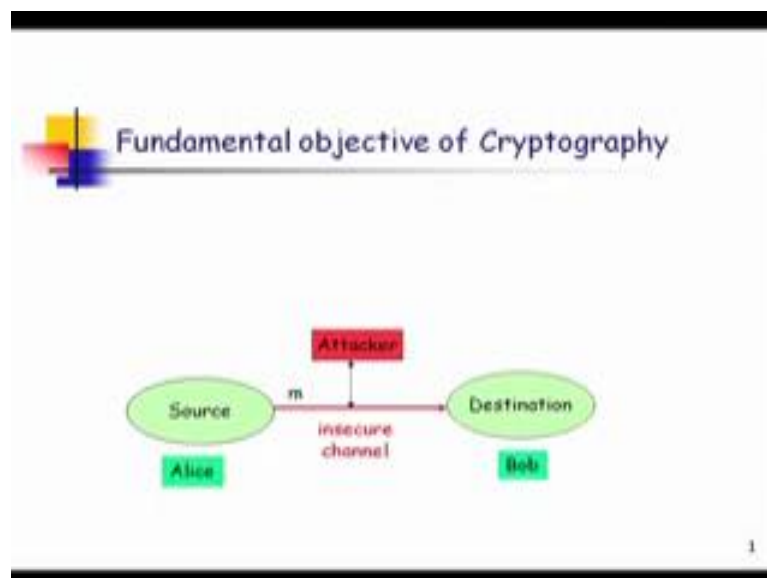


Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 23
Introduction to Public Key Cryptosystem,
Diffie-Hellman Key Exchange

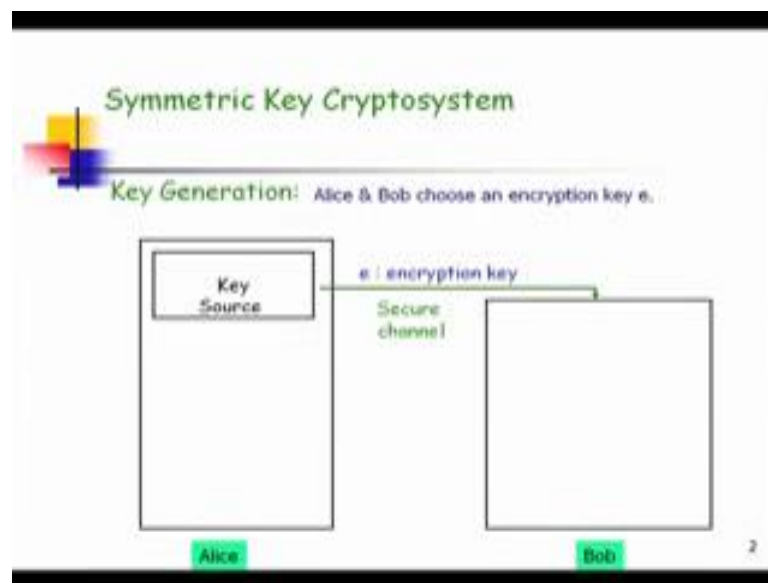
So, today we will introduce what we mean by public key cryptosystem. Before that let us just talk about what are the disadvantage of the system we have seen the symmetric key or the private key cryptosystem, then we will talk about why we need this public key cryptosystem in this stock will talk about the Diffie-Hellman key exchange protocol.

(Refer Slide Time: 00:50)



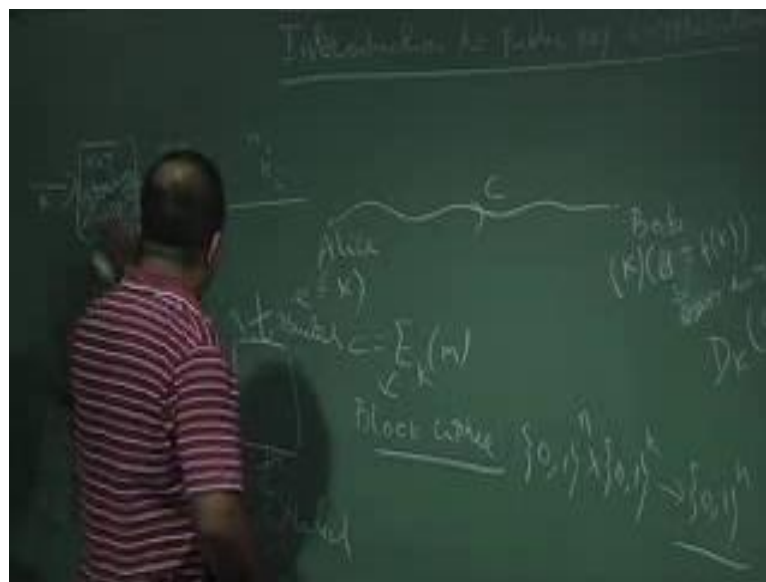
So, let us come back to the; so this is the fundamental objective of a cryptography there are two parties Alice and Bob. So, Alice is choosing a plaintext or the message from a source, this source is basically, source means the Alice which is the sender and Alice is choosing a plaintext and Alice is encrypting the plain, sending the plaintext. Alice wants to communicate to Bob over an insecure and this channel is captured by the protocol. So, how securely we can communicate over an insecure channel. So, that is the fundamental objective of a cryptosystem.

(Refer Slide Time: 01:31)



So, so far we have discussed what is the; what is called symmetric key or the private key cryptosystem. In the symmetric key basically Alice and Bob, they use a common key, this two party.

(Refer Slide Time: 01:45)



So, they use a common key which is basically called secret key between (Refer Time: 01:55) between Alice and Bob. So, this is this is also called encryption key and the decryption key is also either same or it can be generated from the encryption key very easily for the permutation cipher. We have seen the classical cryptography we have seen,

if K is a permutation then the decryption key is the inverse permutation, but if we know the permutation when we know the inverse permutation.

So, mostly there are these two keys as identical or one can be generated from others. So, they agreed to the common key K and then they are communicating using this common key k . So, what Alice is doing? Alice is encrypting this m using the key K this is we can say e and then this is the ciphertext Alice is generating c and Alice is sending to Bob over the public channel.

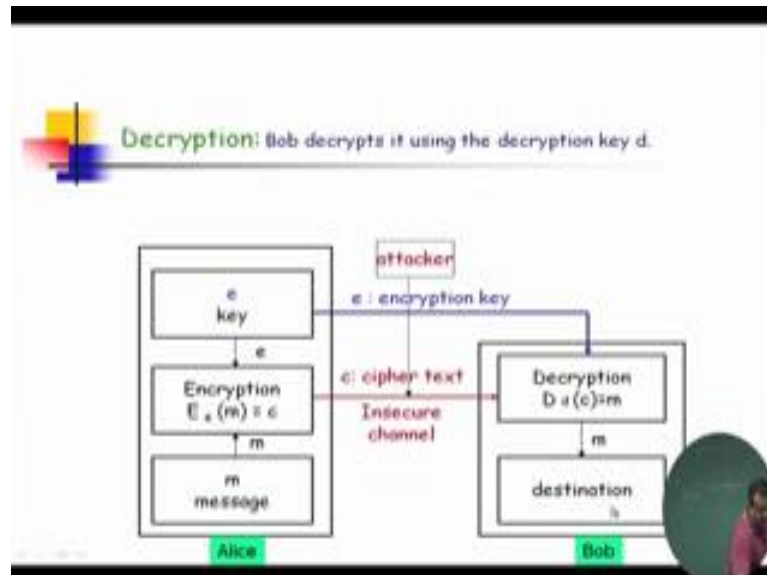
Now, Bob is having this K or the decryption key which is a function of K or which is basically same as K and it is easily, it is easy to get d from e either they are same if there same and both this having the common key K then Bob is doing the decryption algorithm using this decryption key or the K on this ciphertext this is (Refer Time: 03:40). So, this encryption we have seen so far is maybe it could be block cipher. So, block cipher means it could be AES, DES, SPA, an (Refer Time: 04:04) any block cipher we can use. So, it is basically a function which is taking a particular bit say n bit and key size is a k bit and it is given n bit ciphertext.

So, it is a basically a plaintext, a plaintext is n bit or plaintext of message and we have a key and we get the same n bit as a ciphertext this is block cipher encryption that decryption is the reverse way which Bob has to do Bob is give giving the input as ciphertext and the same key and we had get the plaintext or they can use with the any stream cipher. So, they can generate the key stream like you also suppose there is a key stream generator or pseudo random key stream generator or pseudo random bit generator, generator which is taking input as a key secret key and it is generating the key stream K_1, K_2, K_i and so on. So, this is the key stream generator and we choose the, so from this key stream generator we get the key stream and we have the message bit and we XOR with this, we get the ciphertext bit.

So this is the stream cipher, one can use this stream cipher only this can use same stream key generator has to be used by Bob in order to get back the message m . This is the symmetry key setup; in the symmetric key they are having a common key k . So, Alice is having say, so please go back to the slide. So, Alice and Bob they choose encryption key e which is basically K and then which is chosen from the key space and it is then it to share this key, so then it to send this key over a secure channel. So, that is also another

issue that is also another disadvantage of a symmetric key encryption, how they can shared this secret key.

(Refer Slide Time: 06:55)



So, then what Alice is doing? Alice is having this message m which is coming from the plaintext space and Alice is encrypting this and generating the ciphertext c and sending to Bob over the insecure channel which has controlled by the attacker.

Now, what Bob will do? Bob will get the decryption key which is most likely it is same as the encryption key the same key, otherwise it is easy to get the decryption key from the encryption key and Bob will apply the decryption algorithm it could be a block cipher or stream cipher decryption and get back the message.

(Refer Slide Time: 07:43)

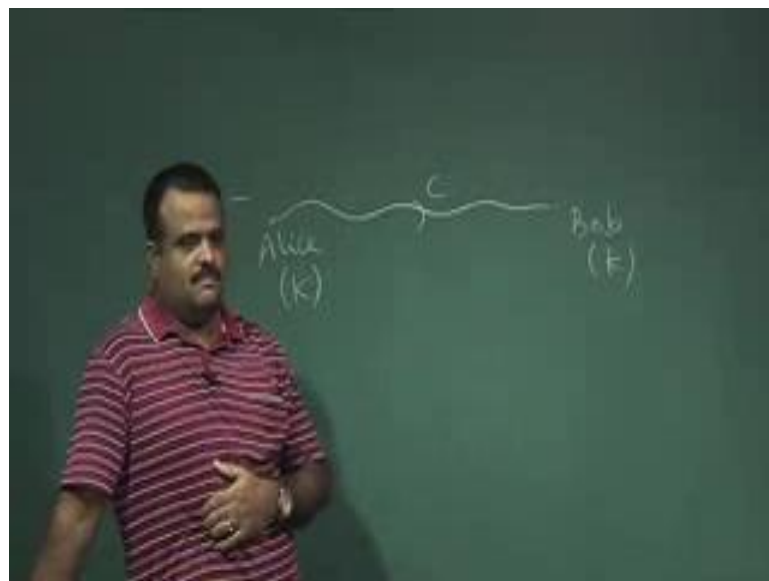
Disadvantages of symmetric or private key cryptosystem

1. Key exchange is a major problem. For key exchange, Alice & Bob need a secure channel
2. If a communication network has n users, then $n(n-1)/2$ secret key exchanges are necessary and these keys have to be stored securely.

The diagram shows four users: Alice, Thomas, Raj, and Bob, each in a green box. Every box is connected to every other box by a line, representing a fully connected network where every user must have a unique secret key for every other user.

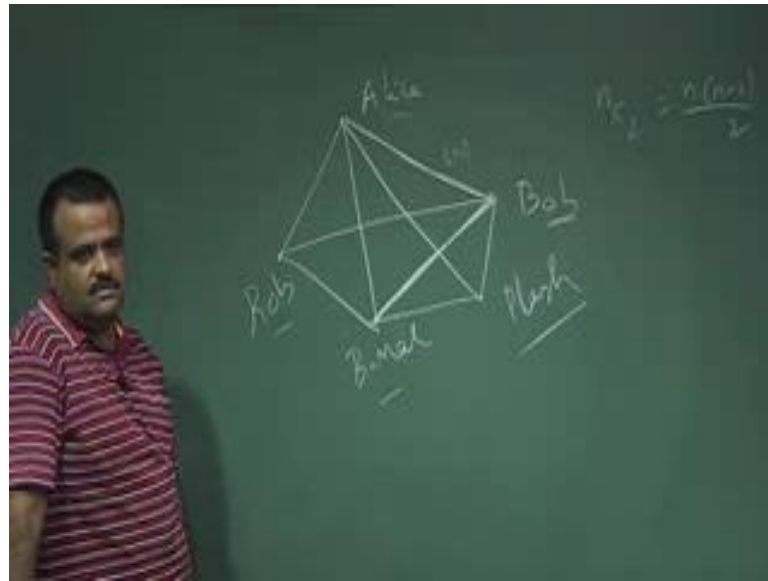
Now, let us talk about disadvantages of this public symmetric cryptosystem.

(Refer Slide Time: 07:54)



So, first disadvantage is how they agree with this common key k . So, either they have to use a secure channel which may not be always possible because you are assuming everything is public over telephone; they cannot say this is the key we are going to use. So, this is one difficulty how they can share this secret key. So, this can be solved by Diffie-Hellman key exchange protocol, we will come to know what is that in a minute. So, this is one disadvantage.

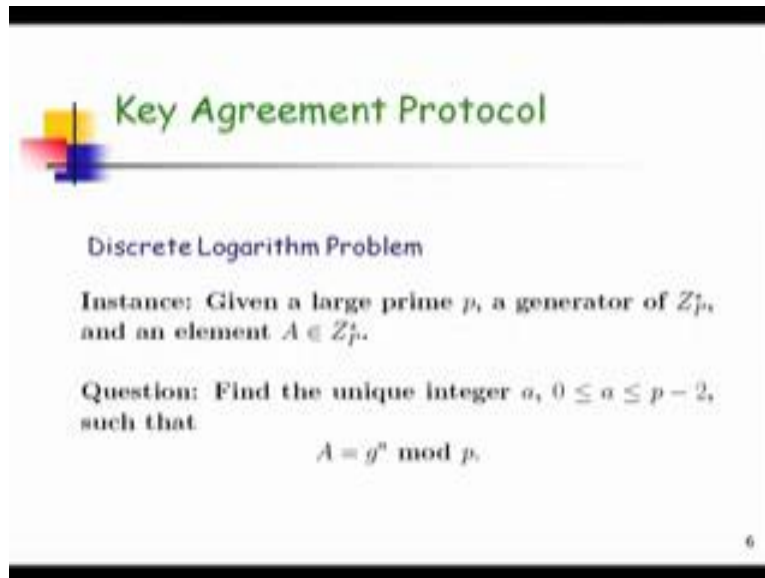
(Refer Slide Time: 08:37)



Another disadvantage is suppose there is a (Refer Time: 08:33) where n people are communicating. So, Alice, Bob, Rob, say Bimal, Plash, so there are many peoples, there are say n peoples there communicating with each other. So, suppose there are communicating with each other, so Alice is communicating with Bimal, Bimal is communicating with Plash, Bimal is communicating with Bob, Plash is communicating with Alice, Rob is communicating with Bob, like this. And suppose they are using a symmetric key setup they are using a symmetric key encryption.

Now, for that this is the complete graph. So, for that each of this connection we need a key we need a secret key and that secret key can used for other connection because then what about this communicating with Alice and Bob will be known to Bimal. So, which over is the key we are using here we cannot use a same key over this, for this for the communicating between Bob and Bimal. So, we have to use different set up, different keys for all this edges, so that means we need to have how many keys; so $n c 2$ keys. So, each edge we need a secret key. So, that is the drawback of this because, so then we have to maintain this many keys symmetric key. So, this is one of the drawbacks of this.

(Refer Slide Time: 10:38)



Key Agreement Protocol

Discrete Logarithm Problem

Instance: Given a large prime p , a generator of Z_p^* , and an element $A \in Z_p^*$.

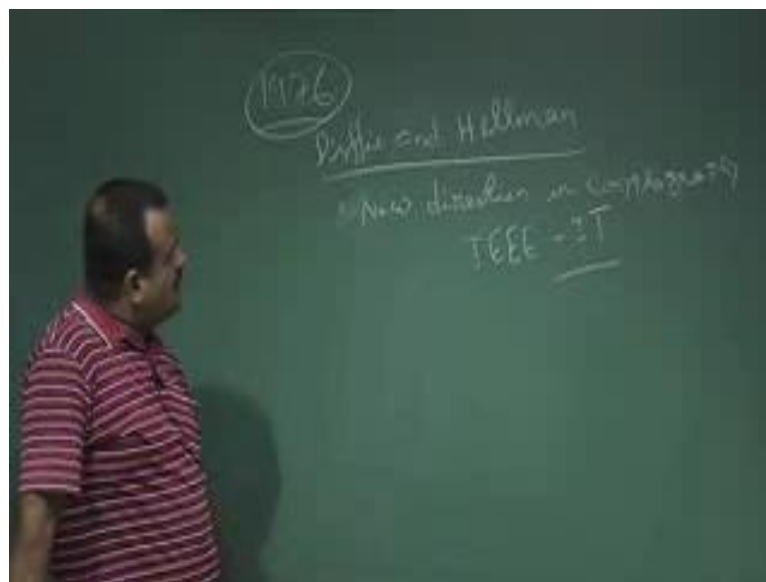
Question: Find the unique integer a , $0 \leq a \leq p-2$, such that

$$A = g^a \text{ mod } p.$$

6

So, now we will talk about the Diffie-Hellman key exchange protocol and this was the first work on which directs us to the public key cryptosystem, and this is the prepared by Diffie and Hellman in 1976.

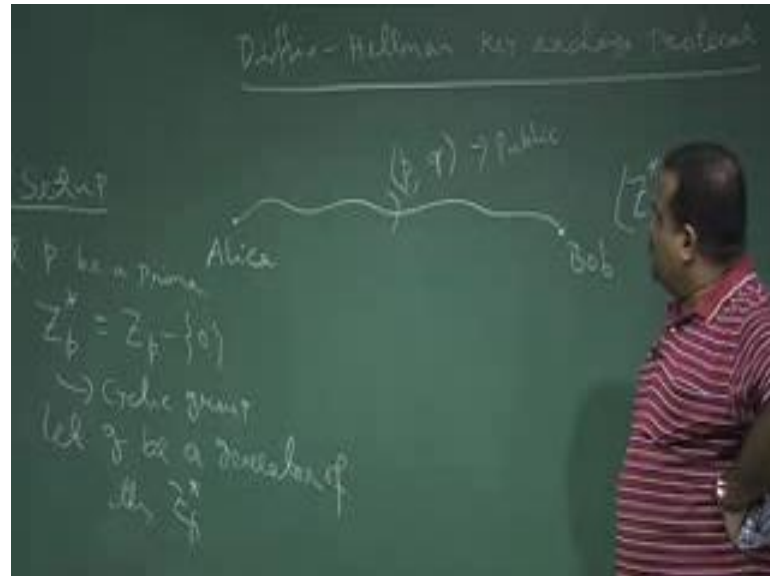
(Refer Slide Time: 10:59)



And this is the prepared by Diffie and Hellman and this paper name is new direction in cryptography; in cryptography and this paper was published in IEEE-IT transaction on information theory IEEE-IT in 1976 and this after this work. So, this is the starting point

of the public key cryptosystem and this work is for this key exchange protocol by Alice and Bob.

(Refer Slide Time: 12:13)



So, now we will discuss this Diffie-Hellman key exchange protocol, key exchange protocol. So, this is a way how this two party Alice and Bob they have staying in remote place I mean two different place how they can agree with the common key K which we can use for our symmetric key encryption. So, to solve this problem this Diffie-Hellman suggested this key exchange protocol. So, this will, how this two part is which are sitting into different place say Alice is sitting in America and Bob is sitting in New Delhi. So, how they can agree with a common key k ? So, what they do? So, this is the setup pairs. So, they first agree with the prime number let p be a large prime why large will come to know. So, for the time being just let p be a prime.

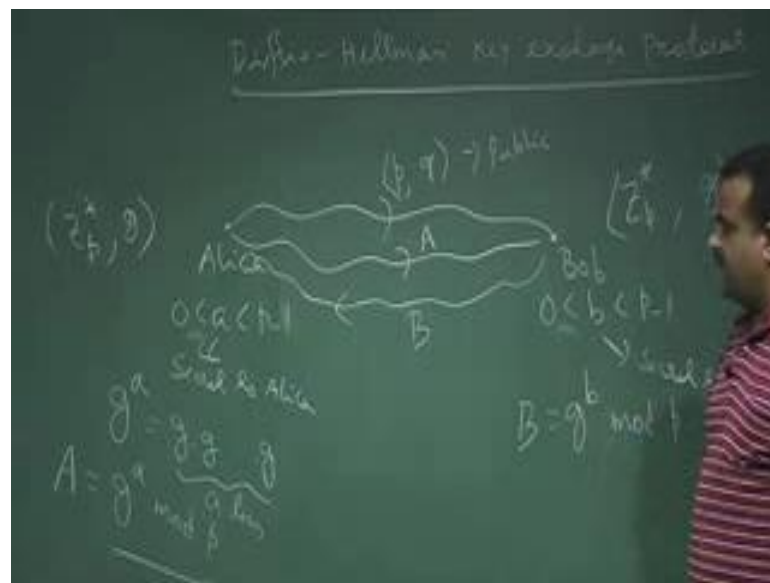
Now, you consider Z_p^* which is basically Z_p minus 0 and this is the cyclic group you know that this is cyclic group and this p we make public. So, Alice can communicate with Bob over the public channel; we choose this prime p .

So, now what Bob will do; what Alice will do now? So, Alice will communicate with Bob this p . So, this they choose p and then they also, so this is cyclic group, let g be a generator they choose a generator; let g be a generator of this group of this cyclic group Z_p^* . So, this g and p Alice make it public, this can be done by Bob also, but anyway this is a setup phase. So, this Alice make it public, this p and g this is public, public

means Alice will phone to Bob. So, this is our prime number and this is a generator we are going to use and this they can send over the public channel which is typically captured by the attacker.

So, now they agree to with this p , so \mathbb{Z}_p^* and the generator g , so both the parties are having. So, this setup can be done by Bob also then in that case Bob has to send this p and g to the Alice, but anyway this is the setup phase. So, they now, they both agree with this p and g .

(Refer Slide Time: 16:07)



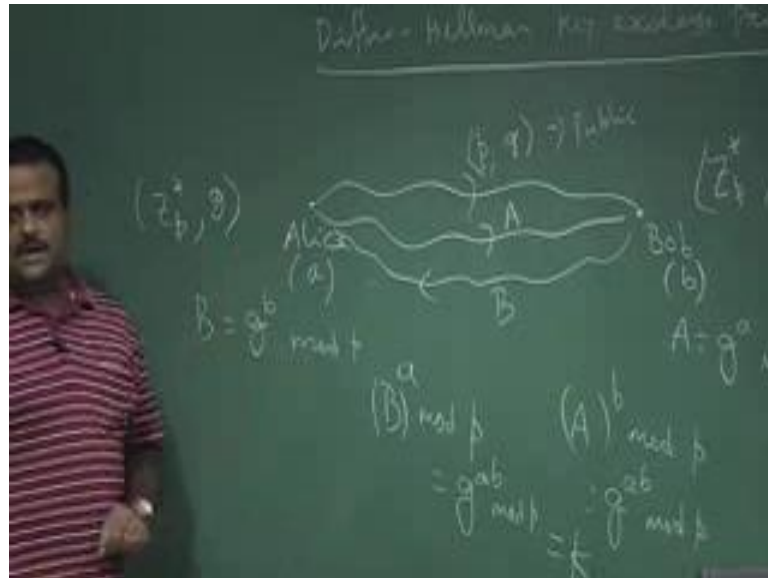
So, now what they do now? So, they both have \mathbb{Z}_p^* and the g generator. Now Alice chooses a , which is between p minus 2 I mean which is less than p minus 1. So, Alice chooses a this is a typical secret to the Alice and this Alice will keep this with herself and Bob chooses b . So, we will not take 0 Bob chooses b .

Now, so this is the secret values this is the; and this is secret to Bob. So, Bob is choosing this and Alice is choosing this and then what Alice is doing? Alice is computing g to the power a . So, this is the cyclic group. So, g to the power a means, this is just \mathbb{Z}_p^* . So, g times g times a , so a times g . So, Alice will compute g to the power $a \mod p$. So, this is what you can denote capital A g to the power $a \mod p$ and Alice will send this to Bob this A .

So, similarly Bob is having its secret b which is chosen by Bob and now Bob computes g to the power $b \mod p$ and Bob will send this to Alice B . So, Alice is computing g to the

power a, Bob is computing g to the power b. Now, Alice is receiving what? Alice is, Alice is having a and this Bob is having b.

(Refer Slide Time: 18:43)



And Alice is receiving B which is nothing but g to the power of b mod m mod p and Bob is receiving A which is nothing but g to the power a mod p. So, now, what Alice will do? Alice is having a, which is a typical secret to the Alice which Alice has chosen and Alice is receiving B. So, Alice will compute B to the power a mod p and Bob is getting A and Bob is having b as a secret, what Bob will compute? Bob will compute A to the power b mod p.

Now, this is nothing but g to the power A b mod p and this is also nothing but g to the power A b mod p. So, this is the common key k. So, now, they have a common key K which is shared between, which is now between Alice and Bob. So, this is the great idea how they can, how the two parties which are sitting in two different place how they can agree with a common key K so that they can use the symmetric key encryption for their further communication of the messages.

So, now, they agree with this K, the K is 64 bit, they can use Alice can use DES to encrypt and send it to Bob. So, Bob is having the same key 64 bit, Bob will decrypt that message and get the plaintext. So, this is the way. So, this idea is just the starting point of public key cryptosystem because here we are having some sort of secret key I mean some sort of this is we are making public and this is we are making secret. So, idea came

into the mind that time that; so what we can think we can use something public, something private and we can make a cryptosystem. So, that is the public key cryptosystem. So, that we will come back in a minute and this is the Diffie-Hellman key exchange protocol, and the secret is the - a or b.

(Refer Slide Time: 21:31)



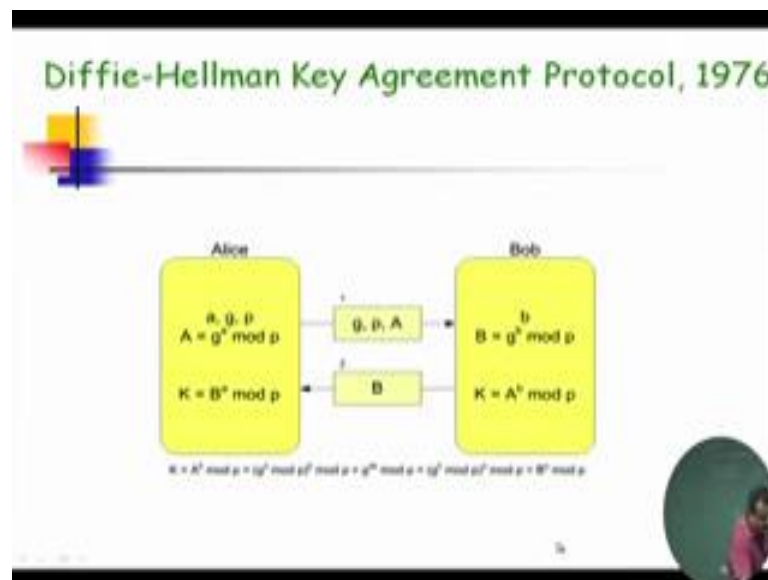
So, now, and these are the public A, capital A is public so, but capital A is g to the power a mod p. So, now, this is public parameter and capital B is also public. So, these are all whichever we are sending over the channel these are all public parameter. So, this is secret. Now to get, so if A is known g is known g is also public, to know the A that is called, that is called discrete log problem. So, this is called discrete log problem.

So, what is discrete log problem? So, discrete log problem means we have given. So, p is public. So, given \mathbb{Z}_p^* g is public generator is public and A is known which is basically g to the power a mod p given this we need to guess A, find A. So, this problem is called discrete log problem and this is usually hard if p is large. So, what we can do? So, a is we know, a is form. So, one way the boot force method we can try for all the possible less, so we know g. So, we can try for all possible ways from this set. So, we come a 1, we compute whether this is capital A or g to the power a 2 like this. So, like this is the boot force method, but the attack time will be the size of the message, size of the sorry size of the p the prime number.

So, that is the reason we have to choose p to be large prime, then it is discrete log problem is hard. So, we will talk about this in more details, so we will discuss the ElGamal cryptosystem which is also based on this hardness of the discrete log problem. So, this problem is usually hard for a large prime, discrete log problem.

So, now let us, so just go to the slide please. So, this is the discrete log problem instance is giving large prime p and a generator, so g ; so question is to find a .

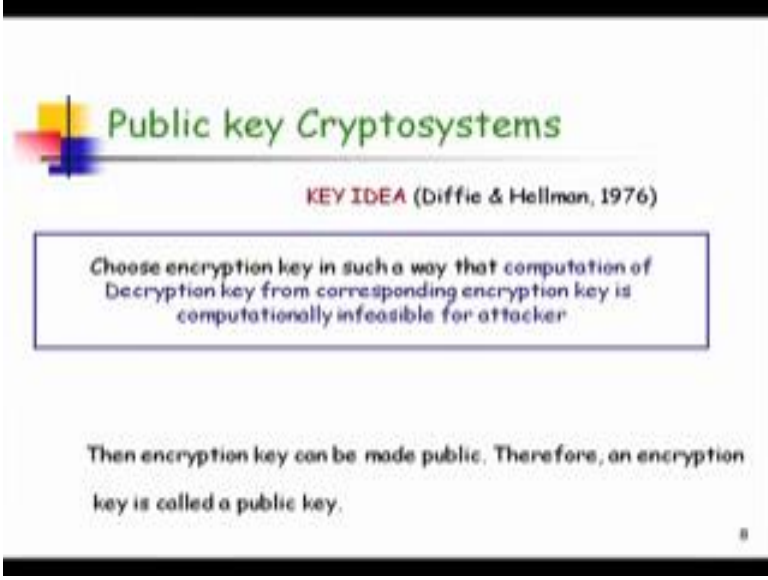
(Refer Slide Time: 24:19)



So, this is the discrete log problem and this is the key exchange protocol we have discussed. So, there are two parties Alice and Bob. So, Alice is choosing this a and Alice is computing g to the power a mod p and this is g^a mod p , these are all public parameter whichever is sending over the channel and then Bob is computing this, Bob is choosing secret b . So, these b is the typical secret with the Bob and a is the secret with the Alice.

So, they are computing g to the power a , g to the power b and then they are sending this and then after receiving this g to the power. So, it is computing A to the power b which is basically g to the power $A \cdot b$ and it is computing B to the power a which is basically g to the power $a \cdot b$. So, this is the common key they are sharing.

(Refer Slide Time: 25:26)



Public key Cryptosystems

KEY IDEA (Diffie & Hellman, 1976)

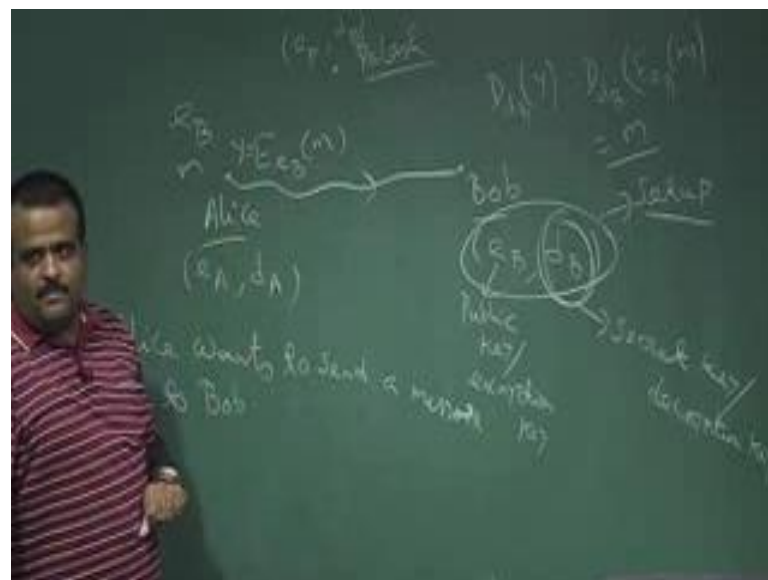
Choose encryption key in such a way that computation of
Decryption key from corresponding encryption key is
computationally infeasible for attacker

Then encryption key can be made public. Therefore, an encryption
key is called a public key.

8

So, this key idea for public key cryptosystem is coming from here. So, this is the starting point of the public key cryptosystem. So, in public key cryptosystem, we have two pair of keys.

(Refer Slide Time: 25:56)



So, there are two parties say or more than two parties Alice and Bob and say another party is Bimal or say Bimal or Plash. So, each of this party they are having a pair of keys. So, this is e_B, d_B ; e_A, d_A ; e_P, d_P and this is called a public key or it is also

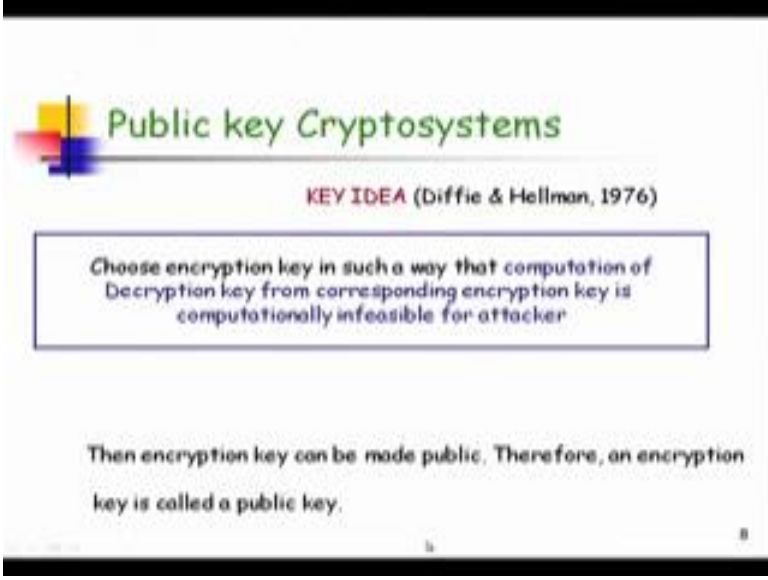
called encryption key and this is called secret key or private key and this is also called decryption key.

So similarly this is the encryption key for Bob, decryption key for Bob. So, now, suppose Alice wants to send a message to Bob, suppose Alice wants to send a message to Bob; that means, Bob has to generate this public key private key pair. So, this is the setup phase Bob has to run. So, this is coming from a particular setup phase and this has to run by Bob after running this. So, Bob got Bob public key private key and Bob makes this public key public. So, it can store into the public key directory or somewhere else or it can announce this is my public key.

So, now if Alice has to send a message to Bob, Alice has to get Bobs public key. So, Alice will encrypt this message using the public key encryption and this is the ciphertext Alice will send to Bob now after receiving this Bob is having Bob secret key. So, Bob has to decrypt decrypted using the public key decryption algorithm. So, using the secret key of Bob so this is basically D of d b and y is e of d of a . So, this should give us m . So, this is the public key setup. So, Alice encrypt the message using the Bob public key and generate the ciphertext send it to Bob and Bob is having his own secret key which is d b.

And apply that decryption algorithm public decryption algorithm and get back the message m . So, this should only done by Bob; so that means, from e B it should be computationally hard to get d B because e B is public, public key is public. So, it should be very difficult to get the public key, I get the secret key from the public key. So, that hard hardness should be there. So, can we please go to the slide?

(Refer Slide Time: 29:32)



Public key Cryptosystems

KEY IDEA (Diffie & Hellman, 1976)

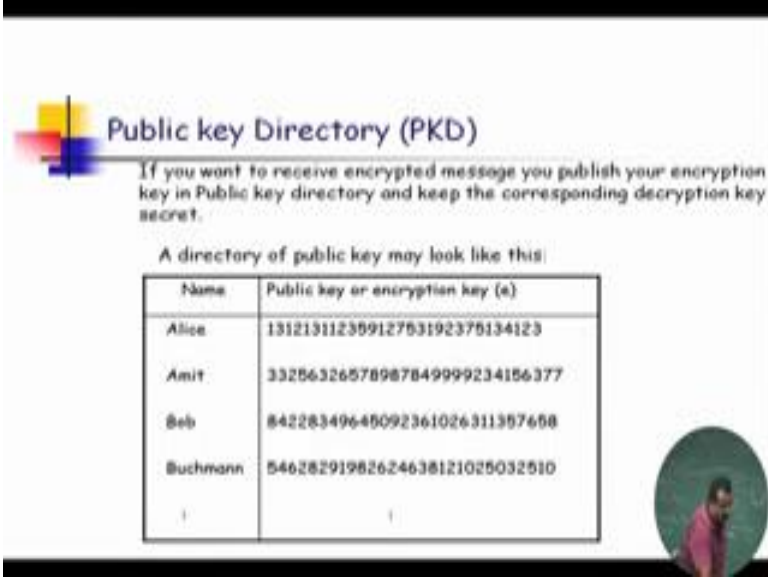
Choose encryption key in such a way that computation of
Decryption key from corresponding encryption key is
computationally infeasible for attacker

Then encryption key can be made public. Therefore, an encryption
key is called a public key.

8

So, choose the encryption key in such a way that computation of the decryption key from the corresponding encryption key is computationally infeasible for the attacker. So, that just now we have seen, then the encryption key can be made public therefore, an encryption key is called public key.

(Refer Slide Time: 29:51)




Public key Directory (PKD)

If you want to receive encrypted message you publish your encryption
key in Public key directory and keep the corresponding decryption key
secret.

A directory of public key may look like this:

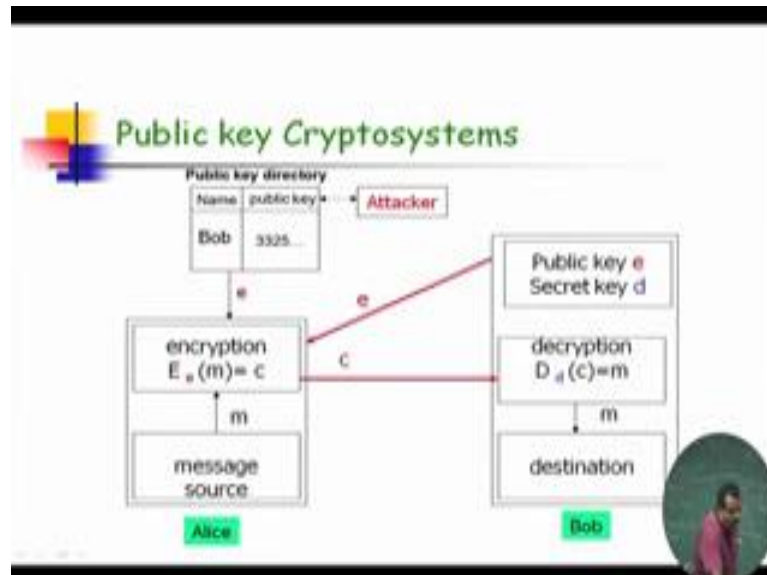
Name	Public key or encryption key (e)
Alice	13121311235912753192375134123
Amit	33256326578987849999234156377
Bob	84228349645092361026311357658
Buchmann	54628291982624638121025032510



So, this public key suppose everybody is generally having running their setup and they have their public key and they can post this public key into the public key directory or

we will discuss how they can manage the how we can manage the public key directory at the later stage. So, this is the public key directory.

(Refer Slide Time: 30:10)



Now, suppose this is the public key cryptosystem suppose Alice wants to send a message to Bob. So, what Alice will do? Alice has to get Bob public key either Alice can ask Bob to send his public key or Alice can get Bob public key from the public key directory which is again captured by the attacker, this channel is also captured by the attacker. So, Alice got Bob public key, now Alice encrypt this message – message is coming from the message space using the Bob public key and generate the ciphertext and send it to Bob.

So, Bob is having his corresponding secret key which is typically secret to the Bob which Bob only knows and which is not which is very difficult to generate from this public key. So, that is the main component of the public, so then using this secret key. So, Bob decrypt this message and get back the m.

So, this is the public key cryptosystem we will talk about some example next like Lapse cryptosystem, RSA cryptosystem, ElGamal cryptosystem.

Thank you.