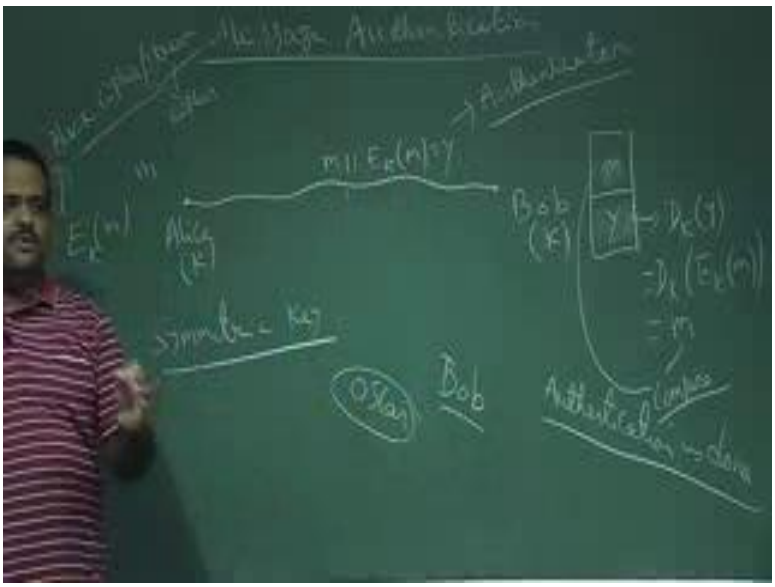
Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 36
Message Authentication

(Refer Slide Time: 00:26)



So, we will talk about authentication - message authentication. So, there are two parties communicating with each other over a public channel. So, this channel is public. So, this channel is captured by the adversary or third party Oscar who is basically called as a cryptanalyst or the hacker. So, now the authentication means suppose Alice is sending a message to Bob; now Bob has to ensure the message is coming from Alice, so that is the authentication. So, how Bob can ensure that the message is coming from Alice, it is not coming from Oscar or some other parties, so that is called the message authentication. So, how Alice can say that the message I am sending.

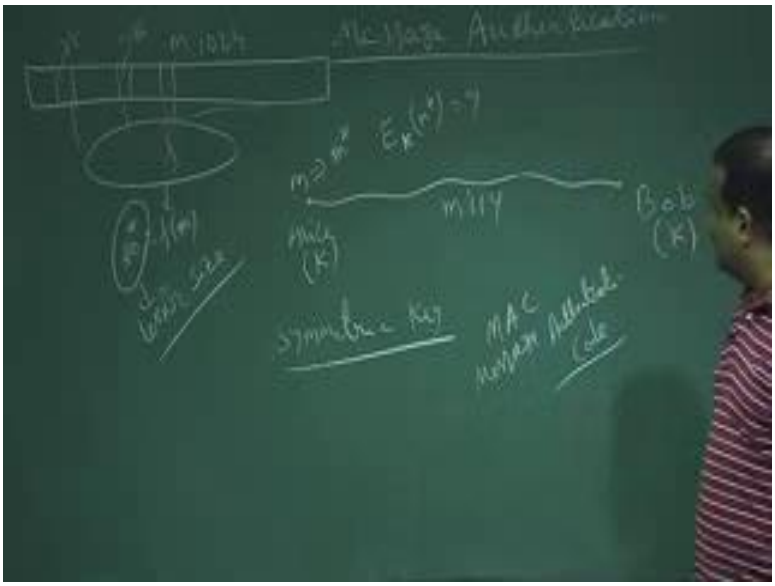
So, one way is to suppose they have a, this is symmetric key setup. Suppose at symmetric key set up, so they have a common key k they agreed to with this common key k. And what Alice can do? Alice can encrypt using this say this could be block cipher or stream cipher encryption. So, Alice encrypt this message using this k. So, this could be block cipher encryption, block cipher or stream cipher, so any symmetric key

encryption stream cipher. So, Alice encrypt the message and generate the cipher text c, and Alice send this message along with this encrypted message to Bob.

So, now what Bob will do? So, Bob is receiving the message M, and the encrypted message. So, what Bob can do, how Bob will authenticate that message is coming from Alice? So, Bob first decrypt this, this is the Y, the Bob is getting Y and this is the Y. So, Bob will first just that symmetric key decryption. So, Bob will decrypt this message cipher text Y. So, this is basically D K M, and this is basically the message M. And Bob will compare this with this. And if this is same as this then Bob will ensure that the message is coming from Alice. So, after comparing, if this is matching then that authentication is done, authentication is done that means, Bob will ensure that Bob agreed that the message is coming from Alice, because Oscar cannot, this - third party cannot send this message because third party cannot do this encryption, because this typical this key is shared between Alice and Bob. So, this is under symmetric key setup.

Now, the there are few issues with this like so message is becoming public because we are sending the message. So, here we are not bothering about the confidentiality of the message. So, if you want the confidentiality of the message so that means, the total cipher text is so this is authentication and the whole cipher text is sharp as a authenticator. So, basically we are generating this authentic. So, this is basically cipher text which is serving as authenticator whole cipher text. Now, here we are not having the confidentiality of the message. Now, suppose the message is big message. So, the encryption may be costly for that. So, instead of that can you do something, so that we will encrypt over a because just for authentication, we do not need to encrypt the whole message.

(Refer Slide Time: 05:32)

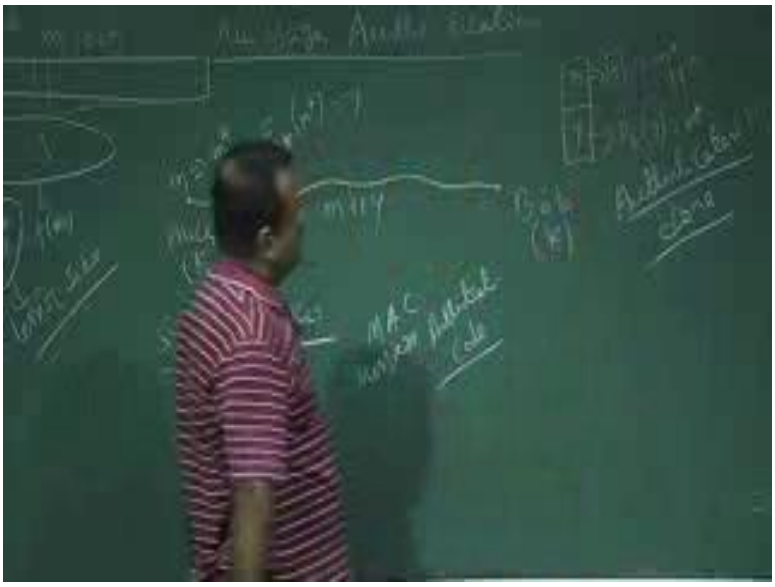


So, what we can do? Suppose message is very long say M is say some long bit and say this many bits. So, among these, we will choose some of the bits say 8 bit, 64 bit like this, 8 bit 16 bit like this. So, we choose some of the bits. So, basically we applied function on these. So, this is M and we get a f of M. So, f of M is basically we construct, we take some of the bits from this message not the whole bit. And then this is our M prime or m star this is of lesser size, because we are not considering all the whole message. We are just taking the some of the bits of the message, this is one way for f function; there could be other way. So, we can just do the bitwise XORing of some blocks and then we can give it a fix block like this. So, this is of lesser size. And then since it is a lesser size, so say if it is 64 bit, so one can go for the DES as a symmetric key encryption. So, if it is 128 bit, one can go for AES as symmetric key encryption or one can go for the stream cipher for the encryption purpose.

So, then we encrypt this. So, then Alice encrypt this. So, Alice will from m Alice will get m star. So, this is small, if it is, this is the message m which is very big I mean. So, Alice is getting m star then Alice is encrypting this m star using this symmetric key encryption, this is called message authentication code or MAC. So, this is basically a function, we are extracting some lesser bit of the message which is the function of the original message, and then we are applying the encryption algorithm symmetric key encryption algorithm on this, and then we generate this y. And we sent m along with y to Bob, and this is called MAC or message authentication code - MAC. So, this is message

authentication code. Then now Bob has to verify, Bob has to ensure that the message is coming from Alice. So, Bob has to authenticate this message. So, how Bob will ensure the message is coming from Alice. So, what Bob will do? Bob is receiving m and y, so this is m and this is y.

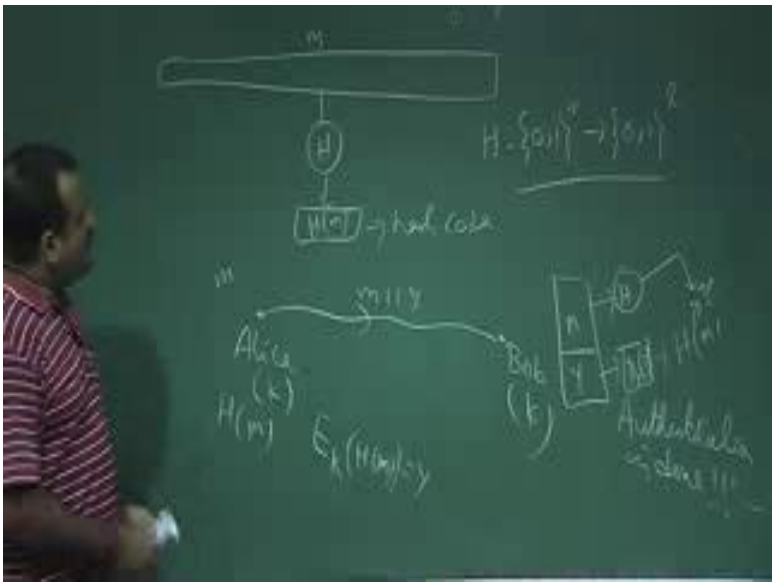
(Refer Slide Time: 08:46)



So, what Bob will do? So, Bob will apply this decryption with this is symmetric decryption algorithm. If it is DES encryption, then it is DES decryption with the y and it is basically gives this is m star. And Bob apply this f function that f function which give us this lesser bits and then it will give m star and then compare this two, whether this two is same or not. If these two are same then the authentication is done, then authentication is done, so authenticated, done. Otherwise, Bob will report that the authentication fails with these two are not same.

So, basically Bob is receiving m along with this y. So, Bob will apply the decryption then get m star then Bob is having this message m Bob will apply that f which is lesser bit and get the m star and compare these two. So, this is called message authentication code. And there is another way we can we can compress this message that is called hash function; we will talk about details of the hash function. So, basically in hash function, what we are doing? We are taking the whole message as input and it could be any size, arbitrary size.

(Refer Slide Time: 10:43)



So, we have a big input any size m, which is the message; and we have a function which is taking the whole message, and it is giving as a fixed size digest. So, this is the hash code. So, basically H is a function, which contains an arbitrary size input and can give as a fixed size of output, so H of m. So, if we have a hash function then Alice and Bob, they can use it for the encryption. So, hash function, it is a public function it does not involve any secret key. Wherever MAC, MAC is also public function that if, but it involve the we are encrypting that after reducing the size, we can take some of the bits after reducing the size lesser size, we apply the encryption on this, so that involves the secret key. But here we are not using any secret key. So, then we can use this MAC code, hash code in order to apply the in order to ensure the authentication. So, this hash we will talk in details. So, this is the scenario k. So, here is her message m. So, we can apply Alice can apply H of m and then Alice can encrypt this using the same key on H of m and this is y. Now Alice is sending m along with y.

So, after receiving M and y, so this is big message M and y. So, Alice will just decrypt it D K of y and get back what is called H of m and then Alice will apply H on this and compare this to m with these two value is same then the authentication is done then the authentication is done. So, we will talk about hash function in mode details. So, now let us talk about the problem with this scheme, this authentication scheme. What are the issues with this authentication scheme? So, this is sort of this is secured against the third party.

(Refer Slide Time: 13:37)

So, if there is a third party Oscar, so Oscar cannot do anything here in terms of the authentication. So, Alice is say they have a common key k and Alice is having a message. So, simply Alice is encrypting the message. So, E of k m encrypting on the original message or on the MAC or on the hash value of this message anyway, but suppose message is reasonably size say if it is 64 bit, this is just a DES encryption. So, then this is our y, now Alice is sending m along with this y to Bob.

So, now, by seeing this Oscar cannot do anything because Oscar cannot encrypt this again, because Oscar is not having the this secret key, but the thing is Bob can be a maliciously like Bob can cheat Alice this authentication scheme. How? Now Bob will receive this m and y, so Bob will decrypt it using the decryption algorithm, and get the message. Now, Bob can change the message Bob can change the message m star and Bob can encrypt this with the m star with the same key, and Bob can claim that this message is coming from Alice.

So, Bob can fudge here by changing the message, because there is no way Alice can prove that he, she did not send this message. So, this is the way this is the attack like if Bob is be a maliciously, Bob is the adversary. So, this is not prevent under these two parties, if the two parties are not behaving properly like if Bob can fudge like this, Bob can change the message and say that the message is coming from Alice. So, there is no way Alice can say that this is I did not send the message. So, this to prevent this we

would like to introduce the concept of what is called digital signature, so that is requires the public key set up, public key cryptosystem setup. So, to prevent this, we need what is called digital signature.

(Refer Slide Time: 16:56)

So, to prevent this I mean to prevent this attack means if Bob is behaving maliciously. So, in this case, this is a public key setup. So, we have two party Alice and Bob. So, in public key setup, so this is public key cryptosystem. So, in public key setup, both the party, so each of these party is having two pair of keys - public key or private key. So, Alice is having Alice public key and this is Alice private key. So, now suppose Alice wants to send a message to Bob for the authentication purpose, and Bob has to ensure the message is coming from Alice. And if they use this symmetric key encryption that is a problem, if Bob can be a maliciously like Bob can the change the message and can claim that this message is message came from Alice.

So, to avoid this problem what Alice will do? Alice will encrypt this message using Alice secret key, and this is called digital signature, and this is all Alice only can do this, because the secret key is secret to the Alice, this is not known to anybody else. So, d of A this is typical the private key or the secret key of Alice. So, what Alice will do? Alice will encrypt this message this is called signing. So, Alice will sign the message using Alice secret key. So, this is basically E of this is the encryption or signature E of m using Alice secret key and this is the y. Now, this is our cipher text or you can say this is our

signature, this is the Alice signature. And now these Alice will send to Bob. So, Y Alice will send to Bob.

Now, how Bob will verify that the message is coming from Alice? So, Bob has to get Alice public key, so either Alice has to send the public key to Bob over public channel that is fine or there is a public key directory PKD, where everybody's public key store this is Alice public key Bob public key, Bimol public key like this, Palash public key. So this is the public key of this is the public key of Alice. So, Bob will access this directory and Bob will get the public key of Alice. And then what Bob will do? Bob will just decrypt it, decrypt y using the Alice public key. So, this is basically give us e of A, and this y is basically e of d of A m. So, this is basically m - the message m.

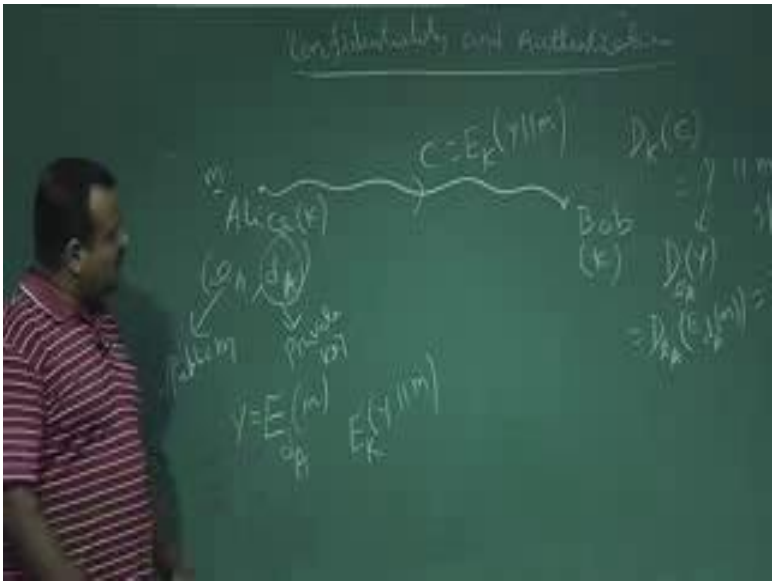
So, this is the Bob is just decrypting this using the Alice public key on the cipher text which was encrypted using Alice secret key. So, these two are reverse. So, it will cancel out, it will should give us the m. So, the authentication is done, and Bob will compare whether this message is matching with the message. So, may be Alice has to send the message over this public channel. So, the authentication is done. So, may be Alice has to send the message over this public channel. So, this is called digital signature. So, Alice is signing on the message by this way.

So, Alice is using Alice's signature I mean Alice signature means Alice private key which is typically secret to the Alice that is my signature, there is a certificate over directed sign on each of the certificate. So, that is the set of authentication like this certificate is authenticated by the director. So, this is the authenticated certificate. So, every certificate has to be signed by the authorized signatory. So, this is the way this is the signature and this director signature can be done by the director only, so that is the typical secret to that person, so that is why we encrypt the message using the secret key which is typically secret to the Alice. So, this is the authentication.

Now, here there is no confidentiality because the message is becoming public, we are sending the message over public channel. So, there is no confidentiality here message confidentiality, because message is becoming; we have to send the message otherwise Bob cannot verify it, either Bob is having the message already or Bob we have to send the message. Now, the question is how we can achieve both the authentication and the

confidentiality, so that is another issue how one can achieve both the authentication and the confidentiality.

(Refer Slide Time: 23:05)

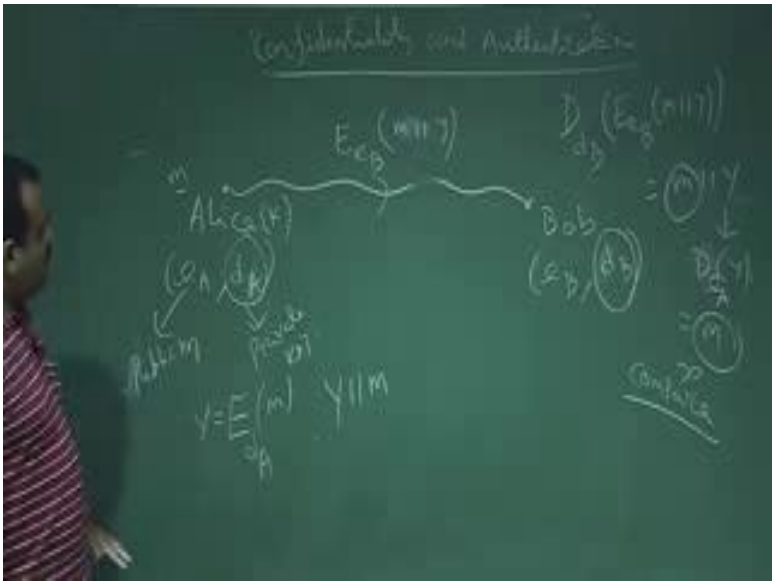


So, confidentiality and authentication, so suppose this is the Alice, so we have to use either mixture of public key, symmetric key or if we want to use only public key we will describe two schemes; one is suppose we want to have a mixture of public key symmetric key. So, this is Alice public key. Now, suppose they agreed with a key k - secret key I mean this can be done using the Diffie-Hellman key exchange protocol or they already have a symmetric key share between them. Then what we do? Then Alice will first sign the message using its her secret key under this public key encryption, this is public key encryption and then Alice will encrypt again this Y using this secret key K under the symmetric key encryption and this is the C. And C Alice is sending to Bob, so may be along with the messages. So, y along with the messages, so this is the concatenation and generating C, so C is basically E of K and sending to Bob.

So, Bob is receiving C. So, after receiving C, what Bob will do? This is the symmetric key encryption. So, Bob will decrypt it using this decryption algorithm. So, Bob will do D K of C using the same key. So, Bob will get back is Y and m. So, after getting Y, what Bob will do? Bob has to do the public key decryption algorithm using the public key of Alice. So, Bob will do D of e A on Y. So, this is basically D of e A y is basically E of sorry d A of m. So, this should give us m. Now, Bob compare these two values; and if

these two value is matching then the authentication is done. So, Bob will ensure the message is coming from Alice. So, this is the way both the confidentiality. So, confidentiality also preserving, because we are not sending the message just like that, we are just encrypting the message along with this authenticated part signature. So, this is under this. Now, we can use only this public key.

(Refer Slide Time: 26:28)



So, suppose Bob is having, so in public key setup everybody has their own pair of public key and private key. So, Bob is having Bob public key and Bob's private key. So, now, what Bob will do? Bob will just, Bob is having, so now, Alice wants to send this message to Bob for the authentication purpose. So, Alice is encrypting the message using this, basically this is the signing, and then what Alice will do Alice is concatenating this message with this, and then Alice is taking Bob public key and encrypting over this using the Bob public key, so that Bob only can decrypt this.

So, what Alice is doing? Alice is encrypting using this is the public key encryption using Bob public key on y along with the m along with the this message I mean concatenation this. Just adding this if m is 64 bit and it is 20 bit or again 64 bit then it will be 128 bit like this. So, just a append function concatenation. So, now this is Bob is receiving this. So, after receiving this, what Bob will do? Bob is having Bob's secret key which Bob will use for the decryption purpose, this is the public key decryption algorithm. So, Bob will decrypt it E b m y. So, Bob will get back m and y.

So, after getting this y, m and y what Bob will do? Bob will again, so Bob this y from y Bob has to get back m so, but y is basically the encryption which is encryption on the message using the Alice's private key. So, Bob has to do the decryption this is again the public key decryption using Alice's public key on y. So, this will give as basically m. Now, Bob will compare this m and this m, if it is same compare if it is same then the authentication is done. So, here both the authentication and confidentiality we are preserving. So, this is the way how we can do the message authentication without losing the confidentiality of the message, without we are making our message to be public.

Thank you.