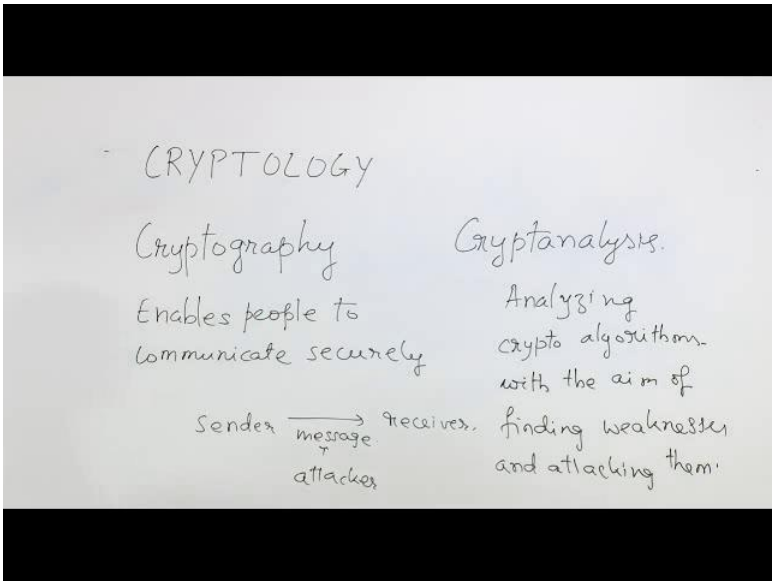
Introduction to Cryptology
Dr. Sugata Gangopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology, Roorkee

Lecture – 01
Introduction, Caesar cipher

Our course is on Cryptology.

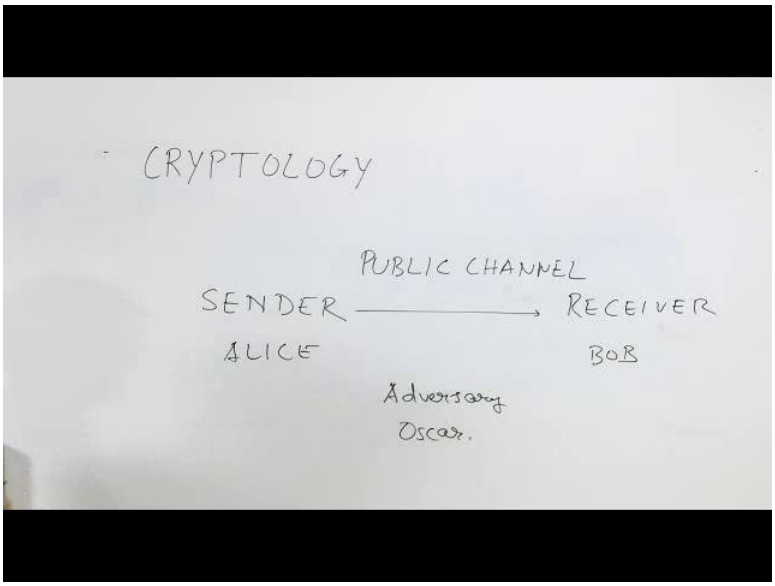
(Refer Slide Time: 00:28)



Cryptology has 2 parts; one part is called Cryptography, and the other part is Cryptanalysis. Cryptography enables two people to communicate securely. So, it enables people to communicate securely that is to say, when a sender sends a message to the receiver if he uses a cryptographic technique then this meaning of this message should not be accessible to an attacker, and that is the goal of cryptography. On the other hand, cryptanalysis is concerned with a analyzing cryptographic algorithms and protocols; analyzing crypto algorithms with the aim of finding weaknesses and attacking them.

So, these two efforts must go side by side. In fact, if somebody has to develop good cryptographic algorithms then he has to know cryptanalysis very well because he has to know what kind of attacks are possible, what are the weaknesses and so on. Now, we come to a model of cryptography where we have a sender and the receiver.

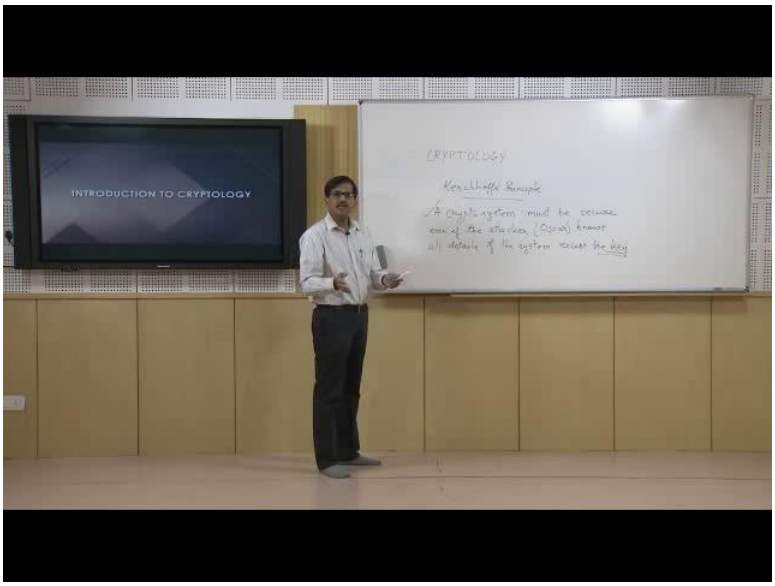
(Refer Slide Time: 03:26)



We have a sender traditionally the sender is named Alice, and the receiver is named Bob. Alice and Bob are connected through a channel which is accessible in principle to everybody, so it is called a Public Channel. Now this channel may be telephone network, it may be wireless network, it may be internet, it may be anything and in fact, it need not be something to do with electronics and computer science, it may be just a courier. It may very well happen that Alice is sending a letter to Bob and she is using a courier or a post and that letter can be accessed by somebody else, someone can open the letter and read what Alice has written.

So, in order to have some kind of privacy Alice would like to hide the meaning of the message from anybody other than Bob. Now here we have the adversary Oscar who is listening to the channel and who would like to know the meaning of the message that Alice is sending to Bob, so this is our basic model of cryptography.

(Refer Slide Time: 05:20)

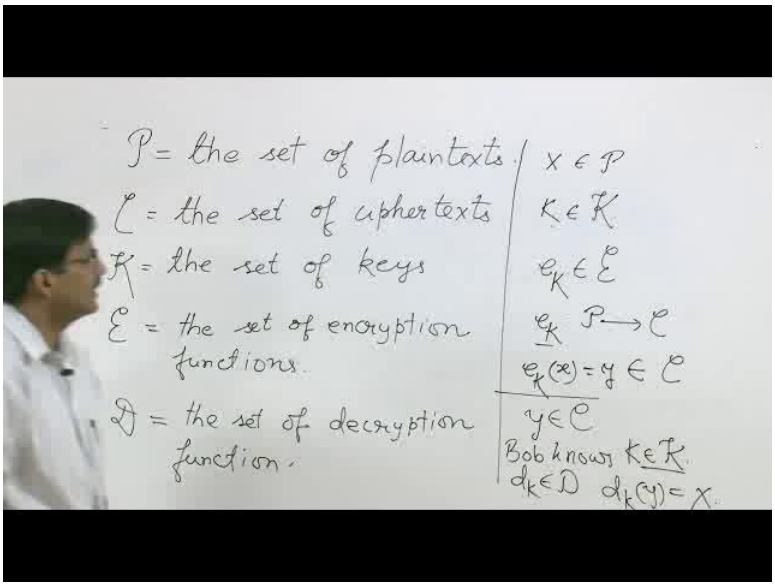


Now there is another assumption which is a very important assumption which is called Kerchhoffs' Principle. Now, Kerchhoffs Principle says that a cryptosystem must be secure even if the attacker, in our case Oscar knows all details of the system except the key. Now this is a big assumption; it says that the attacker knows everything, the attacker knows the algorithm, attacker knows the protocol, attacker knows the language, alphabet which Alice is using to write the message, attacker also knows the device that is used to cipher, and attacker knows everything. Only thing the attacker does not know the particular key that is being used to cipher, but he knows all the set of all possible keys.

So, this is the assumption on which we are working. So we cannot say that we are hiding the method by which Alice is enciphering. The method is known only there is something which is called the key which is not known and the security of the cipher which Alice is used, or the security of the cryptosystem that Alice is using should depend only on the security of the key.

Now, we will slowly talk about the message, key and ciphering and all that in a more formal way. Now we are in a position to use some formalism we take some sets.

(Refer Slide Time: 08:12)



So, the first set we consider is called the set of plain texts, the second text is the set of cipher texts, the third set is a set of keys, and now the fourth set is a set of encryption functions, and the fifth set is the set of decryption functions. Now we will slowly discuss the meanings of these sets and these words. Now the set of plain texts is a set of symbols that Alice is using to a build the message. Set of cipher texts is a set of symbols to which Alice is transferring or transforming the message. K is a set of keys we will come to keys. For each key there is an encryption function that is the transformation which takes plain text to cipher texts.

Therefore, we have a situation like this, that suppose Alice wants to send the message x. X is an element of plain text p. Alice picks up a key from the key space k and corresponding to that key there is a function in e, that function is e sub k this is an element of crypt e, essentially this is a function from p to c. Therefore, Alice can apply this function e k on x and get an element, let us call it y in c. And this is the ciphering that Alice is doing. Please note that we are not talking about particular methods of ciphers we are just talking about a kind of formalism we are saying what is happening in general without going into the details. We will soon be going into the details of ciphers, but that is a little later.

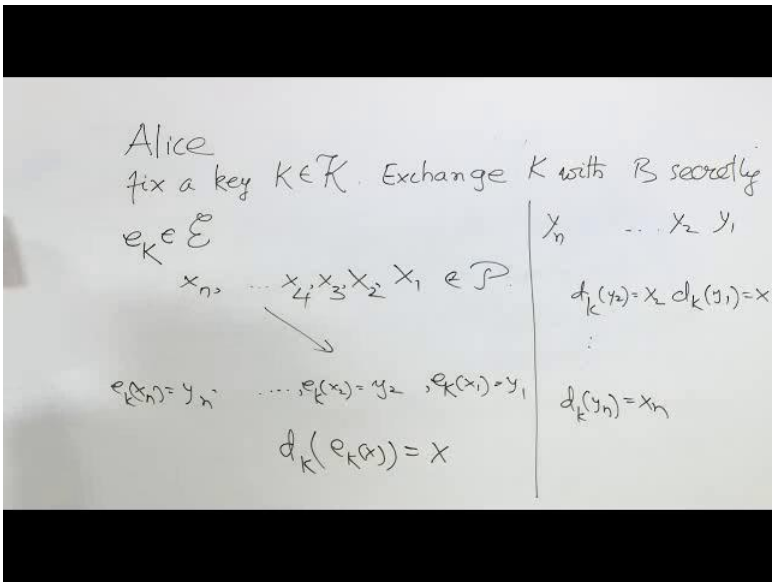
So, now we have a scenario like this is that ok Alice is able to transfer the symbol x which is an element of the plain text p to an element of the cipher text by using a

function e k which is an element of e, and it is also dependent on capital k which in turn is an element of k. So, I change the symbol a little bit instead of small k, I write capital K. So, to me capital K is a key and crypt k is a set of all possible keys. So that is happening here. This is Alice's side of doing a ciphering.

Now let us see what happens to the Bob side. What Bob does is that Bob receives a symbol in the set c that is a cipher that is what Bob is receiving. Now here we assume that somehow Bob also knows the key capital K. So, we have to write somewhere Bob knows belonging to k. Now the question is how does Bob know this key? In our model somehow Alice has to send this capital k to Bob. It might be that they were together sometime in the past where they exchange the key and then Bob has moved far apart and now Alice is sending messages to Bob through a public channel using a encryption function which is dependent on the key capital K. This k has not been transferred to a public channel therefore k is secret.

Now, if Bob knows this then we assume that Bob will be able to compute d k that is the decryption function that is an element in crypt d. And if Bob applies d k over y then he should get x, and that is how the decryption takes place. Let us look at this again.

(Refer Slide Time: 14:35).



So, Alice fix a key capital K inside the key space, exchange k with Bob secretly somehow and then pickup e k belonging to this. And now suppose Alice wants to send a series of messages or series of elements in the set p of plain text like this some x n. So,

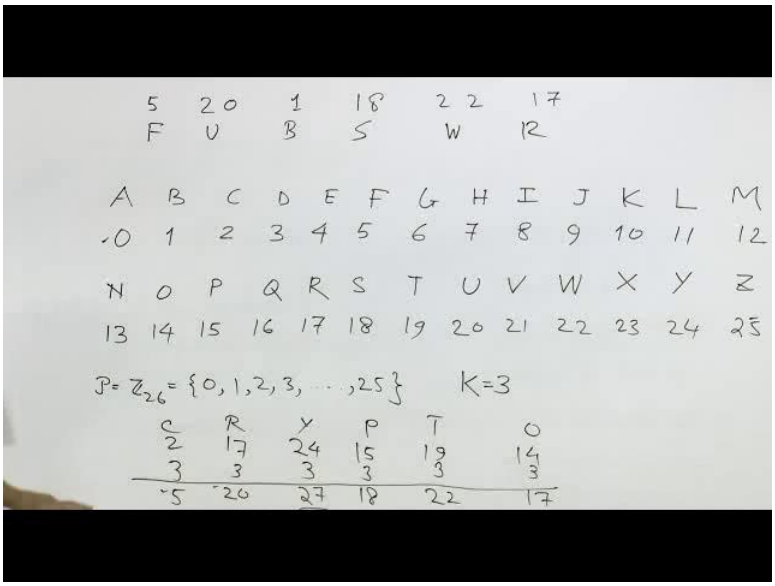
suppose these are the plain text bits, sorry plain text elements that Alice wants to send. She does the encryption with the key which has been shared by Bob. In this way she applies e k to x 1 she gets y 1, then she applies e k to x 2 she gets y 2 and so on, at the end she applies e k to x n she gets y n. So, this is what Alice will be doing.

On the side of Bob, here Bob receives a sequence y 1, y 2 and so on up to y n, he knows the key therefore he knows d k, therefore he applies d k to y 1 to obtain x 1, d k to y 2 to obtain x 2 and so on. Eventually, she applies d k to y n to get x n. Therefore we see that there is something that is essential for the encryption functions and decryption functions that is, if you apply an encryption function e k over x and over that with the same key if you apply d k then you must get back x otherwise decryption will be impossible.

There is another very important property of the encryption function and decryption function that is they have to be one to one functions. That is if you take two different plain text it must not map to a single cipher text, a same cipher text because then the receiver will be unable to decrypt it, because it has come from two different plain text symbols are getting mapped to a single cipher text. So that is also something that we have to keep in mind.

Now, after this we will look at a particular cipher which is a very, very old cipher, and which is of course not secure but still it is worth having a look at it because it explains all the basic properties of a cryptosystem. So, now we have to specify the plain text space, cipher text space, keys, encryption function and decryption function. We move as follows.

(Refer Slide Time: 18:48)



Suppose, using English language to write the messages. So, she is using the English alphabet, so her alphabet is A, B, C and so on up to X, Y and Z. Now what she does is that she changes the letters to numbers so that he can do mechanically few things, Let us see what happens if we change English letters to numbers. We will number A has 0 and move on up to Z equal to 25. So, here we have got 0 1 2 3 4 5 6 7 8 9 10 11 12, these are the first 13 letters. Then we have M N O P Q R T U V W X Y and Z. So we have 12 13 14 15 16 17 18 19 20 21 22 23 24 and 25.

The set of plain texts will be which we will consider is numbers from 0 to 25 and there is a benefit of considering the numbers instead of the letters in the alphabet that we will see very shortly. So we will fix the plain text set to p equal to z by 26, we will also in later lectures discuss what is the meaning of z by 26, but now it is enough if we know that these are numbers from 0 to 25.

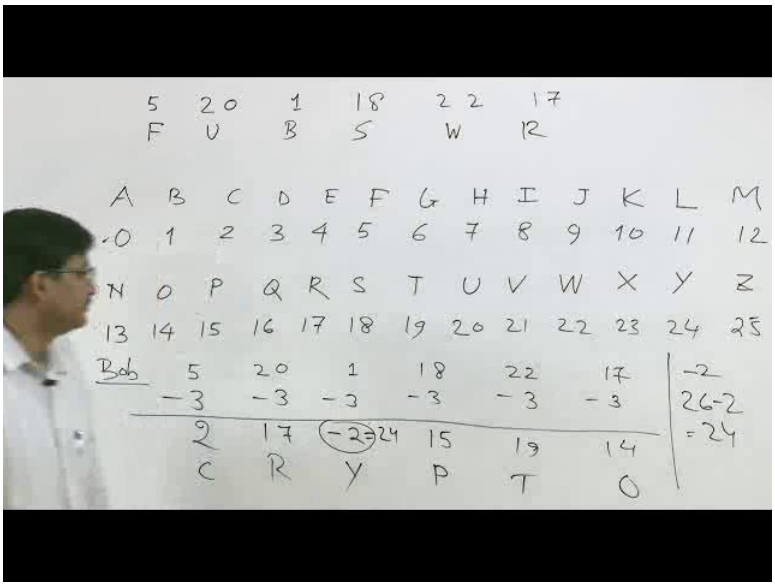
So, z by 26 is a set of numbers between 0 to 25 and this is a plain text. And the strategy that Alice takes is to shift each letter by a fixed amount let us say the amount is 3. So, this amount to which Alice shifted each letter is called the key and this k (Refer Time: 22:08) key is k which is equal to 3. What Alice does is that whenever she wants to send a message she just shifts each letter by this fixed number, so she adds this number to each of the letters.

Now, let us suppose that she wants to send the word cryptology or just let us say that she wants to send crypto. So she writes C R Y P T and O. She converts them to numbers. If she converts that the C is 2, R is 17, Y is 24, P is 15, T is 19 and O is 14. Now she adds 3 to all these numbers to obtain 5, let us draw a line over here 5, then 20, then 27, then she has 18 over here, then this is 22, and this is 17.

Now see that all these numbers are within z 26 except for this 27. Now the question is that what to do with this 27. What Alice does is that she divides 27 by 26 and then takes the remainder which is equal to 0. So, she has got a string like this; let us write it over here. 5 20 27 instead of 27 I will write 0, then 18, then 22, and then 17. And she can change it back 5 20 0, this is not 0 divided by 26 it becomes 1, so 5 20 then 1 18 22 17. Now when she changes back to letters; 5 corresponds to F, 20 corresponds to U, then 1 corresponds to B, 18 corresponds to S, 22 corresponds to W and 17 corresponds to R. So, the cipher corresponding to the word crypto becomes F U B S W R.

Now when Bob receives this word he is suppose to know the shift, here the shift is 3. Therefore, Bob will again use this numbers and subtract three from each of these numbers, so let us see what Bob will do. Let me remove this portion.

(Refer Slide Time: 26:30)

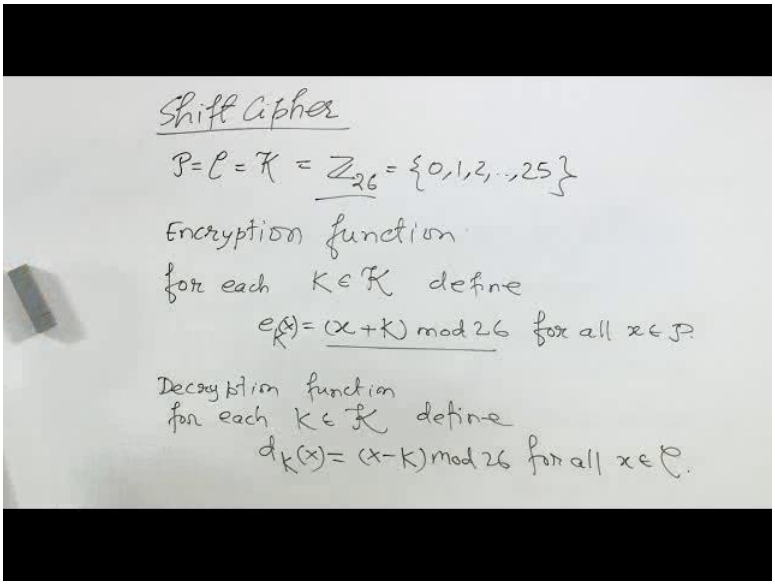


So, it is in the Bob side, Bob he receives 5 20 1 18 22 and 17. He knows that the key is 3, so this is 3 3 3 and 3 and he knows that he has to subtract 3 from all these numbers. If I subtract I get 2 over here, if I subtract I get 17 over here, this is minus 2, this is 15, this is

19, and this is 14. Now let us look at the words; 2 correspond to C, 17 correspond to R. Now what to do with minus 2, here there is a special technique we have to somehow map this minus 2 to something between 0 to 25 and that is uniquely done here by adding 26 to it. So here we process minus 2 in this way, instead of minus 2 we will write 26 minus 2 which is 24 and 24 correspond to Y. So, this minus 2 in a certain way is 24 and then that corresponds to Y, and 15 that corresponds to P, so we have got crypt, 19corresponds to T and 14 corresponds to O. So, we have crypto here.

Now you may of course ask me that why I did, whatever I have done here that we will check in the next lecture. Now, from this point of view in fact Alice has got a crypto system.

(Refer Slide Time: 29:18)



This crypto system if it is written a formal way will be like this; plain text, cipher text, key space all are equal to z sub 26 which is the set of numbers between 0 to 25. So, p c k is properly defined. After that we have an encryption function. Encryption function for each capital K belonging to crypt k define e k as x plus capital K mod 26 for all x belonging to p. Now there is of course question what I mean by x plus capital K mod 26. This means that take x as an integer between 0 to 25 and k is also an integer between 0 to 25 add them and then divide by 26 and take the remainder.

Decryption function is defined in this way, again for each capital K key belonging to crypt k define here I have missed the x so this is x, d k x equal to x minus k mod 26 for

all x belonging to c. And as we know that p and c and k all are same and that is z 26. This cryptosystem is called Shift Cipher.

In the next lecture we will study in details the mathematics related to shift cipher, that is something more on the operations like this x plus k mod 26 and all that, we will generalize shift cipher through something else called Affine Ciphers and so on.

So, for today this is the end.