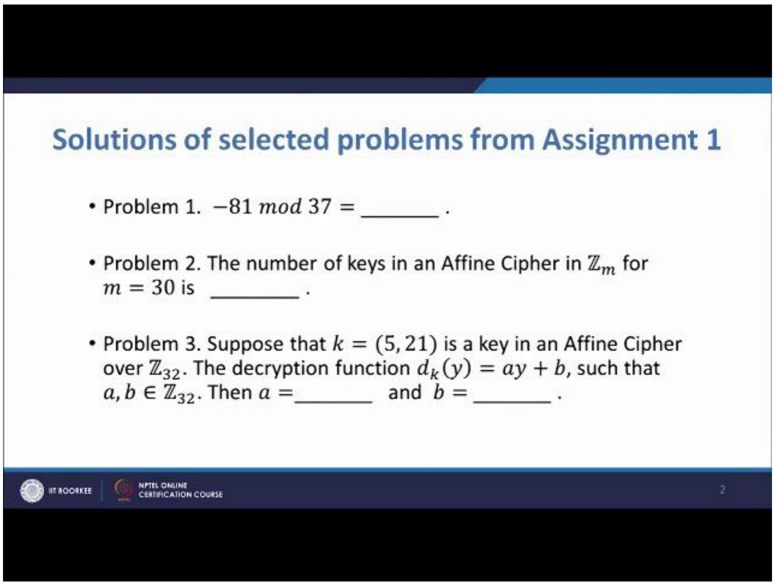
Introduction to Cryptology
Dr. Sugata Gangopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology, Roorkee

Lecture - 10
Problem discussion

(Refer Slide Time: 00:59)

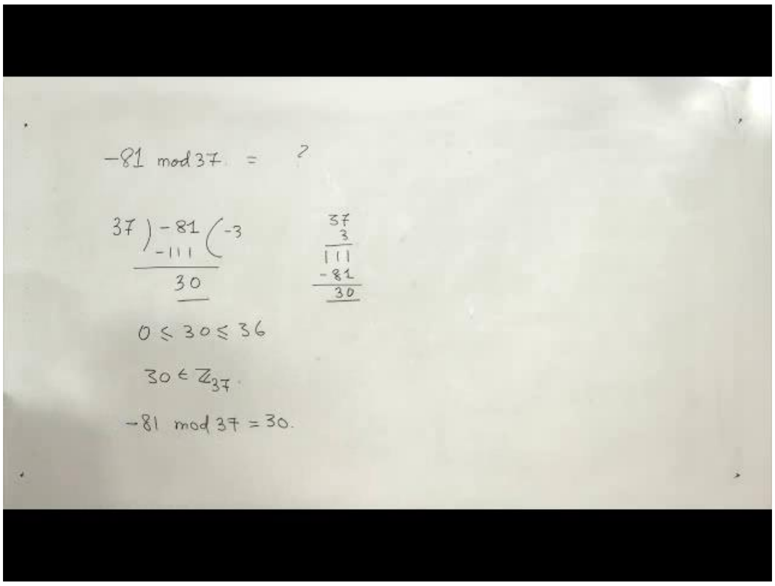


Solutions of selected problems from Assignment 1

- Problem 1. $-81 \ mod \ 37 =$ _______ .
- Problem 2. The number of keys in an Affine Cipher in $\mathbb{Z}_m$ for $m = 30$ is ________ .
- Problem 3. Suppose that $k = (5, 21)$ is a key in an Affine Cipher over $\mathbb{Z}_{32}$. The decryption function $d_k(y) = ay + b$, such that $a, b \in \mathbb{Z}_{32}$. Then $a =$_______ and $b =$ _______ .

Hello, welcome to week 2, Lecture - 5. In this lecture, we will be discussing the problems of assignment 1. I expect that you have already submitted the assignment 1, and you will know your marks in the assignment 1 very soon, but before that let us discuss the problems, and the selected problems and their solutions. The first problem is to find the modular reduction of the number minus 81 modulo 37.

(Refer Slide Time: 01:11)



$-81 \bmod 37 = ?$

$37\,)\,-81\,(\,-3$

-111

30

37

3

111

-81

30

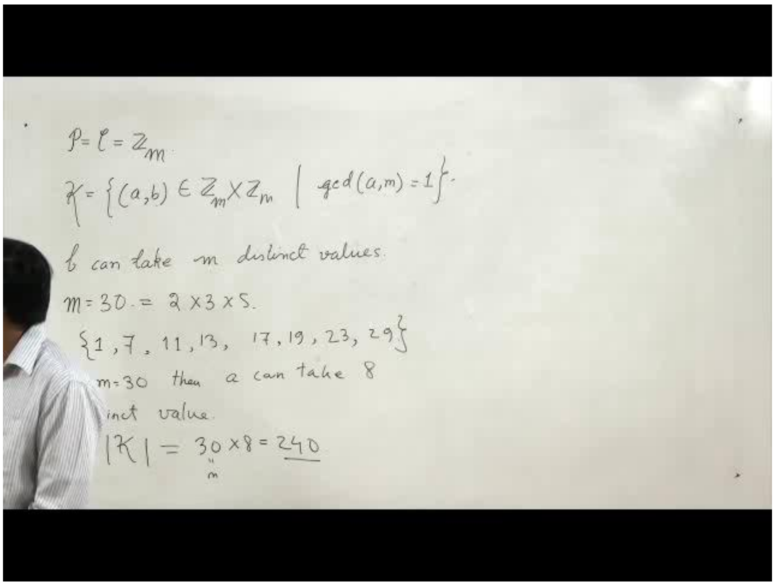
$0 \leq 30 \leq 36$

$30 \in \mathbb{Z}_{37}$

$-81 \bmod 37 = 30.$

So, let us look at this problem. Minus 81 mod 37 is equal to what. Now to solve these problem, we have to divide minus 37 minus 81 by 37 in such way that the reminder after the deviation is complete is something between 0 and 36. Let us start doing that we have 37 over here, and this is minus 81. So, we multiply 37 by 3 to get 111. So, if I multiply 37 by 3, I will get minus 111. Now if I subtract minus 111 from 81, I will get 30. So, I will write 30 here and this is the reminder; and 30 lies between 0 and 36, therefore, 30 is an element of Z sub 37. And therefore, I can say that minus 81 mod 37 is equal to 30. The next problem is on an affine cipher, which is not Z sub 26, but it is Z sub m, where m equal to 30. So, let us look at that.

(Refer Slide Time: 04:22)



$\mathcal{P} = \mathcal{C} = \mathbb{Z}_m$

$\mathcal{K} = \{(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_m \mid \gcd(a,m) = 1\}$.

b can take m distinct values.

$m = 30 = 2 \times 3 \times 5$.

$\{1, 7, 11, 13, 17, 19, 23, 29\}$

m=30 then a can take 8

inct value.

$|\mathcal{K}| = \underset{\overset{\shortparallel}{m}}{30} \times 8 = \underline{240}$

So we are asking to find the number of keys in an affine cipher in Z sub m for m equal to 30. So, in general, let us recall the description of affine cipher over Z sub m. So, P and C that is the set of plain text and set of cipher text is equal to Z sub m; in the set of keys is equal to the ordered pair a, b inside Z sub m Cartesian product with Z sub m, where is the greatest common divisor of a and m is equal to 1 and that is all b varies over set sub m.

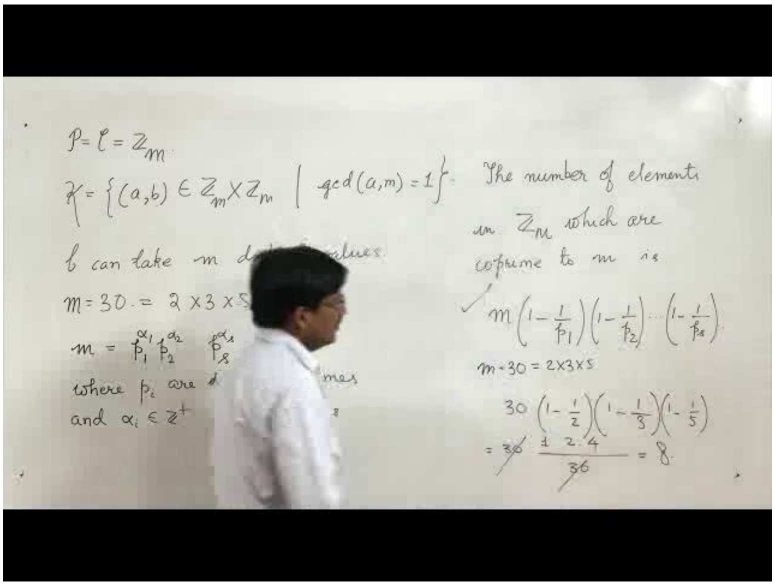
Now, the question is that how many keys are there in general in an affine cipher over Z sub m. Well, if you look at b, when b can vary over Z sub m, therefore the numbers of possible values are b is exactly m. And now what about a, a is an element in Z sub m, but a has to be co prime to m. And therefore, we are coming up against a problem or coming up against the problem or finding out the number of a's inside Z sub m co prime to m. We will discuss a general problem a little later, but let us now take the particular case m equal to 30.

If m equal to 30, then we see that this is 2 into 3 into 5, and we can enumerate directly all the numbers greater than or equal to 1, less than 30 and relatively co prime to 30. So, let us start doing that we have 1, of course and 2 and 3 will not occur, so we will take 1 and then leave out 2, 3, 4, 4 also is not there in our list. So, 4, 5, 5 is not there, 6 does not appear because 6 is not co prime to 30.

Then 7, 7 is of course, co prime to 30 being itself a prime number; 7, 8, 9, 10, 11 again will be there because 11 is prime. Then 12 will not appear then 13 will appear, so I have got 4. Then 14 will not appear, 15 will not appear, because of course, they have got multiple as 2 and 5; 15, 16 will not appear; 17 will appear again; 18 will not appear; 19 is going to appear, because 19 is a prime number 20 will not appear, 21 will not appear, because 3 divides 21 and 30 both. And 21 22 is not going to appear. Then 23 is going to appear; 24 no, 25 no, 26 no, 7 no, 8 no then 29, so the last will be 29.

So, we see that there are exactly 8 numbers relatively co prime to 30 and lying between Z sub 30. Therefore, we can say that if m is equal to a 30, then a can take 8 distinct values, therefore the total number of keys in Z 30. So, keys the number of keys in Z 30 is going to be m that is 30 into 8 this is equal to m equal to 240. So, this is the answer for the second problem. Now we ask a question, can we count the number of keys in an affine cipher in Z sub m for any m and the answer is yes, but I am not go to the theory of finding out all the numbers relatively co prime to a certain number, but I am going to write the result.

(Refer Slide Time: 10:25)



$P = C = \mathbb{Z}_m$

$K = \{(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_m \mid \gcd(a,m) = 1\}$

b can take m d... values.

$m = 30 = 2 \times 3 \times 5$

$m = p_1^{\alpha_1} p_2^{\alpha_2} \; p_s^{\alpha_s}$

where p_i are d... mes

and $\alpha_i \in \mathbb{Z}^+$

The number of elements in $\mathbb{Z}_m$ which are coprime to m is

✓ $m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \cdots \left(1-\frac{1}{p_s}\right)$

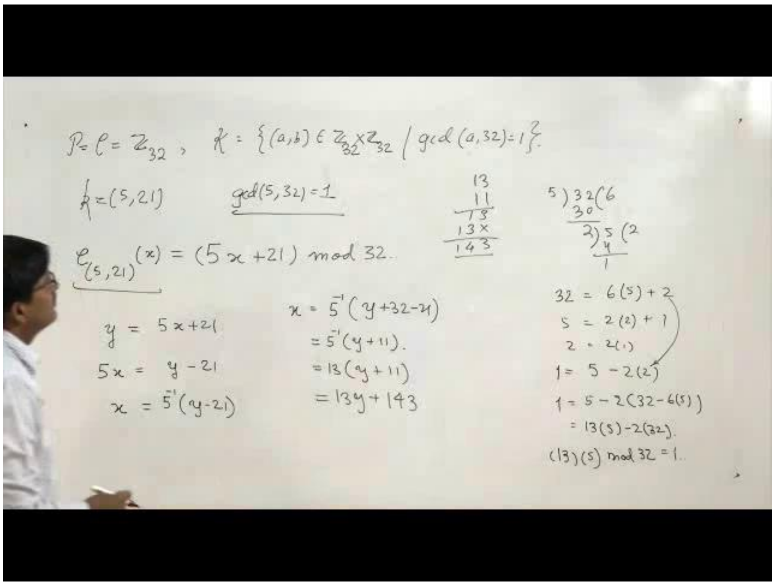
$m = 30 = 2 \times 3 \times 5$

$30\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$

$= \cancel{30} \frac{1 \cdot 2 \cdot 4}{\cancel{30}} = 8$

Let me remove this portion. Now, see suppose that m is equal to something like this. So, if m splits into prime factors like this, P 1 raise to the power alpha 1, P 2 raise to the power alpha 2 so on up to P s to the power alpha s, where P i's a distinct primes and alpha i's are positive integers. Then the number of the number of elements in Z sub m, which are co prime to m is m times 1 minus 1 by P 1 in to 1 minus 1 by P 2 and so on is equal to 1 minus 1 by P s. Now, we can verify this formula, but I am not going to prove this formula right now, but we can verify it. Let us try with m, m equal to 30, which factorizes 2 into 3 into 5. So, this is 30 into 1 minus 1 by 2 1 minus 1 by 3 and 1 minus 1 by 5, this gives us 30 into 30 1 into 2 into 4, which is equal to 8. Please take check this calculation, it is correct and it gives us a number all right.

(Refer Slide Time: 15:01)



$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{32}$, $\mathcal{K} = \{(a,b) \in \mathbb{Z}_{32} \times \mathbb{Z}_{32} \mid \gcd(a,32) = 1\}$.

$k = (5, 21)$ $\quad \underline{\gcd(5,32) = 1}$

$\underline{e_{(5,21)}}(x) = (5x + 21) \bmod 32.$

$y = 5x + 21$

$5x = y - 21$

$x = 5^{-1}(y - 21)$

$x = 5^{-1}(y + 32 - 21)$

$= 5^{-1}(y + 11).$

$= 13(y + 11)$

$= 13y + 143$

$$\begin{array}{r} 13 \\ 11 \\ \hline 13 \\ 13\times \\ \hline 143 \end{array}$$

$5)\,32\,(6$

30

$2)\,5\,(2$

4

1

$32 = 6(5) + 2$

$5 = 2(2) + 1$

$2 = 2(1)$

$1 = 5 - 2(2)$

$1 = 5 - 2(32 - 6(5))$

$= 13(5) - 2(32).$

$(13)(5) \bmod 32 = 1.$

Now let us go onto the next problem. This problem is on an affine cipher on Z sub 32. Now, we are given an affine cipher over Z sub 32. So, when I say that we are given an affine cipher over Z sub 32; that means, my P is equal to Z sub 32, C is equal to Z sub 32, and K is set of ordered pairs of elements of Z sub 32 has the first coordinate is co prime to 32, so that being the case. Let me quickly write the plain text cipher text sets and the key space which is a comma b belonging to Z sub 32 cross Z sub 32 gcd of a comma 32 is equal to 1.

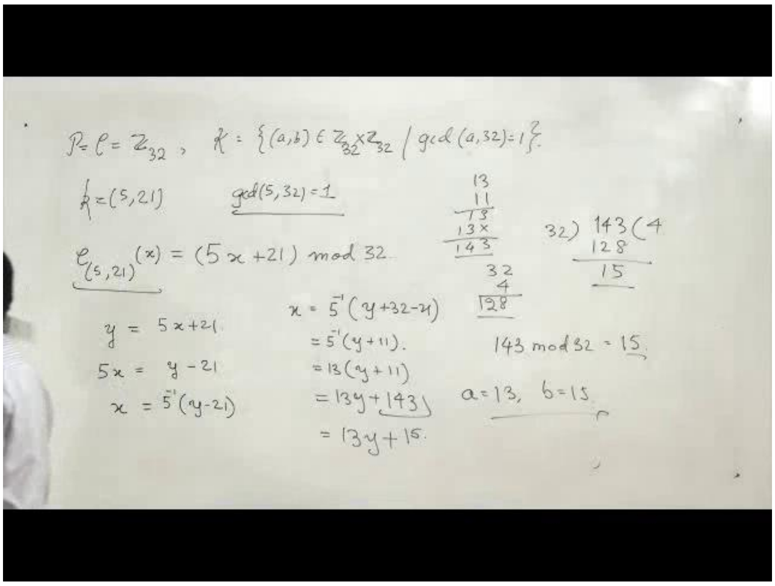
And now I am given a key that is 5 and 21 just to verify that it is a valid key in this affine cipher, we observed that gcd of 5 and 32 is equal to 1, so it is a valid key. And the encryption function will look like this e sub 5 comma 21, x is equal to 5 x plus 21 mod 32, it is not mod 26 for the usual case, it is not mod 32. This is what we have to be careful. And you are going to get this kind of problems in the assignments; you have already got problems in the assignments. And in the next assignment also, you are going to get some problems like this; and in the test you are going to get problems like this. So, please look at it carefully, we have to say mod 32 over here.

Now, I want to know that decryption rule I am saying that the decryption function is d K y is equal to a y plus b where a and b are elements of Z sub 32. So, we have to find the values of a and b between 0 and 31. How to do that we replace this by y and write the formula like this y equal to, and we can more or less you know take for granted that we are doing everything mod 32. So, we do not have to keep on writing mod 32 all the time, and so we have y is equal to 5 x minus 21, we transpose 21 to this side so and then transpose right side and left side. So, we get f x is equal to y minus 21 and then I have to invert 5 modular 32, I know that I can do that because of this. So, I write x equal to 5 inverse y minus 21.

Now I can place small trick over here to make the things possibly little simpler; and write here x inverse equal to 5 inverse sorry it is not x inverse, x is equal to 5 inverse, and then just put a plus 32 because I know that after everything is reduced modular 32 and minus 21. So, I will get 5 inverse y plus 11. And now I have to find 5 inverse. Now for that, we can do this by observation, but we might as well try a general technique that I have discussed before. So, I can write that 5, 32, I divide 32 by 5 to get this, it is 2; and then divide 5 by 2, 4 it is 1.

So, I have a situation like this 32 is equal to 6 times 5 plus 2, then 5 is equal to 2 times 2 plus 1, and of course, then 2 equal to 2 times 1. So, I know that 1 is the greatest common divisor, so I can write 1 is equal to 5 minus 2 times 2, and replace this 2 with this. So, I will write 1 equal to 5 minus 2 times 32 minus 6 times 5, yes, because this 2 is this. So, therefore, 5, so I get 13 into 5 minus 2 times 32 is equal to 1, yes of course, we can check that directly. So, I know that 13 into 5 is equal to 1 13 into 5 mod 32 is equal to 1. So, 5 inverse mod 32 is 13. So, I will put 13 over here. And then y plus 11, so I will get 13 y plus 11 13 into 11, 143 it is 143. And then I have to reduced 1 143 modular 32, 32 4 - 128, 15. So I can write 143 mod 32 is 15 and write it like this – 15.

(Refer Slide Time: 21:56)



$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{32}$, $\mathcal{K} = \{(a,b) \in \mathbb{Z}_{32} \times \mathbb{Z}_{32} \mid \gcd(a,32) = 1\}$.

$k = (5, 21)$ $\quad$ $\underline{\gcd(5,32) = 1}$

$\underline{e_{(5,21)}}(x) = (5x + 21) \bmod 32$

$y = 5x + 21$

$5x = y - 21$

$x = 5^{-1}(y - 21)$

$x = 5^{-1}(y + 32 - 21)$

$= 5^{-1}(y + 11).$

$= 13(y + 11)$

$= 13y + \underline{143}$

$= 13y + 15.$

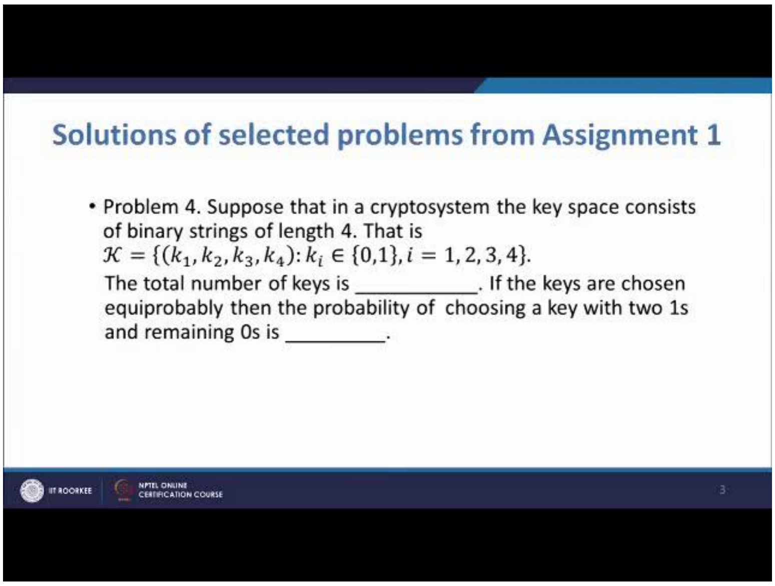
$$\begin{array}{r} 13 \\ 11 \\ \hline 13 \\ 13\times \\ \hline 143 \end{array} \qquad \begin{array}{r} 32 \\ 4 \\ \hline 128 \end{array} \qquad 32)\ 143\ (4 \quad \begin{array}{r} 128 \\ \hline 15 \end{array}$$

$143 \bmod 32 = 15.$

$\underline{a = 13, \ b = 15}$

So we have answer. So, we have got a equal to 13 and b equal to 15 is a answer to the third problem.

(Refer Slide Time: 22:59)

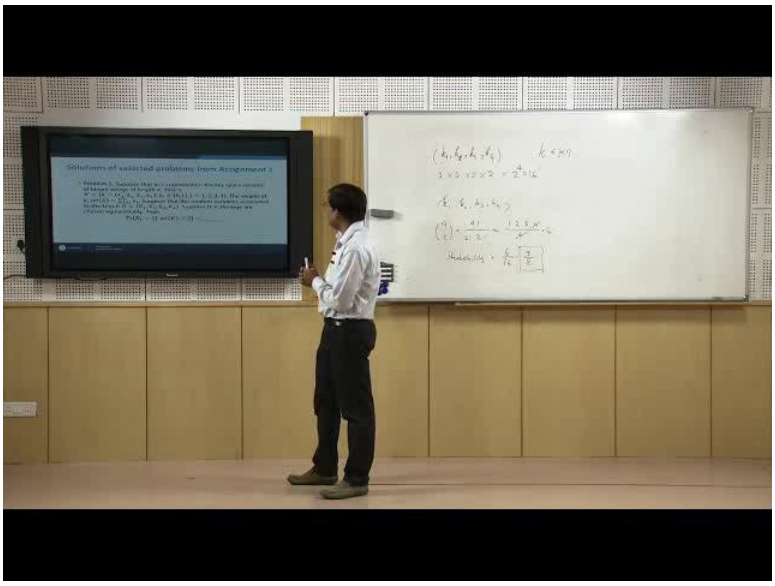


Solutions of selected problems from Assignment 1

- Problem 4. Suppose that in a cryptosystem the key space consists of binary strings of length 4. That is $\mathcal{K} = \{(k_1, k_2, k_3, k_4): k_i \in \{0,1\}, i = 1,2,3,4\}$.
  The total number of keys is ___________. If the keys are chosen equiprobably then the probability of choosing a key with two 1s and remaining 0s is _________.

Problem 4 is a problem on probability. Now, here we are assuming that we have a crypto system whose keys are 4-bit strings or binary strings of length 4. And we are asking some questions related to them. Let us see what happens all right. So, suppose that in a crypto system, the key space consists of binary strings of length 4 that is K is equal to K 1, K 2, K 3, K 4, where K i is 0 1, and i varies over 1, 2, 3, 4, so the question is what is the total number of keys.

(Refer Slide Time: 23:47)



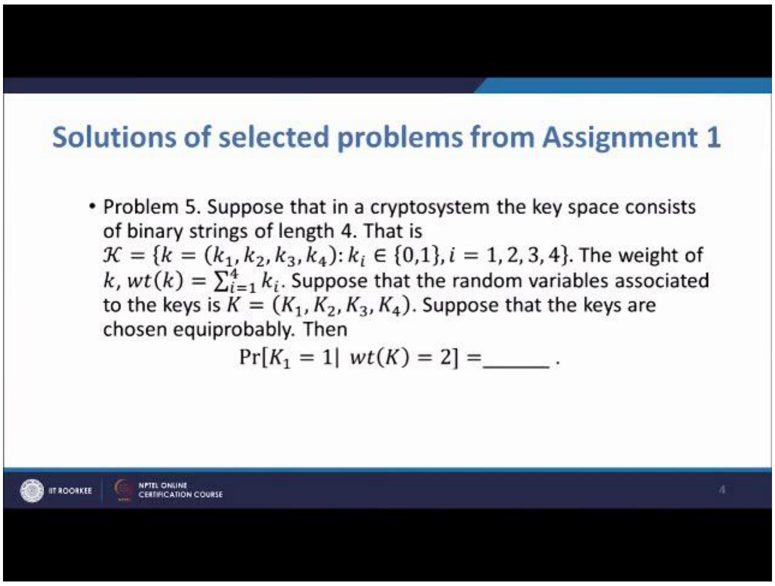
Solutions of selected problems from Assignment 1

(k_1, k_2, k_3, k_4)
$k_i \in \{0,1\}$
$2 \times 2 \times 2 \times 2 = 2^4 = 16$
k_1, k_2, k_3, k_4
$\binom{4}{2} = \frac{4!}{2!\,2!} = \frac{1 \cdot 2 \cdot 3 \cdot 4}{4} = 6$
Probability $= \frac{6}{16} = \boxed{\frac{3}{8}}$

Now, let us look at this counting. I have got keys of this form k 1, k 2, k 3 and k 4 and each k i can take two values 0 or 1. So, first one can be chosen in two ways; the second one can be chosen in two ways; the third one can be chosen in two ways, and fourth one can be chosen in two ways, so the total count is 2 to the power 4 is equal to 16. Now, I have another question that if the keys are chosen equally probably then the probability of choosing a key with two ones and remaining zeros is what. So, now, we are considering the case, where the key is that are getting chosen are having two ones and rest are zeros. So, essentially these are the keys we can say that these keys are of weight 2. We will define weight in the next problem. Now if you have this, so we have to count the number of keys, which have two ones.

Now, let us do that. So, if you if you look at these keys general form of the keys then I have to choose two places and put one there and rest of the places will be filled with zeros. So, the question reduces to the number of ways I can choose 2 places out of 4 places and I know that is 4 choose 2. So, this is 4 choose 2 which is equal to factorial 4 divided by factorial 2 factorial 2, therefore this is 1 into 2 into 3 into 4 divided by 4 which is equal to 6, so there are 6 possibilities of choosing keys with 2 ones and remaining zeros, and these under a total number 16 keys. Therefore, the probability is 6 by 16 which is equal to 3 by 8; this is the solution to the fourth problem.

(Refer Slide Time: 27:10)



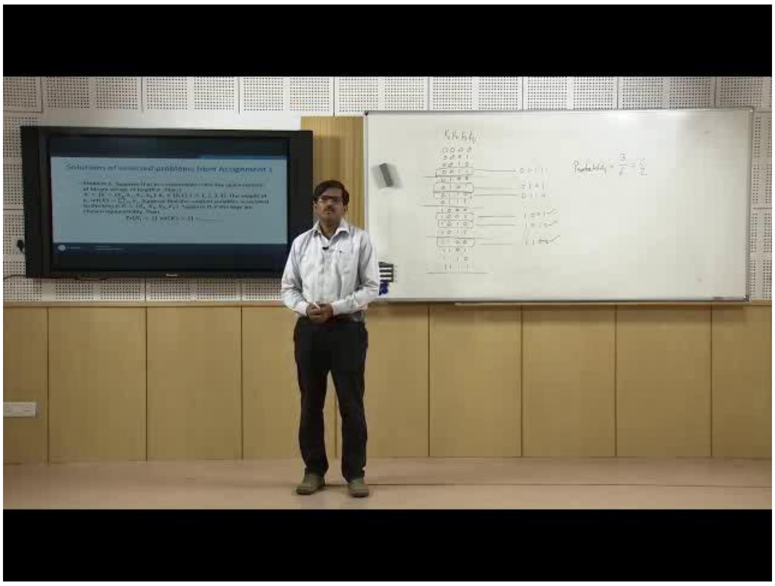
Solutions of selected problems from Assignment 1

- Problem 5. Suppose that in a cryptosystem the key space consists of binary strings of length 4. That is $\mathcal{K} = \{k = (k_1, k_2, k_3, k_4) : k_i \in \{0,1\}, i = 1,2,3,4\}$. The weight of k, $wt(k) = \sum_{i=1}^{4} k_i$. Suppose that the random variables associated to the keys is $K = (K_1, K_2, K_3, K_4)$. Suppose that the keys are chosen equiprobably. Then

$$\Pr[K_1 = 1 | \; wt(K) = 2] = \_\_\_\_\_\_ .$$

Now, problem 5 is an extension of the 4th problem. Now here we are assuming that there is a random variable corresponding to the key and which is written by capital K, since random variables are written with capital letters. And we are defining something called weight of a binary string which is essentially the number of ones that are there in that string. So, it is essentially the integer sum of the components of that string so that is the weight and I am shifting over to the random variables, and I am asking that what is the probability that the first component K 1 is equal to 1 given that weight of K is equal to 2. So, let us try to do these problems. In fact, if I want to do like this, I can do it in the most explicit way of enumerating all the 4-bit strings.

(Refer Slide Time: 28:00)


Solutions of selected problems from Assignment 1
$K_1 K_2 K_3 K_4$
Probability = $\frac{3}{6} = \frac{1}{2}$

Let us write here all right. So, these are all the keys, and let us suppose I write K 1 here, K 2 here, K 3 here and K 4 here. And I am asking what is the probability that K 1 equal to 1 given that the weight is 2. Therefore, I will have to catch those strings with weight 2. So, this is one of those strings, and then I come down the list this is another string this one is the third string, fourth string, then fifth string, and I move down there is another over here, so there are 6 strings which are of weight 2.

Let us write them over here 0 0 1 1, then 0 1 0 1, 0 1 1 0, and here you have 1 0 0 1, 1 0 1 0 and then I have got 1 1 0 0, so the 6 strings. Now this problem is to emphasize the meaning of conditional probability. What I am saying that given that weight of K is 2 that means, that I know that the even that has occurred that is the string that has been chosen is of weight of 2, so this is the certainty.

Now, within that I am asking what is the probability that the string has the first element that is K 1 equal to 1. And then I see that there are 3 such strings and since I know that all the strings such chosen equally probably probability is going to be equal to 3 by 6 which is equal to half. Now this problem can be done by using other formulas of conditional probabilities, but I would like you to check how to do it in the most explicit way, and later on to see whether you can use other formulas that is all for today.

Thank you very much.