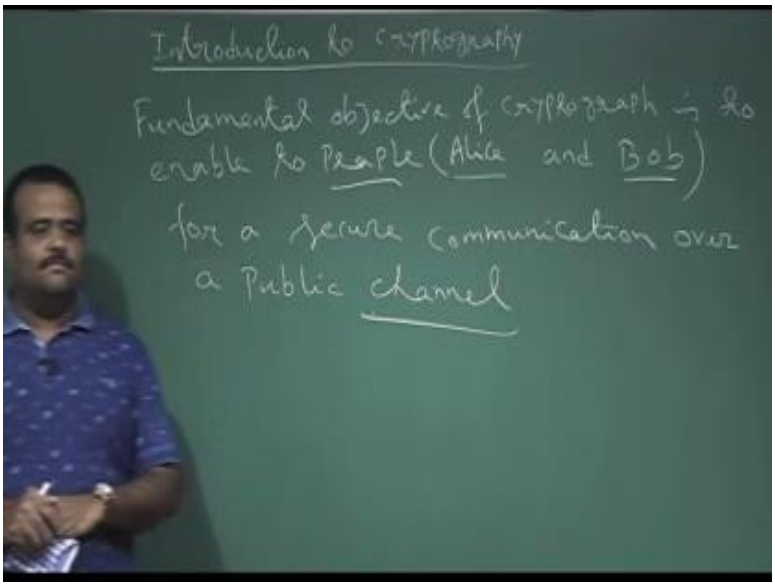
Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 01
Introduction to Cryptography

So we start with introduction to cryptography, what do you mean by cryptography or cryptology? So, the cryptography is the area in by which we can able to communicate two people which are remotely sitting in two different place and that communication should be in a secured way and they are communicating over a in secured channel.

(Refer Slide Time: 00:47)



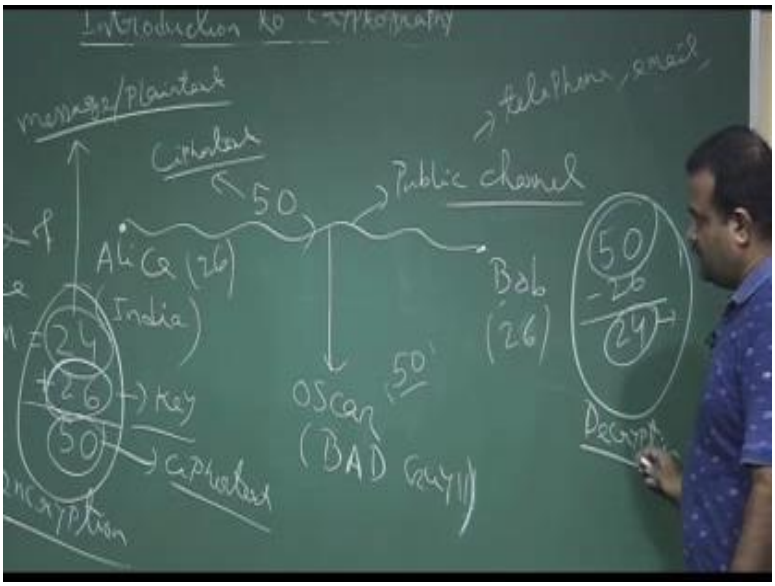
So, usually these two people; this is the fundamental objective of cryptography is to enable two people and these two people namely usually use in a crypto everywhere Alice and the second person is Bob. So, two people is usually referred as name as Alice and Bob, so the fundamental objective of cryptography is to enable two people to communicate over and in secure two people for a secure communication over a public channel.

So, this is the area where which guarantee us or which give us confident for the secured communication between two party Alice and Bob and they are communicating over public channels say Telephone, Internet, E-mail, Facebook, Whatsapp. So, this is objective of cryptography to; it says science of art of secret writing. So, we are

communicating over an in secured channel which is public and which can be captured by any party and, but the communication should be secure. So, whatever is sending by the Alice should not be revealed by anybody else other than Bob.

So, let us draw the picture suppose this Alice and Bob are sitting in two different place.

(Refer Slide Time: 03:02)



Say Alice is sitting in say Delhi or in some part of India and Bob is sitting say New York or USA. So, now they want to communicate, so Alice want to communicate to Bob, so Alice want to send a message to Bob. So, message could be anything like say Bob called Alice and Bob asked; Hey, what is your age? So, this is the say age of Alice; this could be a message Alice wants to send to Bob, so this you say 24; suppose Alice age is 24.

So Alice want to let Bob know that Alice age is 24, so Alice is communicating with Bob over a public channel, so this channel is public. So, public means it could be telephone or it could be e-mail, whatsapp, facebook anything I mean any internet option, so these are all public channels; so which is captured by a third party which is named as Oscar. So, Oscar has access to this channel, full access to this channel. Oscar can hear or Oscar can see whatever communication is going on over this public channel.

So, Oscar is typically referred as a bad guy; so Oscar is hearing everything. So, if just Alice saying that hey my age is 24, then if Alice pass 24 then Oscar will also come to know that 24 is Alice age. So, that way Alice they do not want to reveal their; I mean age

say, so this is the secret; this is the message Alice wants to send to Bob without revealing this information to the third party. So, what Alice can do or, so this is the whole area of cryptography; how we can a securely communicate over an in secured channel, this channel is in secured.

So, now what Alice can do; Alice can do something on the plain text, this is called plain text or message I will come to that. So, Alice can do something on the plain text, so Alice can reverse this; so Alice can. So, 24; 42 and then Alice can send this 42 to Bob, now upon receiving 42; Bob has to get back 22. So, what Bob will do; so Bob has to know was what Alice did. So, Bob has to again reverse this 42 to get back 24.

But if Oscar knows that they just reverse it, then Oscar will also be able to get the Alice original age which is 24. What else Alice can do; Alice can add something on this; say Alice can add 20 on this or Alice can multiply 10 on this, so 10. So, may be Alice can add something on this say Alice can add say 18 on this or 28 on this, say 26, so this would be a round figure. So, Alice is adding 26 on this, so then it is 50, so now, Alice send 50 over this public channel. So, also 50 is not Alice original age, so Alice original age is 24, but Alice did something Alice add 26 with it and got a number which is 50, Alice could multiply 3 that is also possible.

But this way Alice is hiding this message or this original information, so 50. Now 50 Bob is receiving 50, so after receiving 50 and Oscar is also receiving 50. So, Oscar will assume Alice age is 50, but Bob knows what Alice did something. So, Bob knows, Oscar may be also knowing; Alice added something, but how much Alice added that information Oscar will not be having.

So, that information this 26; this 26 is typically shared between Alice and Bob. So, this 26 is called key or the secret key which is shared between Alice and Bob sorry this is 26. So after receiving this 50, so what Bob will do; Bob will subtract this 50 minus this key and get back 24 which is the Alice original age. So, this process is called encryption process or this is called encryption, what Alice is doing this is called encryption and this thing what Bob is doing to get back the plaintext; this is called decryption and this 24 is called the message or the plaintext and this 26 which has been added with the plaintext to get this 50 is called key; secret key shared between Alice and Bob.

So, how they are sharing that is also another issue because they cannot just (Refer Time: 09:22) telephone and say we are going to use 26 as a key then that 26 will be revealed to the Oscar, so Oscar also will be getting the key. So that communication that how they will get this; how they will agree with this common key, so that is another issue. So, that that has to be done in a secured way; otherwise it will be revealed by the third party and after encryption, the output is called ciphertext.

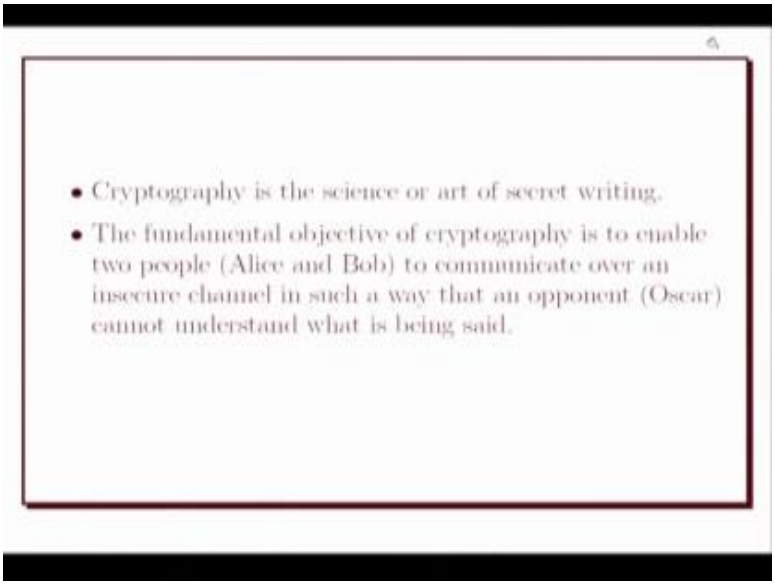
So, this 50 is the ciphertext, so this ciphertext is the output after the encryption algorithm. This encryption algorithm is very simple, we are adding; we are taking the plaintext, we have the secret key shared between Alice and Bob and we are adding this and we are getting the ciphertext and this ciphertext is being sent over the public channel and upon receiving this ciphertext; what Bob is doing to get back the plaintext, Bob is having the key Bob is applying the reverse process of that encryption that is called decryption process.

So, encryption was added, so decryption has to be subtraction. So, Bob is subtracting this 26 and get back the plaintext which is 24, so this process is called decryption process or the decryption algorithm; this algorithm and this is the key and Bob has to use the same key. Now what Oscar can do the third party? So Oscar is having full access to this public channel. So, Oscar is receiving this 50 which is the ciphertext, but Oscar is not having this key, so, this key which is here is 26 is typically with Alice and Bob. So, nobody else is having this key so; that means, Oscar is not knowing what is the key, but Oscar may be knowing that they have added something, so this encryption algorithm is public; we cannot say that we will not reveal we have whether we have added or we have multiplied or we have divided we have used the division for our encryption that encryption algorithm we will make it public.

This is public either we have added something so, but how much we have added that information is not public. So, that key is the secret key which is shared between Alice and Bob, so that is here is 26. So, what Oscar can do Oscar is getting only this ciphertext; Oscar is not having the key. So, Oscar goes up the Oscar is to gives what is the key and what is the plaintext, what is the Alice original age. So, this is the fundamental objective of cryptography, so this will be knowing this encryption algorithm, decryption algorithm the study of this is called cryptography and the who does this the people who are working on this is called the cryptographer.

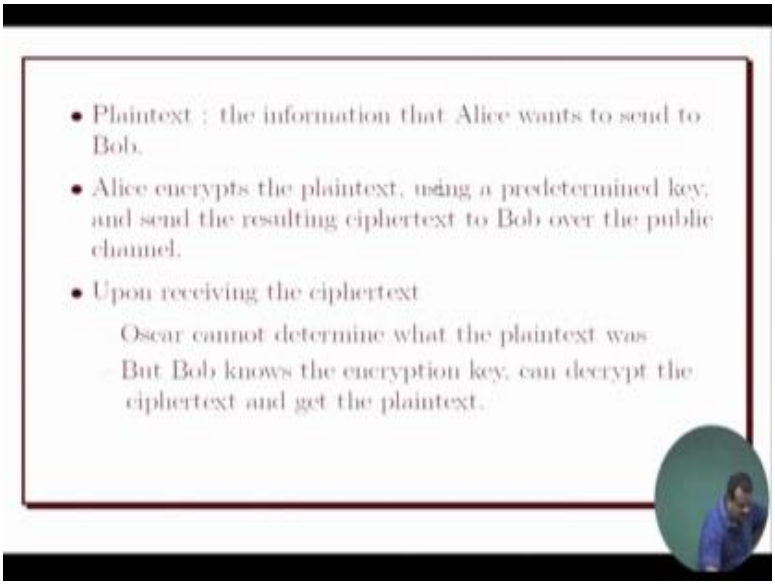
So, what Alice is doing this is the encryption and what Bob is doing that is the decryption algorithm, so can you go to the slide please?

(Refer Slide Time: 12:56)



So, here is the cryptography is the science or art of secret writing, so two party is only referred as a Alice and Bob. So, fundamental objective of cryptography is to enable two party to communicate over an in secured channel such a way that the third party Oscar cannot understand what is being said I mean, so this age should not be revealed by the third party, Oscar should not get what is the age of the Alice.

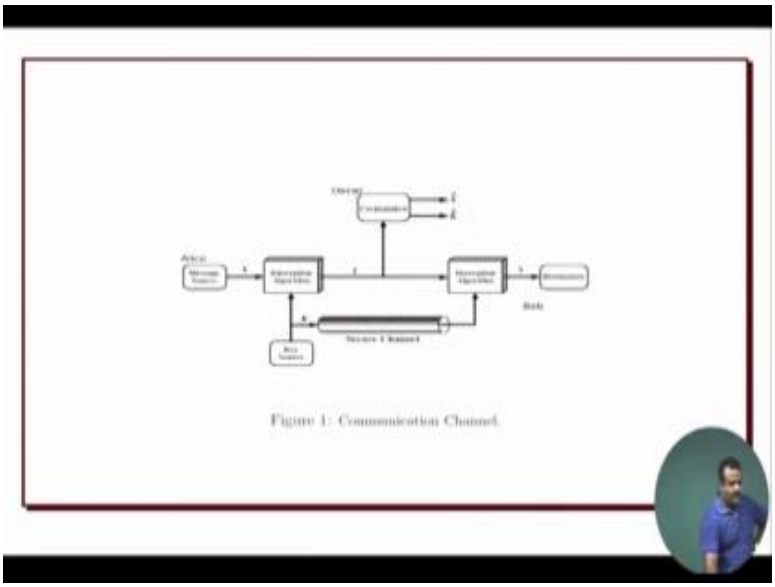
(Refer Slide Time: 13:28)



So, this is the some terminology plaintext which we have discussed, the information that Alice wants to send to Bob that age here in this example, Alice want to send the age to let Bob knows Alice age, so the age here is the plaintext.

So, the information that Alice wants to share with Bob is called plaintext. So, Alice encrypt the plaintext using the predetermined key, so the this key is shared between Alice and Bob and this is the encryption process, now after receiving the ciphertext; Oscar cannot determine what is the plaintext or what is the key, but Bob is having the encryption key, so Bob should able to decrypt it, to get back the plaintext.

(Refer Slide Time: 14:20)



So, this is the typical communication channel, so we have two party Alice and Bob. So, there is a plaintext source of plaintext space and so there is encryption algorithm. So, in this case or encryption algorithm is very simple one, it is a addition, so this is typically called shift cipher.

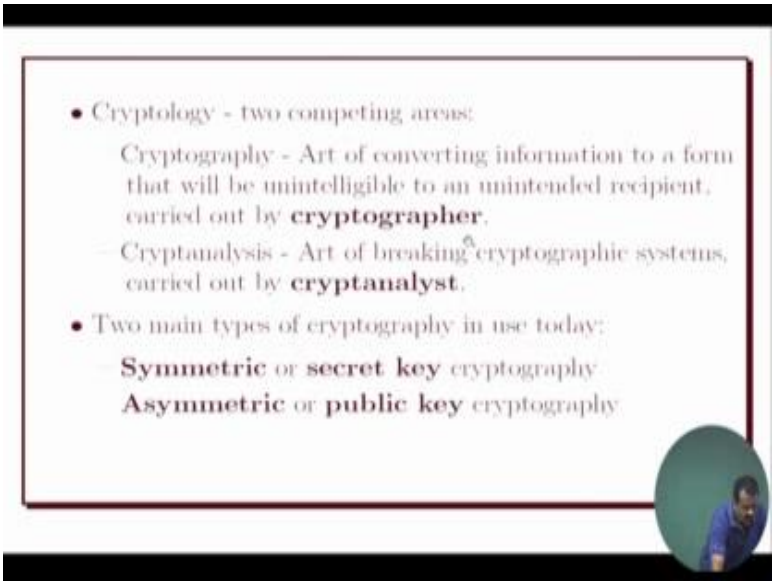
We will formally define what is this shift cipher, so Alice is choosing a plaintext and Alice is choosing a encryption algorithm and they shared with a common key. So, the secret key k; this is shared between Alice and Bob and this is done in a secured way so that I mean either they can meet with each other at some point of time and they can decide, this 26 we are going to use for as our key for next 1 year. So that is one option, they made some December time they made and they decided we are going to use this is our key for our next 1 year communication.

But that is also danger because key may be revealed, so there is a risk of using the same key for long time. So, we need to change the keys depending on the application in our mobile; how much security either we should keep the key for 1 day, 1 week or 1 hour, 1 minute. So, may be our prime minister mobile they change the key in a second, so every second keys are changing; so these are called session key. So, it is not a good idea to decide the key and use for it for long time because it could be revealed. So this is one problem to share the key, anyway somehow they have to agree with this key.

So, these key are coming from the key source and these key they have shared over the secured channel either they meet with each other or they trust on somebody to send the key something like that and this Oscar is the bad guy third party who is the called crypt cryptanalyst who is I mean ready to break the code or the hacker.

So, is to guess what is the key; this is the key hack; I mean the guessing of the key or what is the plaintext the message Alice sent to Bob. So, this is a typical communication channel in cryptography.

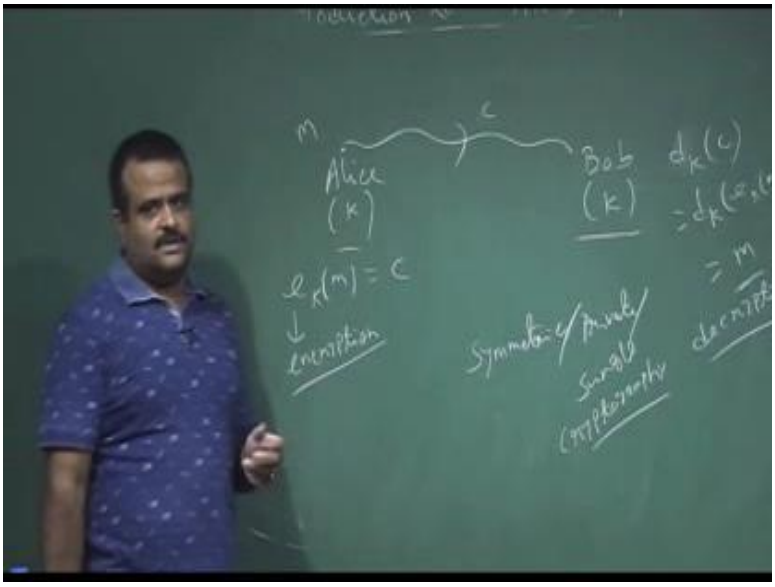
(Refer Slide Time: 16:49)



So cryptography has two components; one is the cryptography which is the area where we know the algorithm like encryption algorithm, decryption algorithm and how we shared the key all these issues come under this cryptography and the other side of the coin is the breaking the code like hacker; the cryptanalyst, so this is called cryptanalyst; the other side of the coin.

So, cryptographer they design the code and crypt analyst; they break the code. So, their job is to breaking the job, so this is called crypt analyst or the people who are breaking the code are called cryptanalyst and this area is called cryptanalysis and the cryptography is to design designer; who design this algorithms and combining two area is called cryptology, this basically the whole area of I mean this cryptography and cryptanalyst. The main two area of cryptography is symmetric key cryptography and public key cryptography.

(Refer Slide Time: 18:06)

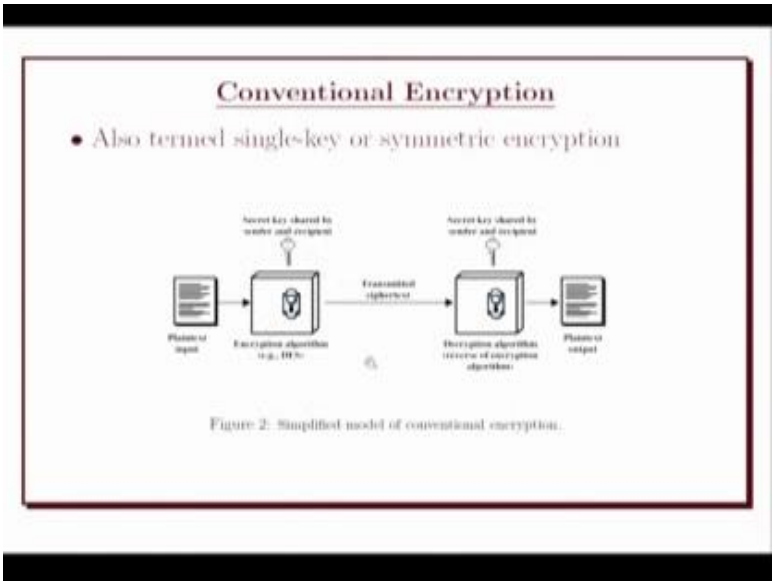


In symmetric key cryptography Alice and Bob, they shared with a secret key k. So, this is single key or symmetric key and they if Alice wants to send a message to Bob, then Alice will apply encryption algorithm which is basically e k of m and get a ciphertext and this ciphertext Alice is, so this is the encryption algorithm encryption function or encryption algorithm and this ciphertext is sending to Bob and this after receiving the c, so Bob will apply another algorithm which is called decryption algorithm; which is used in the same key on c, this is basically d k of c is basically e k of m, so it should give us m; so this is called decryption. So, this is called typically a symmetric key because we have used the same key or the symmetric key or private key or the single key cryptosystem cryptography.

And there are other area which is called public key, so there everybody is having two pair of keys because in this case, but there many issues like how they share with this key

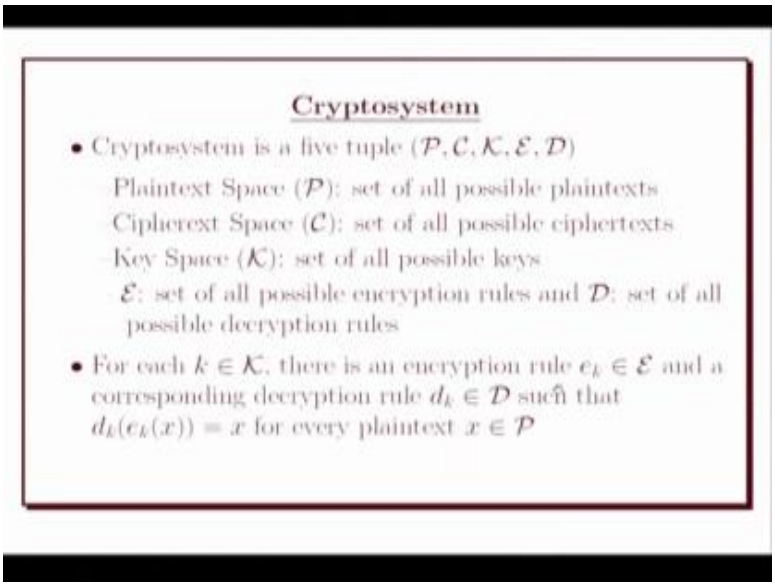
common key. So, to avoid that public key was invented after the work of Diffie-Hellman, he extends protocol; they gave a algorithm where Alice and Bob sitting two different place can agree with a common key. So, after that work this public key was invented, but all the conventional cryptography like shift cipher, Caesar cipher, substitution cipher all are comes under symmetric key crypto system.

(Refer Slide Time: 20:16)



So, this is the conventional crypto encryption algorithm; this is basically symmetric key, so we have a encryption algorithm. So, this algorithm use a key which is a secret key shared between Alice and Bob and this is the plaintext which is the input and another input is the key and it is generate basically the ciphertext; this is Alice is doing, sender and this part is doing which is referred as Bob and this is basically we have this is; Bob is receiving the ciphertext and Bob is having a common key K and that using that key Bob is decrypting that ciphertext to get the plaintext.

(Refer Slide Time: 21:12)



So, come back to the formal definition of a crypto system. So, what do you mean by a crypto system, so typically a crypto system is a five tupel.

(Refer Slide Time: 21:39)

Crypto system is basically a five tuple P set of plaintext, C set of ciphertext, K set of key space, E set of encryption algorithm, D set of decryption algorithm. So, this is called set of all possible plaintexts or this is referred as plaintext space and this is set of all possible ciphertext, this is called ciphertext space and this is the key space; that means, set of all possible keys; and this is the set of all possible encryption algorithm; possible encryption

function or algorithm, so basically this is a function. So, encryption function is basically if you denote this by e of k, it is basically a plaintext space, key space to the ciphertext space.

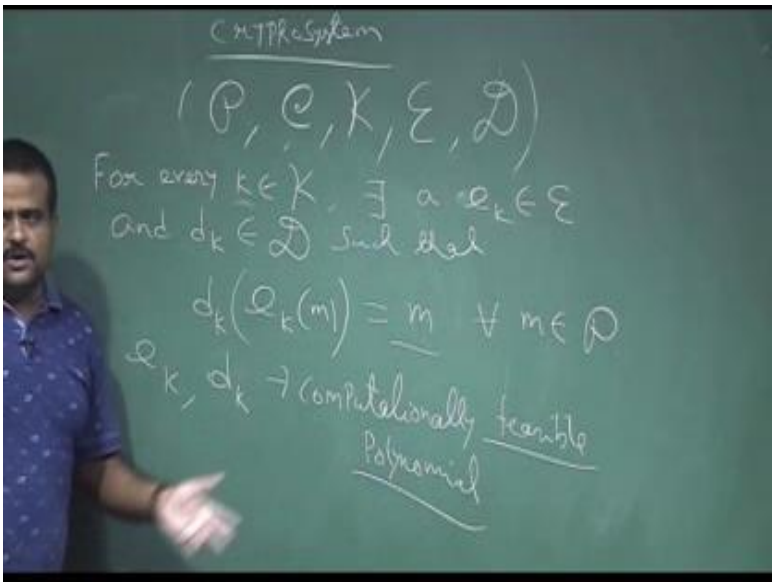
This is function form, so this is taking a key and then a plaintext and giving us the ciphertext. So, basically your e of k of m is basically c, so this is a plaintext, this is the key and this is the ciphertext. So, we choose a key; once I choose a key then our encryption algorithm is fixed and then we use take a plaintext and we encrypt it and we get the ciphertext and this is called set of all possible decryption algorithm.

So that means, this is basically a decryption function set of all possible decryption algorithm or decryption function. So, a decryption function is typically what are the input, so input is a ciphertext and the corresponding key and it will give us the plaintext. So, d of k; c is basically m if and all if e; k of a m is c. So, if this plaintext; if this ciphertext was derived from the encryption algorithm of, after encrypting this plaintext using the key K and then it should give us the it should give us the ciphertext. So, this is the reverse process actually encryption is the decryption is the reverse process of the encryption, so this is five tuple is called the crypto system.

So, but it must have some condition like for a given key; we should there must exist a encryption algorithm such that and there must exist a decryption algorithm such that we should after encrypting the message, we get the ciphertext then their ciphertext if we apply the decryption algorithm, we should able to get back the message.

So this is the condition; this crypto system should have should have, so let us write the condition.

(Refer Slide Time: 26:11)



For every key, so this is the formal way to define a crypto system; for every key even a key from the key space; what we can do? So, there must exist, so this is the symbol we use for their exist; there exist a encryption algorithm e, k from this encryption space and the decryption algorithm from this d; k which is basically reverse of this encryption process. So, decryption is basically the reverse of the encryption process, in our example Alice age was 24; we are adding something on 24, that adding something means that key; key is 26.

So, the key was 26 and the encryption is just the addition, so we are adding 24 plus 26 and we are getting the ciphertext so, but decryption is the reverse. So and there exist a decryption algorithm such that if we encrypt a message, we get the c; now on that c if we apply this decryption algorithm, we should able to get back m and this must be true for all m from the plaintext so; that means, for a given k for a given k; we choose a k, k is typically chosen by the this is the Alice and Bob; this is a two, this is a symmetric crypto system. So, Alice and Bob typically choose a key k and they decide, this is the k key we are going to use for our communication.

So, after selecting the k; they should able to have a encryption algorithm, Alice should able to choose a encryption algorithm from this set of all possible encryption algorithm space encryption function and the corresponding there should exist a corresponding decryption function such that this encrypting a message will give us the ciphertext; this is

c and if we decrypt the c, it should give us the plaintext and this e c; e k; c k this function all should be computationally feasible function, I mean it should not be very hard to compute; it should be computationally I mean feasible; that means, it should be polynomial function, it should not be a hard function like n p hard, n p complete. So, it should be; I mean we should able to encrypt a message that is the idea and you should able to decrypt the corresponding ciphertext to get back the message.

So, this encryption algorithm, decryption algorithm they should be; I mean communication, they should be computationally feasible; it should not be typically hard problem or something, so this is the crypto system. In the next class, we will talk about some conventional crypto system which are called classical cryptosystem like shift cipher, Caesar cipher, substitution cipher.

Thank you.