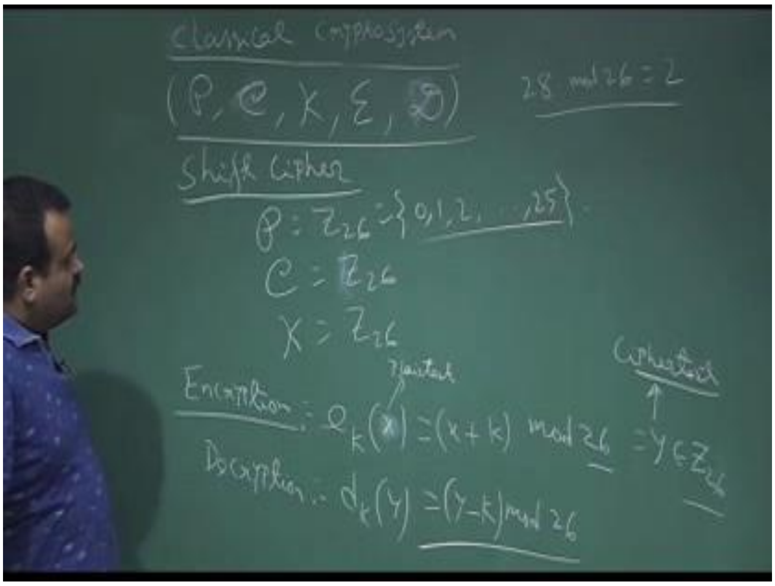
Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 02
Classical Cryptosystem

So we will see the class some of the classical cryptosystems, which are typically old cryptosystem or conventional cryptosystem.

(Refer Slide Time: 00:29)


Classical Cryptosystem
$(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$
28 mod 26 = 2
Shift Cipher
$\mathcal{P} = \mathbb{Z}_{26} = \{0, 1, 2, \ldots, 25\}$
$\mathcal{C} = \mathbb{Z}_{26}$
$\mathcal{K} = \mathbb{Z}_{26}$
plaintext
Ciphertext
Encryption: $e_k(x) = (x + k) \bmod 26 = y \in \mathbb{Z}_{26}$
Decryption: $d_k(y) = (y - k) \bmod 26$

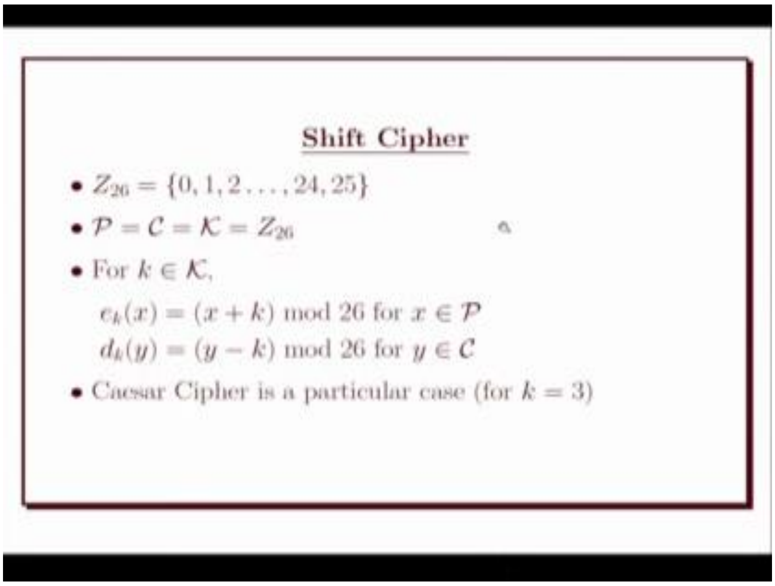
So, we start with a; so we know that cryptosystem is a five tuple P, C; plain text space, cipher text space, key space and set of encryption algorithm, set of decryption algorithm. So, we will start with the shift cipher; which is a classical cryptosystem which is very old cryptosystem. So these are all symmetric key cryptosystem, conventional cryptography. So, in here plain text space is Z 26; which is basically 0 to 25, so that means, if you take any integer and if we divide that integer by 25; 26 then it will give us the remainder from 0 to 26.

Say for example if we have 28, now if we divide this by 26; that means, 28 mod 26 is basically 2. So, this is basically if we divide any integer by 26, you will get this remainder 0 to 25, so this is typically called Z 26 set. So, this is our plain text space and this is also our cipher text space, so cipher text space is also Z 26 and the key space is also Z 26. So, we define the plain text space, cipher text space, key space and now we need to choose an encryption algorithm for this shift cipher. So in shift cipher, encryption algorithm is like this, the message is so e k; so this is the encryption function, so this is shift cipher encryption function. So, e k of m; m is the message which is basically or a naught k we can take by the plain text, so if it is basically x plus k; x is 26, Z 26, k is Z 26, but x plus k could be more than 26 because if it is 20 then it is 40; it is just addition (Refer Time: 03:05) addition, so 40 but 40 is not belongs to g because our cipher text space is Z 26. So, to make it Z 26 what we need to do? We need to take the mod, so mod 26; so this is the encryption function.

So, if you take the mod 26 then this is our y and y very much belongs to Z 26, this is the cipher text. So, this is the plain text x and this is the y is the cipher text, so this is the encryption, this is the shift cipher encryption and what about decryption. So, decryption is basically d k of; so for decryption input is y, y is the cipher text with the same key; this key should be same, it is basically y minus k again we have to take the mod 26, so this is the decryption function of shift cipher.

Now for k is equal to 3; this is called Caesar cipher. So, let us take.

(Refer Slide Time: 04:30)



Shift Cipher

- $Z_{26} = \{0, 1, 2 \ldots, 24, 25\}$
- $\mathcal{P} = \mathcal{C} = \mathcal{K} = Z_{26}$
- For $k \in \mathcal{K}$,

  $e_k(x) = (x + k) \bmod 26$ for $x \in \mathcal{P}$

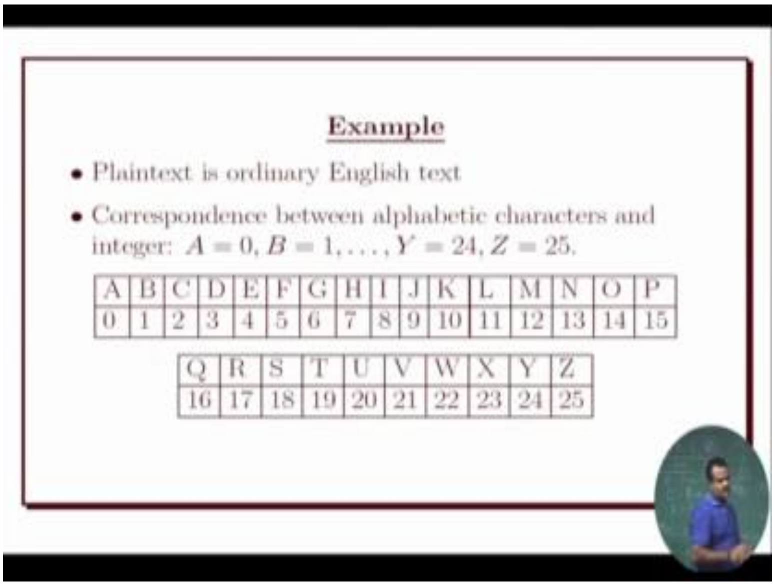
  $d_k(y) = (y - k) \bmod 26$ for $y \in \mathcal{C}$
- Caesar Cipher is a particular case (for $k = 3$)

So, this is the shift cipher, so we are taking Z 26 which is basically this set and these are all plain text, cipher text, key space and if we choose a key from this Z 26 and this is the encryption just add this key with the number and we take mod 26. Why this 26? Because we will be seeing that, we will be encrypting our plain text as the English alphabet, English text.

So if you take the English alphabet, it is starting from a to z; so A to Z means it is basically how many 26 elements are there, so 26 letters are there A, B, C, D up to Z. So, 26 letter; we can have 1, 2 also this is typically A, this is B, this is C and this is Z. So, this is we can have a one to one corresponding, so we can have a one to one correspondent between Z between this English letter to A B; this is the English alphabet, Z; Z 26; by this correspondence.

So, 0 means A, 1 means B; so we want to encrypt English letter. So, that is why we want to take Z 26 because our English alphabet are basically 26 letters are there. So, 26 later means we can just typically assign 0 to 25, so 26 letter. So, this is the shift cipher, so we just take the 26 and we add in mod 26 and Caesar cipher is a particular case of Caesar cipher and k is 3.

(Refer Slide Time: 06:17)



Example

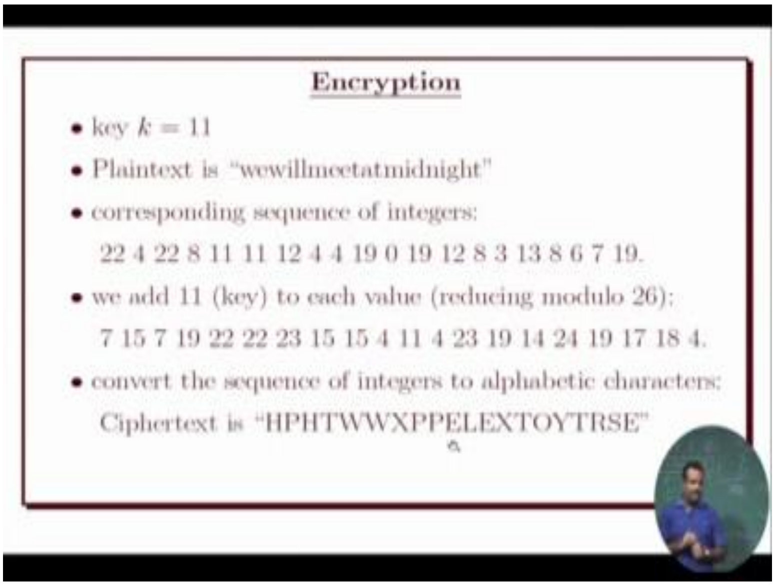
- Plaintext is ordinary English text
- Correspondence between alphabetic characters and integer: $A = 0, B = 1, \ldots, Y = 24, Z = 25$.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Q	R	S	T	U	V	W	X	Y	Z
16	17	18	19	20	21	22	23	24	25

So this is the example, suppose our plain text is the English text; we want to use the English text as our plain text and now we have this correspondence between alphabet character between the set of all alphabet A to Z and Z 26. So, A means 0, B means 1, C means 2, D means 3, E means 4 like this, so this way we continue; this is the one to one correspondence. So, 23 means X, W means 22. So, this is the one to one correspondence we are going to use for our encryption and decryption process, so that is why we will take that Z 26; mod 26 that is the reason we have to take mod 26.

(Refer Slide Time: 07:00)

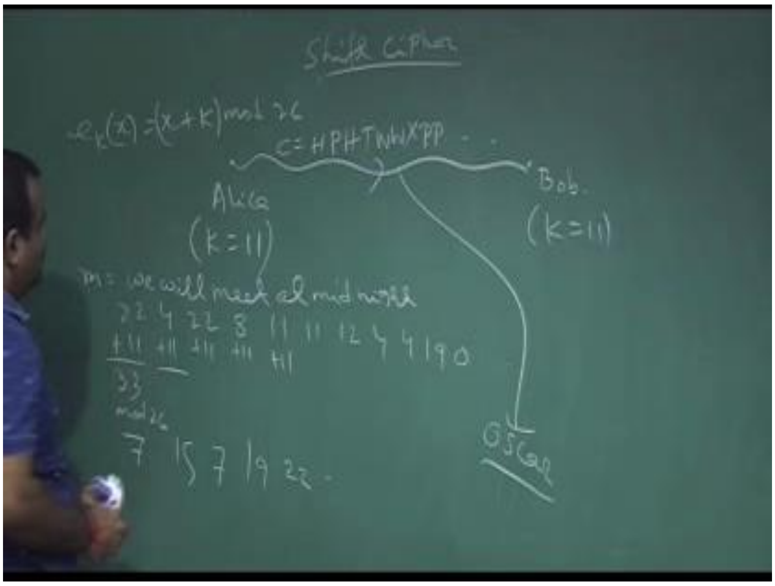


Encryption

- key $k = 11$
- Plaintext is "wewillmeetatmidnight"
- corresponding sequence of integers:
  22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19.
- we add 11 (key) to each value (reducing modulo 26):
  7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4.
- convert the sequence of integers to alphabetic characters:
  Ciphertext is "HPHTWWXPPELEXTOYTRSE"

So now let us take an example of encryption, suppose we choose Alice and Bob; they choose the key.

(Refer Slide Time: 07:25)



So key has to coming from the Z 26 key, so this is the two party; Alice and Bob and they are using the shift cipher for their encryption purpose. So, now suppose they agree if we take among key k is equal to 11; so, they sum up decide that they are going to use k is equal to 11. Now suppose Alice want to send a message; this plain text that we will meet at midnight. Suppose this is the message Alice want to send to Bob, so this is our plain text; we will meet at midnight; so this is the plain text Alice wants to send to Bob.

So, what Alice will do; Alice will just convert it into the corresponding size; corresponding letters I mean from Z 26 because for encryption we need to do the addition. So, we cannot do the addition in the alphabet, shifting we can do, so this is basically letter shifting; if we add 3; that means, A is going to D, so this way; Caesar cipher is 3 shifting so; that means, a is going to B, C, D, so this way. So, Caesar cipher was invented before the shift cipher, but it was not coming from the Z 26 sense it was just coming from the shifting the alphabet.

So, basically we will convert this in, so we will meet at midnight. So, we convert this to corresponding the sequence of integers So, W means 24, so if you just remember this correspondence, so W means 22; so this is 22 and E means what? E means 4, so this is the 4. Again W 22 I; I is what, I is basically 8. So, L if we see these correspondence L is 11, so we have two L; 11, 11. So, we convert everything into the integer, so that by that correspondence between alpha Z of alphabet to Z 26 and then we have chosen a key k, so that is our secret key.

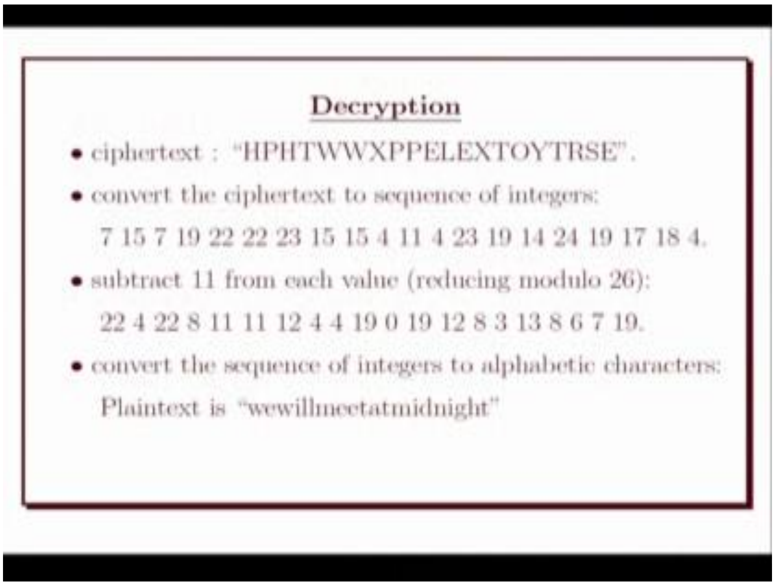
So, we just add this key with this, so basically we will be getting this. So, if we add 11 with 22, so it is basically coming out to be 33, but 33 is what. So, basically we are having, so let us just do it. What is the plaintext? Plaintext is we will meet at midnight, so this is the plain text. So, just if we follow the one to one correspondence between these alphabets and the Z 26, we have 24, 4, 24 then 8, 11, 11 then 12, 4, 4, 19, 0 like this. So, now key is 11, so we will just add 11 with all of this.

So, our encryption algorithm is basically x plus k mod 26, so after these addition; we have to take the mod 26. So, this is 33; so 33 mod 26, so this will give us basically 7, so this has no problem; this is 15; so, this is again 33 mod 7; so this is 19 last 11 like this 22 like this. So, this is the way we just get the cipher text stream; I mean this is the cipher text stream integer in form 7, 15, 7, 19, 22, 22 like this.

So, this is coming out from this plain text by adding 11 with 11 is the key by adding 11 and mod 26 we get this cipher text integer and now we convert this into the alphabet again. So, 7 means basically let us come back to the one to one correspondence; 7 means basically H. So, H and again 15 means; let us come back 15 means P, so this is P again 7 means H like this. So, this is the cipher text corresponding to these plain text, we will meet at midnight. So, these cipher text is sent to Alice over this public channel, the two Bob by the Alice over this public channel this is H P H T W W X P T like this.

So, this is I mean formed by, so Oscar is having access to this, so Oscar is seeing this cipher text. So, this is a cipher text and this is the plain text or the message and this is the cipher text. So, it is very difficult to guess from here what was the plain text, so this is the shift cipher.

(Refer Slide Time: 13:25)



Decryption

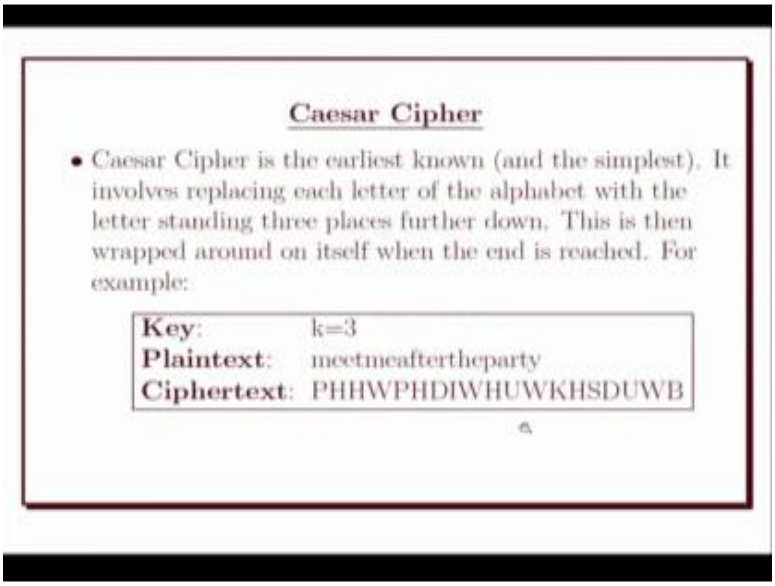
- ciphertext : "HPHTWWXPPELEXTOYTRSE".
- convert the ciphertext to sequence of integers:
  7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4.
- subtract 11 from each value (reducing modulo 26):
  22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19.
- convert the sequence of integers to alphabetic characters:
  Plaintext is "wewillmeetatmidnight"

Now how Bob has to get back the message. So, what Bob will do after receiving this cipher text? Bob will just convert it into the integer again. So, H means 7, P means 15 again H means 7, 19 like this, so Bob will get the integer again the sequence of integer and now what has to apply the decryption algorithm, so decryption was like this d k of; so Bob has to use the same key d k of y; y minus k mod 26. So, Bob will just convert this H to, so H is 7 then P is basically 15, 7 and then 19 like this.

So, what Bob will do? Bob will decrypt minus 11, minus 11, minus 11, minus 11, so every time it has to be mod 26. So, if you do this; this will give us 22, this will give us 4, this will give us 22 again, this will give us 8 dot dot dot like this. So, just if we convert this integer into the alphabet again, so 22 means W, so this will give us we will meet at midnight, so this will give us the original plain text back.

So, this is the decryption process, so this is typically done by the Alice. So, Alice is just subtracting 11 the key savior here the shared between Alice and Bob and get back the corresponding plain text and then Alice convert this integer to the alphabet and get back the message sent by the Alice. So, this is done by the Bob; this decryption, so Bob will get back the message.

(Refer Slide Time: 15:34)



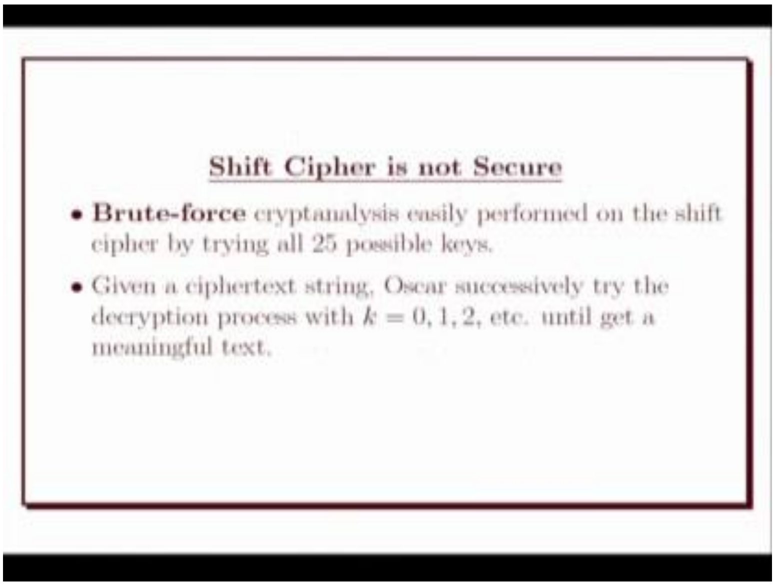
Caesar Cipher

- Caesar Cipher is the earliest known (and the simplest). It involves replacing each letter of the alphabet with the letter standing three places further down. This is then wrapped around on itself when the end is reached. For example:

Key:	k=3
Plaintext:	meetmeaftertheparty
Ciphertext:	PHHWPHDIWHUWKHSDUWB

So as we know Caesar cipher is a particular case of this shift cipher where we choose k is equal to 3. So, just basically we are shifting all the alphabet are shifting three positions. So, if we have a plain text like A, so A will shift to three position, so A is 0, so 0 plus 3; it is basically 3, so, 3 is basically D. So, A, B, C, D; so A is coming if the plain text is A then the cipher text is D. So, we are basically shifting the alphabet position three times, so this is the Caesar cipher which is a particular case of shift cipher by choosing k is equal to 3. So, if this is our plain text then the cipher text will be the same; this thing the cipher text and then for decryption again you have to come back, so this is the circular shifts. So, if we have Z so Z means A B C, so Z is the last one; so Z will shift to three bit next, so this is the circular way shifting.

(Refer Slide Time: 16:54)



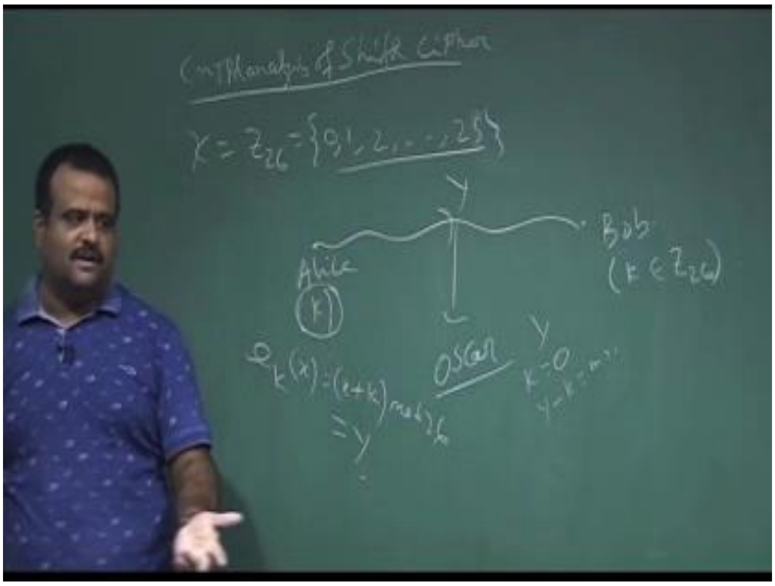
Shift Cipher is not Secure

- **Brute-force** cryptanalysis easily performed on the shift cipher by trying all 25 possible keys.
- Given a ciphertext string, Oscar successively try the decryption process with $k = 0, 1, 2,$ etc. until get a meaningful text.

So, now come back to the security issue of this shift cipher, where the shift cipher is secure or not. So we want to talk about cryptanalysis of shift cipher that Oscar will be doing, so cryptanalysis of shift cipher where the shift cipher is secure or not. So, what Oscar is getting? Oscar is getting a basically cipher text, but this cipher text is basically coming from the plain text which is a typically English text we know, for this case.

Now, what is the key space?

(Refer Slide Time: 17:43)


Cryptanalysis of Shift Cipher
$K = Z_{26} = \{0, 1, 2, \ldots, 25\}$
y
Bob
($k \in Z_{26}$)
Alice
k
$e_k(x) = (x+k) \bmod 26$
$= y$
Oscar
y
k = 0
y − k = …

So, Oscar knows the key space is basically Z 26, so key is basically from 0 to 25. So, Oscar knows the key is coming from 0 to 25, Oscar does not know which one they have used as a key. So, Alice and Bob they are communicating, they have chosen a key which is from Z 26 and this is secret Bob is not knowing, so they are communicating.

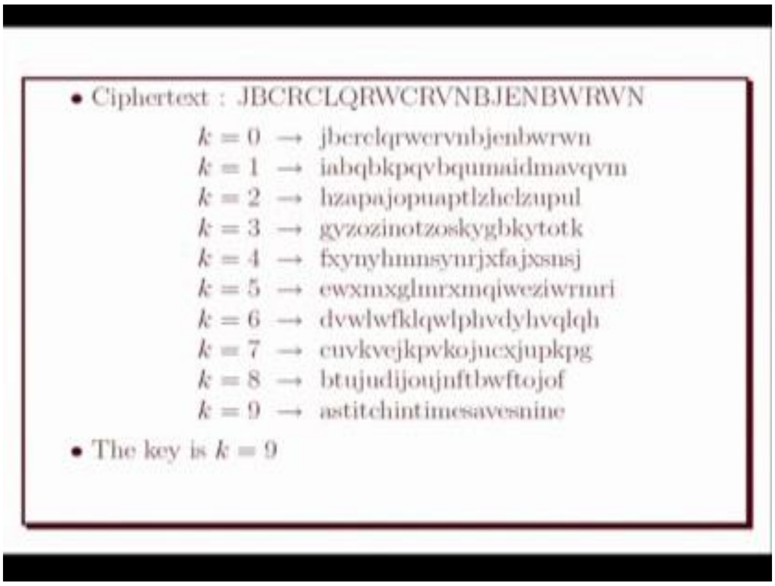
So now this channel is typically captured by the Oscar, this is a public channel nothing to capture, I mean this is everything is public in this channel. Oscar knows that they are using shift cipher; Oscar knows that this in text was encrypted by this way mod 26 and this is the Y, so Oscar is getting Y. So, only thing what Oscar is not knowing is the secret key, Oscar does not know what is the value of key, but Oscar knows that they have used shift cipher, this encryption algorithm must be public.

So we must, we cannot hide that what algorithm we have used, whether we are multiplied, whether we have added, whether we have subtracted that you cannot hide; that should be public; this is the model we use this is the Kirchhoff’s model. So, we cannot say that; I will not reveal whether I have used addition or I have used multiplication on I reversed the bits, so that you cannot say. So, that algorithm must be public, so whatever we have used for the encryption that algorithm is public; one thing is reduce the k, this is the secret.

So, this k is the typical secret, so now well Oscar is getting this y; which is the cipher text and Oscar knows it is coming by adding with the plain text, but Oscar does not know how much it has added; that means, Oscar does not know what is the value of key, but Oscar knows the key is coming from this set; 0 to 25. So, Oscar can try for all possible case, so this is the brute force of way or exhaustive search. So, Oscar can try for K is equal to 0 and Oscar will check Y minus K and N whether any meaningful thing is coming out to be this; like this.

So, Oscar will try for all possible case; k that here key space is very small, it is just 26, so just 26 attempt Oscar can guess or Oscar can reveal the plain text. So, this is the Brute-force method, so just we have to perform the 26; Oscar need to perform the 26 possibilities of the key. So given a cipher text string, Oscar successfully try the decryption process with k is equal to 0, 1, 2 like this until get the meaningful text because we know that our encryption is English text, so once Oscar get a meaningful text; Oscar will stop.

(Refer Slide Time: 21:21)



- Ciphertext : JBCRCLQRWCRVNBJENBWRWN

$$\begin{aligned}
k = 0 &\rightarrow \text{jbcrclqrwcrvnbjenbwrwn}\\
k = 1 &\rightarrow \text{iabqbkpqvbqumaidmavqvm}\\
k = 2 &\rightarrow \text{hzapajopuaptlzhclzupul}\\
k = 3 &\rightarrow \text{gyzozinotzoskygbkytotk}\\
k = 4 &\rightarrow \text{fxynyhmnsynrjxfajxsnsj}\\
k = 5 &\rightarrow \text{ewxmxglmrxmqiweziwrmri}\\
k = 6 &\rightarrow \text{dvwlwfklqwlphvdyhvqlqh}\\
k = 7 &\rightarrow \text{cuvkvejkpvkojucxjupkpg}\\
k = 8 &\rightarrow \text{btujudijoujnftbwtojof}\\
k = 9 &\rightarrow \text{astitchintimesavesnine}
\end{aligned}$$

- The key is $k = 9$

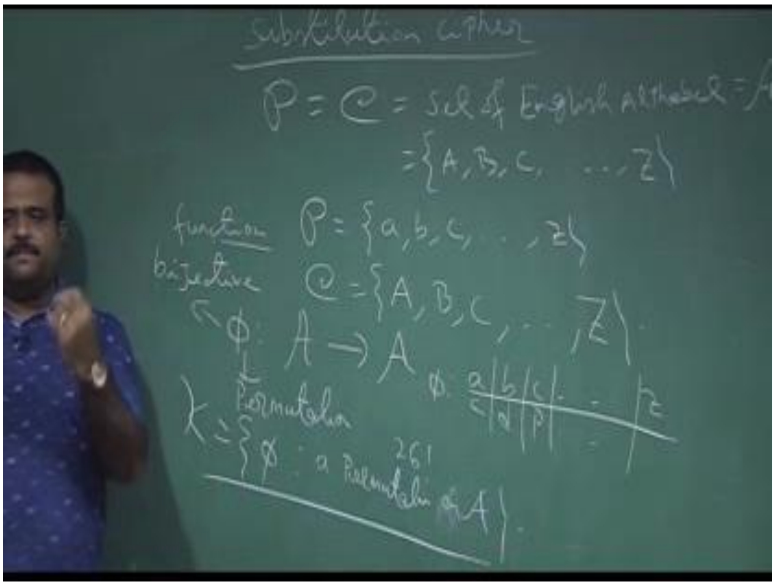
So, let us take an example, so here is an example suppose Alice and Bob they are communicating with each other and this is the cipher text Alice sent to Bob and they have using the shift cipher; this is public, they are using shift cipher; Oscar knows that they have used shift cipher, only Oscar does not know is the key; how much they are added the value of k.

So what the Oscar will do; this is the Brute-force way or the exhaustive search ways. So, Oscar will try for k is equal to 0, this is no change because this is the same. This is the decryption Oscar is going k is equal to 1, so Oscar will convert this into the digit and Oscar will subtract 1, mod 26, Oscar get something this is also nothing too much interesting, k is equal to 2; Oscar will choose this is also not much interesting. Then k is equal to 3 also; no meaningful text is getting, k is equal to 4 something no meaningful text, k is equal to 5; no meaningful text, k is equal to 6; no then this way Oscar will continue and suddenly at k is equal to 9 Oscar will realize; yes we got a meaningful text; so this is the plain text.

So, and Oscar is getting the key, so Oscar is now got the key. So, Oscar now have the key which is shared between Alice and Bob secretly, so that key is 9 here. So, now, Oscar will come to know everything about what they are communicating. So, this message is already revealed, Oscar got this message this is a meaningful message, so Oscar is ensured that the key is 9. So, now for the further communication also Oscar will just use the decryption algorithm of the shift cipher and Oscar will get back the message. So, this is the crypt analysis on shift cipher and that is why shift cipher is not secure. So, shift cipher is not secure because the problem is with the key size; key size is very small.

So now what to do; so shift cipher is not secure, so just by 26 attempt Oscar can get the key. So, now we will talk about something more key space; so this is also a classical (Refer Time: 24:03) system which is called substitution cipher.

(Refer Slide Time: 24:10)

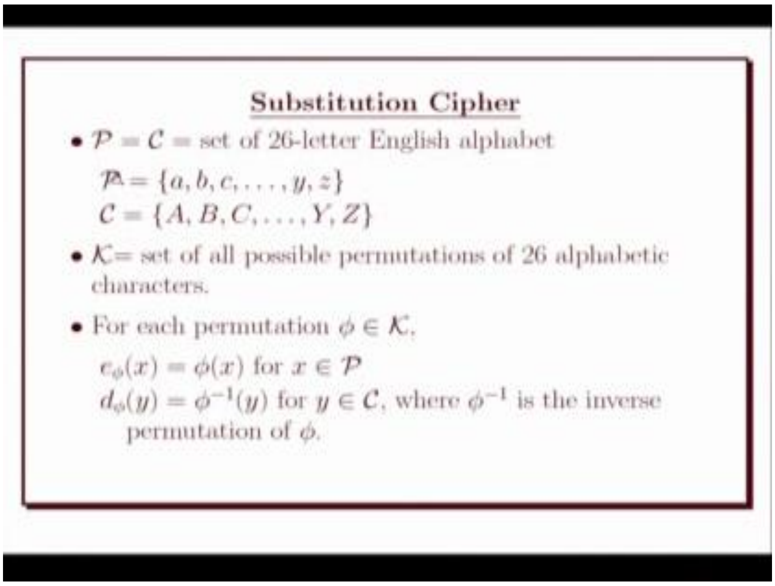


So, here key space and cipher text space is set of all alphabets; set of English alphabet, so; that means it is basically this set A, B, C, D like this up to Z. So, for P we use the small letter just for the; so the difference between the plain text and this is the plain text we use typically small letter for P and for C we use the capital letter.

Now this is the plain text space, this is the cipher text space, so these are all English alphabet. Now our key space is basically a key is a typically a permutation on this alphabets. So, permutation is basically a bijective mapping, so it is a permutation phi from this set to itself. So this is the set of alphabets; we denote this set by say A; A is the set of alphabet, so it is a bijective mapping from A to A. So, this is a permutation so; that means, if we have A, B, C, D like up to Z. So, a can go to c, b can go to d, c can go to P like this, so this is the permutation, so just a shuffling, so linear permutation.

So, how many such from permutation are there, so there are 26 symbols; so 26 factorial; so this is the key space. So, set of all permutation from this set to this same set, this is a bijective mapping; bijective function. So, this is the key space; this collection of all permutation, this is basically the permutation from permutation on A. So, this is our key space, so our key is basically a permutation; we have to take a permutation as a key.

(Refer Slide Time: 27:07)



Substitution Cipher

- $\mathcal{P} = \mathcal{C} =$ set of 26-letter English alphabet

  $\mathcal{P} = \{a, b, c, \ldots, y, z\}$

  $\mathcal{C} = \{A, B, C, \ldots, Y, Z\}$

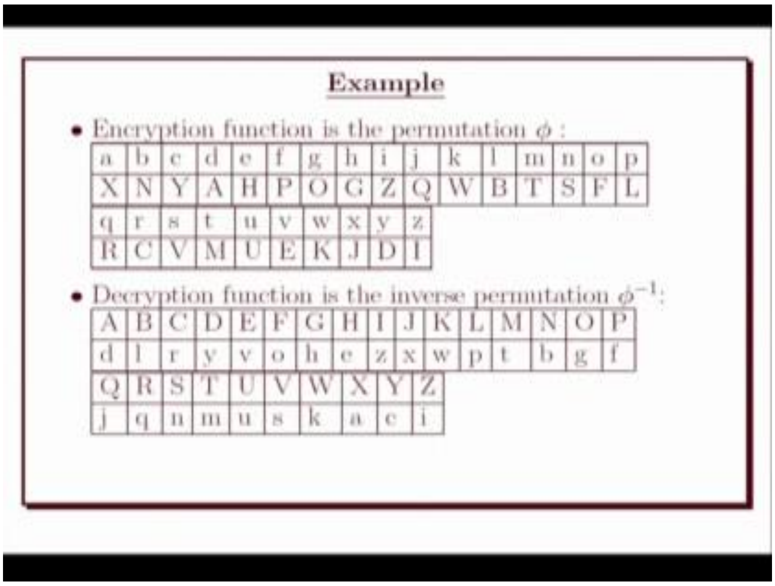
- $\mathcal{K}$= set of all possible permutations of 26 alphabetic characters.
- For each permutation $\phi \in \mathcal{K}$,

  $e_\phi(x) = \phi(x)$ for $x \in \mathcal{P}$

  $d_\phi(y) = \phi^{-1}(y)$ for $y \in \mathcal{C}$, where ϕ^{-1} is the inverse permutation of ϕ.

So, then how we will apply, so this is our plain text space, this is our cipher text space, this is the key space set of all possible permutation on 26 alphabets. So, there are 26 factorial permutation are possible, so now encryption is basically we take a permutation and we take a symbol and this e of phi is basically the permutation of this phi of x. So, we will come to an example and d of phi is basically the inverse permutation on this. So, inverse permutation if we apply, we will get that the message, so this is the typical substitution cipher encryption and it gives.

(Refer Slide Time: 27:48)



Example

- Encryption function is the permutation ϕ :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
X	N	Y	A	H	P	O	G	Z	Q	W	B	T	S	F	L

q	r	s	t	u	v	w	x	y	z
R	C	V	M	U	E	K	J	D	I

- Decryption function is the inverse permutation ϕ^{-1}:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
d	l	r	y	v	o	h	e	z	x	w	p	t	b	g	f

Q	R	S	T	U	V	W	X	Y	Z
j	q	n	m	u	s	k	a	c	i

Let us take an example; suppose this is the permutation we are using, so this is one permutation there are 26 factorial such permutations are there. So, this is the permutation say phi, so a is going to X, b is going to N, c is going to Y like this, p is going to L, q is going to R, r is going to C, s is going to V like this. So, this is one permutation phi we denote this by phi and this is the corresponding inverse permutation; that means, A is going to d; where is d. So, d was going to A, so if we take the inverse permutation; that means, A is going to d by the universe; this is the phi inverse.

So this is the permutation; now under this permutation how we can encrypt.

(Refer Slide Time: 28:46)

.

So, encryption is basically suppose we have the plain text like this, suppose we have the plain text like this meet me; this is the plain text. So, what we do; so now m; so we have to apply; so m will be converted into phi of m and e will be going to phi of e, phi of e, phi of t again phi of m and phi of e, so if we use this phi. So, phi of m is basically m is going to; here if you observe m is going to T. So, this is basically t and phi of e, so E is going to; if you just look at this phi e is going to H.

So, this is the H, this is the H again t, so t is going to where under this permutation t is going to M and again n is going to T and e is going to H, so this is the cipher text. So, this is the plain text and this is the cipher text, so these Alice sent to Bob over this public channel and so this is Alice, this is Bob. So, Alice send this T H H M T H to Bob. So, what Bob will do, Bob has to; so this is the cipher text Alice sent to Bob, so Bob has to get back the message. So what Bob will do after receiving this, Bob will apply the decryption algorithm.

So, decryption algorithm for substitute cipher is just the where you need to apply the inverse permutation on it. So phi inverse of T, phi inverse of H, phi inverse of H like this, so phi inverse of T; if you take the inverse permutation, phi inverse of T. So, let us come back T; phi inverse of T is m. So, this is the single m and phi inverse of H is e, so e, e then in this way, so we will get back meet me, so this plain text. So, this is a plain text we are getting back by applying this decryption algorithm which is the inverse permutation. So, now next we will see whether this is a secure or not in the next class.

Thank you.