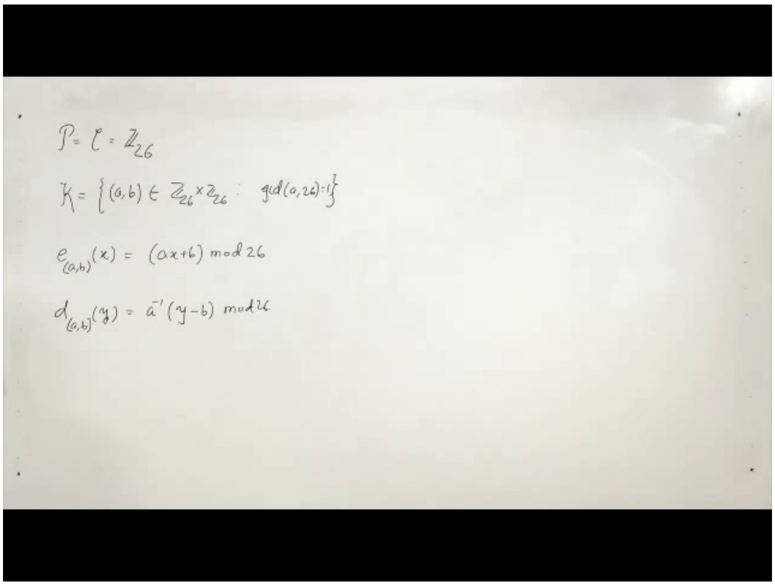
Introduction to Cryptology

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

Lecture – 05
Problem discussion on Affine cipher and perfect secrecy

Hello, welcome to Week 1, Lecture - 5. In this lecture, we will be having a problem solving session; we look at some problems related to affine ciphers and some problems related to Shannon’s theory of perfect secrecy. Now, affine ciphers, what we mean by an affine cipher?

(Refer Slide Time: 00:56)



$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$

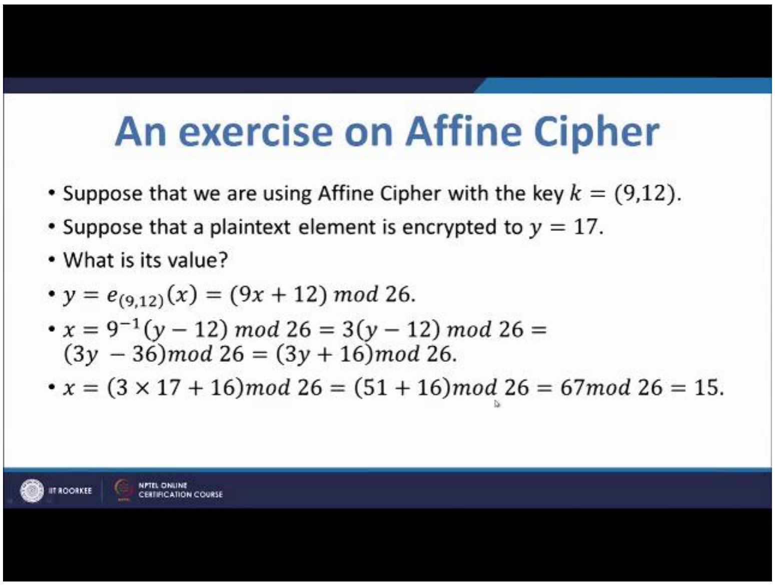
$\mathcal{K} = \{(a,b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a,26)=1\}$

$e_{(a,b)}(x) = (ax+b) \bmod 26$

$d_{(a,b)}(y) = a^{-1}(y-b) \bmod 26$

In the case of affine cipher, p equal to c, both are equal to z sub 26 and the key space k is an ordered pair of elements of z sub 26, such that GCD of a and 26 is 1 and b can be any element is z sub 26. The encryption function e sub a comma b, when it operates over x is a x plus b mod 26 the decryption function d a comma b operated by y which is the cipher text is a inverse y minus b mod 26. Now, we have already studied these things, now we have a question here.

(Refer Slide Time: 02:28)



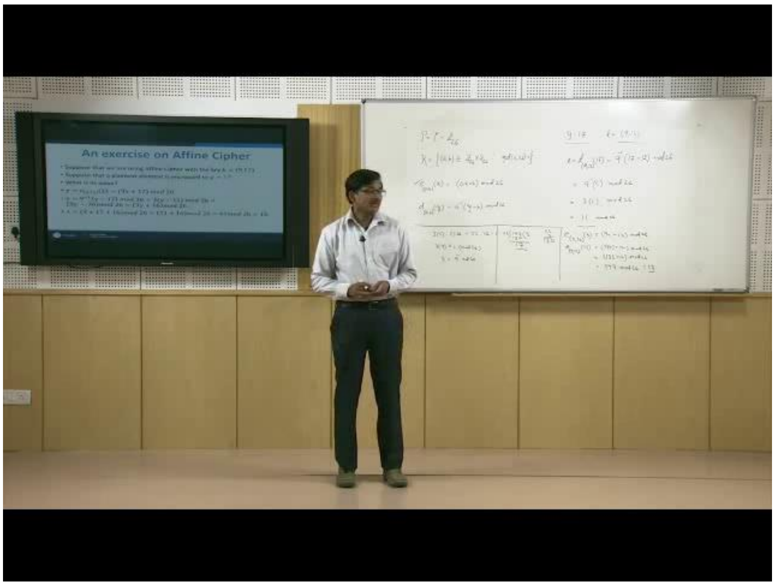
An exercise on Affine Cipher

- Suppose that we are using Affine Cipher with the key $k = (9,12)$.
- Suppose that a plaintext element is encrypted to $y = 17$.
- What is its value?
- $y = e_{(9,12)}(x) = (9x + 12)\ mod\ 26$.
- $x = 9^{-1}(y - 12)\ mod\ 26 = 3(y - 12)\ mod\ 26 =$ $(3y\ - 36)mod\ 26 = (3y + 16)mod\ 26$.
- $x = (3 \times 17 + 16)mod\ 26 = (51 + 16)mod\ 26 = 67mod\ 26 = 15$.

IIT ROORKEE
NPTEL ONLINE CERTIFICATION COURSE

Suppose, somebody gives us a gives us an encrypted character, let us say this cipher text is 17.

(Refer Slide Time: 02:43)



So, suppose it gives us y equal to 17 and asks us to find out the corresponding x, how will we do that? Now, he has also to give me the key. So, suppose the key is k equal to 9,

12. So, we know the decryption rule is d sub a b y is a inverse y minus b therefore, the decryption of 17 will be x which is equal to d of 9 comma 12 and here instead of y, I will put 17, this is equal to a inverse that is 9 inverse and then y is equal to 17 and b is 12. So, I will get this, this is what I have written over here, I have to replace y by 17.

Now, I have 2 options, I can compute the general decryption rule as I have done before and as it is written in the slide, but I can do something else which I am showing here. So, once we know that the encrypted message is 17. Therefore, I can put 17 over here, instead of y and therefore, I have got 9 inverse 17 minus 12 and this is of course, has to be reduced module of 26 and here I have got 9 inverse into 17 minus 12 is 5 mod 26.

Now, the question is what is 9 inverse? When we are actually doing the problems we can use our observations. So, I want 9 inverse mod 26 now; that means, I want a number which when multiplied to 9 and reduced mod 26 gives me 1. What is that number, if we see from 2 9 are 18 is of course, not 1 mod of 26, but we hit the correct answer if we check with 3 because we see that, let me write this note over here, 3 into 9 minus 1 into 26 gives me 27 minus 26 which is equal to 1. Therefore, 3 into 9 gives me is congruent to 1 mod 26 therefore, I can write that 9 inverse is equal to 3 or in other words I can write that 3 equal to 9 inverse mod 26. Therefore, here I will replace 9 inverse by 3 into 5 mod 26 which is equal to 15 mod 26 because I know that if my key is 9, 12 and if my cipher text is 17 then the plain text is 15.

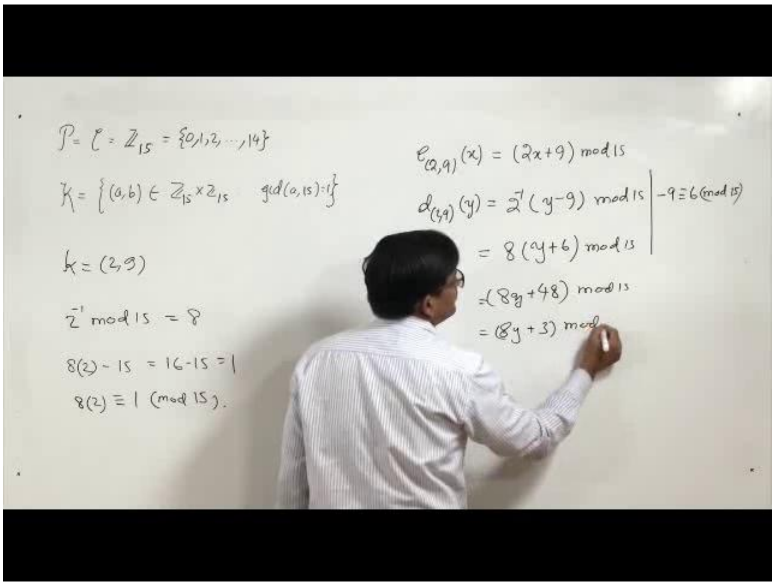
Now, we can have many other problems like this and you will get some problems like this in the assignment. We can as well try to cross check our result by going the other way round just to check whether really everything is alright. We can start from x here and use the encryption rule which is given over here by putting the appropriate values of a and b and then we can check whether we are indeed getting 17, if we start from 15 has the plain text. Now, let us try this one, here I know that a is 9 and b is 12 therefore, I write e sub 9, 12 into x which by definition is 9 into x plus 12 mod 26. Now, I know I am putting x is equal to 15.

So, e 9 comma 12 into 15 gives me 9 into 15 plus 12 mod 26 and this is 135 plus 12 mod 26, this is equal to 147 mod 26 which is 17. Well, this is 17 because if you divide 147 by

26 let us see this division over here as a note here. So, suppose I take 26, I divide 26 by 147. So, 26 into 5 is 130. So, if you put 5 this is 130, 26 into 5 is 130. If you subtract 130 from 147 we get 17 which is the remainder and therefore, I am writing it over here thus we see that our calculations are correct. We started with 17 y equal to 17 then key was 9 12 and we computed the inverse transform of the affine cipher, which is the decryption of affine cipher and we got 15, we start from 15 use the key and use the function for the affine cipher and we find that we are getting 17. So, everything was alright. So, we have got our answer.

Now, there is just 1 note over here that we are defining affine ciphers. We really do not have to stick to the modulus 26. We can define affine ciphers over other module. Let us say 15. So, we can take m equal to 15 and consider affine ciphers over z sub 15. So, let us look, how it will look like.

(Refer Slide Time: 10:35)



$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{15} = \{0,1,2,\dots,14\}$

$\mathcal{K} = \{(a,b) \in \mathbb{Z}_{15} \times \mathbb{Z}_{15} \quad \gcd(a,15)=1\}$

$k = (2,9)$

$2^{-1} \bmod 15 = 8$

$8(2) - 15 = 16 - 15 = 1$

$8(2) \equiv 1 \pmod{15}.$

$e_{(2,9)}(x) = (2x+9) \bmod 15$

$d_{(2,9)}(y) = 2^{-1}(y-9) \bmod 15$ | $-9 \equiv 6 \pmod{15}$

$= 8(y+6) \bmod 15$

$= (8y+48) \bmod 15$

$= (8y+3)$ mod

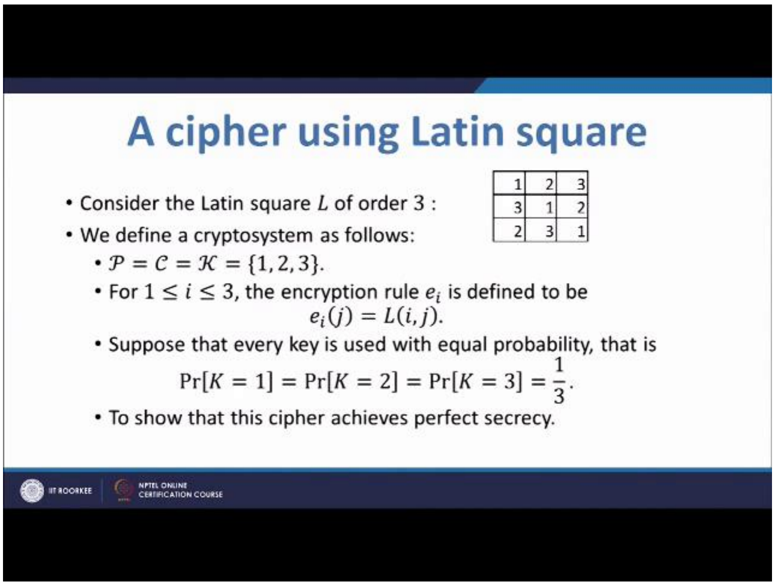
We will just change this z by z sub 26 to z sub 15. So, these are numbers from 1 to 0, 1 to up to 14 and the key space will change to something like this, it will be a, b, z 15 cross z 15 and GCD of a and 15 is 1. Now, let us quickly check 1 key and how to find out encryption and decryption functions?

So, here in this case k equal t to 2 comma 9 is a key. Please note that this is not a key if we take z sub 26 because 2 is not co prime to 26, but in this case 2 is co prime to 15 and therefore, it is a key and suppose we have to find 2 inverse mod 15 that is also not difficult to see 2 inverse mod 15 is going to be 8. The reason is that 8 into 2 minus 15 gives me 16 minus 15 equal to 1 and therefore, 8 into 2 is congruent to 1 mod 15.

Thus the encryption function will be like this e sub 2 comma 9 of x is going to be twice x plus 9 mod 15 and the decryption function d 2 comma 9 of y is going to be 2 inverse, again 2 y minus 9 mod 15 and I can safely put 8 instead of 2 and y minus 9 well I can put instead of minus 9, I can always put plus of 6 this is because minus 9 is congruent to 6 mod 15 and I have got this mod 15 and therefore, this is 8 y plus 48 mod 15, I can reduce further it is 8 y plus 3 mod 15. So, this is the decryption function and now I can plug in any x and y to find out the encryption or decryption of particular values between 0 to 14, we will also see many problems like this in our assignments.

Next, we come to a problem related to perfect secrecy and the computations of different probabilities of plain text and cipher text and keys.

(Refer Slide Time: 14:26)



A cipher using Latin square

- Consider the Latin square L of order 3 :

1	2	3
3	1	2
2	3	1

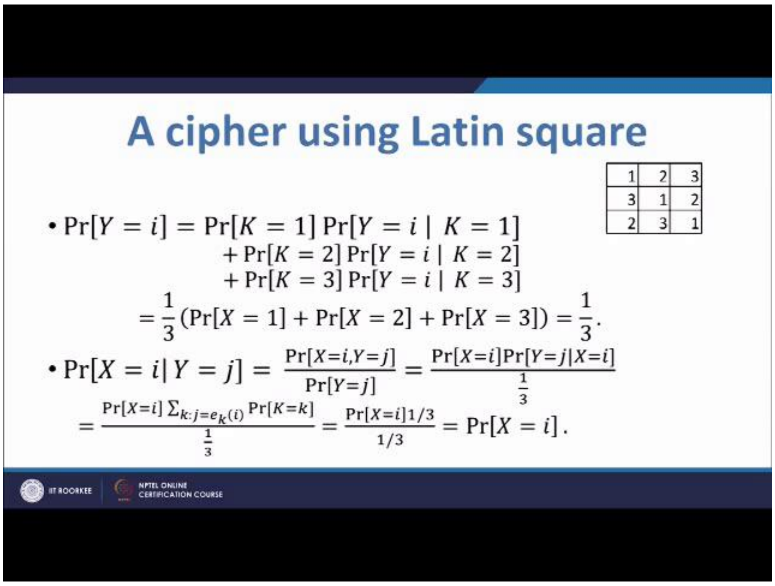
- We define a cryptosystem as follows:
  - $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{1, 2, 3\}$.
  - For $1 \leq i \leq 3$, the encryption rule e_i is defined to be
    $$e_i(j) = L(i, j).$$
  - Suppose that every key is used with equal probability, that is
    $$\Pr[K = 1] = \Pr[K = 2] = \Pr[K = 3] = \frac{1}{3}.$$
  - To show that this cipher achieves perfect secrecy.

IIT ROORKEE
NPTEL ONLINE CERTIFICATION COURSE

Now, here we have a cipher using a Latin square a Latin square is a 2 dimensional array of numbers such that no number is repeated in a row or a column. So, here we have a Latin square l of order 3, where we have got 3 numbers in a 3 by 3 array and please note that there is no repetition either in the rows or in the columns. So, I have got 1, 2, 3, 3, 1, 2, 2, 3, 1 and I have got 1, 3, 2, 2, 1, 3, 3, 2, 1. Now, we can use a Latin square to construct a cryptosystem and this cryptosystem is 1 such cryptosystem. Now, we take the PCK to be 1, 2 and 3 and the encryption is defined in this way we choose a key i which is a number between 1 and 3. We write e sub i and j is my plain text it is again a number between 1 and 3 and e, i, j is the element l (i, j), l (i, j) is the element of the i th row and the j the column of the Latin square l and that number is the cipher text.

Now, suppose that every key is used with equal probability that is probability that capital k equal to 1 is equal to probability that capital key is equal to 2 is equal to probability that capital k is equal to 3 equal to 1 third. So, keys are equi probable, now we will go to show that this cipher system achieves perfect secrecy. Here, in order to do that we have to show that the conditional probability of x that is plain text given any value of y is same as the probability of x. So, we will show that, but the first step is to check the probabilities of y, i.

(Refer Slide Time: 16:59)



A cipher using Latin square

1	2	3
3	1	2
2	3	1

- $\Pr[Y = i] = \Pr[K = 1]\Pr[Y = i \mid K = 1]$
  $+ \Pr[K = 2]\Pr[Y = i \mid K = 2]$
  $+ \Pr[K = 3]\Pr[Y = i \mid K = 3]$
  $= \frac{1}{3}(\Pr[X = 1] + \Pr[X = 2] + \Pr[X = 3]) = \frac{1}{3}.$
- $\Pr[X = i \mid Y = j] = \frac{\Pr[X=i, Y=j]}{\Pr[Y=j]} = \frac{\Pr[X=i]\Pr[Y=j|X=i]}{\frac{1}{3}}$
  $= \frac{\Pr[X=i]\sum_{k:j=e_k(i)}\Pr[K=k]}{\frac{1}{3}} = \frac{\Pr[X=i]1/3}{1/3} = \Pr[X = i].$

So, here I have chosen any i between 1 to 3. So, we have probability of y, i, now let me write down 1 step in between whatever is shown in the slide. So, this is equal to the probability of y, i and k 1 k equal to 1 plus plus probability of y equal to i k equal to 2 plus probability of y equal to i comma k equal to 3 because these are the possible keys. So, we have to see that what is the probability that y equal to i occurs with k equal to 1. What is the probability y equal to the probability y is equal to i when k is equal to 2 what is the probability of y equal to i when k equals to 3 it is this 1.

Now, we can always write it a conditional like this. So, this is probability that k equal to 1 and probability of y equal to i given k equal to 1 plus probability of k equal to 2 into probability y equal to i given k equal to 2 plus probability of k equal to 3 into probability y equal to i given k equal to 3. We know these probabilities these are all one-third, we have seen that before. Now, what about the probability of y equal to i given that k equal to 1 for that let us check this Latin square. So, here we see that suppose k equal to 1. So, I know that k equal to 1, now let us see if i equal 1 that is 1 when I have got k equal to 1, I will fix to this row and in this row there is no repetition.

So, for any y any particular value of y, in this case i it maybe 1, 2 or 3. Let us say i equal to 1. So, if I take i equal to 1 then y 1 occurs in the first place and the corresponding x this corresponds to the plain text x equal to 1. So, there is only when k equal to 1, y equal to 1 will occur only if x equal to 1. Similarly, y equal to 2 will occur only or I can say if only if x equal to 2 and similarly for x equal to 3. So, therefore, I can say that probability of y equal to is given k equal to 1 is is a probability of either x equal to 1 x equal to 2 or x equal to 3.

So, I really do not know which one will it be, but it is exactly one of them and therefore, be the value of i, I can take since I know that these are equal to one-third, I can take one-third over here and I will get within a bracket probability of k equal to 1 plus probability of y equal to i k equal to 2 plus probability of y equal to i given k equal to 3, what I claim here that this sum will be same for all values of i. So, we have only 3 values of i what I will ask you is to do on your own and check that if you put y equal to 1, if you put y equal to 1 probability that y equal to 1 given k is equal to 1 is probability that x equal to 1 probability of y equal to 1 given k is equal to 2 y equal to 1 given k equal to 2 is going to be y equal to 1 given k is equal to 2 is going to be x 2 probability that x equal to 2 and probability of y equal to l given k is equal to 3 is going to be probability x equal to 3.

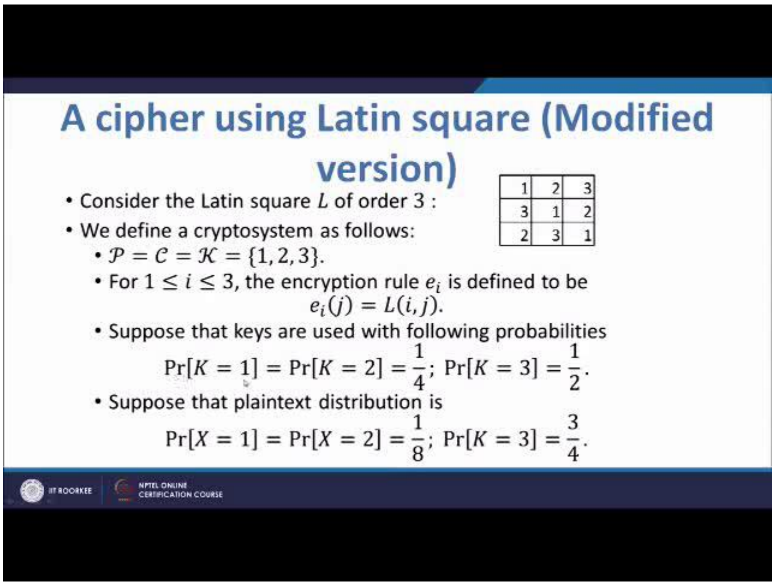
Similarly, if you put probability of y equal to 2 k equal to 1 y equal to 2 k equal to 1 x equal to 2 y equal to 2 k given k equal to 2 y equal to 2 given k equal to 2 x equal to 3 y equal to 2 given k equal to 3 is x equal to 1. So, you will have permutations of these 3 probabilities therefore, I can write this as one-third probability of x, x equal to 1 plus probability of x equal to 2 plus probability of x equal to 3 and we know that whatever be the distribution of the plain text the sum of all the probability is going to be 1 and therefore, it is going to be one-third this is what we have in our slide.

And then we have a question that what is the probability of x equal to I given y equal to j? So, let us look at that probability of x equal to i given y equal to j is equal to probability of x equal to i and y equal to j divided by probability of y equal to j which is equal to probability of x equal to i and probability of y equal to j given x equal to i.

Now, this is equal to probability of x equal to i and this sum that is the sum over all case for which I is transferred to j and here we will see that given any pair of i, j you have got a unique k for which transfers i to j that is clear from this table and therefore, I will replace it by one-third and therefore, I have got probability of x equal to i and thus I have got whatever be the values of i and j probability of x equal to i given y equal to j is equal to probability of x equal to i.

We end our lecture by another problem in the same direction and this is a modification of the problem that I have done just now. Here, also we have got the same Latin square and we have the same cryptosystem. We have the same plain text cipher text and key space, but we have got and the encryption rule e, i is also the same we have written here, but there is a little difference from the last example here we have a different probability distribution of the keys.

(Refer Slide Time: 25:35)



A cipher using Latin square (Modified version)

- Consider the Latin square L of order 3 :

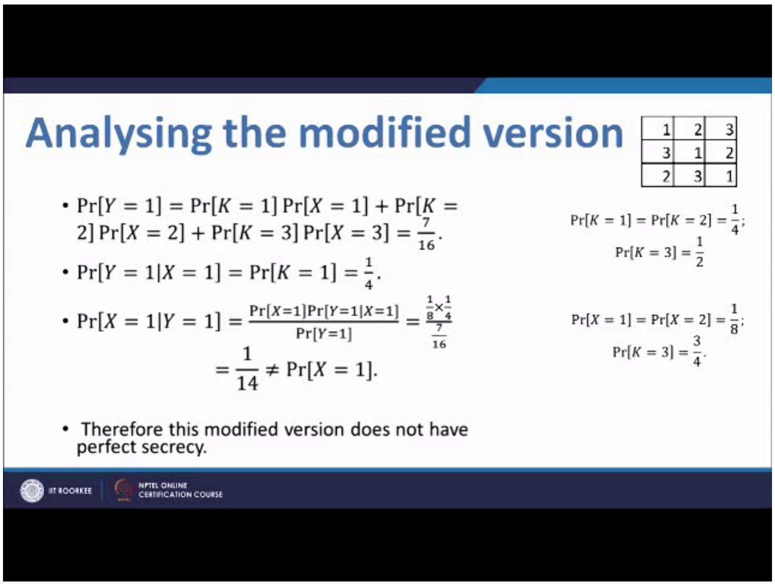
1	2	3
3	1	2
2	3	1

- We define a cryptosystem as follows:
  - $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{1,2,3\}$.
  - For $1 \leq i \leq 3$, the encryption rule e_i is defined to be
$$e_i(j) = L(i,j).$$
  - Suppose that keys are used with following probabilities
$$\Pr[K = 1] = \Pr[K = 2] = \frac{1}{4}; \ \Pr[K = 3] = \frac{1}{2}.$$
  - Suppose that plaintext distribution is
$$\Pr[X = 1] = \Pr[X = 2] = \frac{1}{8}; \ \Pr[K = 3] = \frac{3}{4}.$$

IIT ROORKEE NPTEL ONLINE CERTIFICATION COURSE

So, I have got probability of k equal to 1 probability of k equal to 2 and probability of k equal to 3 they are different probability of k equal to 1 and probability of k equal to 2 are equal and is equal to one-forth and probability of k equal to 3 is one-half and you can check that it will all sum up to give me 1 and we are assuming another plain text distribution that is probability of x equal to 1 equal to probability of x equal to 2 is equal to one-eighth and probability of k equal to 3 is 3 by 4. Again, if you see that if you sum up you are going to get 1. Now, the question is does this cryptosystem achieve perfect secrecy and the answer is no, but we will see - why no.

(Refer Slide Time: 26:29)



Analysing the modified version

1	2	3
3	1	2
2	3	1

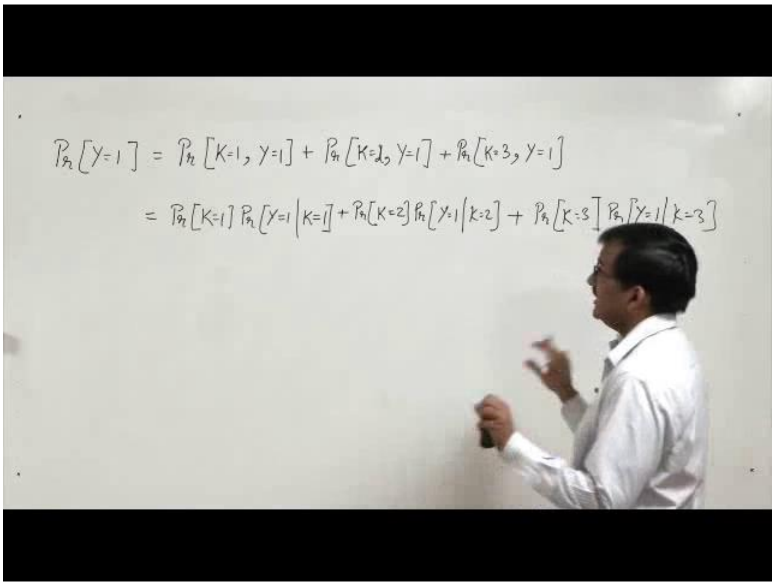
- $\Pr[Y = 1] = \Pr[K = 1]\Pr[X = 1] + \Pr[K = 2]\Pr[X = 2] + \Pr[K = 3]\Pr[X = 3] = \frac{7}{16}$.
- $\Pr[Y = 1 | X = 1] = \Pr[K = 1] = \frac{1}{4}$.
- $\Pr[X = 1 | Y = 1] = \frac{\Pr[X=1]\Pr[Y=1|X=1]}{\Pr[Y=1]} = \frac{\frac{1}{8}\times\frac{1}{4}}{\frac{7}{16}}$
  $= \frac{1}{14} \neq \Pr[X = 1]$.
- Therefore this modified version does not have perfect secrecy.

$\Pr[K = 1] = \Pr[K = 2] = \frac{1}{4}$;
$\Pr[K = 3] = \frac{1}{2}$

$\Pr[X = 1] = \Pr[X = 2] = \frac{1}{8}$;
$\Pr[K = 3] = \frac{3}{4}$.

Now, we again from the same point we will like to now the distribution of cipher text. So, probability of y equal to 1 it is a sum.

(Refer Slide Time: 26:51)

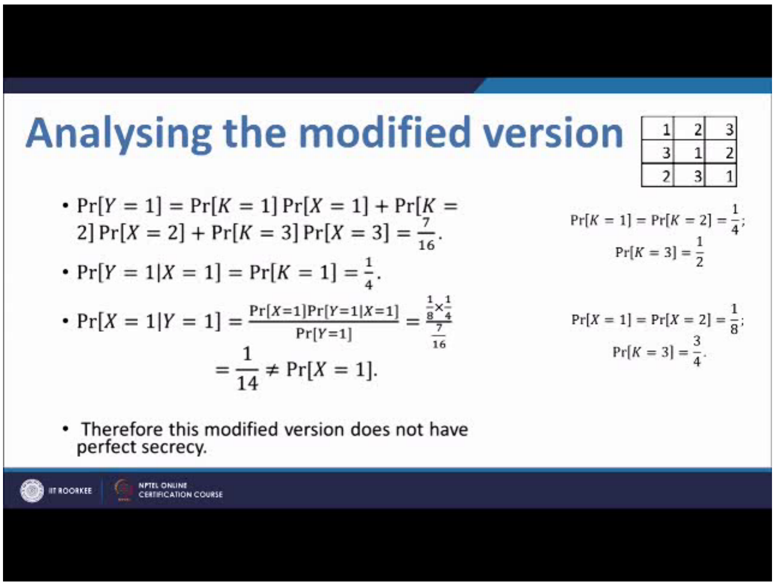


$$\Pr[Y=1] = \Pr[K=1, Y=1] + \Pr[K=2, Y=1] + \Pr[K=3, Y=1]$$
$$= \Pr[K=1]\Pr[Y=1|K=1] + \Pr[K=2]\Pr[Y=1|K=2] + \Pr[K=3]\Pr[Y=1|K=3]$$

Now, let us see why it should be, whatever I have written probability of y equal to 1 and that is equal to probability of k equal to 1 and y equal to 1 plus probability of k equal to 1 and k equal to 2 and y equal to 1 and probability of k equal to 3 and y equal to 1.

Now, this means that this is probability of k equal to 1 and probability of y equal to 1 given k equal to 1. This is equal to probability of k equal to 2 and probability of y equal to 1 given k equal to 2 and lastly it is probability of k equal to 3 and into probability of y equal to 1 given k equal to 3 see. We have this step; we are not yet in the place where we have come to after y equal to probability of y equal to 1 in the slide, we are in somewhat in the intermediate step.

(Refer Slide Time: 28:25)



Analysing the modified version

1	2	3
3	1	2
2	3	1

- $\Pr[Y = 1] = \Pr[K = 1]\Pr[X = 1] + \Pr[K = 2]\Pr[X = 2] + \Pr[K = 3]\Pr[X = 3] = \frac{7}{16}$.
- $\Pr[Y = 1|X = 1] = \Pr[K = 1] = \frac{1}{4}$.
- $\Pr[X = 1|Y = 1] = \frac{\Pr[X=1]\Pr[Y=1|X=1]}{\Pr[Y=1]} = \frac{\frac{1}{8}\times\frac{1}{4}}{\frac{7}{16}}$
  $= \frac{1}{14} \neq \Pr[X = 1]$.
- Therefore this modified version does not have perfect secrecy.

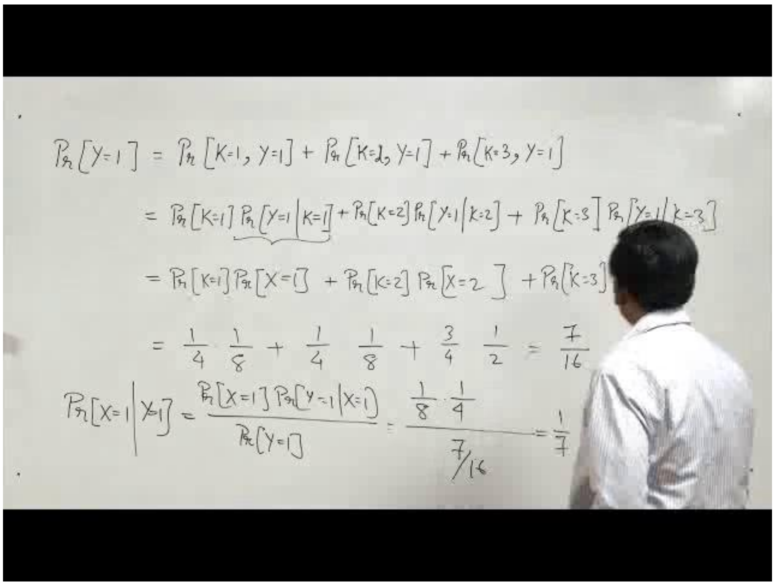
$\Pr[K = 1] = \Pr[K = 2] = \frac{1}{4}$; $\Pr[K = 3] = \frac{1}{2}$

$\Pr[X = 1] = \Pr[X = 2] = \frac{1}{8}$; $\Pr[K = 3] = \frac{3}{4}$.

IIT ROORKEE
NPTEL ONLINE CERTIFICATION COURSE

The next step is to analyze this conditional I am asking a question that suppose, I know that k is equal to 1, what is the probability of getting y equal to 1? If k equal to 1 that means, I am over here, y equal to 1 will occur if x equal to 1 and it will occur only once its x equal to 1 then k equal to. So, this probability is same as getting probability of x equal to 1. So, I will replace this as probability of x equal to 1.

(Refer Slide Time: 29:02)



$$Pr[Y=1] = Pr[K=1, Y=1] + Pr[K=2, Y=1] + Pr[K=3, Y=1]$$

$$= Pr[K=1]\underbrace{Pr[Y=1|K=1]} + Pr[K=2]Pr[Y=1|K=2] + Pr[K=3]Pr[Y=1|K=3]$$

$$= Pr[K=1]Pr[X=1] + Pr[K=2]Pr[X=2] + Pr[K=3]$$

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

$$Pr[X=1|Y=1] = \frac{Pr[X=1]Pr[Y=1|X=1]}{Pr[Y=1]} = \frac{\frac{1}{8}\cdot\frac{1}{4}}{7/16} = \frac{1}{7}$$

Then here we have got probability of k equal to 2 and probability here, I have been told that k is equal to 2 and I am asking a question, what is the probability of getting y equal to 1, if k equal to 2? I am in the second row and y equal to 1 occurs only once because it is a Latin square and it occurs in the second column corresponding to x equal to 2. So, that probability that you will get y equal to 1 given that x equal to 2 is same as getting probability of x equal to 2. So, therefore, here I will write therefore, I will write here x equal to 2 and in the similar way I have got probability of k equal to 3 and here I will write probability of x equal to 3 and therefore, I have to sum up and now it is not. So, nice that everything is same.

So, here we see this is what we have been doing and if you are careful and take the products properly. Here, we have k equal to 1, k equal to a, k equal to 2, one-forth and all that. So, if you do them properly then you will see that you are getting 7 by 16. So, this whole thing turns out to be 7 by 16 because let us see k equal to 1 is one-forth x equal to 1 is one-eighth plus k equal to 2 is one-forth and x equal to 2 is one-eighth plus k equal to 3 is 3 by 4 and x equal to 3 is one-half.

We have to add it, if you add it we should get 7 by 16 and now we have to do the inversion I mean we have to use base theorem. So, we would like to know, what is the probability of x equal to 1 given that y equal to 1? For that in the denominator, we write probability of y equal to 1 which we have already computed in the numerator, we will be writing probability of x equal to 1 into probability of y equal to 1 given x equal to 1, and this is something that we have already known.

We have not seen this given x equal to 1. So, here in the denominator I will put 7 by 16 in the numerator I will put 1 by 8 instead of probability of x equal to 1 and this 1. So, now, again I ask a question that I have got x equal to 1 given x equal to 1 I know x equal to 1 has occurred that means, here now what is the probability that y equal to 1? Now, when you have x equal to 1, y equal to 1 will occur only in 1 place and this is when key k 1 is chosen and the probability of choosing k 1 is 1 forth therefore, I will replace this conditional by 1 forth and I have this and this gives me 1 by 7 and please see that this is not equal to probability of x equal to 1, which is 1 be 8.

So, this is what I wanted to say, thus we have seen that if I fix y equal to 1 then probability that x will be equal to 1 is different, small error over here this is going to be 1 by 14 probability of x given y, x equal to 1 given y equal to 1 is going to be 1 by 14, which is not equal to probability of x equal to 1 and therefore, the cryptosystem under consideration does not achieve perfect secrecy. I will put many problems like this in the assignments for exercise and I will welcome your comments and your questions in the discussion forum. So, this is the end of first week lectures.

Thank you.