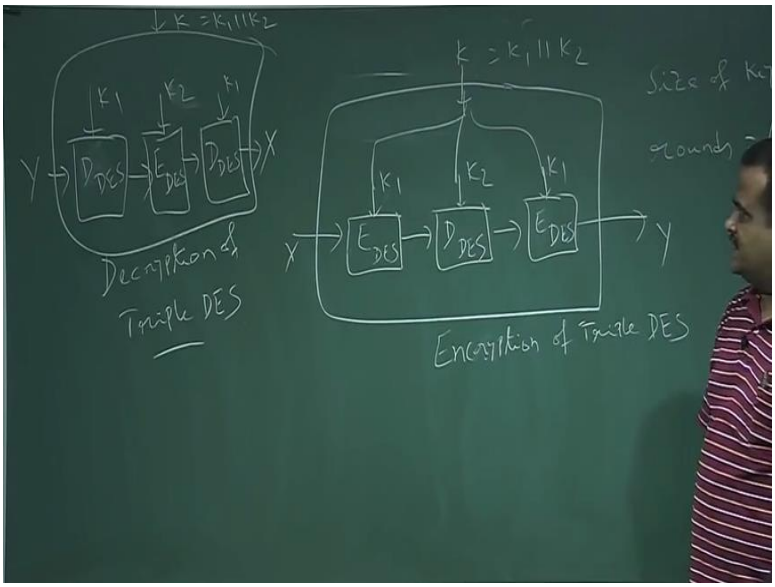
Internetwork Security
Prof. Sourav Mukhopadyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 08
Triple DES and Modes of Operation

We talked about triple DES. So, we have seen that DES as some problems; the DES is broken. So, DES has some issues with those boxes those are not I mean some non-negative problems we will see those details, but DES is broked I mean and the main problem was the key size is just 56 bits. So, that is also a security issues in terms of the exhaustive search attack so we can mount the generic attack on DES.

So, DES is broke, so now we need to have a replacement of DES. So people thought of that time to instead of building a new block cipher, so why do not you try to use the DES and have a new block cipher which would be better than DES. So, this is called triple DES.

(Refer Slide Time: 01:25)



Basically idea is we will use the DES three times. This is the triple DES encryption. So, here we have key is basically key has two part k 1 and k 2. So, here key size is, each is 56 bit so it is basically 1 on 2 bits this is the key size for triple DES. So, we just break the key into two parts this is 56 bit and this is 56 bit. Basically you want to use the DES.

So, this is the plaintext x, now we apply the DES encryption; encryption of DES with the key k 1 and then followed by a decryption of DES. This is the DES decryption with the k key to k 2 and then will use the DES encryption again with k 1. And finally, we got the y the ciphertext. So, this is the tipple DES encryption, so we have a key k which is basically k 1 and k 2 from catenation so this is the input so this is the block cipher. So, this is the block. So, this is the encryption of triple DES; encryption of triple DES; this is called triple DES because we are using DES three times.

And the key size is ok, key size is visible k key size is size of the key is 1 on 2 bit so it is difficult to think of the exhaustive searched at a even if we have many processors. So, parallel components even the time (Refer Time: 03:54) attack will would not be possible for this. So now, what is the number of rounds of error r, because for each of this DES is having; each of this DES encryption decryption encryption each is having basically 16 round. So, basically total we have 40 48 round; no 16 sources is total we have, so 48 rounds; so 16 into 3, so 32 plus 16 so 48 rounds.

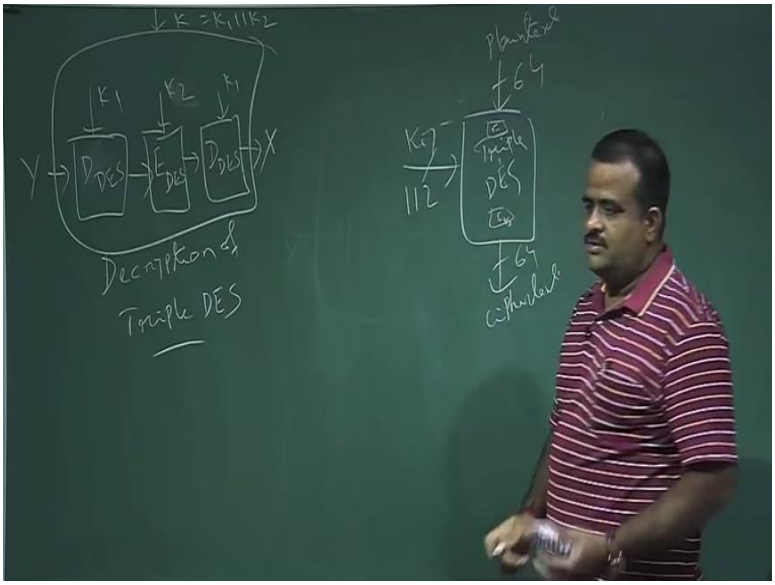
So, that is a major drawback of this atom, because it is a huge time 48 round blocks cipher nobody will be accepting this. So, because each DES round is a little complicated in the sense that it is having those is boxes which are not properly documented how it is coming. And moreover another issues that non generic attacks, those non generating attack can also be mount on DES, DES is broked by differential attack, linear attack. So, those types of attack can also be mount here; one can think of that because this is basically underlined block cipher is DES. So, if DES is broked by the linear attack, so one can think of those attack on this triple DES.

So, this is the encryption. So, what is the decryption? Decryption is just we have y is the input. So, for decryption you have to start from here we should get back x, so we have to reach here so for that we will use the DES decryption using the key k 1. So, this is the DES decryption using the key k 1 then we reach here then we are using decryption, so you have to use encryption. Encryption is the inverse process of decryption. So, DES encryption with the key k 2; so this will reaches here. Now we have encryption. So, we have to use decryption using the same key k 1 so that will come back to the x.

So, this is the decryption of DES using this k 1 and you will get back this x. So, this is the decryption process of triple DES. So, this is the; so we have the key input p s k 1 x or

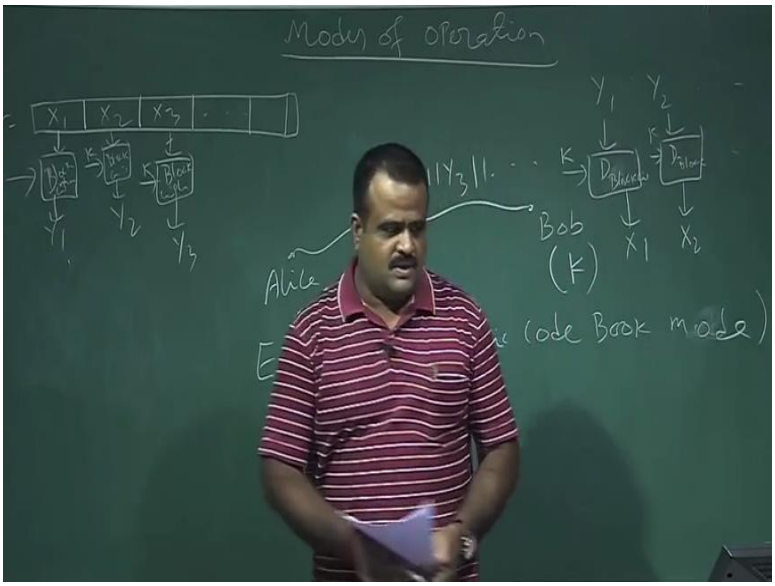
k 2 I mean conceding that with k 2. So, this is the decryption of to triple DES. But it is not very interesting in a sense that number of round is more and also the generic attack can be mound on this. So, people did not like it very much, so they wanted to have a replacement so now DES is replaced by AES advanced encryption standard that is the Windell. We will talk about Windell in later lectures.

(Refer Slide Time: 07:52)



So, this is the block cipher triple DES which is basically a 64 bit block cipher and the key size is 1 on 2 and the cipher text is 64 bit. So, this is the plaintext, this is (Refer Time: 08:05) and this is ciphertext, and this is the key; but inside we have I have 48 rounds that is the major problem of this because we are using three times DES.

(Refer Slide Time: 08:37)



Next we will talk about modes of operation on block cipher. So, this is under symmetric cryptosystem. So Alice and Bob, they are communicating with each other and they have a common key k that is the secret key they have. Now suppose Alice is having a plaintext, which is a long plaintext a long message; this is the message this is the plaintext m of the message.

Now, suppose Alice they want to use the block cipher for their encryption purpose. So, they have a block cipher, so they have a say l bit blocks cipher, l bit block cipher with the key size is same key. So, this could be DES AES SPN depending on l; I mean if it is DES l e 64 bit, if it is AES l e is 128 bit. So, but they have a block cipher, they agreed with a block cipher and then they want to use this block cipher for encrypting this message m. So, what Alice will do? So, Alice will break this into l bit blocks like this, last block may not be l bit may be you have to happened some dummy bit over there to in order to apply this block cipher.

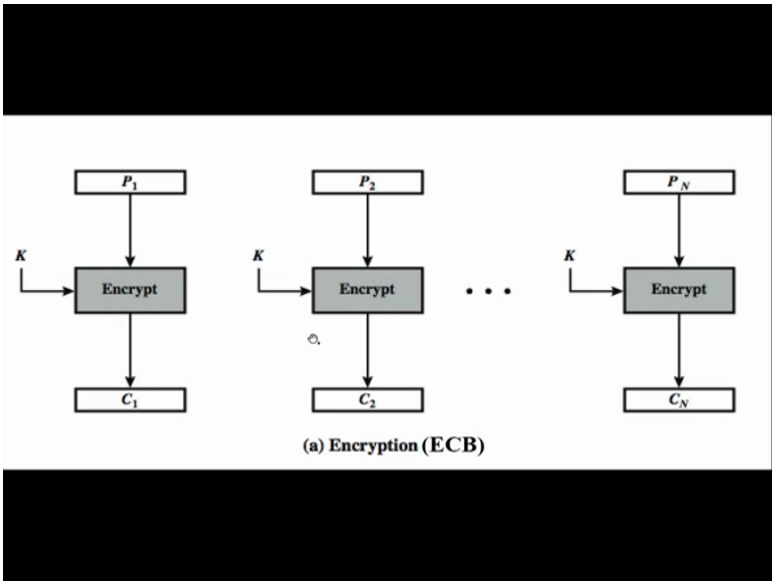
So, then this is l bit; now we can very well apply this block cipher or block cipher we use k the key and this, so this is say x 1, x 2 x 3 dot dot dot something like that. So, this is y 1, so on these also using the same key k; this is basically block cipher same block cipher and this is y 2 k, this is y 3 this would be DES or AES depending on the size of l. So, this is the block cipher, this block cipher encryption. So, we get this y 1 y 2 y n. So this is the

encryption, and Alice send this y 1 concatenate y 2 concatenate y 3 to Bob and Alice mention the length of this message.

So, what Bob will do? How Bob can decrypt it? So, Bob has this y 1 y 2 like this so Bob will do the, this is the encryption Bob will do the decryption; D decryption of the block cipher using the same key Bob will get the next one, Bob will use the same key for decrypting this block cipher decryption; if it is DES then DES decryption algorithm we have to use, if it is AES then a is a encryption you have to use there and AES decryption you have to use. So, this is the general things it could be any block cipher like this.

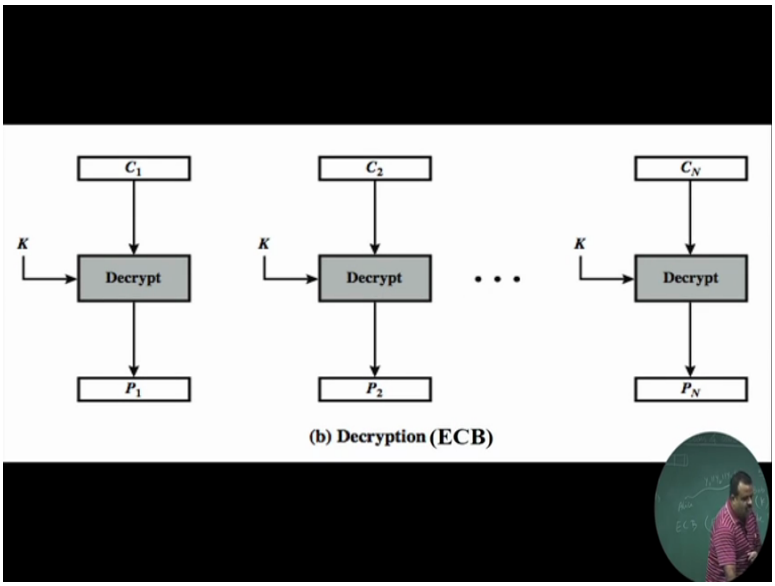
So, this is the way Bob will get back the message. So, this is one mode of operation this is called ECB or it is called Electronics Code Book mode.

(Refer Slide Time: 13:17)



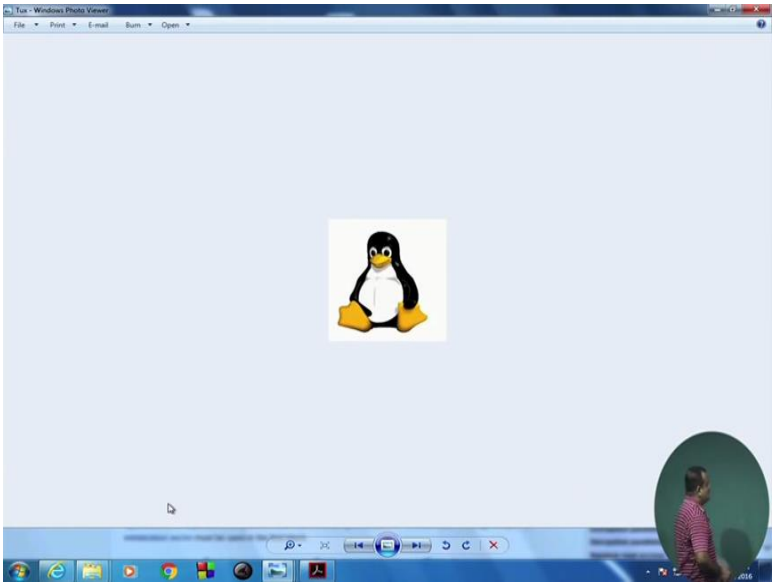
So this is using the just basically; this can you go to the slide please. So, this is basically we are breaking the plaintext into blocks depending on the size of our block cipher and we are using the same key and we are encrypting this blocks parallely, separately, simultaneously and then we get the ciphertext C 1, C 2, C N. So, this is the ciphertext. So, we concatenate this C 1, C 2, C N and we got the ciphertext.

(Refer Slide Time: 13:53)



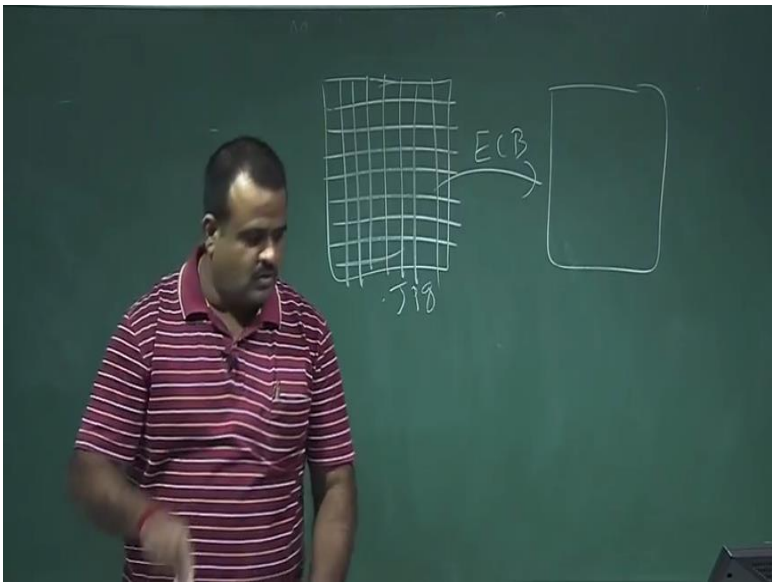
Now, this Alice is doing this is the encryption of this modes of operation. And now how Bob will get back? Bob is getting this C 1, C 2, C N, so Bob will using the description of that blocks particular block cipher using the same key and Bob will get back this plaintext.

(Refer Slide Time: 14:37)



So, this method has a problem in a sense that if we suppose our input is this image. Suppose this is our input, this we have taken from Wikipedia, this is this picture is there in the Wikipedia, so you have taken this picture from this is a penguin picture.

(Refer Slide Time: 14:51)

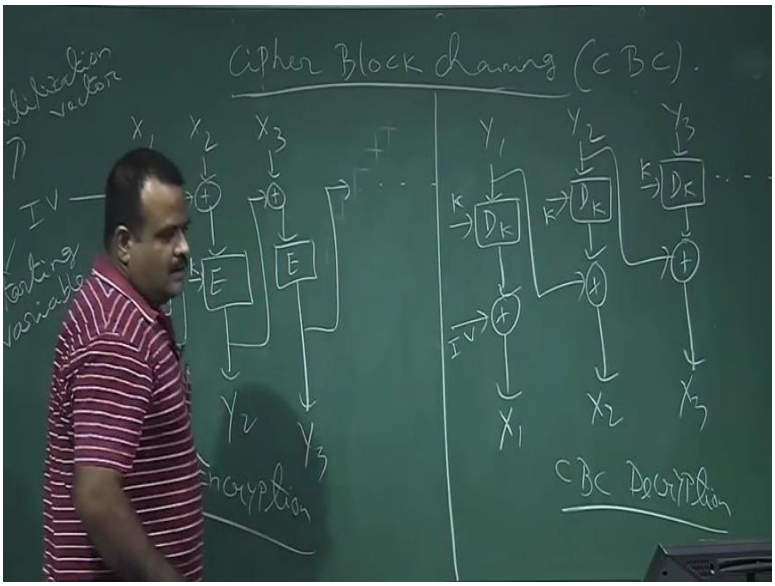


So, suppose this is our plaintext just a penguin picture dot jpg. Now, if we encrypt using our that ECB mode of operation then we are getting the output like this; I mean this is if we apply the ECB modes of operation and we are getting this output the penguin this picture. So, can you go to the slide please? So, this picture, so is this secured because by seeing this picture we can easily guess that this was the picture of the penguin. So, this is not secure.

So why it is happening, because in the image if we partition this into the pixel values and these are pixel values we are taking some blocks and we are encrypting and we are generating this ciphertext block. But if that block is having same value then the cipher text block will get the same value. So that is why this picture is coming like this, but this is not a secure encryption because anyone can guess that this was a penguin.

So, now we want to do something more in the modes of operation to avoid this problem. Next modes of operation are CBC modes of operation.

(Refer Slide Time: 16:43)



So, this is called cipher block changing; CBC. So, here what we are doing? We have the, this is a plaintext in a x 1, x 2, x n form. So, we are just XORing, this is on IV this is called initialization vector or starting variable. This is called initialization suggestion vector or the starting variables, because we have to start with something starting variable.

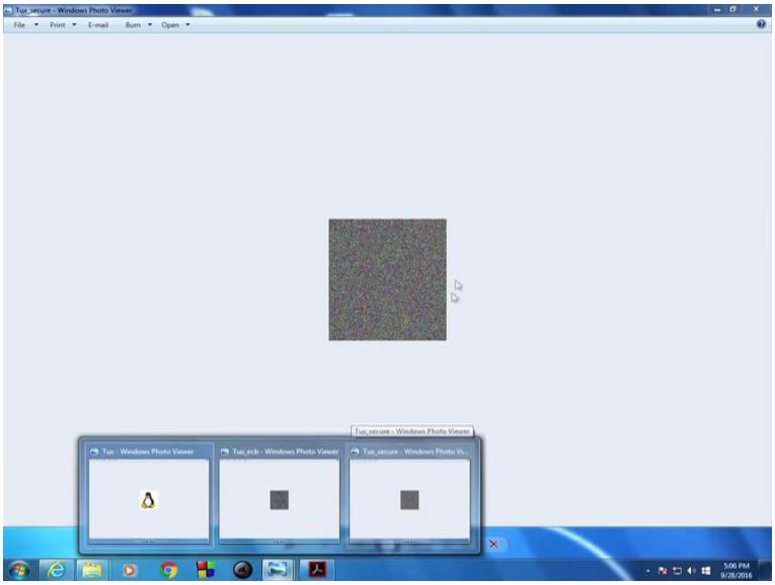
So, then now this we encrypt using our underlined block cipher; it could DES, AES is depending on the size of this. So, this is e of k the block cipher encryption. So, encryption of this block cipher DES or it could be anything any block cipher of that size, using the same key which is shared between Alice and Bob and we get the y 1. And this y 1 will give the feedback over here in order to avoid that penguin picture, because if we give the feedback then it will not give us the same value for the same input.

So, then we encrypt this using the same key and get the y 2. Again this y 2 will put it here and we encrypt this and get y 3, so this way dot dot dot. So, this is the encryption; this is the CBC encryption, this is Alice is doing and Alice is generating this y 1 y 2 and send it to Bob. Now Bob also has to get back this message. So, Bob is receiving this y, y 1, y 2, y 3, like this. So now the question is how Bob will get back this x 1 x 2 x 3. So, Bob has to reverse this, so Bob is having y 1 to get back x 1. What Bob has to do? Bob has to decrypt it Bob to go back here then Bob has to x or with this. So, it will cancel out we will get the x 1.

So, let us try that. So we will first decrypt it D of k using the same k and this will XOR with this IV for the first block and this is our x 1. And for the second block, so this is a y 2 and for the second block we just; second blocks means y 2 so if we decrypt it we are here now this has to be XOR with this y 1 to get back the x 2. So, we decrypt it using the same key so we reach here, now we have to XOR with this y 1 and this will give us x 2. Similarly, y 3 d k, so this is with the same key. You have to use the same key. This is basically this one this is x 3 dot dot dot dot dot. So, this is the CBC decryption.

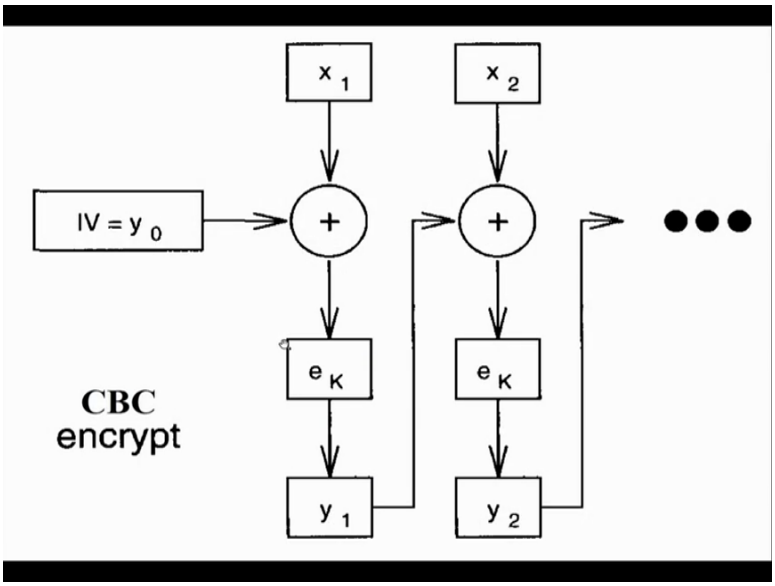
Now if we use this then the penguin if this is the; can we go to the slide please, if this is the image or this is the input. Then the output will be; so if this is the input and if we use the CBC encryption then the output will be this one.

(Refer Slide Time: 21:33)



Because, it is just taking the feedback and it is giving us this image. This image is the output of the CBC modes of operation after encryption. So, this is perfectly secure because we cannot guess it was penguin. So, this is one modes of operation where we are taking the feedback to avoid that scenario. Now another to most of operation will discuss one is CFB. So, let me just check whether the picture for CBC. So, can you please go to the slide?

(Refer Slide Time: 22:38)



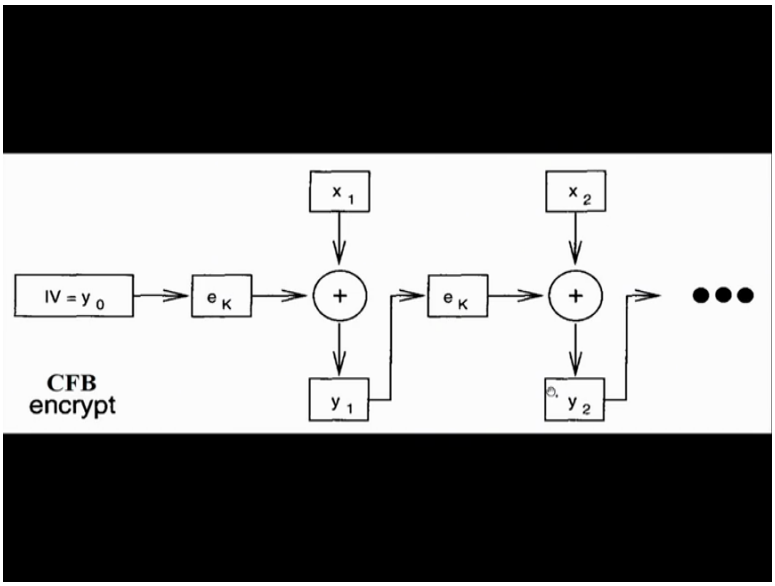
So, this is the CBC modes of operation encryption. We have the blocks the intakes blocks x 1 x 2 like this, so this is the starting vector or the initialization vector. We just XOR with this and then we encrypt using the same using the key shared between Alice and Bob and then we get the y 1. Then this y 1 we are taking the feedback to this and then we XOR with this x 2 and encrypt using the same key we are using y 2 like this. So, this is the encryption what you have discussed and this is the corresponding decryption, so we are taking this y 1 y 2 by y 1 then we decrypt it using the same key and we are using this IV XORing, x 1 we are getting, then white we are decrypting IV this we are getting.

So, this is the one modes of operation, now we will talk about other modes of operation which is called CFB. So, this is the Cipher Feedback Mode; CFB. Here what we are doing? We have this x 1 x 2 like this, so we are just encrypting. So, this is the encryption using the same key first we are encrypting the IV and then we are XORing with this and get the y 1. And in the next step we are encrypting this e k using the same key, and then we are XORing this with x 2 and we get y 2. So, like this.

So, this is encryption; encryption of CFB modes of operation. Now how to decrypt? Decryption is basically we have given y 1 y 2 so on and we have to get back the message x 1 x 2 x n. So what we do? From y 1 how we can get x 1? So basically again we have to encrypt this e k using the same key and then we XOR this with the y 1. So, this will give

us x 1. And now again to get back x 2 we have to encrypt this y 1 again and XOR with the y 2 to get back x 2. That is basically we are encrypting this v of k and then we are XORing this with y 2 and we get back x 2. So, this way we continue. So, this is the decryption; this is the decryption of these CFB modes of operation.

(Refer Slide Time: 26:29)



Let me see whether I have picture or not. So, can you please go to the slide? So, this is the CFB modes of operation, so we have this messages plaintext we are making into the blocks. So, this is the initialization that we are encrypting, then we are occurring then we are getting y 1 are then again y 1 we are encrypting. So, here we are using only the encryption, we are not decrypting the block cipher. We are not using the decryption of the block cipher. So, this is the CFB encryption and similarly CFB decryption is this one. Basically we are using all the encryption, so we are not using the decryption.

Next operation is OFB; output feedback mode. So, encryption is basically, we have this IV using the same key we are using so these we are XORing with the plaintext x 1 and we are getting the y 1 and here this encryption we are taking this and this we are XORing with x 2 and this is our y 2 like this.

So, again this is we are encrypting using the same key; key is same this is a block cipher. So, p has to be same that key is shared between Alice and Bob. So, this we are encrypting with x 3, this is basically y 3 and so on. So, this is the encryption. And then the description will be we have given this y 1 y 2 y so on and you have to get back this x.

So, how to get x 1? X 1 is basically, we have to again encrypt we have to get this then if we x or with this will get x 1; so that we have to write. So, this is the IV we are encrypting using the same key and this we are; so we reach here. So, these we have to XOR with y 1 and this will give a x 1. So, similar way this is the e k and this will keep it here and this will XOR with y 2 you will get x 2 dot dot dot. So, this is the decryption of OFB modes of operation, so just we will use the reverse process.

Now there is another mode of operation which is called counter mode of operation or CTR. In CTR we just use a counter, so we can set some counter then this is counter plus 1 counter plus n something like that. So, depending on how many blocks we have. So, we partition into the block, so we just encrypt this counter then the output we XOR with this P 1 the first block of the plaintext and then we get C 1. And then similarly we will do like this we get C 2 and so on.

So, this is the counter mode of operation encryption. Now for decryption we have to do the reverse. We have given this C 1's and we have to get back this P 1's. So, we just do the same encryption process and then we XOR with this C 1 to get the P 1 and these we XOR with C 2 to get the P 2 like this. So, this is the counter mode of operation.

Thank you.