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

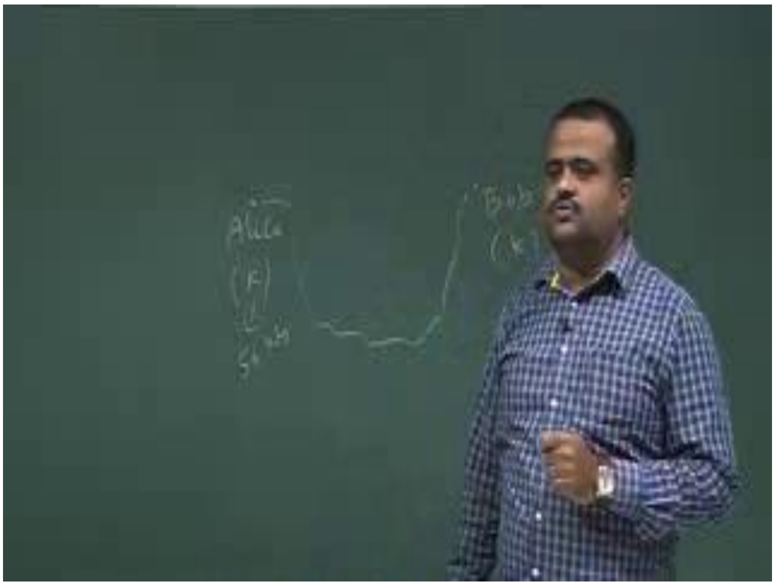
Lecture - 39
Key Exchange

(Refer Slide Time: 00:26)

So, we talk about key exchange protocol, we have seen one protocol like Diffie Hellman protocol. So, the issue is suppose two party Alice and Bob, they wants to communicate. So, they can either use private key cryptosystem or they can use public key cryptosystem for communicating a message like for symmetric key we need to have common key, common k. So, the question is how they can say at this common k, this is one issue. And for public key cryptosystem, they do not need to have a common key they can just if Alice wants to send a message to Bob, then Bob has to run this key generation algorithm in order to generate Bob's public key private key pair. So, Bob has to generate public key, private key pair and then Alice has to know bobs public key and then Alice will encrypt. So, if it RSA, Alice will choose a message Alice will encrypt this ab and send it to Bob.

But we know for RSA or any other if we use the even elliptic curve, so those are very expensive operation like exponentiation. Suppose, you want to find out say 100 to the power 50231. So, these operations are very expensive. So, usually public key is very expensive than the computationally expensive than symmetric key. On the other hand, in symmetric key, what we do? We will use either DES AES or some stream cipher, so those are basically, if we use DES. So, if we just use DES means it has some operation like we it is a Feistel cipher. So, DES symmetric key is encryption algorithm are very fast. So, symmetric key is faster than symmetric key encryption or decryption time is usually very much faster than public key, public key encryption and decryption. So, if we want to communicate with a large message or something, so we prefer to use in terms of the computation complexity, we prefer to use symmetric key.

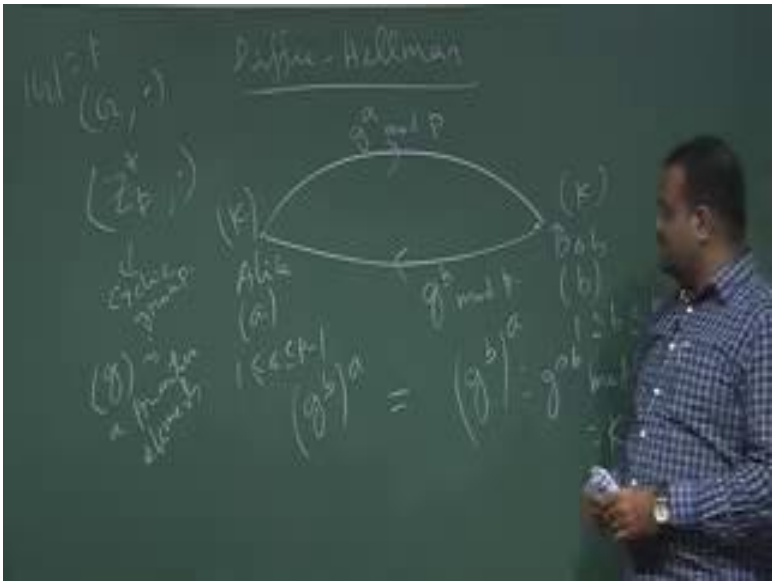
(Refer Slide Time: 03:48)



So, now, the question is so for symmetric key once these two party need to agree with a common keys so how they can exchange a common key. So, they wants to suppose they decided that they are going to use the symmetric Alice and Bob, they decided they are going to use DES for their communication so that means, they need to agree with a key k which is basically 56 bits. So, now the question is how they can agree with such key. So, this is the key exchange protocol how we can distribute the symmetric k between two parties which are not seating together I mean they are communicating over the public channel.

If there is a secret channel then Alice can send this over the secret channel to Bob, but there is no such secret channel or secured channel exist in the world. So, everything is public, so we have to do something, so that over this public channel, they should able to agree with the key; and that key they are going to use for their encryption and decryption purpose using the symmetric key encryption either block cipher or stream cipher because that is must faster than the public key encryption. So, we have seen one such key exchange protocol which is Diffie-Hellman key exchange protocol.

(Refer Slide Time: 05:04)

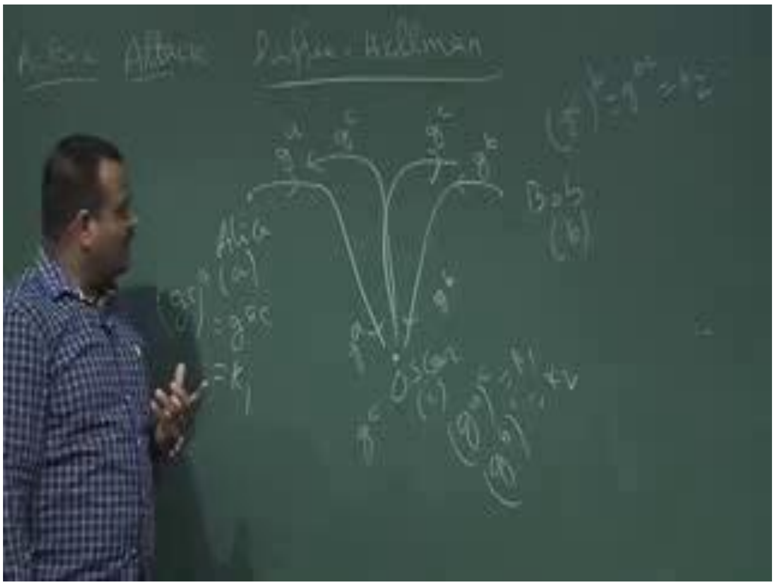


Let us just recall that and then we will talk about some active attack on this. So, for Diffie- Hellman key exchange protocol, we have two party Alice and Bob. So, they choose a group g which is usually taking as additive group. So, if p is a prime we can take Z p star which is a additive which is this is usually choose as a multiplicative sense. So, multiplicative group, because Z p star is a cyclic group not only Z p star we can take any group g. So, g is a group, and this is in multiplicative sense it could be in additive sense also. And suppose small g is a generator, g is a primitive element of that group or generator; that means, it generates the group. So, these are all public. So, they can just decide and they can make this group to be public. So, g is public.

So, now and suppose the order of this group is say p minus 1 or p, order of group is say p minus 1 or say some order g. Now, Alice chooses secret a, I am just recapping Diffie-Hellman Bob chooses secret b. So, a is typically 1 less than equal to a less than equal to p minus 1; and b is also is the index p minus 1. These are basically secret of these two party Alice and Bob, and they kept it secret. Now what they are sending? So, Alice is sending, Alice is computing g to the power a and sending to Bob. So, g to the power a may be mod p, p is public and Bob is sending g to the power b mod p. So, then after receiving g to the power b Alice is having a. So, Alice is computing g to the power b to the power a, and Bob is computing after receiving g to the power a Bob is having b. So, Bob is computing g to the power b to the power a. So, these are basically same these are basically g to the power a b I mean mod p. So, this is the common key they agreed. So, now they have a key for their symmetric key encryption and decryption. So, this is the Diffie-Hellman key exchange protocol we know.

Now we talk about attack on this, active attack active attack means the adversary is active. Adversary is passive adversary means adversary only listening to the public channel, adversary are seeing what is being communicating between Alice and Bob receiver and sender. But active attack means adversary not only have the control of this channel by listening, adversary can change the message. So, adversary can actively participate in this public channel, adversary can change the message. So, we will talk about that active attack on this protocol.

(Refer Slide Time: 09:03)



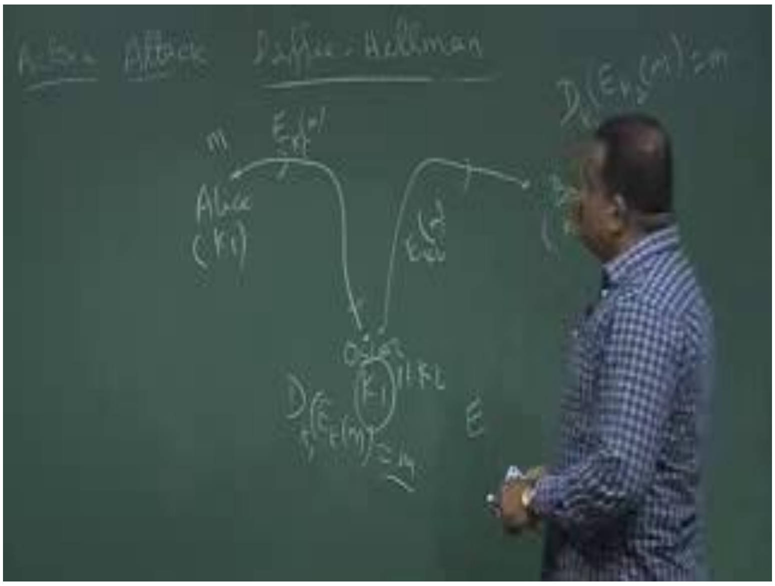
So, let us talk about active attack, active attack means the adversary is active. So, adversary means we name adversary as Oscar. So, Oscar is sitting here. So, we are running Diffie-Hellman. So, they have chosen their secret and Oscar is also chosen a secret c, which is also from less than or equal to order of the group, less than order of the group, Oscar is also choosing this. So, now Alice is sending g to the power a to Bob and

Bob is sending g to the power b to Alice, I mean they are sending means they are broadcasting they are putting this value into the public channel, but this channel is totally captured by the third party Oscar.

So, what Oscar will do? Oscar will take this value, and Oscar will take this value, and now Oscar will compute g to the power c and Oscar will send g to the power c to over the public channel so that means, so g to the power c to Alice and g to the power c to Bob also. So, as if Alice is thinking because Oscar stopped this communication between Alice and Bob. So, Oscar is taking g to the power a and g to the power b, and Oscar is not allowing g to the power b should go to Alice, and g to the power a should go to Bob. So, instead of that what Oscar is doing, Oscar is just computing g to the power c and sending this g to the power c over this public channel. And as if Alice will think the g to the power c is coming from Bob, and Bob will think as if g to the power c is coming from Alice.

So, now what is the attack? Now Alice is getting g to the power c. So, Alice will compute g to the power c to the power a, which is basically g to the power a c. So, this is basically k 1. And Bob is receiving g to the power c, so Bob will compute g to the power c to the power b which is basically g to the power b c which is k 2. Now, what Oscar will do? Oscar is getting g to the power a and also g to the power b. And Oscar is having Oscar secret c. So, Oscar can compute g to the power a to the power c which is basically k 1 and g to the power b to the power c which is basically k 2. So, now, they have Alice is having k 1, Bob is having k 2, but Oscar is having both the key k 1, k 2. So, as if Alice will think I agreed this k 1 with Bob, Bob will think I agreed this k 2 with Alice, but they are not knowing that this is this key is not the same keys.

(Refer Slide Time: 12:27)

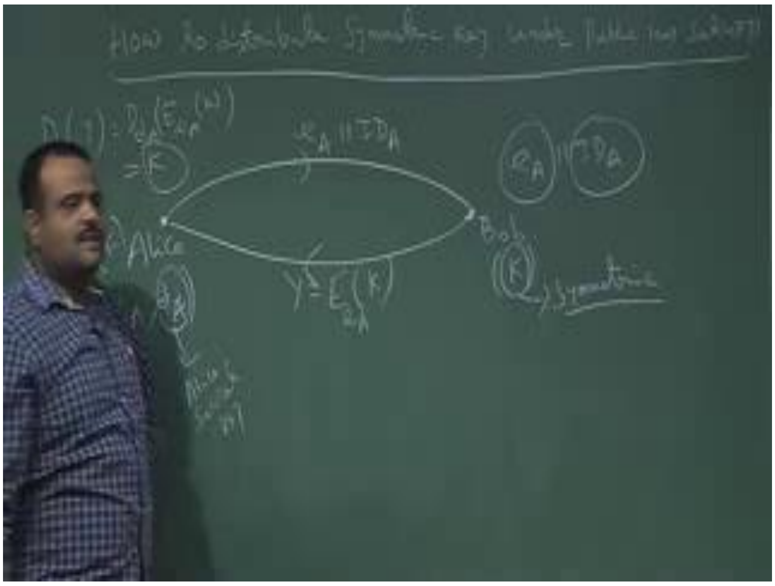


Now after this, what Oscar can get the advantage? So, now Alice is having k 1 - the symmetric key; and Bob is having k 2, and Oscar is having both k 1, k 2. So, now, Alice will choose a message. And suppose if k 1 is say 56 bit, and they decided to have the DES for their encryption purpose. So, Alice will encrypt this using the block cipher or anyways stream cipher symmetric key encryption, encrypt this message with this k 1 and sending to Bob over this public channel. Now, Oscar will take this message and Oscar is having k 1. So, what Oscar will do? Oscar will decrypt this message, this ciphertext d of using this k 1. So, Oscar will reveal the message which is Alice is sending to Bob.

And what Oscar will do now? Oscar will encrypt now again this message using now K 2, and Oscar will send this ciphertext to Bob. Now, Bob is having K 2 Bob is thinking this message is coming from Alice with same key they have shared as if. So, what Bob will do? Bob will decrypt it using K 2, and Bob will get back the message. So, there Bob is after receiving this Bob will get back the message, but unknowingly Alice is also getting the message. So, Alice is knowing what is being communicating between sorry Oscar is knowing what is being communicating between Alice and Bob.

So, this is the active attack on Diffie-Hellman protocol. So, if the adversary is actively participating in the over the public channel actively participating means if it can change the message that power we should give to the adversary this is called active attack. So, to prevent this, we need to do something called some signature or authentication we need to do. So, we will talk about that scheme.

(Refer Slide Time: 15:30)



So, this scheme is the candidate of under active attack. So, now we will talk about, so how we can distribute the secret key under the public key setup. So, now we will take help of the public key because otherwise if we just do the Diffie-Hellman then it is not secured. So, the question is how to distribute symmetric key under public key setup public key setup. So, this is the question so that means we are going to use the symmetric key for our encryption, because as we said that symmetric key is faster than the public key. But we will do the key generation of public key because to share this symmetric key to exchange this we are going to make use of the public key cryptosystem; otherwise it is not secured, only Diffie-Hellman will not help us Diffie-Hellman is not secured.

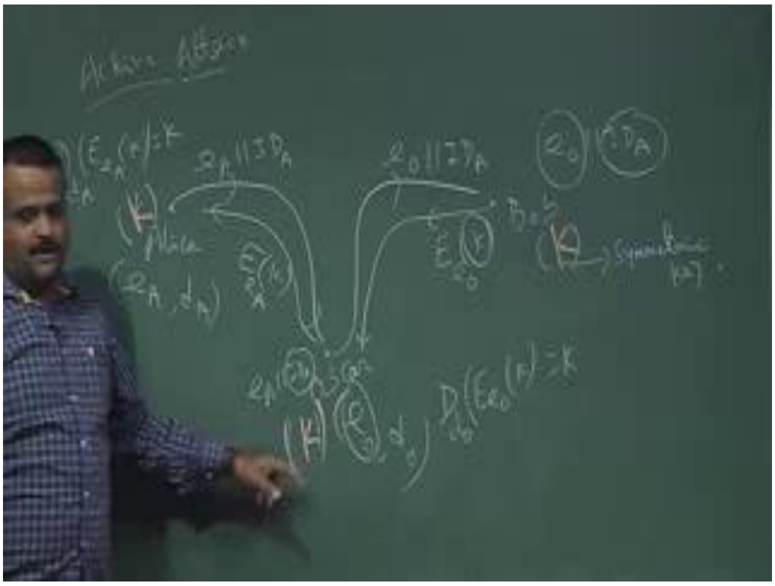
So, how we can do that? So, suppose Alice and Bob two party under public key setup. So, suppose Alice generates his public key and the private key pair. So, this Alice can generate, it could be RSA or any other public key cryptosystem. So, this key generation is running by the Alice, Alice is generating this public. So, this is Alice public key and this is Alice secret key or the private key. Now, Alice will send this to Bob, Alice public key along with the ID of Alice, because they want to agree with a key k symmetric key, so that they can use that symmetric key encryption for their further communication.

Now Bob will receiving this. So, Bob will check the ID, so Bob is receiving e of A an ID of this. So, Bob will check the ID of Alice and Bob will be happy to see the yes ID is Alice ID. So, then Bob will get this public key of Alice now Bob will choose a symmetric key, this is the symmetric key. Bob will choose a symmetric key may be randomly Bob is choosing. If he decided to use AES, so Bob will choose 128 bits just random bits. So, anyway so Bob is choosing a k and then Bob is encrypting this k public k encryption using the Alice public key and sending to Alice.

Now Alice is having Alice secret key, so this is the y. So, Alice is having Alice secret key or corresponding decryption key. So, after receiving y, what Alice will do Alice will decrypt this using Alice corresponding secret key. So, this is basically D of d A and y is basically E of e A k. So, this should give us K. So, now, Alice and Bob they both agree with this common key K.

So, now, Alice is having this k, Bob is also have this k, because this k is generated by Bob this can be done by Bob also, this communication can be this way also. So, instead of Alice Bob also can send this. So, anyway that does not make any difference because ultimately they have to agree with a symmetric key k. And they agreed with the symmetric key k. Now, they can happily use the symmetric key encryption and decryption for their further communication. Now, this scheme is also this scheme is also not secured under the active adversary under active attack. So, how to see it is not secured? So, this scheme is not secured under the active adversary.

(Refer Slide Time: 20:26)



So, let us just talk about that attack on this scheme. So, the attack on this scheme is basically this is active attack. So, adversary is actively participating over the public channel. So, Alice, Bob, now we have a third party - Oscar, who is active over this public channel. So, what we will do? So, let us just write the scheme. So, Alice is generating this. Now, Oscar is also generating Oscar public key private key pair. So, Oscar is also running the key generation algorithm and Oscar is generating the cryptosystem, the public key cryptosystem they agreed that may be they agreed that we are going to use the RSA cryptosystem. So, under this so Alice has to run those key generation algorithm like choose p q then 5 n equal to p minus 1 so like this. So, Oscar is also doing the same thing Oscar is also generating Oscar public key private key pair.

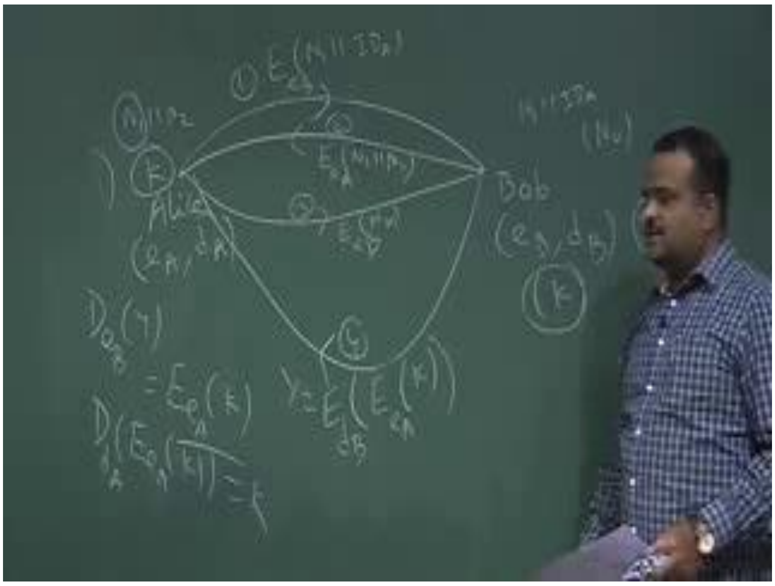
Now, Alice is sending e of A along with ID of Alice over the public channel to Bob. Now, Oscar has frontal of this channel. Now, Oscar will just stop this communication and Oscar will take this value to himself. Now Oscar is doing what Oscar is just sending to Bob Oscar public key and Alice ID, because Oscar is receiving Alice public key and Alice I D. So, Oscar will send Oscar public key with the Alice ID through the public channel to Bob. Now, Bob is check Bob is receiving e of A an ID of a. So, Bob is checking ID of a and Bob is convinced that he is communicating with Alice only. So, then Bob will think this is the Alice public key. So, Bob will choose a key k which is symmetric key and Bob will do what? Bob will just encrypt this public key encryption of this k using the public key, which Bob has received which is supposed to be Alice public key, but Oscar has changed it, Oscar made his own public key. So, this is send to over the public channel.

So, now what Oscar will do? Oscar will also take this. Now, Oscar is having Oscar own secret key. So, Oscar will decrypt this decrypt this message coming from Bob using his own secret key or the corresponding private key. So, Oscar will get k. So, now Oscar is also knowing this k, the symmetric key which Bob has chosen. Now, what Oscar will do? Now Oscar is having e of Alice public key. Now, Oscar will encrypt this k using Alice public key, and send it over to Alice over the public channel. So, Alice will think as if this is coming from Bob.

So, after receiving this, what Alice will do? Alice will decrypt this, the message which is coming from Bob, but it is actually coming from Oscar, but Alice does not know that it has changed by the third party. So, this is basically k. So, this is d of A. So, Alice is also getting the k. So, now, they all agreed with this k. So, now, Alice and Bob both agree with this message k, but they are not knowing that this also agreed by another. So, this k is now with Alice and this k is with Bob, but they are not knowing that this k is with the third party Oscar also, because Oscar did this Oscar participate this channel or I mean actively. So, Oscar changed this. So, this is the attack.

So, now, if Alice is using this k for their communication symmetric key encryption may be stream cipher or it could be AES if this is 128 bit then that message will be seen by the Oscar, because Oscar is also knowing this same value k - the key. So, key is revealed to the third party Oscar. So, this is the attack. So, to prevent this attack we do some more rounds on this key exchange protocol.

(Refer Slide Time: 25:57)



So, how to prevent this attack? So, this is supposed to be secured scheme anyway we have to check it secured scheme in the sense that it is secured under the active attack. So, let us just talked about this scheme, but this is not a one round, this is multiple round. So, if in the earlier scheme is also two round, it is sending then, but Diffie-Hellman is one round. So, in this scheme, so first step, so they both have a public key private key pair, so this is under PKI. So, they both generate the public key private key pair. Now, they want to use the public key cryptosystem to securely key exchange the symmetric key.

So, now, what Alice is doing? Alice is choosing a nonce, this is called nonce, nonce is something called nonce time stamp, it is a typically time for this time stamp for this particular communication. So, now, what Alice is doing? So, Alice is encrypting. So, this is the first communication number 1. So, Alice is encrypting these nonce along with Alice identity using the Bob’s public key e of B, let me write it very neatly. So, this is the first communication Alice is encrypting, this is number 1, Alice is encrypting the nonce and the ID of Alice using the Bob’s public key.

Now Bob is choosing another nonce N 2 and then Bob, this is the number 2. So, what Bob is doing Bob is encrypting this nonce N 1 and N 2 using Alice public key. So, after receiving this Bob can decrypt this N 1 and N 2, because Bob is having Bob secret key. So, Bob can decrypt this. So, Bob is choosing a N 2 sending to Alice. Now, Alice is having Alice’s secret key, so Alice will decrypt it and got this an Alice we will check whether this N 1 is same as this. So, Alice will convince that Alice is communicating with Bob.

Now Bob has to convince. So, for that, what Alice will do? So this is number 3. So, Alice is receiving N 2. So, Alice will encrypt this N 2 using Bob’s public key yes. And after receiving this Bob will decrypt it using Bob’s secret key and Bob will get N 2. So, Bob will check whether this N 2 this N 2 same or not, then Bob will convince that it is he is with Alice only. Now, Bob will choose a key - symmetric key, and then what Bob will do? Bob will just, this is the final communication, this is the confidentiality and the authentication, Bob will first sign on this. So, using Bob secret key sorry Bob will first encrypt this using Alice public key, so that it only can decrypt by Alice and then Bob will sign on this message. So, this is another encryption on this using Bob secret key and this Bob will send to Alice this is the final communication.

Now, upon receiving this, what Alice will do? Alice will first decrypt y using Bob’s public key. So, this was signed by Bob. So, then it should give us E of A and k. Now, again Alice will just decrypt this using Alice secret key, so this is D of A. So, Alice will get k, now this k is agreed between Alice and Bob. So, this is secured in the sense the Oscar will not get any advantage because we are doing so many time stamping, the confidentiality, authentication. So, this is a secured scheme for the symmetric key distribution over the public key setup.

Thank you.