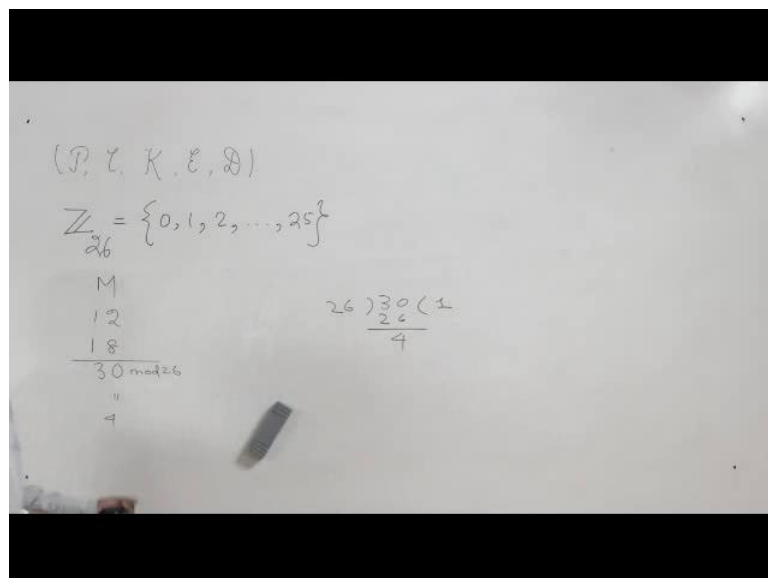


Introduction to Cryptology
Dr. Suguta Gangopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology, Roorkee

Lecture – 03
Affine cipher, Vigenere cipher

Hello, welcome to our course on introduction to cryptology, this is Lecture - 3 of the first week. In the previous lecture, we have studied modular arithmetic. And in this lecture, we will see how modular arithmetic is used in cryptology.

(Refer Slide Time: 00:59)



We start with shift ciphers now as we have seen in our previous lecture that in order to specify a crypto system; we have to specify few sets. The sets are the set of plain text Z ; the set of Cipher sets K , the set of keys and then E the set of encryption functions which are labeled by the keys. And then D the set of decryption functions which are again labeled by the keys we will see that see how it happens in this particular example, but this five tuple is needed to specify a crypto system.

(Refer Slide Time: 01:42)

Shift Cipher

- $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$
- Encryption function: For each key $k \in \mathbb{Z}_m$, $e_k: \mathcal{P} \rightarrow \mathcal{C}$ is defined by
$$e_k(x) = (x + k) \bmod 26$$
for all $x \in \mathcal{P}$.
- Decryption function: For each key $k \in \mathbb{Z}_m$, $d_k: \mathcal{C} \rightarrow \mathcal{P}$ is defined by
$$d_k(y) = (y - k) \bmod 26$$
for all $y \in \mathcal{C}$.

IT ROORKEE | NPTEL ONLINE CERTIFICATION COURSE

Now, our specific crypto system which is called shift cipher; here P, C, K all is equal to Z by 26. So, we have studied Z up m that is a class of residues module m and which can be written as 0, 1, 2 up to m minus 1. In this case, we are taking m equal to 26 in order to associate with the letters in the English alphabet, and then so that is why we are specifying P, C, K as Z by 26. And here please read this m as 26, so our k is Z by 26 which I have writing as Z by m, m equal to 26.

And the encryption function e_k is a function from P to C which is defined by $e_k(x)$ equal to x plus k mod 26 for all x belonging to the k plent x at P, thus the encryption function. And the decryption function is the inverse function which takes encrypted letters to the original decrypted letters, so that is naturally $d_k(y)$ is equal to y minus k mod 26 so that is the description. Now we go to an example, which makes this encryption and decryption clear in the case of shift ciphers.

(Refer Slide Time: 03:42)

Encryption by using Shift Cipher

- Let key agreed upon by Alice and Bob be $k = 18$.
- The sequence of plaintexts Alice intends to send to Bob:
MEETINGTIMEATFOUR
- Encryption and decryption using Shift Cipher.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24	25

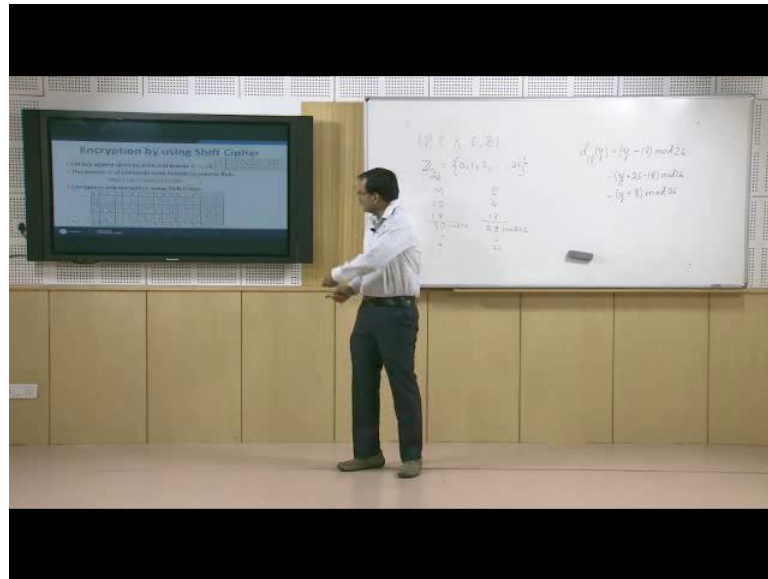
M	E	E	T	I	N	G	T	I	M	E	A	T	F	O	U	R
12	4	4	19	8	13	6	19	8	12	4	0	19	5	14	20	17
18	18	18	18	18	18	18	18	18	18	18	18	18	18	18	18	18
4	22	22	11	0	5	24	11	0	4	22	10	11	23	6	12	9
E	N	W	L	A	P	Y	L	A	K	W	S	L	X	G	M	J
4	22	22	11	0	5	24	11	0	4	22	10	11	23	6	12	9
12	4	4	19	8	13	6	19	8	12	4	0	19	5	14	20	17
M	E	E	T	I	N	G	T	I	M	E	A	T	F	O	U	R

This is our example so this is encryption by using shift ciphers. Now, at the first step, we see that we have encoded the letters into elements of Z by 26, so Z by 26, the set of integers modulo 26 which we denote by 0, 1, 2, dot dot dot up to 25. And here we see the association, A is associated to 0, B is associated to 1, C is associated to 2, D to 3 and so on at the end X is associated to 23, Y is 24 and Z is 25.

Now, suppose that Alice wants send to bob a sequence of plain texts, which ultimately adds up or ultimately becomes a sentence. This is the sentence meeting time at four, suppose she wants to send to bob, the sentence meeting time at four. So, she writes this what she as to do if she is using a shift cipher is that she must agree upon a key with bob. Let us suppose that is in particular case, that key is a tin, so the key k is a tin.

Now she takes this letters, meeting at meeting time at 4, and first if is to encode that to numbers in Z by 26. Now, so see meeting M, M is 12. So, here in this table, we see that M is 12, we write 12 here. E is 4, so we write 4 here. Again E which is 4 then we have T, T is 19, so we write 19 here. I is 8, we have written 8 here. Then N is 13, we have written 13 here and so on we write the whole sequence of letters. Once we do that the next step is the key. The key gets added to each letter, so we are writing 18, 18, 18, 18, and so on and on all the places, we fill with 18. So we know that we have to add 12 and 18, and that addition is going to be modular 26. So, 12 plus 18 let us see what happens to modular 26.

(Refer Slide Time: 07:38)



So, the first letter is M which is 12, and our key is 18. So, if I add, I am going to get 30; and then I have to do $30 \bmod 26$ which is equal to 4. The question is why we can check this by doing usual division, so we have let say here, we have 30, we have 26, 26×1 is 26, the remainder that is 4. So, we write 4 over here. In the case of next letter, we see that we have E. Now, E is encoded to 4, and then I add 18 then have 22. And now if I take $22 \bmod 26$, I get 22 because 22 is 0 times 26 plus 22, so this 22, and that tally's with my table over here. We have to keep do on like this.

Well, you can try it at your home that this to check that each letter is indeed ciphered in the way I have written down over here. And then what Alice might like to do is to shift them over again to letters in the English alphabet and if she does that then we will see that she is going to get something like this 4 here it is 4 for 4 is E, so that means, M is getting transformed to E, E is getting transformed to W, because 22 is W. Again, we encounter E which gets transformed to W, which is 22 and so on. We keep on she might keep write like that and send this segment to bob, and so what bob is getting is E, W, W, L, A, F, Y, L, A, E, W, S, L, X, G, M, J so bob gets that.

Now the question is that what Bob has to do. Now, bob goes back to the decryption function, which is over here. Please see that this is the decryption functions, so in this particular case, the decryption function is going to be like this. So, d the chosen k is 18 and the encrypted plain text letter is y, so I have $y - 18 \bmod 26$.

Now this means that I have to replace minus 18 by something within Z by 26; in order to do that I might add 26, and then take minus 18, so this becomes $y + 8$. And of course, the whole thing has to be reduced mod 26; this also has to be reduced mod 26, so we do this. So, now, we have the decryption function ready for our purpose.

Now, let us go to this table. Now here bob receives E, when bob receives E, he changes E to 4 which is the agreed upon an encoding and then he adds 8 to 4 to obtain 12. And then see that he is obtaining the original symbol back, so he knows the encoding, so 12 is m, so he knows that Alice wanted to send m to him. Similarly, he can do stepwise and get back all the letters that Alice wanted to send him that is the shift cipher.

Now the trouble with shift cipher is that in fact, there are many troubles with shift cipher, but one trouble with shift cipher is that it has got a small key space, so the key space is only Z by 26, so then there are only 26 possible keys. And therefore, attackers just as well check with all possible keys and then he will get a meaning full message. For example, suppose the adversary does not know this key 18, so what he may do, he is to start from 0, so 0, 1, 2 like that and he can do this process over and over again. And suddenly he may get or definitely for 1, he will get this that is 18.

So, essentially, it is starting from zero he is going to go 18 steps, 18 times he can do it, and he can do it essentially by hand, it may take a little more time. So, once he does that he will get the message meeting time at 4. He may, in some cases may get several different meaning full messages, but that probability is very small. So, if Alice is sending a reasonably large amount of plain text cipher text to bob, and attacker is very, it is indeed very less probable that the attacker will get two or more meaning full plain text when he checks with all the possible keys, so that is shift cipher.

(Refer Slide Time: 13:35)

Affine Cipher

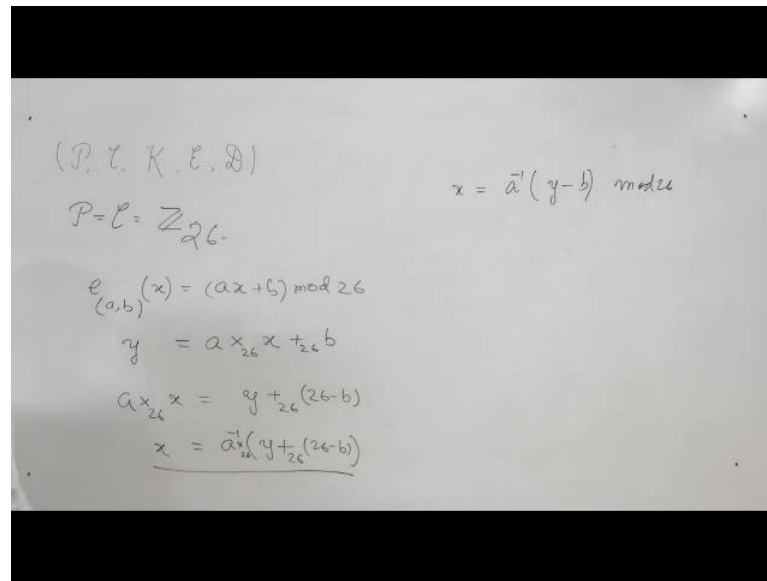
- $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$
- $\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\}$
- Encryption function: For each key $(a, b) \in \mathcal{K}$, $e_{(a,b)}: \mathcal{P} \rightarrow \mathcal{C}$ is defined by
$$e_{(a,b)}(x) = (ax + b) \bmod 26$$
for all $x \in \mathcal{P}$.
- Decryption function: For each key $(a, b) \in \mathcal{K}$, $d_{(a,b)}: \mathcal{C} \rightarrow \mathcal{P}$ is defined by
$$d_{(a,b)}(y) = a^{-1}(y - b) \bmod 26$$
for all $y \in \mathcal{C}$.

IT ROOBBEE | NPTEL ONLINE CERTIFICATION COURSE

Now, what people started thinking is that probably is there any way of extending the key space so because that is one of the problems in case of shift cipher the key space is small. Well, it is possible to do that and for that we come to affine ciphers. In the case of affine ciphers, again we have P and C equal to Z by 26, I am sorry Z sub 26, so we have Z sub 26 for P and C, but the key space is different. So, let us see here P and C both are Z sub 26 and whereas k, k is a subset of the Cartesian product of Z sub 26 by Z 26. So, we have two components of each coming from subset Z 26, but there is a restriction on one of the components particularly first component.

The first component A over here has to be co prime to 26 that is the greatest common deviser of a and 26 has to be 1. We will see why, but let us first check the encryption function. For the encryption function, they use the key a comma B that is in the key space and E sub a comma B is defined as a function from P to C by this E sub a B x is a x plus B whole mod 26. So, let us look at we will look at an example very soon, let us just have an idea of the decryption function, but for that we can we can try to derive the decryption function.

(Refer Slide Time: 15:35)


$$\begin{aligned} & (P, C, K, E, D) \\ & P = C = \mathbb{Z}_{26} \\ & e_{(a,b)}(x) = (ax + b) \pmod{26} \\ & y = a \times_{26} x +_{26} b \\ & a \times_{26} x = y +_{26} (26 - b) \\ & \underline{x = a^{-1} \times_{26} (y +_{26} (26 - b))} \end{aligned}$$

So, what I am saying here is that $e_{a,b}(x)$ which is the key x is equal to $ax + b \pmod{26}$. Now, we change the notation a little, we have done this before. So, we just write like this, this is a and this is the mod 26 multiplication that we have seen in the last lecture. And then we have x plus this is mod 26, and we have b , so this is essentially retransformation for affine ciphers. And let us suppose this Cipher text is y , now we would like to see the scenario where bob has y , and bob wants to calculate x based on the fact that he knows a and b .

So, he can quite legitimately do this, this is y , and well this is 26 and he has to write minus b over here modulo 26 minus b is 26 minus b , he writes this and then he multiplies both sides by the inverse of a . If he does that then he has something like this x is equal to $a^{-1}y + \pmod{26}$, 26 minus B . In fact, this thing we can be written somewhat in another way, because we have to be very careful about these things if my notation this is multiplication mod 26, but we do not have to worry that much of about this. We can even write something like this that x is equal to $a^{-1}(y - b) \pmod{26}$. So, something that is very strictly something like this can be written in a little less strictly like this, it is that is not a problem. So, we have something like this so that is a decryption. Now let us look at an example which will clarify the matter.

(Refer Slide Time: 18:24)

Encryption and decryption by Affine Cipher

- Let $k = (15, 18) \in \mathcal{K}$.
- Encryption: $e_{(15,18)}(x) = (15x + 18) \bmod 26$, for all $x \in \mathcal{P} = \mathbb{Z}_{26}$.
- Decryption:
$$d_{(15,18)}(y) = 15^{-1}(y - 18) \bmod 26$$
$$= (7y + 4) \bmod 26,$$
for all $x \in \mathcal{P} = \mathbb{Z}_{26}$.

IT ROORKEE | NPTEL ONLINE CERTIFICATION COURSE

So, here we take the key to be 15 and 18. Now as we see that 15 is co prime to 26 and there we will see that why that is useful.

(Refer Slide Time: 18:41)

$(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$
 $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$
 $\mathcal{K} = (15, 18)$
 $e_{(15,18)}(x) = (15x + 18) \bmod 26$
 $d_{(15,18)}(y) = 15^{-1}(y - 18) \bmod 26$

$-18 \bmod 26 = (26-18)$
 $= 8$
 $15^{-1} \bmod 26 = 7$
 $26 = 15 + 11$
 $15 = 11 + 4$
 $11 = 2(4) + 3$
 $4 = 3 + 1$
 $3 = 3(1)$

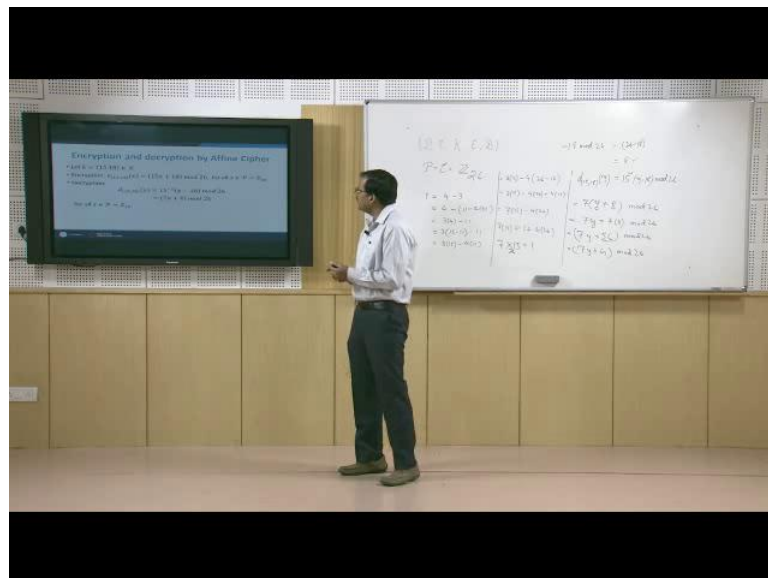
So, here our key is 15 comma 18. So, if we want to encrypt x , then we will have something like this $e_{15,18}(x)$ which is equal to $15x + 18 \bmod 26$. Now let us try to compute the decryption function. So, the decryption function is going to be $D_{15,18}(y)$, this is going to be sorry I write y here for the cipher text, y which is going

to be 15 inverse into $y - 18 \pmod{26}$. Now we can ask that what is 15 inverse and what is minus 18.

Please refer to the previous lecture on the modular arithmetic, we have here minus 18, minus 18 strictly speaking is not an element of \mathbb{Z} by 26, we have to map it to an element of \mathbb{Z} by 26, and we have seen how to do that. And for that we take my right minus 18 mod 26 and which is 26 minus 18 this is a way to map and so I get 8 so that is 8 for me; and here for minus 15 sorry 15 inverse. Now we have also seen in the last lecture on modular arithmetic how to calculate inverse of an element in \mathbb{Z} sub m , if and that is possible only if that element is co prime to m that is it is gcd with M is 1.

In this case, 15 have gcd 1 with 26, so we try to do that. For that we will have to use for that we will have to use the technique that we have studied in the last lecture. Let us do that, so I have got 26, and I want to invert 15 here, so 26 is equal to 15 plus 11, then 15 is equal to 11 plus 4; and then 11 is equal to 2 times 4 plus 3, and then 4 is equal to 3 plus 1. And then of course, 3 is equal to 3 times 1. So, we know that one is the greatest common deviser between 26 and 15.

(Refer Slide Time: 22:18)



We run this thing backward, so we know that 1 is equal to 4 minus 3; and then 3 is over here, we put 3 the value of 3 here. So, 3 is 11 minus 2 into 4, which gives me 3 times 4 minus 11 is 1, of course, that is true. And then we have come up to 4, again now we have

4 over here, so we write 4 as 15 minus 11, so we have got 15 minus 11 minus 11, so this 3 times 15 and then minus 4 times 11.

And now we have to somehow write 11 in terms of 15 and 26, so for that let us use this space, so for that we come here 3 times 15 minus 4 times 26 minus 15, yeah of course, and therefore, we have got 3 times wait a moment yeah so it is 3 times 15 minus 4 times 26 plus 4 times 15 and that gives me 7 times 15 minus 4 times 26. And so I have 7 times 15, well I transpose this part the other side, so I have this is equal to 1 plus 4 times 26.

So, if something like this therefore, I can safely write that 7 multiplications modulo 26, 15 is equal to 1. So, 7 is the inverse of 15 modulo 26 and that is what we get. So, if we now look at this line, it explains so I have to first I replace 15 inverse by 7, and 18 by 8, so let us see so I have a scenario like this. So, I have well d comma 18 y I wrote that 15 inverse y minus 18 mod 26. Now here I replace 15 inverse by 7, and then y and this is 8, I am replacing minus 18 by 8, and I will have this is mod 26. And then I have 7 y, then I have 7 into 8 mod 26, which gives me 7 y plus 56, this whole thing mod 26, and I reduce 56 mod 26 that gives me 4, so 7 y plus 4 mod 26.

So, this calculation, after this calculation, we get the decryption function in a quite nice way, we see that d 15 comma 18 y gives me 7 y plus 4 the whole thing mod 26, we can now calculate the decryption very easily. There are limitations of shift and affine ciphers; the limitations of both the ciphers are firstly that the key space is small.

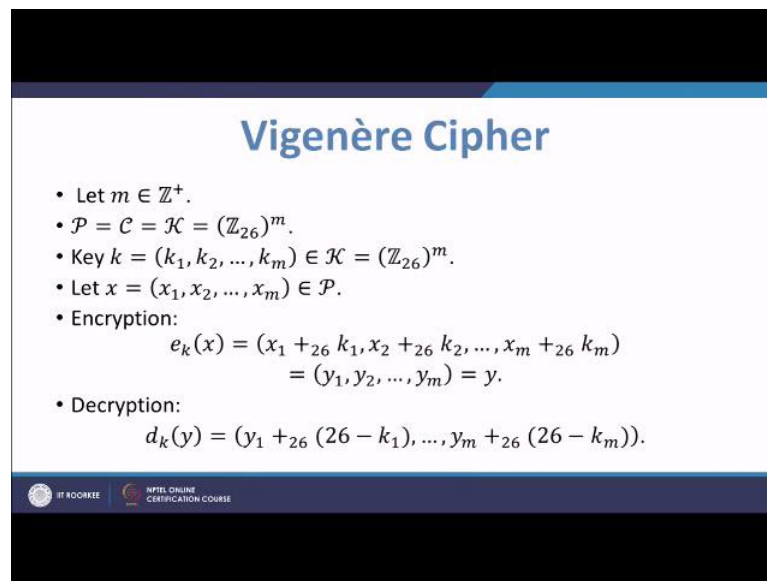
Another limitation is that each letter gets transformed to a specific letter then the key is fixed; that means, suppose in any one of these ciphers A is transformed to M for a particular key then wherever in the sequence A is encountered, A is going to be encrypted to that particular letter let us say M. Now that is the problem because that kind of leaks information and the adversary kind of able to sometimes able to guess the letter, because in any language in particular English letters have a specific frequency of occurrence.

For example, E occur maximum number of times, and then it is followed by T. So, suppose a sequence of plain text is ciphered by using a shift cipher, affine cipher and there is an adversary who keeps on looking at the sequence and then he see that a particular letter is particular cipher text is getting repeated several times much more

many times then the other letters then he will guess probably it is E, then fix E and then try to guess the key and or compute the key and then he will use that key to decrypt.

If he get something mean meaningful that means, he is true, otherwise he will check the next possible next maximally occurring letter and like that. So, it makes the attack much more efficient than exhaustive search. So, these are the limitations.

(Refer Slide Time: 28:52)



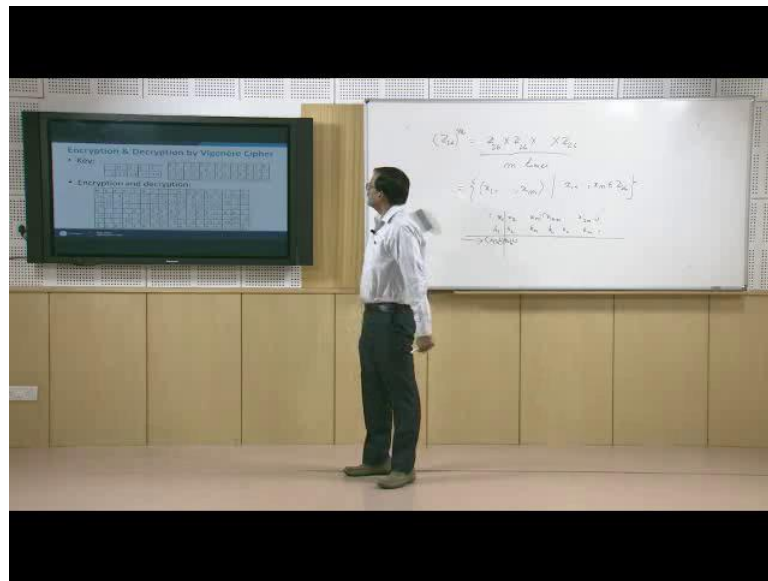
Vigenère Cipher

- Let $m \in \mathbb{Z}^+$.
- $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$.
- Key $k = (k_1, k_2, \dots, k_m) \in \mathcal{K} = (\mathbb{Z}_{26})^m$.
- Let $x = (x_1, x_2, \dots, x_m) \in \mathcal{P}$.
- Encryption:
$$e_k(x) = (x_1 +_{26} k_1, x_2 +_{26} k_2, \dots, x_m +_{26} k_m)$$
$$= (y_1, y_2, \dots, y_m) = y.$$
- Decryption:
$$d_k(y) = (y_1 +_{26} (26 - k_1), \dots, y_m +_{26} (26 - k_m)).$$

IT 800822 NPTEL ONLINE CERTIFICATION COURSE

Now people started thinking that probably we should try to get over that limitation, so there was a cipher which was propose some time at the end of the 19 century 1880s and that is called Vigenere cipher, so that goes like this that here we start with a positive integer m that is an element of Z superscript plus. And P C k all are Z sub 26 to the power m that means, that if they are elements of Z 26 Cartesian product by itself m times.

(Refer Slide Time: 29:27)



So let me write it down over here. So, I have taken a positive integer m and Z_{26} to m is simply $Z_{26} \times Z_{26} \times \dots \times Z_{26}$ this goes m times. So, in a set notation is going to be something like this x_1, x_2, \dots, x_m , where x_1, x_2, \dots, x_m all are elements of Z_{26} . So we will get something like this. And so our P, C, K all are these and the encryption the encryption goes like this suppose I have a stream of plain text, so what I do is that I my plain text are now blocks of length m .

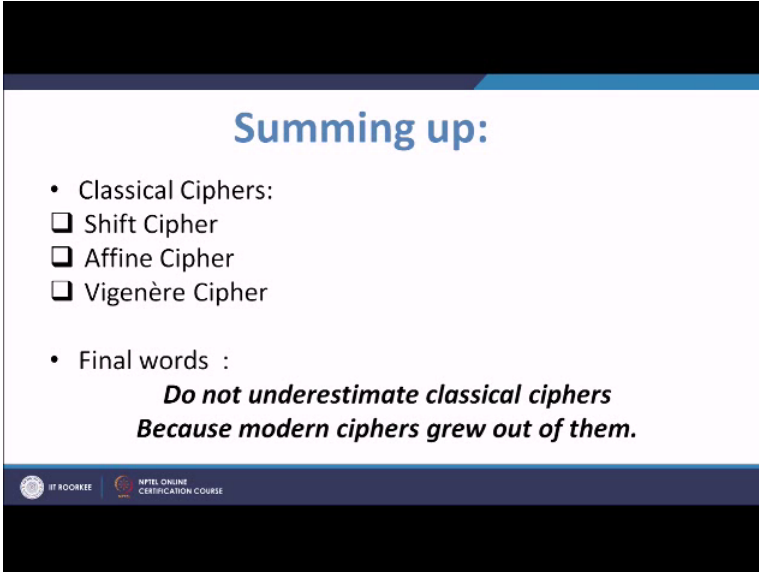
And to each block, I am adding mod 26, the key block k_1 up to k_m , so here the plain text will be like this x_1, x_2 up to so on x_m , then it will be something else $x_1 + m$ let us write like this $m + 1, m + 2$ and so on up to $2m$ like this. So, I have got blocks like this, and key goes like this k_1, k_2 so on up to k_m . Then again I repeat that the same key k_1, k_2 so on up to k_m and so on. And the encryption is computed in this way this one, I will take x_1 substitute $(x_1 + k_1) \bmod 26$ that is $x_1 + k_1 \bmod 26$ $x_2 + k_2 \bmod 26$ and so on so. This is the encrypted stream.

And for decryption, when I get the encrypted sequence, I will just do the inverse function that is addition modular 26 with minus of k_1, k_2 like that here, and I will get the decrypted sequence. This example clarifies whatever we have discussed just now, suppose the key is the segment script, so we write C equal to 2, R equal to 17, Y equal to 24, P equal to 15, and T equal to 19.

Now, let us see the plain text string meeting at meeting time at 4, so we are first of all we are encoding that to element of Z by 26, and then we are putting 2, 17, 24, 15, 19, over and over again 2, 17, 24, 15, 19, 2 17, 24, 15, 19 like that and then we are computing addition modular 26 each time we get another segment and we are getting a string of letters.

If we do the other way round apply the decryption function, so then again we have this and then we will get meeting at 4. Now please see the specialty of Vigenere cipher here for example, we had E twice, once E is getting encrypted as v and the next time E is encrypted as C. And for example, here T is getting encrypted as I, but somewhere down the line you might encounter T, so here T is getting encrypted as well as 17, so that is the specialty of this Cipher.

(Refer Slide Time: 34:09)



Summing up:

- Classical Ciphers:
 - Shift Cipher
 - Affine Cipher
 - Vigenère Cipher
- Final words :
***Do not underestimate classical ciphers
Because modern ciphers grew out of them.***

IIT ROORKEE NPTEL ONLINE CERTIFICATION COURSE

So, in today's lecture, we have covered ciphers which are technically called classical ciphers, we have seen shift cipher, affine cipher and vigenere cipher. We will move on to more modern ciphers soon, but my final words here do not underestimate classical ciphers, because modern ciphers grew out of them. We will move on to modern ciphers within a very few lectures that is the end of Lecture - 3 of week 1.

Thank you.