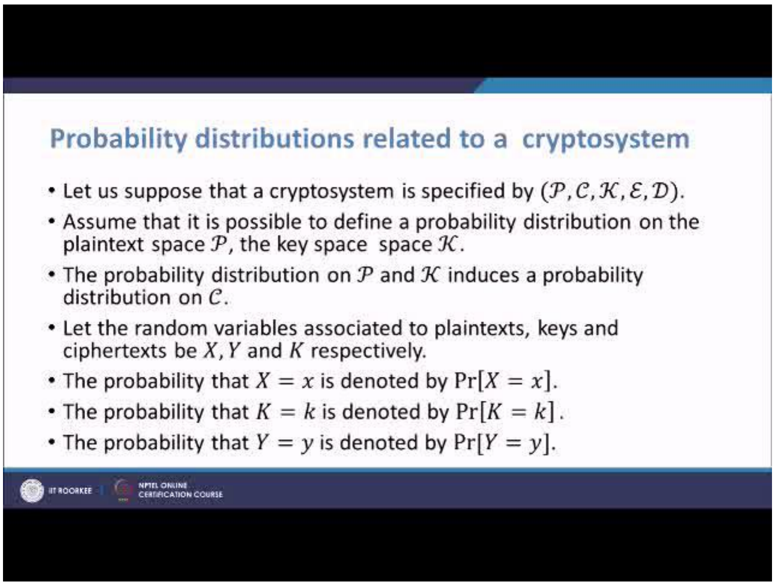
Introduction to Cryptology
Prof. Dr. Sugata Gangopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology, Roorkee

Lecture – 04
Perfect Secrecy, Application on Shift cipher

Hello. Welcome to our course on Introduction to Cryptology. Today is week 1, lecture 4. Today we will cover the idea of Perfect Secrecy introduced by Shannon, but before we do the idea of perfect secrecy introduced by Shannon we have to recall a bit of probability theory.

(Refer Slide Time: 01:04)

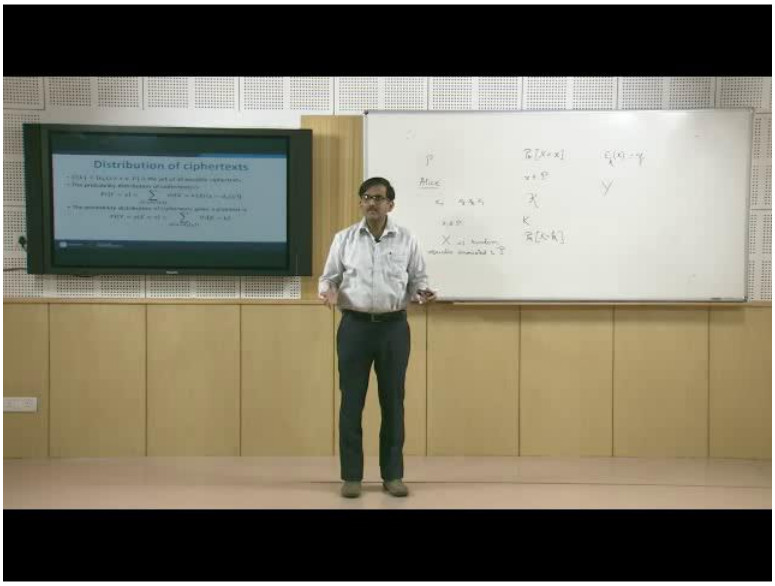


Probability distributions related to a cryptosystem

- Let us suppose that a cryptosystem is specified by $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$.
- Assume that it is possible to define a probability distribution on the plaintext space $\mathcal{P}$, the key space space $\mathcal{K}$.
- The probability distribution on $\mathcal{P}$ and $\mathcal{K}$ induces a probability distribution on $\mathcal{C}$.
- Let the random variables associated to plaintexts, keys and ciphertexts be X, Y and K respectively.
- The probability that $X = x$ is denoted by $\Pr[X = x]$.
- The probability that $K = k$ is denoted by $\Pr[K = k]$.
- The probability that $Y = y$ is denoted by $\Pr[Y = y]$.

We assume that you know basic definitions of probability and all that, now we also know that a cryptosystem is specified by the five (Refer Time: 01:08) P, C, K, E, D. Now, what happens is that suppose Alice is sending a sequence of letters taking from p which basically part of a language.

(Refer Slide Time: 01:17)



So, suppose Alice is sending x 1, x 2, x 3, x n and so on, where each x I belongs to p. Now each time Alice sends an element from p we can imagine that it is a outcome of random experiment. We can relate to the associate random variable to those plenteous symbols. So, what we will do is that we will say that there is a random variable x associated to p, so x is a random variable associated to the set of plaintext and each time Alice sends a plaintext letter we get an instance of that random variable. This is what I have written here that assume that it is possible to define a probability distribution on the plaintext p and x is the random variable corresponding to the plaintext.

So, with the random variable there is of course a probability distribution. We can talk about things like this that what is the probability that the random variable capital X takes a particular value small x, where small x is inside p. This probability will typically depend on the language that Alice is using and the encoding of that language to the plaintext symbol strings. On the other hand Alice also chooses a key and transfers a key through a secret channel b, that key is chosen from the key space which is denoted by script k. Each time Alice wants to send encrypted message to Bob she has to chose a key, that key is also associated to a random variable because Alice is choosing the key in a randomly from the key space. So we associate a random variable capital K with respect to key space k and of course it gives the probability that particular key is chosen.

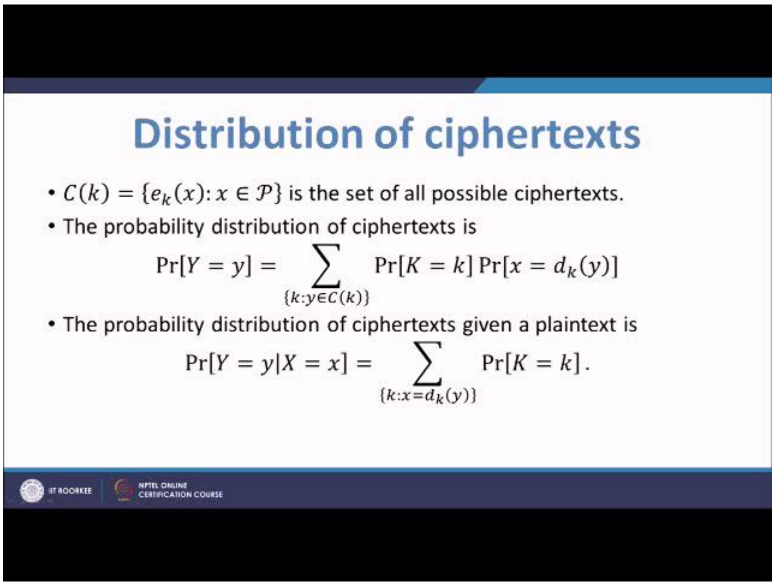
Suppose this particular key small k is chosen then we will write the probability of that choice as this one, probability of k equal to small k.

And now, we know that encryption function is a function which depends on small k that is the key and x that is the plaintext and I write like this y. So, in a way y is also an instant of a random variable, but that random variable distribution is dependent on the distribution of x and k. So, I will write y a random variable associated to the ciphertext in c. If you look at the slides I have written those things formally, so we assume that it is possible to define a probability distribution on the plaintext space P, the key space K, the probability distribution on P and K induces a probability distribution on C. Let the random variables associated to plaintexts keys and ciphertexts be X, Y and K that is exactly what we have discussed before.

And the probability that capital X that is the random variable is equal to small x is denoted by probability capital X is equal to small x. The probability that capital K is equal to small k is denoted by probability capital K is equal to small k. Probability that capital Y that is the random variable corresponding to a ciphertext is equal to small y is denoted by probability a Y equal to small y

Now, we have assumed here that there is a probability distribution on the set of plaint plaintexts, and we know that random variable corresponding to that that is x we have assumed there is a probability distribution on the key space and there is a random variable corresponding to that that is capital K. And we know that x and k determines y. So the question is what is the probability distribution of y? And here we have that, let me explain that to you.

(Refer Slide Time: 07:32)



Distribution of ciphertexts

- $C(k) = \{e_k(x) : x \in \mathcal{P}\}$ is the set of all possible ciphertexts.
- The probability distribution of ciphertexts is

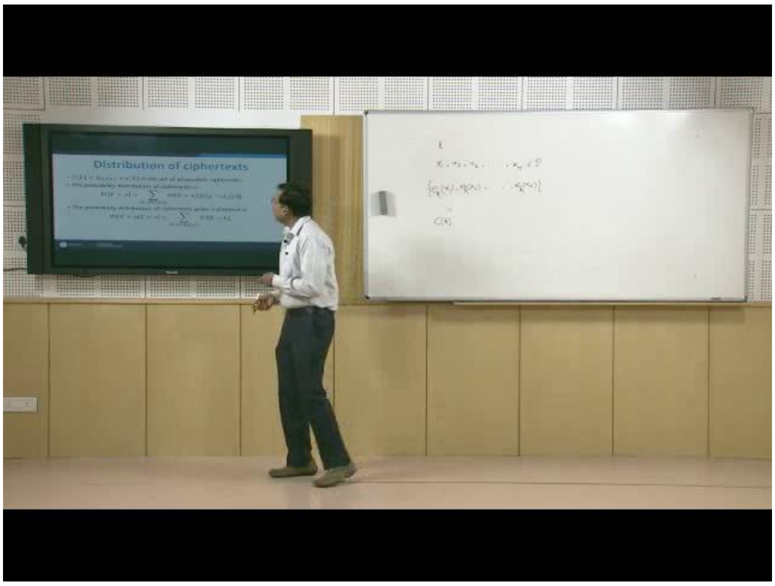
$$\Pr[Y = y] = \sum_{\{k : y \in C(k)\}} \Pr[K = k] \Pr[x = d_k(y)]$$

- The probability distribution of ciphertexts given a plaintext is

$$\Pr[Y = y | X = x] = \sum_{\{k : x = d_k(y)\}} \Pr[K = k].$$

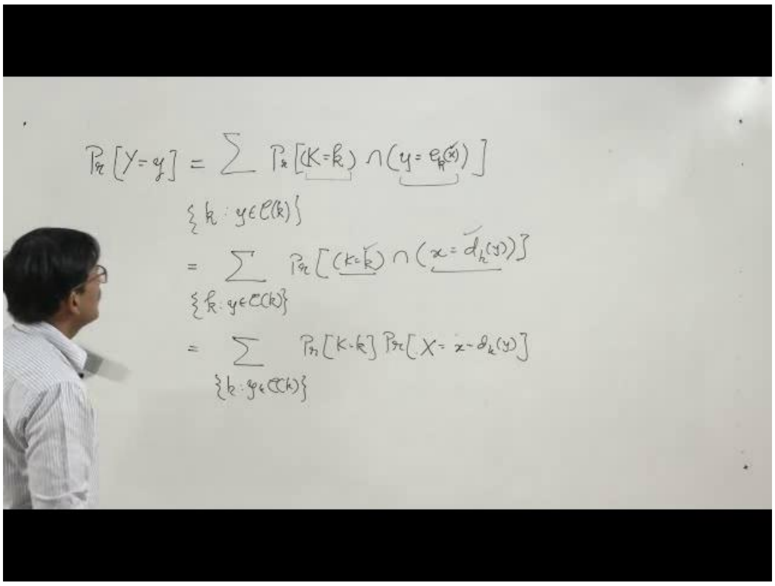
Yes. So first of all we have to consider a set C k which is e k x, where x runs over the set of plaintext. This is the set of all possible ciphertexts given a key k.

(Refer Slide Time: 07:59)



That is we choose a key k and then suppose x 1, x 2, x 3, and so on up to x capital M are the plaintext elements. Suppose all the plaintext elements, so what I do is that we take the encryption x 1 encryption function with respect to k x 2 and so on up to e k x M. And then we put that within a set symbol and this is going to be my set C k. And now the probability distribution of ciphertext is probability Y equals to small y equal to summation now this is a product of two probabilities; probability k equals to small k into probability x equal to d k y where k runs over the set such that y belongs to c k. So, we have to take all the c k's of which y is an element and take that k and sum these over all those k's. Now, let us try to see what happens here.

(Refer Slide Time: 09:54)



$$\Pr[Y=y] = \sum_{\{k : y \in \mathcal{C}(k)\}} \Pr[\underbrace{(K=k)} \cap (\underbrace{y=e_k(x)})]$$

$$= \sum_{\{k : y \in \mathcal{C}(k)\}} \Pr[(\underbrace{K=k}) \cap (\underbrace{x=d_k(y)})]$$

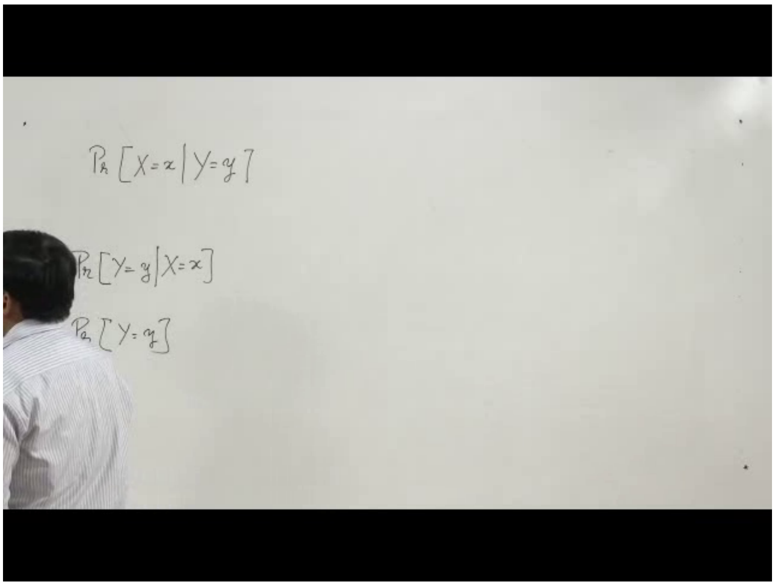
$$= \sum_{\{k : y \in \mathcal{C}(k)\}} \Pr[K=k] \Pr[X=x=d_k(y)]$$

So, let us take the left hand side of this equation that is probability of capital Y equals to small y this is equal to, so we will always have a key so I have a key probability that there is some key k and this intersection the event that we are getting y from the x. For a given k inside the key space if I find that there is a plaintext whose encryption is y then I know that I will get the encrypted, encrypted symbol as y and we have to sum over all possible k's. And of course, if there is no y corresponding to that k I will not take that. I must have at least 1 x for which I get that y. Therefore, we have to vary k in such a way that y is inside c k.

And now we assume that the choice of the key and the choice of plaintexts are independent. We write another step here, so K equal to small k intersection y equal to e k x is same as x equal to d k y. I know that these two events must occur together to get y and then I have to vary over all k. And I know that what I assume very reasonably that the key and the plaintexts are independent therefore these can be replaced by a product. In fact, I should write this as I should write this in this way that it is capital X equal to small x equal to d k y should write like this. So, here I have got this please read that. It is capital X equal to small x equal to d k y.

Now that is the probability of y equal to y small y, and then we have another probability over here that is as a conditional of probability that suppose we know that X is equal to small x then what is the probability of Y being equal to small y, and that is exactly the probability that you have a k such that d k y equal to x. So, sum over all such case we do that if the sum over that we get this condition of probability.

(Refer Slide Time: 14:05).



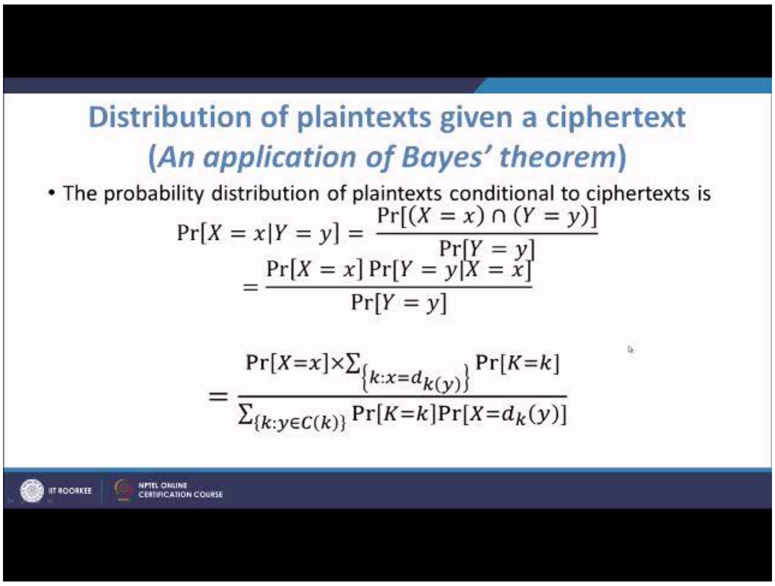
$Pr[X=x \mid Y=y]$

$Pr[Y=y \mid X=x]$

$Pr[Y=y]$

Next, now we can use whatever we have learned to obtain an expression of a very important conditional probability which is probability of capital X equal to small x given that capital Y equal to small y. What we know is we know probability of capital Y equal to small y given capital X equal to small x that we have seen before, and we know the probability of capital Y equal to small y. What we do is that, we use the basic definition of conditional probability.

(Refer Slide Time: 14:47)



Distribution of plaintexts given a ciphertext

(*An application of Bayes' theorem*)

- The probability distribution of plaintexts conditional to ciphertexts is

$$\Pr[X = x|Y = y] = \frac{\Pr[(X = x) \cap (Y = y)]}{\Pr[Y = y]}$$

$$= \frac{\Pr[X = x]\Pr[Y = y|X = x]}{\Pr[Y = y]}$$

$$= \frac{\Pr[X=x] \times \sum_{\{k:x=d_{k(y)}\}} \Pr[K=k]}{\sum_{\{k:y \in C(k)\}} \Pr[K=k]\Pr[X=d_k(y)]}$$

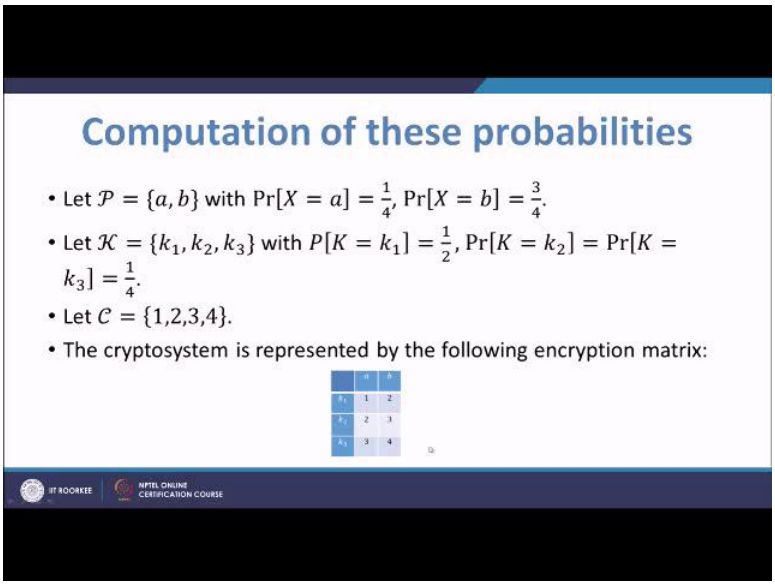
IIT ROORKEE | NPTEL ONLINE CERTIFICATION COURSE

Here, probability capital X equal to small x given Y equal to small y equal to probability of capital X equals to small x intersection Y equal to small y divided by probability of Y equal to small y. And this one we can write by using the definition of conditional probability as this; probability of capital X equal to small x into probability of capital Y equal to small y given X equal to small x and we divide it by Y equal to small y.

And now we go back to our previous expressions here, we have the expression for probability of Y equal to small y and we have the expression for the probability of Y equal to small y given X equal to small x. If you plug in those things we get this expression probability of capital X equal to small x into the sum which is equal to this thing, and in the denominator we have the other sum that we have discussed in the previous slide. So this is the probability that capital X equal to small x given Y equals small y.

And once we have this expression we can we are closer to discussing the concept of perfect secrecy as proposed or as initiated by Claude Shannon. But before that we will take a small cryptosystem and see how to calculate these probabilities. Now we have a small toy cryptosystem.

(Refer Slide Time: 16:59)



Computation of these probabilities

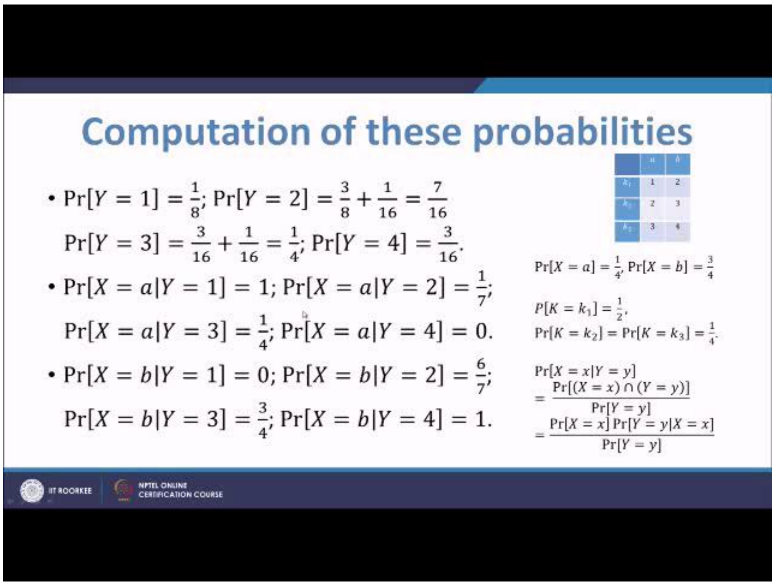
- Let $\mathcal{P} = \{a, b\}$ with $\Pr[X = a] = \frac{1}{4}$, $\Pr[X = b] = \frac{3}{4}$.
- Let $\mathcal{K} = \{k_1, k_2, k_3\}$ with $P[K = k_1] = \frac{1}{2}$, $\Pr[K = k_2] = \Pr[K = k_3] = \frac{1}{4}$.
- Let $\mathcal{C} = \{1,2,3,4\}$.
- The cryptosystem is represented by the following encryption matrix:

	a	b
k_1	1	2
k_2	2	3
k_3	3	4

So, what we have here is that we have the set of plaintexts having 2 elements a and b, and set of keys having 3 elements k 1 k 2 and k 3 with the probabilities. So, we know that probability of X being equal to a is one fourth and probability of X equal to b is 3 by 4. Probability of K equal to k 1 is equal to half and probability of K equal to k 2 equal to probability of K equal to k 3 is equal to one fourth, as we have written here. And the ciphertexts consists a 4 elements 1,2,3,4.

Now we can represent the cryptosystem that we have formed in this way. If you look at this table there on the horizontal side that is the columns are marked a and b and rows are marked k 1 k 2 and k 3, we should read like this that if I take choose the key k 1 then if my plaintext is a then my encryption is 1, if my claim plaintext is b then my encryption is 2, if I choose k 2 if my plaintext is a then my encryption is 2, and if my plaintext is b then my encryption is 3 and so on.

(Refer Slide Time: 18:26)



Computation of these probabilities

- $\Pr[Y = 1] = \frac{1}{8}$; $\Pr[Y = 2] = \frac{3}{8} + \frac{1}{16} = \frac{7}{16}$
  $\Pr[Y = 3] = \frac{3}{16} + \frac{1}{16} = \frac{1}{4}$; $\Pr[Y = 4] = \frac{3}{16}$.
- $\Pr[X = a|Y = 1] = 1$; $\Pr[X = a|Y = 2] = \frac{1}{7}$;
  $\Pr[X = a|Y = 3] = \frac{1}{4}$; $\Pr[X = a|Y = 4] = 0$.
- $\Pr[X = b|Y = 1] = 0$; $\Pr[X = b|Y = 2] = \frac{6}{7}$;
  $\Pr[X = b|Y = 3] = \frac{3}{4}$; $\Pr[X = b|Y = 4] = 1$.

	a	b
k_1	1	2
k_2	2	3
k_3	3	4

$\Pr[X = a] = \frac{1}{4}$, $\Pr[X = b] = \frac{3}{4}$

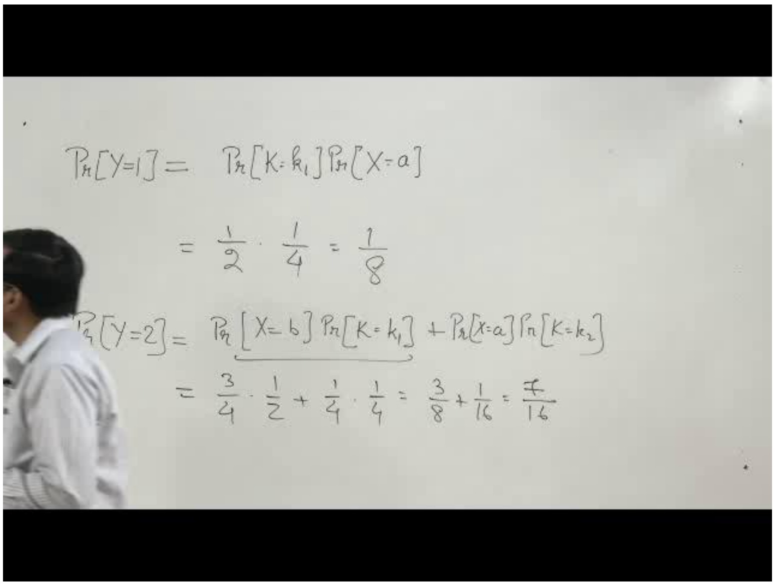
$P[K = k_1] = \frac{1}{2}$,
$\Pr[K = k_2] = \Pr[K = k_3] = \frac{1}{4}$.

$$\Pr[X = x|Y = y] = \frac{\Pr[(X = x) \cap (Y = y)]}{\Pr[Y = y]} = \frac{\Pr[X = x]\Pr[Y = y|X = x]}{\Pr[Y = y]}$$

Now, let us look at the slide here I have written down the cryptosystem over here and the related formulas over here and we will derive the particular values over here. So let us see what happens.

Suppose I am asking, what is the probability that capital Y is equal to 1? For this we can invoke the previous formulas but we can just see that from the table where are we can understand this. In this body of the matrix we try to find out where is 1, 1 is over here. That means, there is only one situation where I get a ciphertext 1, that is when plaintext is a and key is k 1. So we can in fact forget all the formulas that I have discussed just before this and write and understand that I get ciphertext y equal to 1 if key is k 1 and plaintext is a and never otherwise.

(Refer Slide Time: 18:46)



$$\Pr[Y=1] = \Pr[K=k_1]\Pr[X=a]$$

$$= \frac{1}{2}\cdot\frac{1}{4} = \frac{1}{8}$$

$$\Pr[Y=2] = \underbrace{\Pr[X=b]\Pr[K=k_1]}_{} + \Pr[X=a]\Pr[K=k_2]$$

$$= \frac{3}{4}\cdot\frac{1}{2} + \frac{1}{4}\cdot\frac{1}{4} = \frac{3}{8} + \frac{1}{16} = \frac{7}{16}$$

Therefore, I will write like this is the probability of getting K equal to k 1 and probability of getting X equal to a. Probability of K getting k equal to k 1 is given over here which is half and probability of X equal to a which is given over here which is one fourth, so I get 1 by 8 which I have listed over here

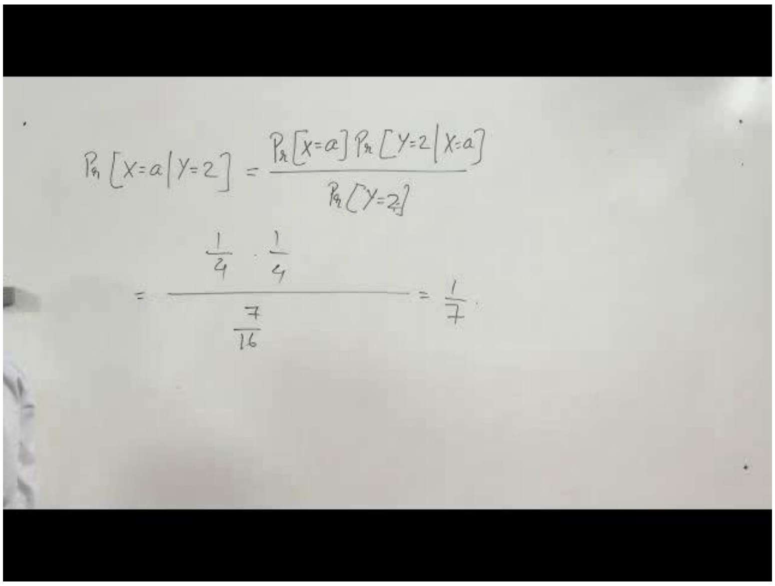
I have a question that what is a probability of getting Y equal to 2. Of course, if you patiently go back and see the formulas that I have discussed you will be able to do that then you have to talk about c k's and all those things, but basically for working we can do otherwise. So, what we can do is that we can say that where I am getting 2, I am getting 2 over here, and 2 over here. What is this case we are getting 2, because we have key equal to k 1 and we have plaintext equal to b, and here we are getting 2 because we have got k equal to k 2 and plaintext equal to a. So, these are the 2 cases.

When the plaintext is b and key is k 1 we are getting 2 and when the plaintext is let us see the plaintext is a and key is k 2 then also we are getting 2, and that these are the only places we are getting 2. And these events are mutually exclusives and I am writing for this probability as product because we are assuming that plaintext and ciphertexts they are independent. And now we put the probabilities over here, so x equals to b is 3 by 4 and k equal to k 1 is half and x equal to a is 1 by 4 and k equal to k 2 is going to be 1 by

4; so I have got 1 by 16, so I have got 3 by 8 plus 1 by 16 is exactly what I have got here and let me check that it is 7 by 16.

Now, we can calculate all these probabilities in this way. I will show here because that they here we have to use something else. Now suppose I have a situation there I want to find out the probability of x equal to a given y equal to 2.

(Refer Slide Time: 23:09)



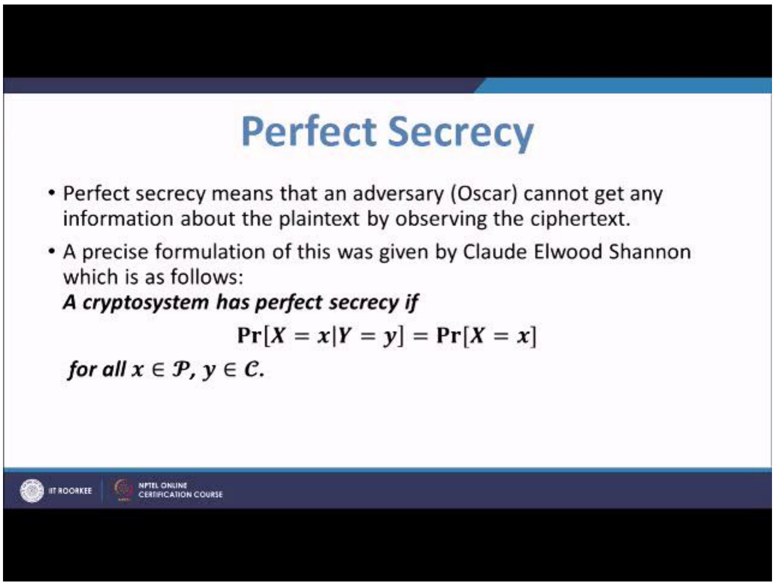
$$\Pr[X=a \mid Y=2] = \frac{\Pr[X=a]\Pr[Y=2 \mid X=a]}{\Pr[Y=2]}$$

$$= \frac{\frac{1}{4} \cdot \frac{1}{4}}{\frac{7}{16}} = \frac{1}{7}$$

Probability of X equals to a given y equal to 2, so what is this. Now this is, if you look at this formula use this one this is probability of x equal to a and then probability of y equal to 2 given x equal to a, and then divided by probability of capital Y equal to small y. Now I know what is probability of X equal to a that is one fourth and I know that what is probability of Y equal to 2 given x equal to a, what is that? Given x equal to a y equal to 2 if k 2 occurs, this is probability of getting k 2, probability of getting k 2 is one fourth and probability of Y equal to 2 is what, we have computed that that is 7 by 16 so this gives us 1 by 7. So, these conditional probabilities can be computed in this way.

This leads us to our last topic of this lecture that is perfect secrecy or this is a topic to which we are driving at.

(Refer Slide Time: 25:01)



Perfect Secrecy

- Perfect secrecy means that an adversary (Oscar) cannot get any information about the plaintext by observing the ciphertext.
- A precise formulation of this was given by Claude Elwood Shannon which is as follows:
  A cryptosystem has perfect secrecy if

$$\mathbf{Pr}[X = x|Y = y] = \mathbf{Pr}[X = x]$$

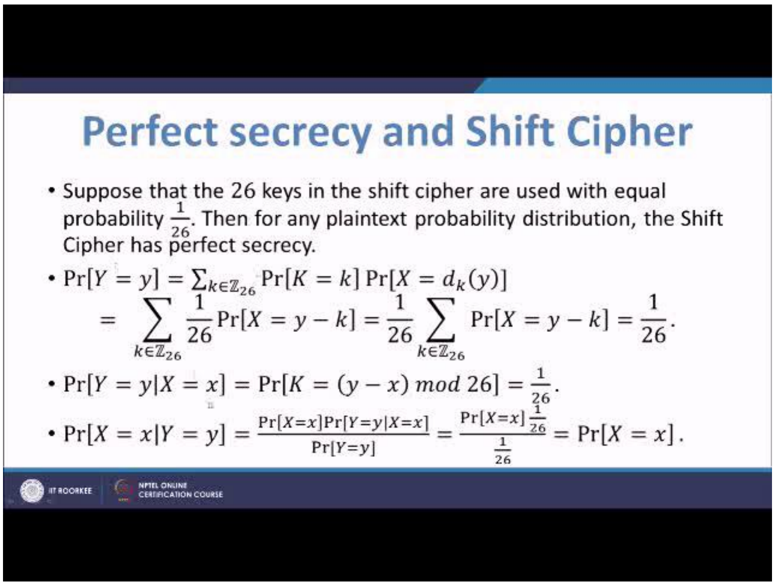
for all $x \in \mathcal{P}, y \in \mathcal{C}$.

IIT ROORKEE | NPTEL ONLINE CERTIFICATION COURSE

The idea of perfect secrecy was formulated by Claude Elwood Shannon around 1948. He stated that a cryptosystem has perfect secrecy if probability of x equal to x given y equal to y is equal to probability of X equal to small x, for all x inside p and for all y inside c. If you look at this cryptosystem that we have seen, we see that probability of X equal to a given y equal to 2 is 1 by 7 whereas probability of X equal to a is 1 by 4. Therefore, it proves that it does not have perfects secrecy.

But if there is a cryptosystem for which this is true for all x and y then it has perfect secrecy. And now the example of such a cryptosystem interestingly such a cryptosystem is shift cipher with a condition. Now let us read.

(Refer Slide Time: 26:14)



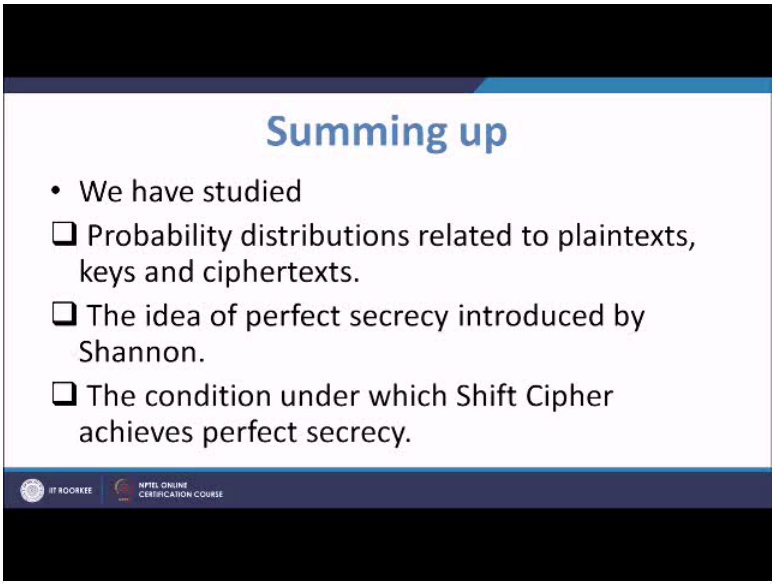
Perfect secrecy and Shift Cipher

- Suppose that the 26 keys in the shift cipher are used with equal probability $\frac{1}{26}$. Then for any plaintext probability distribution, the Shift Cipher has perfect secrecy.
- $\Pr[Y = y] = \sum_{k\in\mathbb{Z}_{26}} \Pr[K = k] \Pr[X = d_k(y)]$
$$= \sum_{k\in\mathbb{Z}_{26}} \frac{1}{26} \Pr[X = y - k] = \frac{1}{26} \sum_{k\in\mathbb{Z}_{26}} \Pr[X = y - k] = \frac{1}{26}.$$
- $\Pr[Y = y|X = x] = \Pr[K = (y - x)\ mod\ 26] = \frac{1}{26}.$
- $\Pr[X = x|Y = y] = \frac{\Pr[X=x]\Pr[Y=y|X=x]}{\Pr[Y=y]} = \frac{\Pr[X=x]\frac{1}{26}}{\frac{1}{26}} = \Pr[X = x].$

Suppose that 26 keys in the shift cipher are used with equal probability 1 by 26 then for any plaintext probability distribution the shift cipher has perfect secrecy. How do we prove that? We can prove that and let us look at this line and the following lines. We start with Y equal to small y that is equal to k running over z sub 26 probability of capital K equal to k into x equal to d k y this is exactly the formula that we have derived. Now our assumption is that keys are chosen equi-probably, that means there is no bias. If there is no bias then probability of K equal to k is 1 by 26, I take one by 26 out so I get something like this. And now I am varying k over z sub 26, but y is fixed over here. Therefore, y minus k modular 26 is going to vary over the whole space and therefore this probability is going to sum up to 1, so I have one by 26.

On the other hand, if I consider probability of Y given probability of given x equal to x then that is probability of getting the key y minus x mod 26 which is 1 by 26 because each key chosen equi-probably. And now we see the conditional probability formula probability of X equal to x given Y equal to small y, that is this probability of X into probability of Y equal to small y given X equal to small x divided probability of Y equal to y. We know probability of y equal to y is 1 by 26, this is 1 by 26 so we are we end up the probability of X equal to x so we have probability of X given x, sorry X equal to x given Y equal to small y equal to probability of X equal to small X and that is perfect secrecy.

(Refer Slide Time: 28:50)



Summing up

- We have studied

❑ Probability distributions related to plaintexts, keys and ciphertexts.

❑ The idea of perfect secrecy introduced by Shannon.

❑ The condition under which Shift Cipher achieves perfect secrecy.

IIT ROORKEE
NPTEL ONLINE CERTIFICATION COURSE

So summing up, in this lecture we have studied probability distribution related to plaintext, keys, and ciphertexts. And we have studied the idea of perfect secrecy introduced by Shannon. And finally, we have studied the condition under which shift cipher achieves perfect secrecy. And now I go back to my last slide of my previous lecture where I said that do not under estimate classical ciphers. Shift cipher is the first cipher that we studied. When we study shift cipher it seems that it is too simple, it cannot have any security. But very soon we see the shift ciphers can have perfect secrecy, but with one condition that each time in cipher a plaintext you have to choose a key equi-probably from z sub 26. So that is the condition and that is a very difficult thing to achieve. But never the less it is provably secure if we have the condition.

So, this is the end of today’s lecture. We will continue discussion on cryptology in our subsequent lectures.

Thank you.