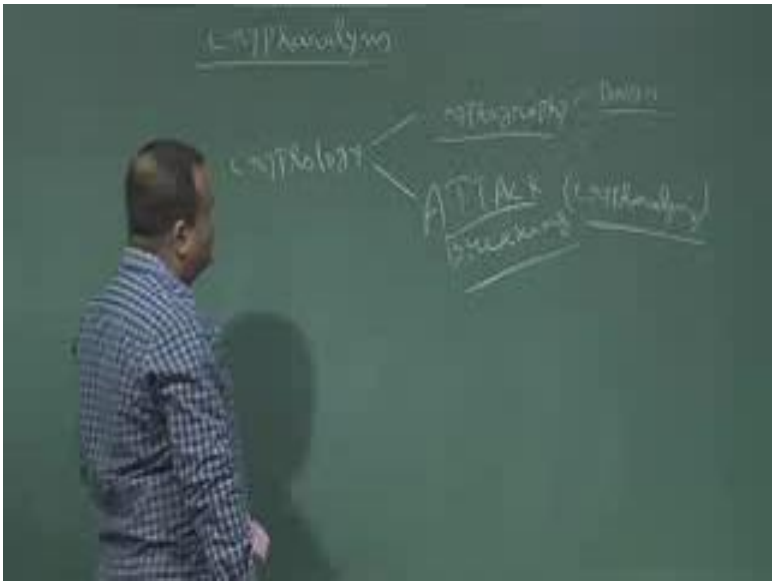
Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 46
Cryptanalysis

We talked about cryptanalysis or that means how to attack the cryptographic scheme or get cryptographic protocol. So, basically this is the other side of the coil. So far we have seen the design phase like cryptography.

(Refer Slide Time: 00:39)



Basically cryptography so, cryptology has 2 part one is cryptography so which we have talked about so far which is basically this area deals with cryptographic protocols cryptosystem RSA, EL Gomal, AES, DES. So, all the design techniques like design of the cryptographic protocol and this is the attack or breaking the code breaking. So, we have a cryptographic protocol, how we can attack that. So, this is this area is called cryptanalysis; cryptanalysis.

Basically cryptology is consists of cryptography and cryptanalysis. So, cryptanalysis means the attacker I mean the attack on the protocol, how we can break the code, how we can give the key or the message sending between Alice and Bob. So, all the type of job is done in this area cryptanalysis and the person who is doing this is called cryptanalyst and that is named as Oscar. So, that is a traditional name we used to denote

a attacker Oscar. So, this is this so, cryptanalysis is the other side of the coin. So, this is the design phase crypt cryptography and this is the breaking phase.

We talk about we start the cryptanalysis. So, we will talk about the models of cryptanalysis attack models especially on this is so attack models.

(Refer Slide Time: 02:40)

There are basically usually 4 types of model, but there are some combination of this type also 1 is the known plaintext attack by known ciphertext attack. So, the Alice and Bob they are communicating over a public channel. So, either by symmetric key encryption or by public key encryption and the Oscar is having access to this, this is the public channel and Oscar is having full access to this channel, it could be passively or actively the passively means Oscar passively means Oscar can only see what is being communicating and actively means Oscar can change the communication. So, these under this attack model means.

Oscar knows the ciphertext. So, what is called ciphertext, the Alice is the message, Alice wants to send to Bob that is called plaintext or the message and while it is encrypting to see either by symmetric key encryption or by public key encryption this is called ciphertext and it is being send to Bob over the public channel. So, this is called known ciphertext only attack known ciphertext only attack. So, Oscar knows only the ciphertext.

So, this is more secure scenario or we are not giving any extra facility to the Oscar, Oscar is only have the access to this public channel which is quite obvious to assume because if we say that we will not allow Oscar to listen what is being communicating over public channel that nobody will believe you. So, your scheme should be secure at least under this model.

(Refer Slide Time: 05:08)

The second 1 is known plaintext attack. So, the first 1 is known ciphertext only attack; ciphertext only attack the second 1 is known plaintext known plaintext attack known plaintext attack. So, in this attack model Oscar knows some pair of plaintext and the ciphertext. So, Alice and Bob; they are communicating over this public channel and Oscar is sitting here. So, in this known plaintext attack means Oscar knows the third party or the adversary Oscar is the adversary Oscar knows some plaintext and the corresponding ciphertext for some i is equal to 2 2 K suppose K many.

Oscar knows maybe these are the old communication between Alice and Bob. So, we can send the history of these 2 Oscar these are old communication maybe 2 years ago, they are they were communicating I mean their message was like this. So, m o p or plaintext and the ciphertext of this has no much relevance now I mean this is already being I mean communicated 2 years ago. So, under this model Oscar knows or Oscar has given some Oscar knows some p i c i p i and corresponding c i i is equal to 1 2 n 1 2 K and the goal of the Oscar is to goal is to get the key, key is not known the secret key is

not known if it is pub symmetric key encryption that symmetric key is not known to the Oscar.

Goal is to get the key what is the K and suppose Alice and Bob now communicating this p star and corresponding c star, this is the current message, they are communicating current massive Alice is wants to send to Bob. So, Alice compute c start from p star is the new message or to guess p star from c star the new message this is a new message or the current message they are communicating this is the challenge to the adversary and this third one is basically telling us known plain chosen plaintext attack chosen plaintext attack. So, this is you are giving little more power to the Oscar adversary in the sense that the adversary can choose the plaintext and can get the corresponding ciphertext without knowing the key. So, the Oscar can choose p i and can get the c i so; that means, this p i c i p r Oscar is having as many as so; that means, so, we are giving the encryption machinery to the Oscar temporary axis. So, maybe so, this is the encryption algorithm we can in build the key over here key is not known to the Oscar we are not giving the key to the Oscar then everything is gone.

But without knowing the key we are giving the temporary access to the en encryption missionary to the Oscar. So, that Oscar can give a plaintext and can get the corresponding ciphertext again another plaintext and can get the corresponding ciphertext without knowing the key so; that means, this could be dot e x e file encryption dot e x e where we are keeping the key in build. So, if it is c code then in the c code itself in the program dot c file will keep the key there. So, key will be; not be asking in the runtime. So, only in the runtime will be asking the plaintext. So, we are giving that encryption missionary temporary access of this encryption machinery to the Oscar it could be software it could be in hardware.

So that Oscar can choose a plaintext and can get the corresponding ciphertext. So, this is the now, what is the challenge of the Oscar? What is the goal of the Oscar? So, Oscar goal is to guess what is the key goal is to get the key e K or. So, or now we stop the stop; the temporary access of this encryption missionary or to guess what is p star from the system this or guess p star from the c star.

This is the p star is the now they are communicating. So, this is 1 model. So, here we are giving temporary access to the encryption machinery now the third 1, 4th 1 is chosen ciphertext attack.

(Refer Slide Time: 11:29)

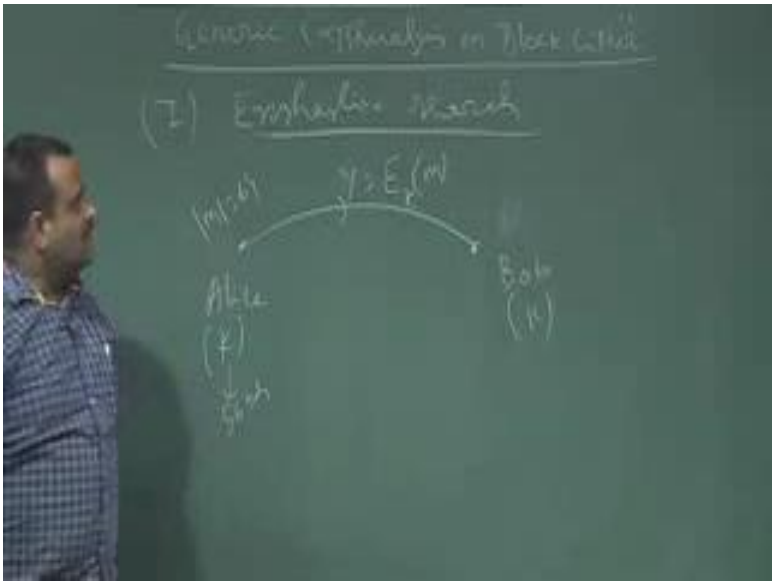
Chosen ciphertext only attack so, here we are giving the temporary access of the decryption missionary to the Oscar. So, we have the decryption function say it could be DES decryption key is inbuilt. So, Oscar can give a ciphertext and can give the corresponding plaintext. So, we are giving the temporary access of the decryption machinery temporary access then you have to take it back otherwise Oscar can give the new ciphertext and get the p star.

We are giving the temporary accept access of this decryption machinery to the Oscar. So, what we are doing here? We are just keys inbuilt. So, Oscar can choose p i I mean c i p i c i and can get the corresponding p i. So, Oscar knows this p i p i c i or some k, now the challenge of the Oscar is to get the key K which is not known and to now we stop this temporary access to this decryption machinery to Oscar now Alice and Bob is communicating p star c star and to guess p star from c star.

This is another model. So, this is more if we can claim that our 2 system is secured under this model, this is we are giving more power to the adversary so; that means, how powerful our adversary is even though our cipher is our scheme is secure. So, that is our goal, we are making our adversary more and more powerful now there are some

combinations of this 4 model. So, those we are not going into details, but these are mainly 4 models.

(Refer Slide Time: 14:13)



Now we will talk about some generic attack on the cryptosystem specially on block cipher generic cryptanalysis on the block cipher or it could be done for steam cipher also let us start with block cipher, the first one is basically we know is the exhaustive search, the exhaustive search or the boots force method. So, what this we have already seen suppose, we have a, we are Alice and Bob. So, suppose they are they are communicating over the public channel using the DES and they agree with the common key say 56 bits DES. So, it is 56 bit key. So, now, they encrypt. So, Alice chooses a message which is 64 bit and then Alice encrypt this message using this K key. So, this is DES encryption and sends it to Bob. So, Bob is receiving y and Bob is you apply a decryption algorithm to get back this message.

(Refer Slide Time: 15:54)

Now, how we can do the exhaustive search on this block cipher DES? So, basically so for that Oscar need to have a so this is a non plaintext attacks. So, Oscar is having so, Oscar is having p and c this is known. So, this is a known plaintext attack Oscar is Oscar is no having a plaintext and the corresponding ciphertext, but Oscar is not knowing the key. So, now, the challenge of the Oscar is to get the key if once Oscar get the key Oscar can get the new message. So, for that what Oscar will do Oscar will try for all possible key. So, this is a key space so, Oscar will try for so, if it is made by DES. So, Oscar will try for all possible keys. So, Oscar will choose a key from here the K i and Oscar will encrypt this p and get a c i and Oscar will check whether this c i is basically c or not if it is c if c i is c then K i is the key because we know this p r. So, this is known plaintext attack, we know this p r.

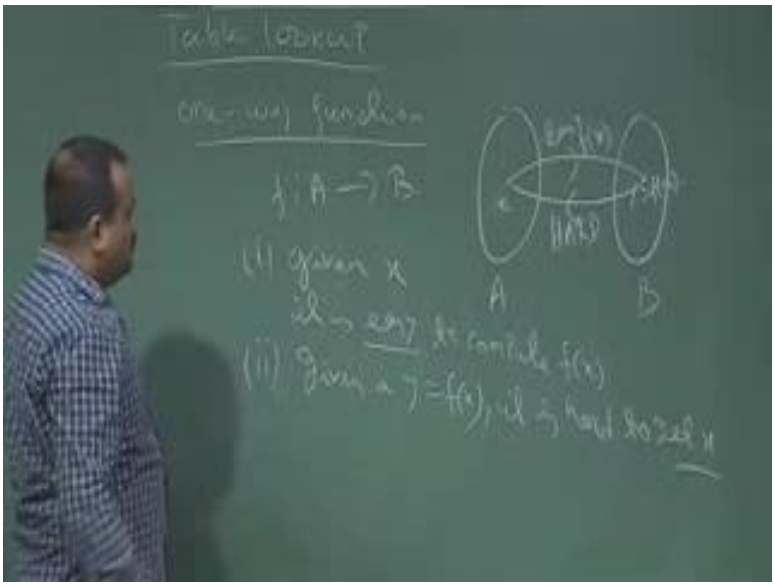
This is basically exhaustive search attack or the boot force attack. So, this way we have to search for all possible keys in the key space. So, the time complexity is basically the depending on the size of the key space if it is DES then 2 to the power 56 into time for DES encryption, if it is 1 second then this many seconds, this is huge, but we know there are some attack using the parallel processing if we have many processors then this can be reduced by the parallel processing and this type of attack you have seen.

This is the exhaustive search attack and this is the generic attack generic in the sense here we are not using any information about the how this DES is designed we are not

looking inside the block cipher or inside the cipher we are just we need to have just to know the key size this 56 bit. So, instead of DES if it is some other cipher like sod up of cipher and which is having key size 56 bit then also we can have we can mound this attack by similar way. So, that sense it is generic attack; that means, this attack idea can be mound for any block cipher which has same key size. So, we are not looking into the inside design of this cipher we are just looking into the key size. So, that sense it is a generic attack.

Anyway so now, we will talk about another generic attack which is called table lookup attack so table lookup.

(Refer Slide Time: 18:53)

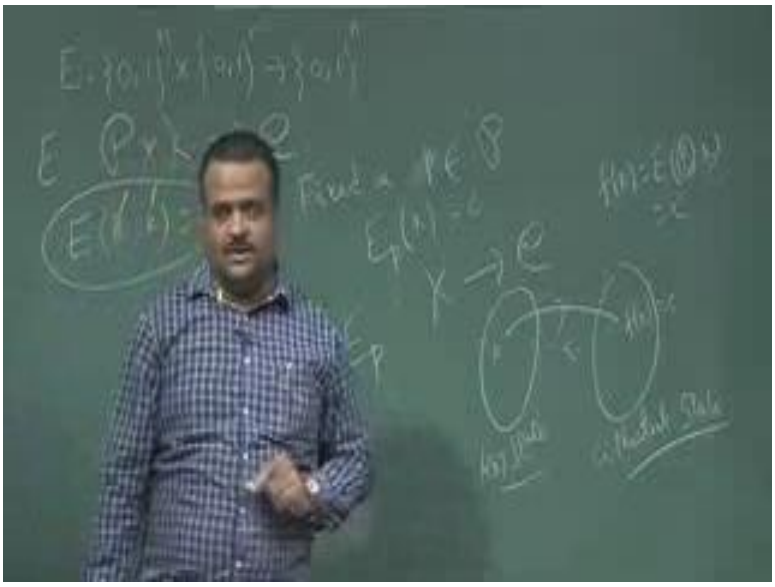


Basically under this attack it is also generic under this attack we have 2 face 1 is so, basically what we have to do? This is basically this attacking this is basically inverting a one way function, what is a 1 way function? It is defined a one way function suppose F is a function from a to b. So, this is a set this is b set it is a mapping basically. So, if you take a x over here then this is F of K this is basically y or we can denote this by x this is basically F of x. So, one way means this part it is easy given a x we can easily.

Say if we if given x, it is easy, again easy is a x sense easy means computationally feasible. So, we do have a polynomial time algorithm to compute this easy to compute F of x. So, one way it is easy, but the other way it is hard. So, given a y which we know it is basically F of x these way F is hard this is hard, but this must be using. So, given a y it

is hard to inward given a y which is basically F of x it is hard to computationally hard had to get x that is the one way function. So, one way it is one way. So, this forward direction it is easy, but backward direction it is tuff. So, every cryptographic protocol is basically one way function like if we consider a block cipher.

(Refer Slide Time: 21:13)



This is basically a block cipher is basically we have say n bit to so, if it is say n bit block cipher. So, we have a K bit key. So, block cipher is basically function form. So, this is basically function from plaintext phase key space to ciphertext space. So, we take a message from the plaintext space it take a key from the. So, it will. So, basically it is basically e of m comma K will give us c. So, it is a coming from plaintext space it is coming out key space it is a c.

Now if we fix a plaintext n p from the plaintext base this is p you can also write convention. So, then this p is fixed now this is a function from. So, then e p is a function form key space to the ciphertext space. So, this function is a one way function, these we different by F, now key space and ciphertext space may be different size. So, this is function form key space to the. So, this is key space. So, this is a known plaintext attack ciphertext space. So, here what we have a, we have a key. So, this is a plaintext is fixed. So, you have a key and then we basically apply. So, F of F of K is basically e of t comma k. So, p is fixed.

This is a function of 1 K. So, this is basically F of K. So, this is a ciphertext c. So, this way it is this is one way because for this should be easy because otherwise is our block cipher only popular. So, this is this is just encryption algorithm of the block cipher, but these way it is hard because if we have a ciphertext then to get back this key is basically breaking the block cipher under the known plaintext attack. So, that is hard. So, basically this is a one way function F is a one way function.

Now the question is how we can attack this so by table lookup method so, we have seen 1 attack by exhaustive search generic attack; another attack is my table lookup. So, we will do something in the pre possessing step. So, offline step. So, if you have time. So, we can do something. So, this has 2 step 1 is offline another 1 is online.

(Refer Slide Time: 24:39)

Table lookup; so, 1 is it has 2 step offline or this is also called pre processing pre processing phase or offline phase and another one is online attack online attack. So, what we do at the offline. So, at the pre processing phase what we do we compute the. So, basically we are converting this function. So, we have a function a to b. So, this is key space this is ciphertext space we have a x and this is F of x. So, the question is we have given a y we need to get back x. So, that is the challenge. So, what we do? We make a table, so, we will choose all possible keys K 1 and we get F of K 1 K 2 F of K 2.

K if we if the key size is say depending on the size of the key if it is K m or n c capital n this is basically F of K n. So, if it is d s then n is 2 to the power sixty fifty six. So, in the

table what we do we store this K, K 1 and this F of K one p i. So, K i F of K i like this K n F of K n p i like this. So, now, this is for all K as we are doing. So, we have a huge memory. So, we are storing this. So, this is we are doing offline phase and online phase what we have? So, this is the online phase we have a ciphertext this is non plaintext attack we have a cipher text y or basically c which is basically F p of i mean e p of basically a for K, but we do not know the K or K star. So, what we do we have this c or so, if we store this in a sorting order of this endpoint this points then we can search it, we can do the binary search on this c. So, suppose this is some K l F of K l say.

Now, suppose this is matching with c then we can get the key then K l is our key, this is just a table lookup attack. So, we just search for our; this y or c into the table now we know all the keys are there. So, it has to be matched with one of this then once this matching is done. So, we take the corresponding key as our key. So, this is the attack, but here we need to have the storage. So, because this table has to be store and this is, but online phase we are not doing anything we are just doing the table lookup. So, if it is just binary search it is logarithm time log of in time capital in time which is very faster.

So, online search less time, but we are having we need to have huge memory because to store this whole table. So now, there are some technique which we can trade up between the time and this space. So, that is called time memory trade off attack, which we will discuss in the next class.

Thank you.