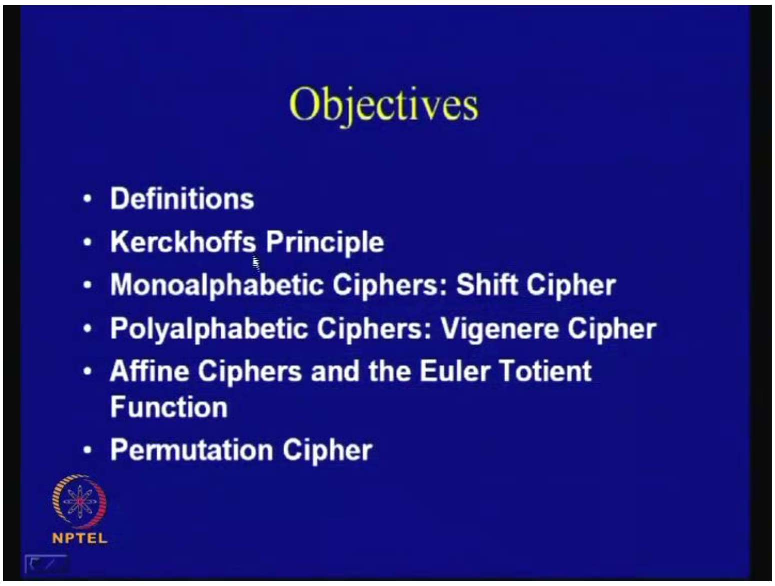
Cryptography and Network Security
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur

Module No. # 01
Lecture No. # 05
Classic Cryptosystems

(Refer Slide Time: 00:42)



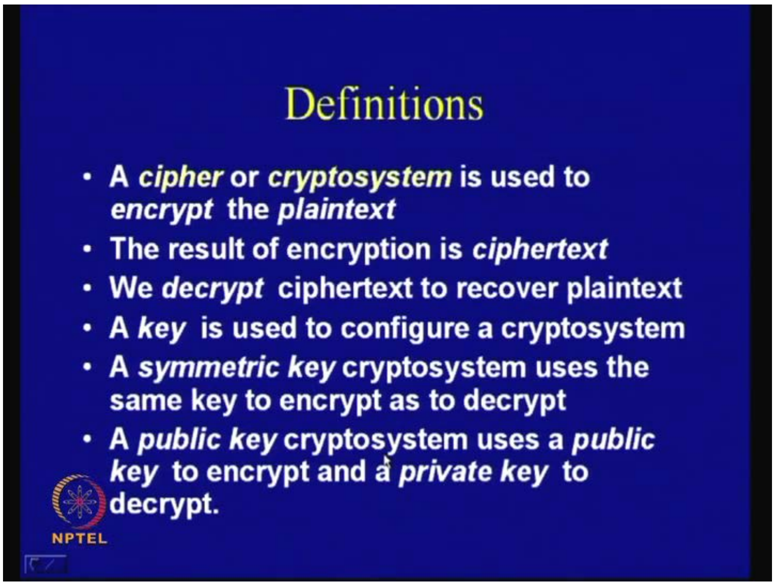
Objectives

- Definitions
- Kerckhoffs Principle
- Monoalphabetic Ciphers: Shift Cipher
- Polyalphabetic Ciphers: Vigenere Cipher
- Affine Ciphers and the Euler Totient Function
- Permutation Cipher

So, welcome to this lecture on classical cryptosystems. Today, we shall be essentially talking about some important definitions, which exist in very old literature of ciphers, and we will be seeing that many of the concepts essentially as we proceed in a course are also applicable to the modern ciphers that we have in the present day.

So, today's objectives will be essentially to talk about some of the important definitions behind cipher designs; and then, we will be talking about very important principle which is known as Kerckhoffs principle; and then, discuss about some important class of old ciphers, which are called as monoalphabetic ciphers and an example of that is the shift ciphers; and then, polyalphabetic ciphers, which are called Vigenere cipher; and then, we discussed about affine ciphers and used our previous days concepts of Euler totient function to find out the size of the key in a fine ciphers; and then, conclude our discussion with a note on permutation cipher.

(Refer Slide Time: 01:18)



Definitions

- A *cipher* or *cryptosystem* is used to *encrypt* the *plaintext*
- The result of encryption is *ciphertext*
- We *decrypt* ciphertext to recover plaintext
- A *key* is used to configure a cryptosystem
- A *symmetric key* cryptosystem uses the same key to encrypt as to decrypt
- A *public key* cryptosystem uses a *public key* to encrypt and a *private key* to decrypt.

So, to start with essentially, today, we will be discussing about cryptosystems. So, as we have, I mean, made amount of idea that when we are discussing about cryptosystems, the cryptosystems are essentially used to encrypt the given plaintext. So, we have been provided by the plaintext and we are supposed to kind of transform these texts and modify them and produce a text which is known as which is different from the plaintext.

And this modified plaintext is something which is known as ciphertext. Now, the objective is that the ciphertext should not the leak any information about the original content of the plaintext to the person or a third person who does not have a possession of a secret material which is known as the key.

So, the key is essentially is used to configure a cryptosystem, that means, that it essentially defines the mapping of a plaintext to the given to a particular ciphertext.

So, there are essentially two very broad categories of ciphers, one of them is called symmetric key cryptosystems, where essentially the encrypted and the decrypted that is, the sender and the receiver use the same piece of key; the key is the same.

That means, if you need to kind of communicate using symmetric key cryptosystem, then it is if that both the sender and the receiver essentially shares the keying material beforehand.

So, basically there should be some other secured channel through which the sender and the receiver have shared this piece of information. So, an opposed so that so that adds the cost of the symmetric key cryptosystem, that is, it had there is an inherent assumption that initially there is a secure that is a secure channel through which the encrypter and the decrypter have shared these piece of information.

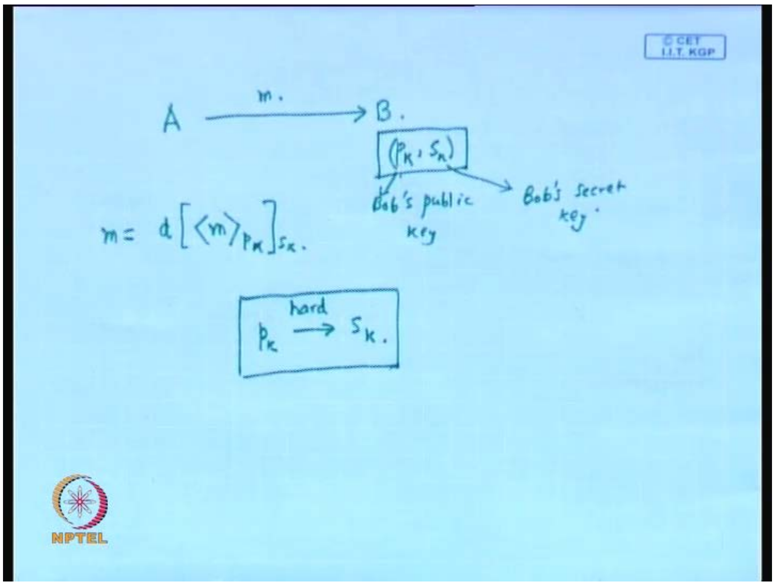
Now, a very, I mean, a very innovative second, I mean, the other type of ciphers which essentially relies upon mathematical assumption is something which is called a public key cryptosystem.

In a public key cryptosystem, there are two concepts of keys. So, as you saw that in a symmetric key cryptosystem in the sender and the receiver has got the same piece of key and the need to kind of exchange the key beforehand, this problem is some sort of aggravated in context of public key cryptosystem, because there are two concept of keys, one of them is called a public key and the other one is the private key.

Now, when we are using for encryption, then the public key is used for encrypting, that means, this piece of key, which is known to everybody can be used for the encryption. So, ideally anybody can encrypt, but when you are decrypting, then you need some need some key, which is known as the private key and essentially which is not known to everybody apart from the only person which is who is supposed to decrypt the information.

So, that means, that your public key cryptosystem anybody can encrypt, but only a particular intended person can decrypt the information. So, that means, that if Alice would like to communicate with Bob, then what Alice does is that, Alice uses a piece of key which is known as… So, if Alice wants to send a piece of information to Bob, then Alice uses the public key of Bob, because Alice use the public key of Bob and when Bob receives this information, then Bob decrypts it using its own secret key or private key.

(Refer Slide Time: 04:54)



So, that means, that, it is some sort like this, that is cryptographically if Alice and Bob are two persons who are communicating between each other, and Alice send Alice sends the public key say call it.. I will define this, as we precede more in the class, but this is just to have a flavor of the topics that we will be discussing. So, there is a public key called Pk and Bob also has a secret key called Sk. So, when Alice wants to send a piece of message to Bob, then what Alice does is that, Alice encrypts this m using the public key of Bob. So, P Pk is Bob's public key so Pk is Bob's public key and Sk is Bob's secret key.

So, what Alice does is that, Alice encrypts m using Pk and sends it to Bob; now when Bob needs to decrypt this, then Bob decrypt this using the decryption function called d, but the internal key is essentially Sk. So, that means, Bob uses its own secret key to decrypt this information and this should be back to M; so, that means, that completes the decryption procedure.

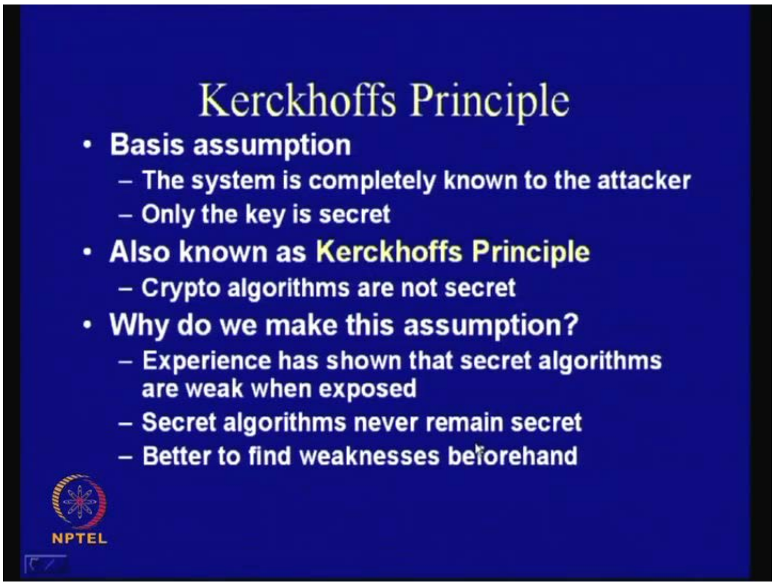
Now, there are some interesting points here, like about the key. So, it should be that Pk is known to everybody and Pk also should, I mean, doing the encryption also should be easy, but when you are kind of decrypting, I mean, then you need this piece of information called Sk which is the secret key.

And another important, I mean, been mathematical, I mean, the base on which the public key cryptosystems rely upon is that, from Pk which is the public key information extracting the Sk that is the secret information should be a computationally difficult task; so this should not be easy.

And this gives us kind of, I mean, we do not really have exact definitions in computer science which actually proves that, there are some problems which are actually hard; but we also but on the other hand, we have got some common number theoretic problems, which have actually for times for many times actually, I mean, it has they have been evaluated and they have been found to be difficult, so they are kind of assumed to be difficult. But we really do not have any rigorous mathematical proof to justify that they are indeed difficult problems.

So, there are essentially some grey areas some place, where we kind of need to assume and based upon this assumptions, which are actually which took for lot of analysis, lot of attack methods, we actually develop this science of public key cryptosystems. We will see more concrete examples as we proceed in the class.

(Refer Slide Time: 07:56)



Kerckhoffs Principle

- Basis assumption
  - The system is completely known to the attacker
  - Only the key is secret
- Also known as Kerckhoffs Principle
  - Crypto algorithms are not secret
- Why do we make this assumption?
  - Experience has shown that secret algorithms are weak when exposed
  - Secret algorithms never remain secret
  - Better to find weaknesses beforehand

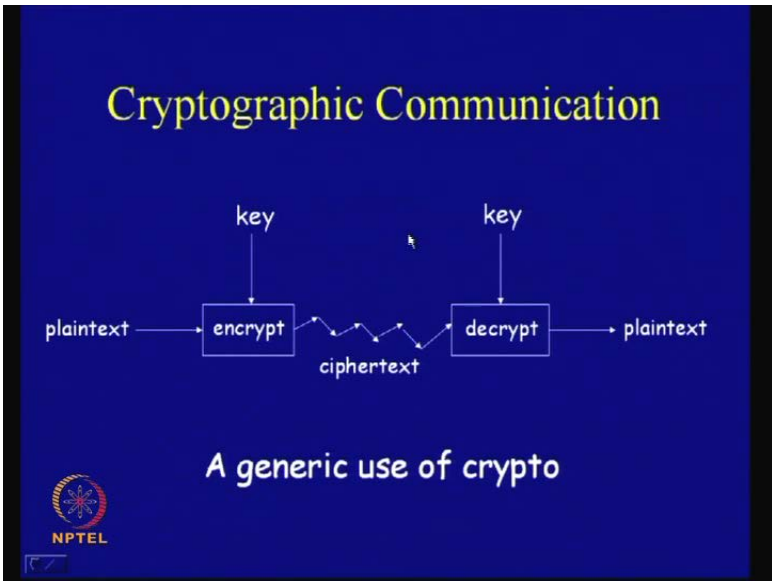
So, let me come to the definitions. So, again back to the definitions that is, so we have symmetric key cryptosystems and public key cryptosystems, which are essentially two broad categories of ciphers. Then I would like to kind of comment upon a very important principle which is there, is that, they are the basic assumption is that the entire system is completely known to the attacker. So, if we build a cipher, then you have to publish the cipher so that everybody knows that cipher but, what is not known to the attacker is only the secret piece of information which is called the key. So, this principle is known as Kerckhoffs principle, which says that the crypto algorithms are never secret.

So, the idea is that, our experience shows that secret algorithms are weak when exposed, that is, if you kind of have an indoor algorithm and relies upon indoor algorithm, which has not been scrutinized properly, then experience shows the secret algorithms are indeed weak and there are saved examples of such type. I mean, if you do not properly i mean criticize your algorithms properly, analyze your algorithms, then there are lot of possibilities that they may be weak inherently. Therefore, the idea is that, make a new cipher and publish it and so that people analyses them and then only you will be kind of sure that your algorithm is or rather you can me more confident that your algorithm is secure.

And secret algorithm and it has been found the secret algorithms are never actually never remains secret that finally, somehow they are weak; so it is better to find weaknesses beforehand. Therefore, the idea is that, whenever you make a cipher, assume that the ciphering algorithms is known to the attacker, but the attacker does not know the piece of information which is secret which is called the key.

Even then it should be difficult for him or her to obtain the plaintext from the ciphertext and also it should be difficult, I mean, from the attackers point of view to obtain the piece of information, which is known as the key from the ciphertext. And there are some more evolved models of attacks which says, it should be also difficult to obtain the key even if you know the ciphertext and the plaintext.

(Refer Slide Time: 10:02)



Cryptographic Communication

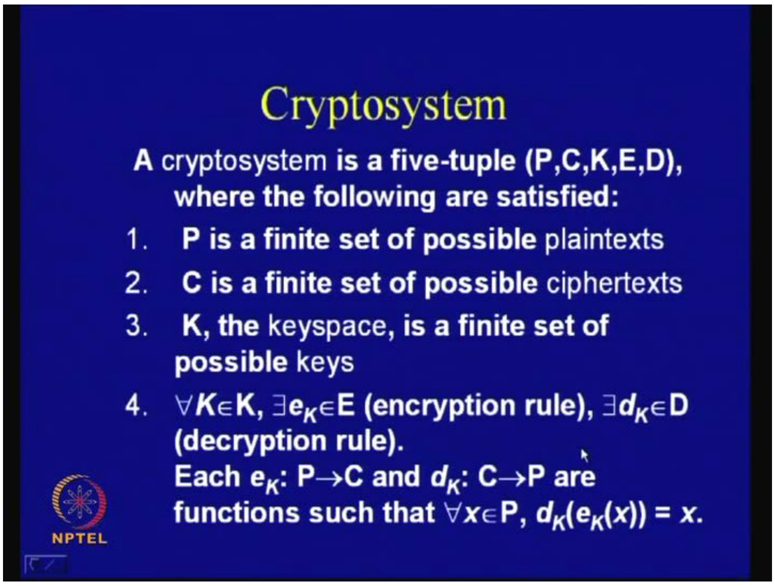
A generic use of crypto

So, the idea is that, we have to do more and more kind of scripted analysis of your cryptoalgorithms to gain more confidence that your algorithm is indeed secure. So, this is the broad picture of how you are communicating a plaintext; there is a encryption algorithms; there is a key; you generate the ciphertext, then you receive have been this piece of information; you decrypt that using the key and you obtain back the plaintext.

So, these algorithms, that is, encryption algorithms and decryption algorithms and by the symmetric key, if they are symmetric key, then this key and this key are the same, that is, the encryption key and decryption key are the same; but if there is a public key cryptosystems, then this is essentially the public key, but this piece of information is the private key.

So, there can be other uses of this public key, private key which in context to signatures, where essentially we use the private key to do the encryption operation, because we are signing using the private key, but you verify using the public key. So, anybody can verify, but only the person who is supposed to sign can sign. So, that is another application of very important application of public key cryptosystems.

(Refer Slide Time: 11:00)



Cryptosystem

A cryptosystem is a five-tuple (P,C,K,E,D), where the following are satisfied:

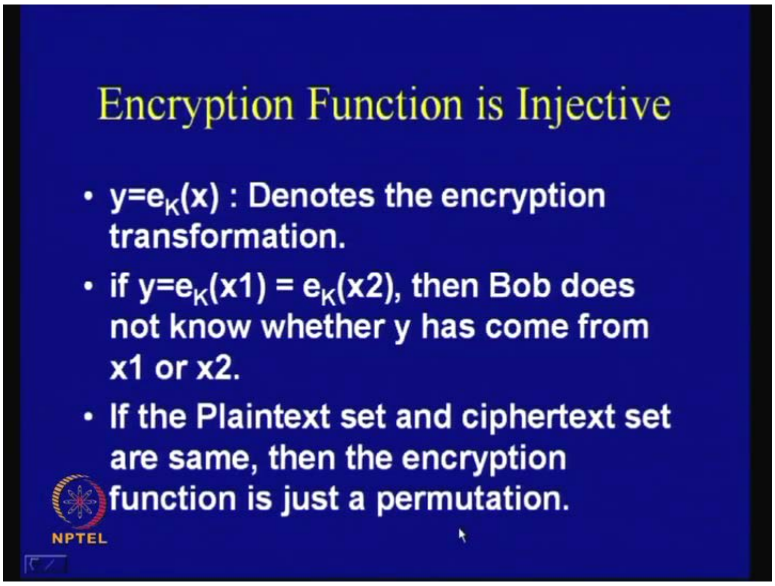
1. P is a finite set of possible plaintexts
2. C is a finite set of possible ciphertexts
3. K, the keyspace, is a finite set of possible keys
4. $\forall K \in K$, $\exists e_K \in E$ (encryption rule), $\exists d_K \in D$ (decryption rule). Each $e_K: P \to C$ and $d_K: C \to P$ are functions such that $\forall x \in P$, $d_K(e_K(x)) = x$.

So, little bit more formally, your cryptosystem is essentially a five-tuple, where there are five tuple members are there in the plaintext; we denoted by P which is finite set of possible plaintexts, then embed the C which is a finite set of possible ciphertexts. So, this could be alphabet, this could be number, this could be bit streams, but they are essentially drived from a finite set of possible values, then K is the keyspace, which is a finite set of possible keys, then idea is that for all k, which belong to these for all key which belong to these key set, there should exist the encryption algorithms. I mean, there should be exist a encryption rule and there should exist a decryption rule such that for each, if you have got P and C, that is, P to C mapping, there should be a corresponding C to P mapping.

So, that means, what I want to say is that, if you take x which belongs to P and encrypt it using this piece of information which is called k, and then, decrypt it back using the decryption algorithm and decrypt it using the decryption key, (Refer time: 12:00) then you should actually get back the original plain-text, that is, you should recover the original message.

.

(Refer Slide Time: 12:07)



Encryption Function is Injective

- $y=e_K(x)$: Denotes the encryption transformation.
- if $y=e_K(x1) = e_K(x2)$, then Bob does not know whether y has come from x1 or x2.
- If the Plaintext set and ciphertext set are same, then the encryption function is just a permutation.

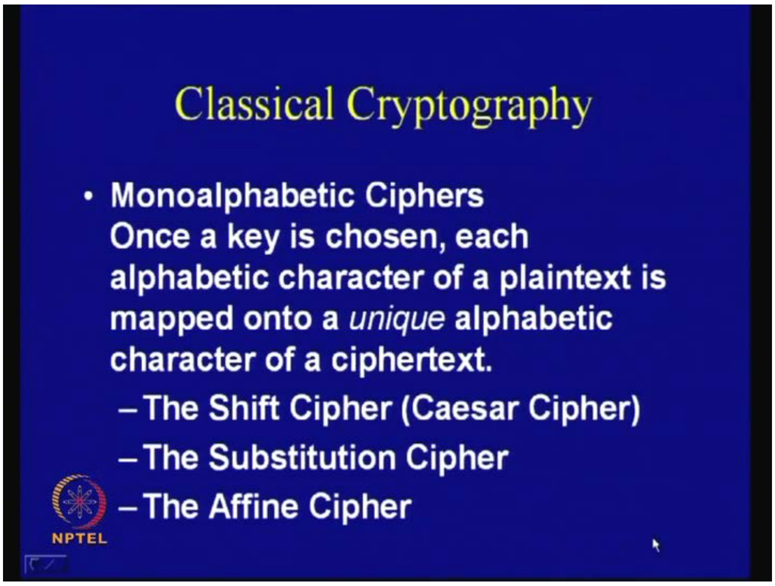
So, that means, the essentially encryption function should be injective, that means, it denotes, I mean, suppose y is equal to e k x is the encryption transformation and imagine that, if there are two different x 1 and x 2, which are kind of distinct, they are not equal; and if you encrypt it encrypt them using the k the key k and you obtain y in both the cases; so this is a example of function which is not injective.

Then Bob will be confused; when Bob receives y and he knows that he has to decrypt it using the corresponding key, then Bob will not be able to kind of get, I mean, be convinced whether the plaintext is x1 or x2. So, that should not happen; Bob should kind of uniquely identify that, whether x1 is the plaintext or x2 is the plaintext. Therefore, these kinds of functions are not and not used; therefore, we need functions which are kind of which are injective.

So, therefore, if the plaintext set and ciphertext set are same, then essentially, I mean, for example, if you take alphabets in a plaintext set and also ciphertext set is alphabets, then the encryption function is just a permutation. So, if a for example, the plaintext set could be a 0 one string and the ciphertext set is also a 0 one string, then the ciphertext set is nothing but rearrangement of the 0 one string.

So, therefore, this a example, where, I mean, i mean you need kind of i mean if you are plaintext set and the ciphertext set are the same, then essentially there is a permutation and the permutation is defined by the key, because the encryption function and the decryption function are known to everybody, but what is not known is the key. So, the key is the kind of material, which the cipher designer has to protect and which the crypt analyst who is trying to attack will try to recover using some way, I mean, using algebraic techniques, using statistical techniques and various other methods.

(Refer Slide Time: 13:56)



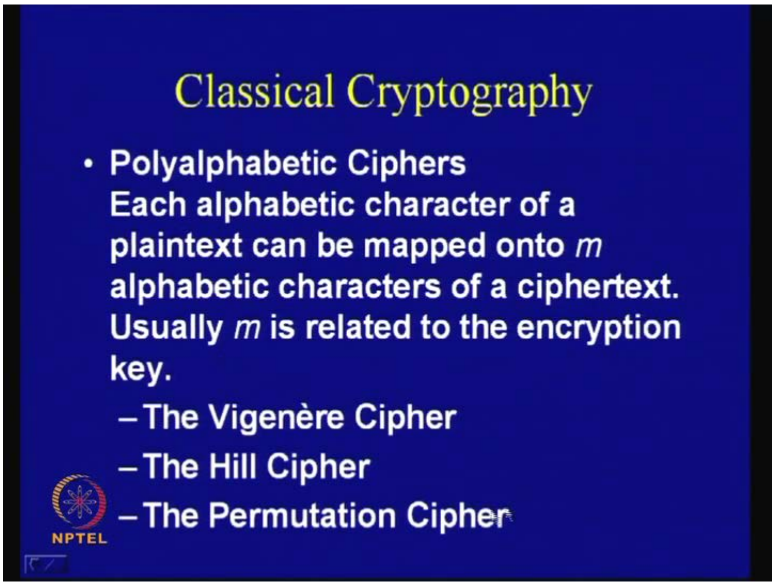
Classical Cryptography

- Monoalphabetic Ciphers
  Once a key is chosen, each alphabetic character of a plaintext is mapped onto a *unique* alphabetic character of a ciphertext.
  - The Shift Cipher (Caesar Cipher)
  - The Substitution Cipher
  - The Affine Cipher

So, in classical cryptography, we will essentially see two important classes of ciphers, one of them is called the monoalphabetic ciphers and these are actually some of the primitive ciphers that we will be that we have come across, which means that once the key is chosen, the each alphabetic character of a plaintext… So, in this case, let us consider the plaintext to be made of an alphabetic characters, so I will be considering English alphabet, which is essentially as 26 letters. So, there are alphabetic character of a plaintext is mapped onto a unique alphabetic character of a ciphertext.

So, therefore, if I take a and if it maps to c, then it will map to c, that means, that it will always map to c; so it is a kind of unique and unique and fixed transformation.

(Refer Slide Time: 14:49)



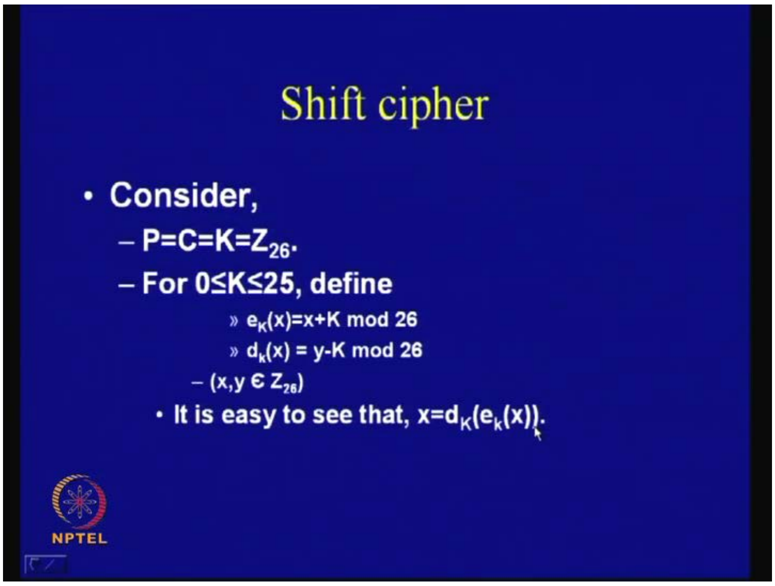
Classical Cryptography

- Polyalphabetic Ciphers
  Each alphabetic character of a plaintext can be mapped onto *m* alphabetic characters of a ciphertext. Usually *m* is related to the encryption key.
  - The Vigenère Cipher
  - The Hill Cipher
  - The Permutation Cipher

Some other example of classic, I mean, ciphers are the caesar cipher or something which is more generalized as shift cipher, then we have the substitution cipher and the affine cipher. So, let us see, I mean, some of them like and the other types of them polyalphabetic ciphers, where each alphabetic character of a plaintext can be mapped onto m alphabetic characters of a ciphertext. So, therefore, each alphabetic character of a plaintext can be mapped onto m alphabetic character of a ciphertext.

Usually m is related to the encryption key, so which mean that, if a in case of monoalphabetic ciphers, a will suppose to get mapped to c, so that is fixed. But in case of polyalphabetic ciphers, a can be mapped to, say m possibilities, it could be map to c; it could be map to e; it could be map to f and so there can be m possibilities. And usually this m is related to a size of the encryption key, an example of such kind of ciphers are the Vigenere cipher, the hill cipher and the permutation cipher. So, we will also see some of them.

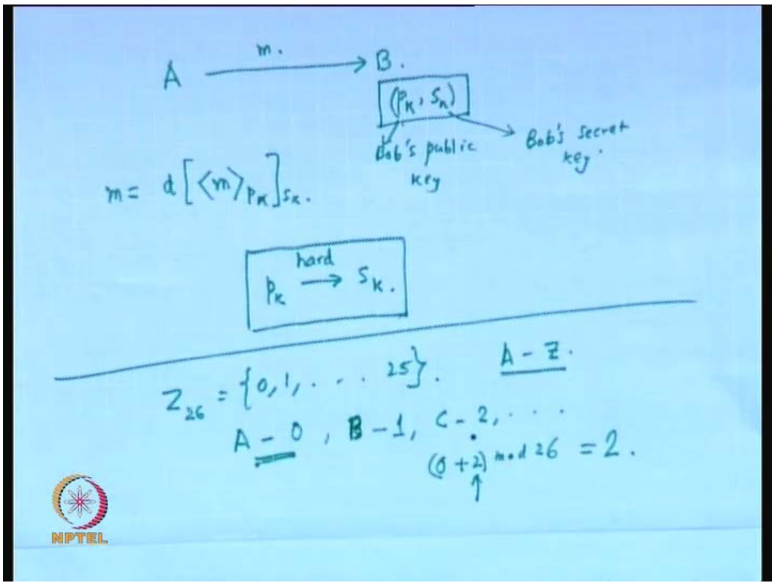
(Refer Slide Time: 15:38)



Shift cipher

- Consider,
  - $P=C=K=Z_{26}$.
  - For $0 \leq K \leq 25$, define
    - » $e_K(x)=x+K \bmod 26$
    - » $d_k(x) = y-K \bmod 26$
  - $(x,y \in Z_{26})$
  - It is easy to see that, $x=d_K(e_k(x))$.

(Refer Slide Time: 15:58)



$A \xrightarrow{m.} B.$
(P_K, S_K)
Bob's public key
Bob's secret key.
$m = d[\langle m \rangle_{P_K}]_{S_K}.$
$P_K \xrightarrow{hard} S_K.$
$Z_{26} = \{0, 1, \ldots 25\}.$
A - Z.
A - 0, B - 1, C - 2, . . .
$(0+2) \bmod 26 = 2.$

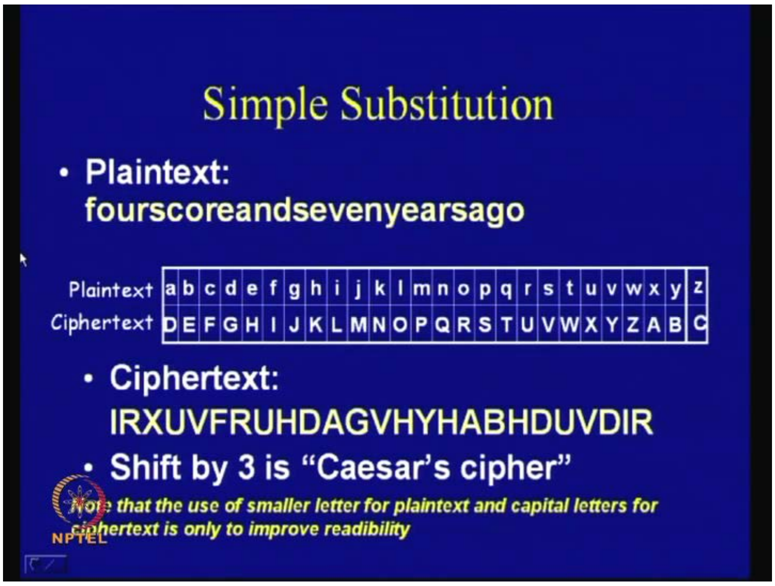
Like So, let us start with the most kind of one of the most primitive ciphers which is known as the shift ciphers. In case of a shift ciphers, let us consider Z26; so you know what is it 26 phi now? Z26 means a set, Z26 is essentially the set 0, 1 to 25; these numbers, that is, these 26 numbers can be used to encode the letters from A to Z. So, I am considering that the plaintext is made of the letters from A to Z.

So, now, if you take, I mean, a key also belongs to this set, that is, from 0 to 25 some of the these values, then you can define the encryption function like this, that is, you can take x and when we apply this encryption function, then you simply add x with K and then you take a module operation with 26.

So, we have seen what is a module operation in the last day class. So, suppose in that case, the letter x assume that the letter x is A, and suppose the letter K is B therefore, a will essentially be denoted by 0, and K which is B, will be k is b so B will be denoted by 1; c will be denoted by 2 and so on. right So, therefore what we do is, suppose A, I mean, you take if you take for example, that A is denoted by 0 and suppose the key is 2, then what you do is, simply you add 0 with 2, and then, you take a mod 26, there is no problem. So, therefore, since this number is lesser than 26, so the result is 2.

So, therefore, that means, that A will get mapped to C. So, similarly, if you want to kind of recover A from C, then you just need to subtract this piece of information, and this piece of information is nothing but the key and which is known to the kind of the sender, it is known to the receiver as well. So, there is simple kind of function, so it says that e k x equal to x plus k mod 26 and d k x which is that, actually it should be d k y is equal to y minus k mod 26. So that it is very easy to see that, if you kind of apply d k over e k, that is, if you apply d k over e k x, then you get back x; therefore, this function is indeed an injective function.

(Refer Slide Time: 18:01)



Simple Substitution

- Plaintext: fourscoreandsevenyearsago

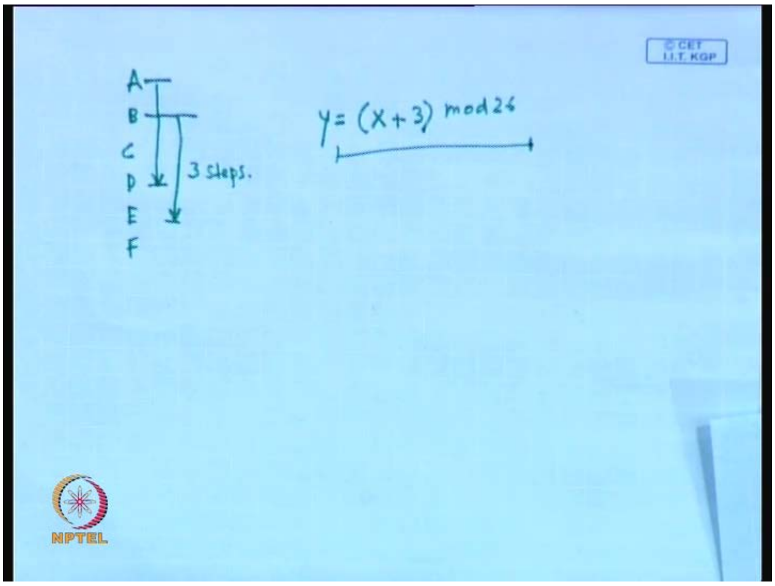
Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Ciphertext: IRXUVFRUHDAGVHYHABHDUVDIR
- Shift by 3 is "Caesar's cipher"

Note that the use of smaller letter for plaintext and capital letters for ciphertext is only to improve readibility

So, a simple example could be like this; so suppose the plaintext is this, that is, four score and seven years ago, so this is some kind of alphabetic characters. You take that this could be anything this; does not matter this is just an example; you just have got this encoding, you take this plaintext and a very simple substitution could be like, instead of having A getting mapping to A what you do is, shift this by three steps; therefore, A will get mapped to B, C and D; so, I mean, a will get mapped to D.

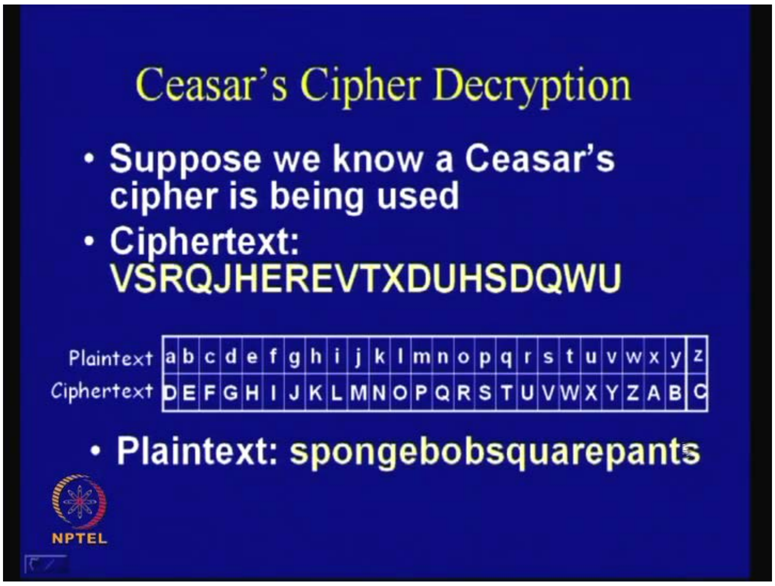
(Refer Slide Time: 18:35)



So, that means, that what I am saying is this, that is, if you take the characters like this A, B, C, D, E F and so on. So, if you just add A, I mean, whether shifted by three steps that actually you come to hit this place. So, therefore, A will get mapped to D; B will get mapped to E and so on; so you can actually form a table this way; so these are all three steps. you these are three steps So, therefore, in this cipher, if you have got X and there is fixed shift of this X; you just add with 3 and take a module of 26 and that is your y. So, therefore, in this case, this key is fixed.

And this cipher essentially was used by Julia Caesar therefore, commonly referred as Caesar cipher. So, therefore, the corresponding ciphertext for this particular plaintext will be this. So, you can see that F will be get getting mapped into I, that is, g h arise that is three steps, and similarly, you can actually obtain the corresponding mapping of each of these letters and this particular cipher was known as the Caesar cipher and note that the use of the small letter… So, we are actually what we have done is that, we have for the plaintext, we have used the small letter and for the capital letters, we have use ciphertext; there is nothing to do with the ascii value, but just to improve rigidity of the corresponding mappings.

(Refer time: 20:00)



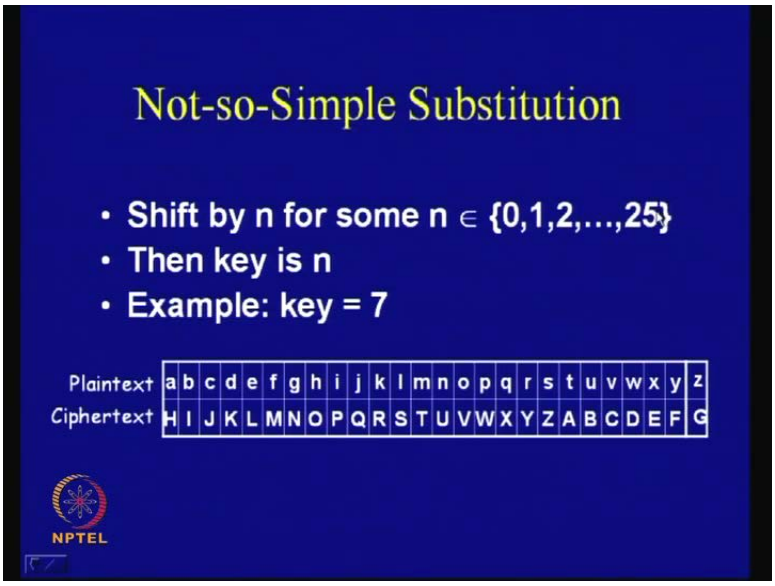
Ceasar's Cipher Decryption

- Suppose we know a Ceasar's cipher is being used
- Ciphertext: VSRQJHEREVTXDUHSDQWU

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Plaintext: spongebobsquarepants

(Refer Slide Time: 20:28)



Not-so-Simple Substitution

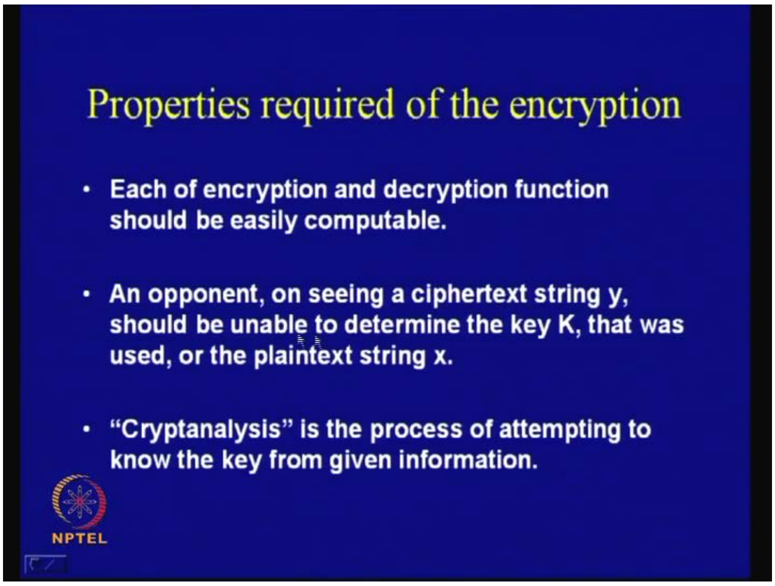
- Shift by n for some n ∈ {0,1,2,...,25}
- Then key is n
- Example: key = 7

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

So, obviously understand this is not a very kind of secure cipher, but just a kind of for the other completeness set. So, if you are got the ciphertext, then you can also easily decrypt it, because what you just need to doing is that, you just need to go back by three steps. So, you know, if the corresponding cipher text is D, you need to go back three steps and obtain back a.

So similarly, you can actually decrypt this information and you know that the plain for this particular ciphertext is easy to obtain the corresponding plaintext; so it is quite easy. Now, we will just discuss about something which is a little bit more complicated. So, what we do here is that, instead of shifting by three steps, we shift by some value which lies between 0 to 25.

(Refer Slide Time: 20:58)



Properties required of the encryption

- Each of encryption and decryption function should be easily computable.
- An opponent, on seeing a ciphertext string y, should be unable to determine the key K, that was used, or the plaintext string x.
- "Cryptanalysis" is the process of attempting to know the key from given information.

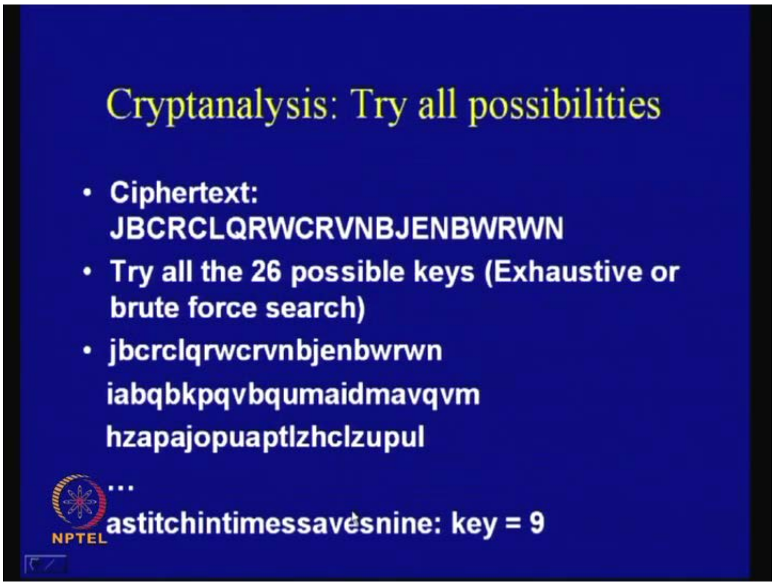
So, the key could be in that case, for example, the key could be 7 what we do is, we take the corresponding in the mapping; the corresponding mapping is denoted here, where a is mapped to 7 that is down the line, but this key actually we can would like to change; you will not like to keep this as fixed. So, therefore, that is the objective.

So, some of the properties that, we will see that for… So, we can actually make changes this for each of encryption function, but actually it should kind of satisfy some important property, that is, in each of the encryption and decryption function should be easily computable. We have seen that in case of Caesar cipher, it is called easily computable, both the encryption and decryption are easy to compute.

And the other thing is that, an opponent, on seeing a ciphertext y, should be unable to determine the key K, that was used or the plaintext string x. That is for an attacker, which absorbs the ciphertext string y, it should not be able to find out what is the value of the key, because if he gets the key, then he can easily understand what is the plaintext or he should not also get back plaintext string some other way also. So, therefore, it should kind of leak no information about the corresponding plaintext of the key.

So, cryptanalysis as we have already defined previously is the process of attempting to know the key from given information; so we will see that. We will see some more concrete examples of cryptanalysis in our next class on in context to classical cipher and also more techniques as we proceed in the class, but this is the main definition.

(Refer Slide Time: 22:10)



Cryptanalysis: Try all possibilities

- Ciphertext: JBCRCLQRWCRVNBJENBWRWN
- Try all the 26 possible keys (Exhaustive or brute force search)
- jbcrclqrwcrvnbjenbwrwn
  iabqbkpqvbqumaidmavqvm
  hzapajopuaptlzhclzupul
  ...
  astitchintimessavesnine: key = 9

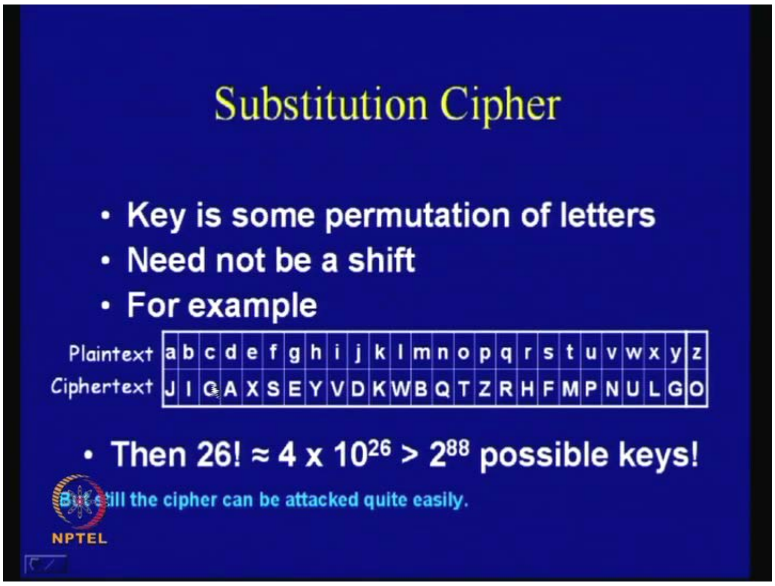
So, for a Caesar cipher one way of crypt analysis will be like, if i mean let us talk one about the Caesar cipher, because there is no key in the Caesar cipher. Let us talk about the case of the not so simple substitution, where essentially the key can take all 26 possible values essential values.

So, suppose they have been provided in a ciphertext like this, then what you do is that, if you know that this particular cipher essentially is nothing but, I mean, in each of the letter has been shifted by K steps, where K can vary from 0 to 26. So, what we will do as an attacker? If you are interested in obtaining the plaintext, what you will do is that, you will try for all the possible 26 keys and then kind of start decrypting this information until and unless you get something which is a meaningful piece of information.

So, if you get a meaning meaningful piece of information, then you can be more or less convinced that since it occurs for all Bob’s letters and this fairly, I mean, modern style stream, then you can be convinced that the key is indeed corrected retrieved. That is the key in this case is 9, it says that, this particularly tells from the fact that, you are actually trying all possible key search here, that is, which is called exhaustive or the brute force search and we actually get back the key for which you have for which the corresponding plaintext make sense.

This is the way common way of doing i would doing crypt analysis. In this case what we see is that, main pitfall is that the key size are the total number of possible search that an attacker needs to make is very small, it is only 26. So, we would first of all like to improve this particular fact, that is, we would like to make it a little difficult for the attacker.

(Refer Slide Time: 23:45)



Substitution Cipher

- Key is some permutation of letters
- Need not be a shift
- For example

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	J	I	C	A	X	S	E	Y	V	D	K	W	B	Q	T	Z	R	H	F	M	P	N	U	L	G	O

- Then $26! \approx 4 \times 10^{26} > 2^{88}$ possible keys!

But still the cipher can be attacked quite easily.

So, in this case, one example which is tried here is that, the key is some permutation of letters therefore, it need not be a shift, but instead of the shift let us consider which is something which is called as substitution cipher. So, this concept of substitution cipher says like this, that is, if you take a and if you map to J, I mean, map say a to J, then b you will not map to J. Because if you map a to J, and b also to J, then immediately the probability of injectiveness is lost. So, that means, if you take J, then you see that J can actually come from a both a and b, that is not kind of allowable.

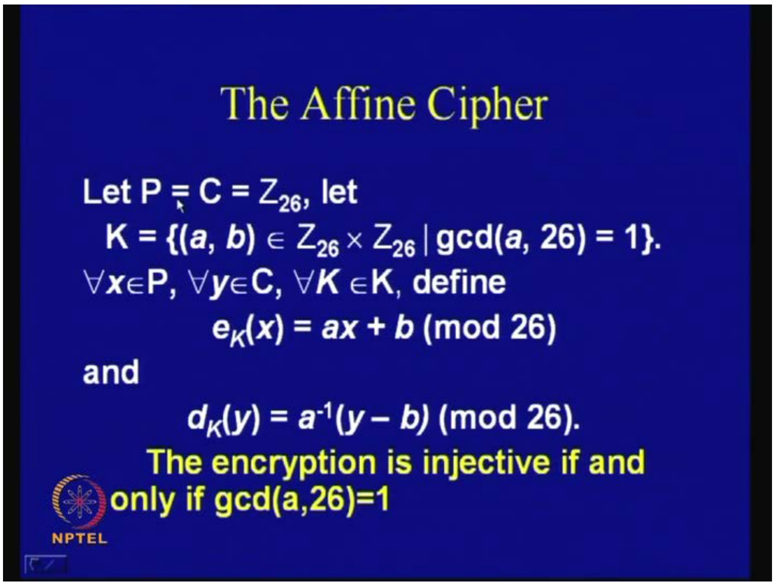
So, therefore, that will lead to kind of in ambiguity in the decryption process; so it is not an injective function. So, therefore, what essentially b will get mapped into is, b will get mapped into something else other than a, than what a has got mapped into; so it could be I; similarly, c could get mapped into something which is not J or I.

So, this particular mapping or this particular table can define a particular key; so this table is essentially supposed to kept secret. So, this means, that the number of such possible mappings that can actually arise is the first letter can be mapped into 26 letters; the second one can be mapped into 25; the third letter can be mapped into 24; similarly, to this one. So, that means, that there are 26 factorial possible mappings and this number is quite huge, it is more than the 2 power 88 possible keys.

That means, that the total key size there are is quite large. So, which means that, if an attacker could try to kind of try all possible try all possible tech all possible keys to actually obtain back the plaintext from the ciphertext, then it needs to do a lot of search, which means, that particular attack method is not possible, but still this cipher is weak, and we will see in our next day’s class why it is weak on or other how to extract the information of the plaintext.

So, therefore, in this case, this is an example of something which is called as substitution cipher and what we will see is the concept of substitution cipher still prevails in the modern day cipher. I mean, there are lot of examples of modern day ciphers, where still these kind of concepts are used again and again. So, therefore, although we know that this cipher, I mean, as independently if I call this is as a cipher, this is weak, but these component actually can be used in today’s ciphers to make a ciphers which is more strong, which is much more strong actually. So, they are very important concepts that we need to pick up, but we are never say that the substitution ciphers is secure and this is still can be attacked and we will see how it can be attacked.

(Refer Slide Time: 26:31)



The Affine Cipher

Let $P = C = Z_{26}$, let

$K = \{(a, b) \in Z_{26} \times Z_{26} \mid \gcd(a, 26) = 1\}$.

$\forall x \in P$, $\forall y \in C$, $\forall K \in K$, define

$$e_K(x) = ax + b \pmod{26}$$

and

$$d_K(y) = a^{-1}(y - b) \pmod{26}.$$

The encryption is injective if and only if gcd(a,26)=1

So, then you have something which is called affine cipher. So, what the affine cipher does is that, again your plaintext and the ciphertext have both from this 0 to 25, that is, it belongs to the 26. i was in 26 And assume that your key is instead of one particular is Z 26 element, it could be a tuple like, it could be an ordered pair of (a, b), where a is also chosen from the Z 26 and b is also chosen from Z 26 such that a satisfy the particular property, which means that a is co-prime to 26, that means, gcd are the greatest common divisor of a, and 26 is actually 1 y, because it comes from the definition.

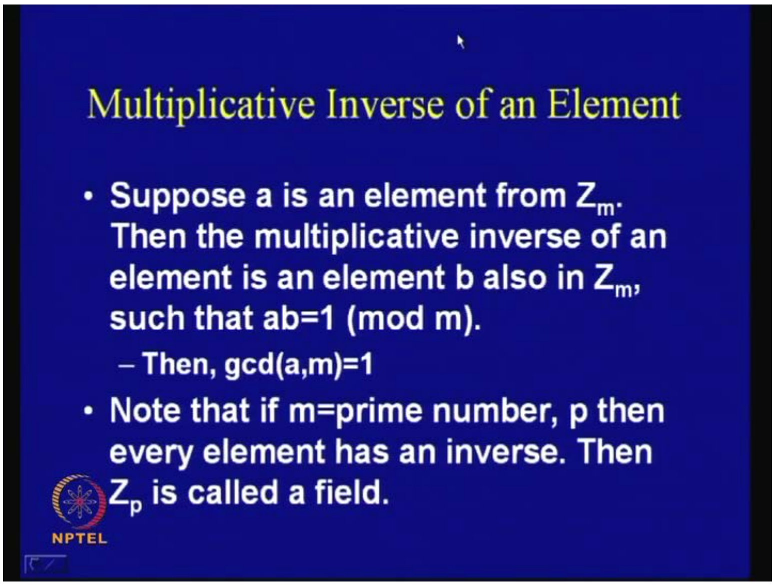
So, what we take as the plaintext like x, which is chosen from P the way, I mean, we choose the K, and then, encryption operation is defined as follows: what we do is that, we multiply x with a and then add with b, take a modular 26.

So, from our previous days discussion, we know that, what we can also do is that, we can take a and multiply with x, and then, if this number is bigger than 26, then we can take a modular of 26, reduce it to less than 26, and then, add b; again if there is an overflow, I mean, we will get the result is more than 26, then we again take a modular 26; if it is equal to more than 26, then we again take a modular 26. The decryption operation is defined as like this.

So, you see that for this decryption operation to exist rather this function to be injective, you need a particular fact that is, you knew that a has to be has to have a multiplicative inverse in this modular 26. So, therefore, that means, that if you need a kind of, I mean, in the last days class, we saw that if the multiplicative inverse of a the modular 26 has to exist, that need to satisfy the particular property which is that, a should be co-prime to 26. That means, that the gcd of a and 26 should be equal to 1, only then the multiplicative inverse of a exists. So, that we have seen in the last days class on number theory.

So, that means, that all a is not reliable, only those a's are possible or rather are allowed which essentially have co-prime to 26. So, how many numbers are there in the 0 to 25, which are actually co-primed to 26? So that we need to find out in order to find out the number of keys.

(Refer Slide Time: 28:54)



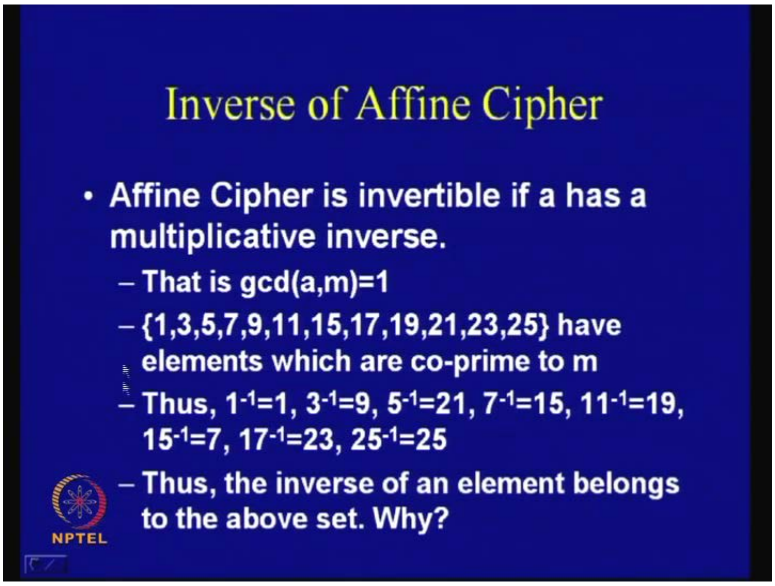
Multiplicative Inverse of an Element

- Suppose a is an element from Z_m. Then the multiplicative inverse of an element is an element b also in Z_m, such that ab=1 (mod m).
  - Then, gcd(a,m)=1
- Note that if m=prime number, p then every element has an inverse. Then Z_p is called a field.

Therefore, I mean, it is a kind of recapitulation of what we have seen in the last days class, that suppose a is an element from Zm, then the multiplicative inverse of an element is an element b also in Zm, such that a b is equal to 1. So, therefore, a b is equal to 1 module m of course. So, then it needs to satisfy a property, which is the gcd of (a, m) is equal to 1.

So, note that, if m is prime number, then p as a then every element has an inverse because Z p of the number and p will of course be equal to 1. So, therefore, Z p in that case is called a field; it is called a field, because every number is a multiplicative inverse, but in this case m is say 26, then every number does not have a multiplicative inverse which belongs to 0 to 25 set and not a co-prime to 26.

(Refer Slide Time: 29:41)



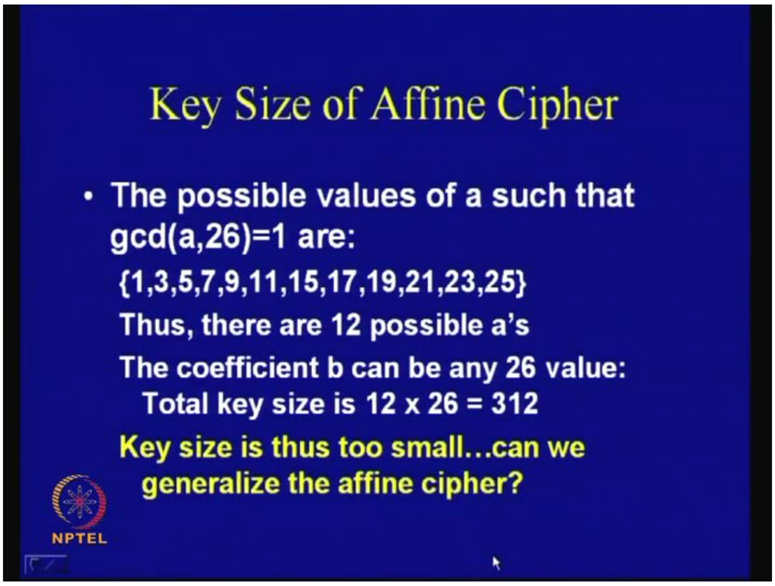
Inverse of Affine Cipher

- Affine Cipher is invertible if a has a multiplicative inverse.
  - That is gcd(a,m)=1
  - {1,3,5,7,9,11,15,17,19,21,23,25} have elements which are co-prime to m
  - Thus, $1^{-1}=1$, $3^{-1}=9$, $5^{-1}=21$, $7^{-1}=15$, $11^{-1}=19$, $15^{-1}=7$, $17^{-1}=23$, $25^{-1}=25$
  - Thus, the inverse of an element belongs to the above set. Why?

So, we can actually enumerate this and we will find that these are the numbers which are co-prime to 26 like, we can see that 1 is co-prime; 3 is co-prime; 5 is co-prime; 7 is co-prime; 9 is co-prime, so 11, 15, 17, 19, 21, 23 and 25, so how many numbers are there? So, there is 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 and 12; so there are 12 numbers in this particular set. So, that means, that all these numbers are actually co-prime to m.

So, you can actually verify that, they had they have multiplicative inverse, because 1 inverse is equal to 1; 3 inverse is equal to 9. So, if you see that, multiply 3 into 9, you get 27; if you take modular 26, that is, 1; 5 inverse is 21 you can verify this; 7 inverse 15; 11 inverse is 19; 15 inverse is 7; 17 inverse is 23; 25 inverse is 25, that means, that all these number essentially have multiplicative inverse. Thus the inverse of an element belongs to the above set. So, therefore, in it belongs to the above set and if you can reflect why.

(Refer Slide Time: 31:06)



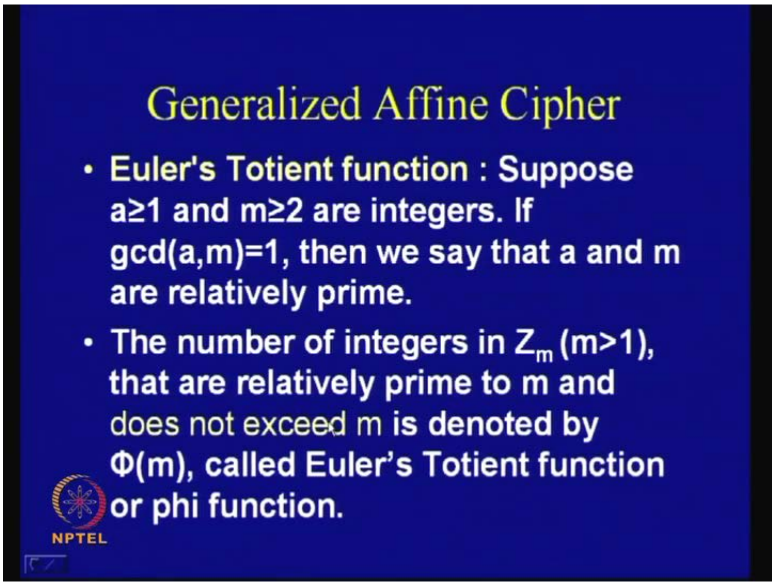
Key Size of Affine Cipher

- The possible values of a such that gcd(a,26)=1 are:
  {1,3,5,7,9,11,15,17,19,21,23,25}
  Thus, there are 12 possible a's
  The coefficient b can be any 26 value:
    Total key size is 12 x 26 = 312
  Key size is thus too small…can we
    generalize the affine cipher?

So, therefore, the question is that, is the how many possible keys are allowed in this affine ciphers. So, therefore, these the a can essentially a the value of a can essentially take any of these 12 values and b can take any of the 26 values; so the total key size is essentially 12 into 26, which is equal to 312.

And the key size of course small, I mean, we can verifying 312 for possible keys is not a very big matter. So, that means, that the question is that, can we generalize this affine cipher? I would like to kind of increase the 26 values so that this size is essentially increased. So, therefore, I would like to do a kind of generalized analysis, if this 26 is replaced by some value say m.

(Refer Slide Time: 31:35)



Generalized Affine Cipher

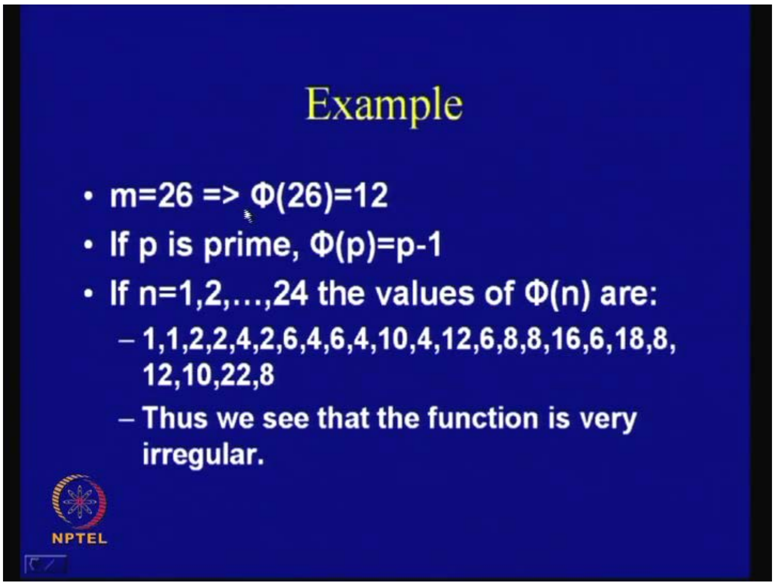
- Euler's Totient function : Suppose $a \geq 1$ and $m \geq 2$ are integers. If gcd(a,m)=1, then we say that a and m are relatively prime.
- The number of integers in Z_m (m>1), that are relatively prime to m and does not exceed m is denoted by $\Phi(m)$, called Euler's Totient function or phi function.

So, in this case, I mean, I will use the previous days concepts of Euler’s Totient function and it is a kind of recapitulation, which says suppose a is greater than 1, and m is greater than equal to 2 are integers and if gcd of (a, m) is equal to 1, then we see say that a and m are relatively prime. This is the definition of Euler’s Totient function which says that, if a is greater than or equal to 1 and m is greater than or equal to 2 are integers, then this is a definition a and m are co-prime, then gcd of (a, m) equal to 1, then we say that a and m are relatively prime.

So, that means, if a is equal to 1, this is the kind of case if I just kind of I would like to make a note that, if a is equal to 1, then gcd of (a, m) is also equal to 1 and say that 1 is also co-prime to m. So, therefore, this there may be a kind of ambiguity about this, let us make it clear, so a is greater than equal to 1.

So, the definition of Euler’s Totient function is as follows: that if the number of integer in Zm, where m is greater than 1 that are relatively prime to m and does not exceed m; therefore, these numbers are essentially lesser than m. So, it will be kind of lesser than m means, it will be kind of from 0 to m minus 1. Because they belong in Zm, and Zm actually has 0; also the numbers will vary from 0 to m minus 1 and those numbers of values which are co-prime to m, we need to find them and they are kind of denoted by some letter, which is called as phi m that is the symbol of the Euler’s Totient function and this is also sometimes referred to as a phi function.

(Refer Slide Time: 33:14)

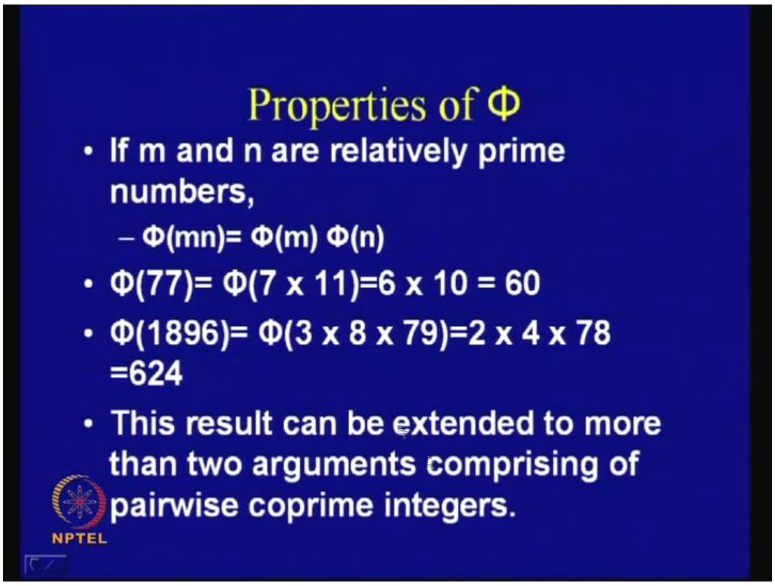


Example

- m=26 => Φ(26)=12
- If p is prime, Φ(p)=p-1
- If n=1,2,…,24 the values of Φ(n) are:
  - 1,1,2,2,4,2,6,4,6,4,10,4,12,6,8,8,16,6,18,8, 12,10,22,8
  - Thus we see that the function is very irregular.

So, as you as you will remember that, if m is equal to 26, we have seen that, phi of 26 is 12. If p is a prime number, then phi of p is p minus 1, and if you vary like m from 1 to 24 these are some of the value of phi n and we can actually see that phi n does not have a nice nature; it is not a monotonically increasing value, even a monotonically non-decreasing value. You see that, if you start increasing n, there example there are cases, where actually the values of phi n dimensions like from 12 to 6, there is a reduction.

(Refer Slide Time: 33:51)



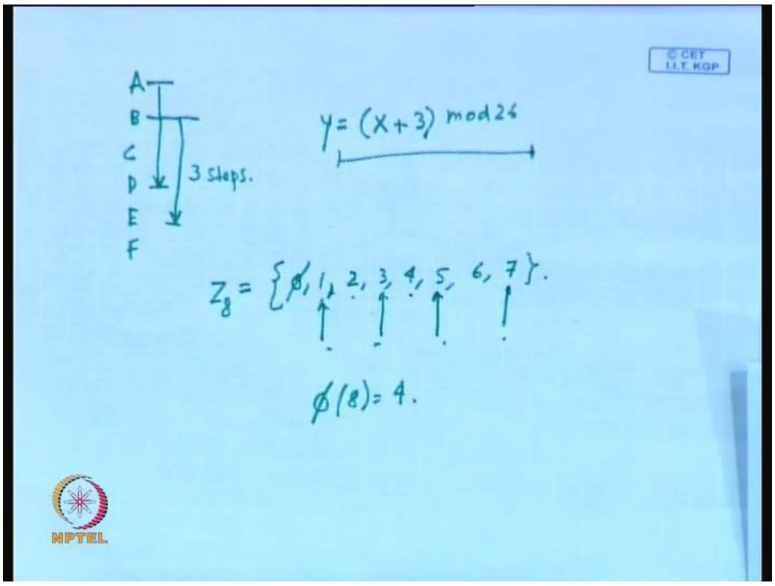
Properties of Φ

- If m and n are relatively prime numbers,
  - Φ(mn)= Φ(m) Φ(n)
- Φ(77)= Φ(7 x 11)=6 x 10 = 60
- Φ(1896)= Φ(3 x 8 x 79)=2 x 4 x 78 =624
- This result can be extended to more than two arguments comprising of pairwise coprime integers.

So, we see that the function is very irregular and therefore, we kind of would like to have a way of calculating the phi m. So, there is a result which says m and n are relatively prime numbers, then phi of m n is equal to phi of m multiplied by phi. So phi of 77 will be in this result; if i factorize this 7 into 11 will be equal to phi of 6 multiplied by phi of 7 using this result, and phi of 6 is essentially is equal to, I mean, phi of 7 multiplied by phi of 11, and phi of 7 is 6 why because since 7 is a prime number, then of course from 0 to p minus 1, there are six numbers which are actually co-prime to 7, because all the numbers are co-prime except 0; 0 is not a co-prime by our definition. So, if you take a… and the phi of 11 will be essentially equal to 10, that is, minus 1; so 11 minus 1, again 0 is not there.

So, that means, that this is equal to 10 therefore, that is 6 to 10 is 60, but what about phi of 1896? So, you can again factorize, it will be phi that is equal to 3 into 8 into 79 and all of them are prime numbers, so this into prime factorization and therefore, 5 of 3 will be equal to 2 phi of 8; phi of 8 is phi of 2 q and this is not a prime number actually, but if you if you kind of like that in that in terms of its prime factors, then this will be this is equal to 2 q and we can say that, this is equal to 5 of 8 will be actually equal to 4, and we can actually see this, that phi of 8 is 4 and then you have got phi of 79 which is 78.

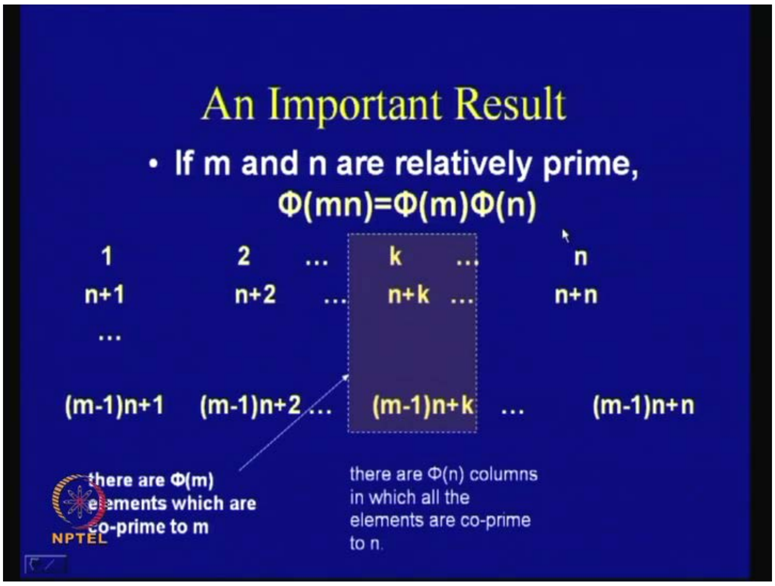
(Refer Slide Time: 35:30)



So, why is phi of 8 equal to 4? You can easily verify this, because if the numbers if you take the numbers from 0, 1, 2, 3, 4, 5, 6 and 7, then these are the number which are belonging to Z 8, you immediately cancel out 1; this is co-prime; this is not co-prime; this is co-prime; this is not a co-prime; this is co-prime and this is co-prime. So, there are 4 such values therefore, phi of 8 is equal to 4.

So, therefore, if I use this fact here, then phi of 3 into 8 into 79 will be equal to 2 into 4 into 7 8 that is equal to 624. So, this result can be extended to more than two arguments comprising of pair-wise co-prime integers.

(Refer Slide Time: 36:21)



An Important Result

- If m and n are relatively prime, $\Phi(mn)=\Phi(m)\Phi(n)$

1	2	…	k	…	n
n+1	n+2	…	n+k	…	n+n
…					
(m-1)n+1	(m-1)n+2	…	(m-1)n+k	…	(m-1)n+n

there are $\Phi(m)$ elements which are co-prime to m

there are $\Phi(n)$ columns in which all the elements are co-prime to n.

So, we will try to kind of again reflect upon the proof, which we kind of hurried up in the last class. So, phi of m n is equal to phi of m multiplied by phi of n.

So, what we have done here is that, we are kind of laid down the numbers from 1 to m n. So, actually we should have done from 0 to m minus 1, but if you see, I mean, with the background of the number theory discussion which we have done, you know that is same as the enumerating from 1 to m n. Because m n if you take mod m n is nothing but 0 therefore, you can actually numerate the number from 1 to m n; so this is nothing but m n; you see that the m minus 1 n plus n, so that is m n.

So, these numbers are actually written in a array kind of function; so 1, 2 and so on to n and again the next row is n plus 1, n plus 2 so on to n plus k to n plus n and similarly, there are m rows and n columns. So, we need to find out 5 m n, which means that, we need to find out those numbers which are co-prime to m n and you note that m and n are relatively prime. So, that means, that these numbers have to be co-prime to both m and both n; so it has to be co-prime to both m and n.

So, first of all let us see the columns. So, you see, let us try to find out there are columns or rather the numbers which are co-prime to n. So, you see how the numbers are noted down; so these numbers are, I mean, if you just observe say a particular column, then we will see that the numbers are like k, n plus k and m minus 1 till so on like this to m minus 1 into n plus k. If this numbers have to be co-prime to n, then by our previous days discussion we know that, the remainder if i just for example, if you take n and if you divide it by n, so this number is n plus k; if you divide it by n, then the remainder is k and if this number has to be co-prime to n, then it means that, key has to be, remainder has to be co-prime to n.

So, that means, that the same holds for all of them. You see that this is m minus 1 into n plus k, again the remainder is k and if this number has to be co-prime with n, then k has to be co-prime with n; the same holds for this one also. That means, that if this number, if this entire column, I mean, if k is co-prime to n, then all these numbers are co-prime to n therefore, if k is I repeat, if k is co-prime to n, then all these numbers are co-prime to n. So, that means, how many if i need kind from these number if I am interested in finding out how many numbers are co-prime to n, then obviously I need to find out those numbers which I mean from 1 to n, which are all the possible values of k and which are co-prime to n. And we know by the previous definition that, there are phi n such values which are co-prime to n; from 1 to n, there are phi n such values which are co-prime to n.

So, that means, that there are phi n columns in which all the elements are co-prime to n. Now, let us consider assume that k is co-prime to n and we let us find out how many numbers among these n numbers the n numbers are here which are actually co-prime to n.

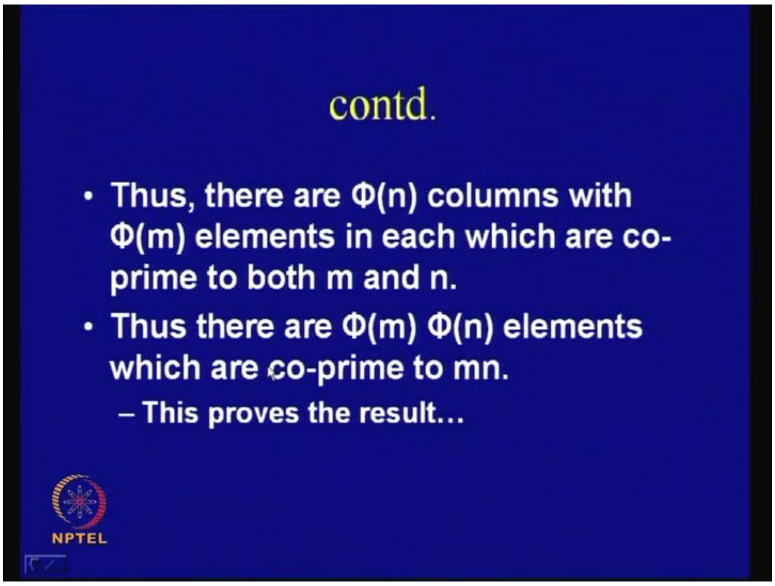
We know that, in this again, these are number like from k, n plus k and so on to m minus to 1 into n plus k. We know that there are phi n elements which are actually co-prime to n; we know that there are phi n values which are co-prime to n.

So, therefore, we if therefore, if I can kind of apply both of them, so there are again so I repeat, there are phi n columns which are actually there are phi n columns in which all the elements in the columns, all the numbers are co-prime to n and if you just take one of those column, where this particular k is actually co-prime to n, then in this column, there are phi n elements which are co-prime to n.

So, therefore, if I need to find out the number of elements which are co-prime to both m and both n, then we just need to find out, we just need to multiply phi n with phi m, that is, phi n will give us the number of columns, where which are co-prime to n, and if I multiply with phi n, I get exactly those numbers which are co-prime to both m and n. It is the kind of very interesting proof and very interesting regard very useful regard.

So, therefore, phi of m n, where m and n are relatively prime is nothing but the product of phi m and phi n.

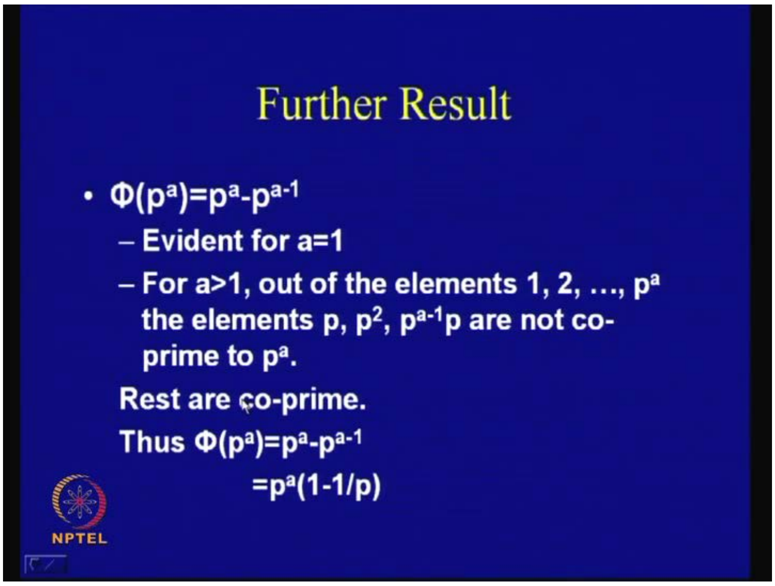
(Refer Slide Time: 40:40)



contd.

- Thus, there are $\Phi(n)$ columns with $\Phi(m)$ elements in each which are co-prime to both m and n.
- Thus there are $\Phi(m)$ $\Phi(n)$ elements which are co-prime to mn.
  - This proves the result…

(Refer Slide Time: 40:44)



Further Result

- $\Phi(p^a)=p^a-p^{a-1}$
  - Evident for a=1
  - For a>1, out of the elements 1, 2, …, p^a the elements p, p^2, $p^{a-1}p$ are not co-prime to p^a.

Rest are co-prime.

Thus $\Phi(p^a)=p^a-p^{a-1}$

$=p^a(1-1/p)$

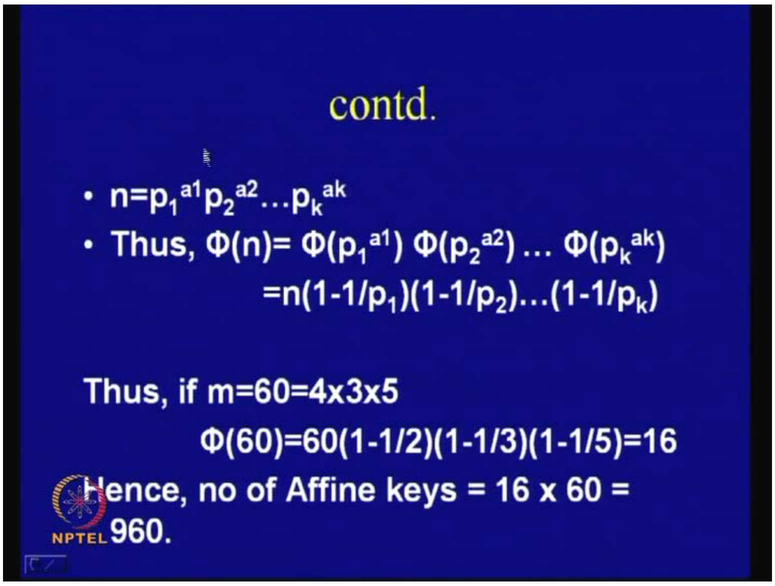
So, now, what we do is that, I mean, this is a kind of conclusion of the previous days proof and so, we can actually apply this to find out phi of phi p to the power of a; phi of p to the power of a is nothing but p to the power of a minus p to the power of a minus 1 why? Because this evident for a equal to 1, we have seen this already that, phi of p is p minus 1; so that is the evident. For a greater than 1, let us try to find out what is phi of p to the power of a, for a greater than 1.

So, the numbers could be like 1, 2 and so on till the p to the power of a; so, there how many numbers are there from 1, 2, to p the power of a? There are p to the power of a numbers in total; from there let us subtract those numbers which are not co-prime to p to the power of a and just a little bit of observation. You can actually understand, whether numbers which are not co-prime to p to the power of a or rather which are not co-prime to p to the power of a are actually p, p square, p to the power of a minus 1. So, it is just steering like that, it is like this till p to the power of a; actually they should be some dots here.

P, p square and so on and till p to the power of a, so p, p square and you just keep on kind of adding on to the power. So, therefore, p multiplied with the next power and so on. So, how many such powers are how many elements are there? If you just observe this various p to the power of a has been written, it is p to the power of a minus 1 into p therefore, the power here has actually varied from… So, there are actually how many possible values? there Actually you will find that, if you just find out the numbers of such terms which are there , is nothing but p to the power of a minus 1. So, therefore, there are p to the power of a minus 1 values or one elements which are actually not co-prime to p to the power of a.

So, therefore, you need to subtract from p to the power of a, p to the power of a minus 1 those numbers which are no co-prime to p to the power of a and therefore, you can actually represent these are p to the power of a multiplied by 1 minus 1 by p, this is same way of writing this.

(Refer Slide Time: 42:38)



contd.

- $n=p_1^{a1}p_2^{a2}\ldots p_k^{ak}$
- Thus, $\Phi(n)=\Phi(p_1^{a1})\,\Phi(p_2^{a2})\ldots\Phi(p_k^{ak})$
  $=n(1-1/p_1)(1-1/p_2)\ldots(1-1/p_k)$

Thus, if m=60=4x3x5

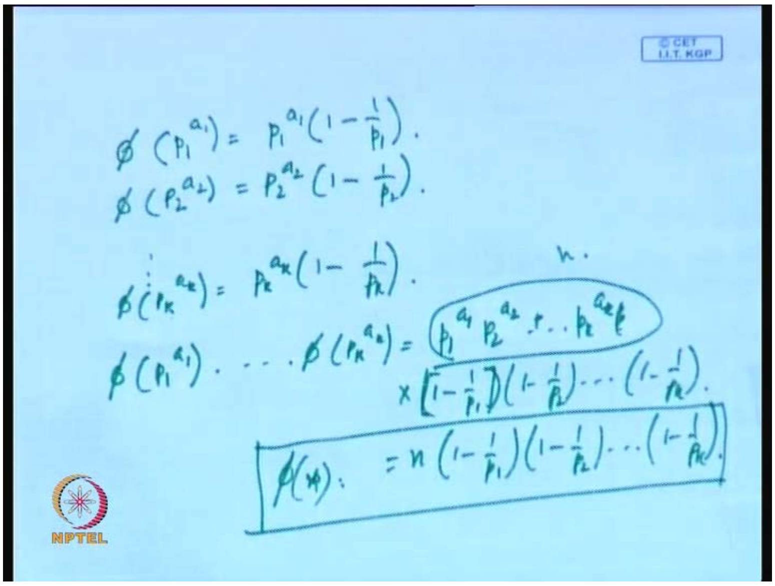
$\Phi(60)=60(1-1/2)(1-1/3)(1-1/5)=16$

Hence, no of Affine keys = 16 x 60 = 960.

So, therefore, the in then if you need to kind of find out the phi of n, then you know that from the fundamental theory of arithmetic, you can actually factorize any n of like this, like p 1 to the power a 1 p 2 to the power of a 2 and so on Pk to the power of ak. And therefore, phi is nothing but phi of p 1 to the power of a 1 multiplied by phi of p 2 to the power of a 2 and so on.

Because of the simple fact that, p to the power of a 1 and p 2 to the power of a 2 are co-prime to each other, you can actually write them like this, and then, you can actually apply the theorem of, I mean, the formula of phi of m n is equal to phi of m into phi of n. When m and n are co-prime successively, you can apply them tentatively over more than two values like m and n and therefore, you can actually get this particular equation and therefore, by the previous thing that you can remember phi of p 1 to the power of a 1 is nothing but p 1 to the power of a 1 into 1 minus 1 by p 1.

(Refer Slide Time: 43:35)



© CET I.I.T. KGP

$$\phi(p_1^{a_1}) = p_1^{a_1}\left(1 - \frac{1}{p_1}\right).$$

$$\phi(p_2^{a_2}) = p_2^{a_2}\left(1 - \frac{1}{p_2}\right).$$

$$\vdots$$

$$\phi(p_k^{a_k}) = p_k^{a_k}\left(1 - \frac{1}{p_k}\right).$$

$n.$

$$\phi(p_1^{a_1}) \cdots \phi(p_k^{a_k}) = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \times \left[1 - \frac{1}{p_1}\right]\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

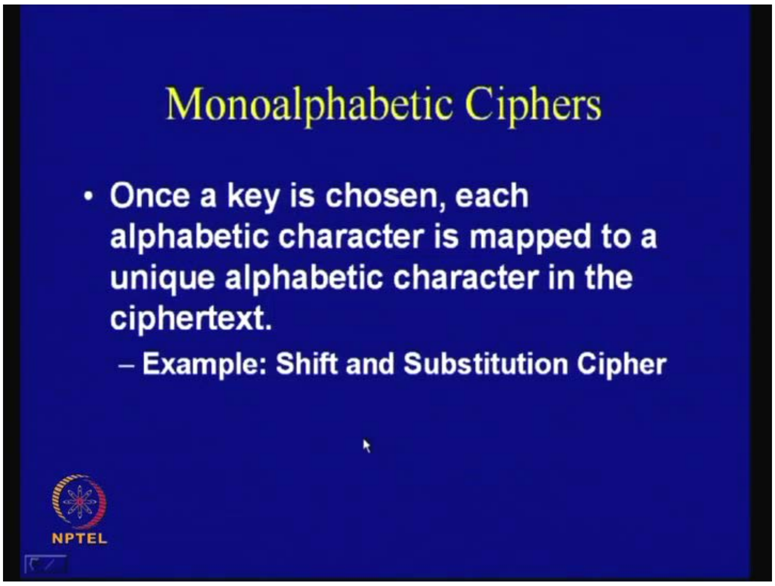
$$\boxed{\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).}$$

You know that, phi of p 1 to the power of a 1 is nothing but p 1 to the power of a 1 into 1 minus 1 by p 1. So, similarly, phi of p 2 to the power of a 2 is nothing but p to the power of a 2 into 1 minus 1 by p 2; so similarly, till phi of Pk to the power of ak is equal to Pk to the power of ak into 1 minus 1 by p k.

So, now, if you kind of find out phi of p 1, multiply all these things till phi of Pk to the power of ak, then what you get is, p 1 to the power of a 1 multiplied by p 2 to the power of a 2 and so on till Pk to the power of ak into, so this will be multiplied by 1 minus 1 by p 1 1 minus 1 by p 2 and so on till 1 minus 1 by Pk.

This essentially can be actually substituted by n itself; so you get n into 1 minus 1 by p 1 into 1 minus 1 by p 2 and so on till 1 minus 1 by Pk. So, this is the formula to compute the value of phi n; phi n is nothing but this. So, phi n is n multiplied by 1 minus 1 by p 1 1 minus 1 by p 2 and so on till 1 minus 1 by Pk.(Refer Slide Time: 44:50) So, phi of 60, you can verify phi of 60 like them as 4 into three into 5, then you know that this is equal to 60 into 1 minus 1 by 2, because 2 is the prime factor, and then, 1 minus 1 by 3 and 1 minus 1 by 5, this actually works out to 16. So, therefore, if instead of 26, if you use 60, then the number of affine keys actually increases to 16 multiplied by 60 that is 960, so that is increased.

(Refer Slide Time: 45:21)



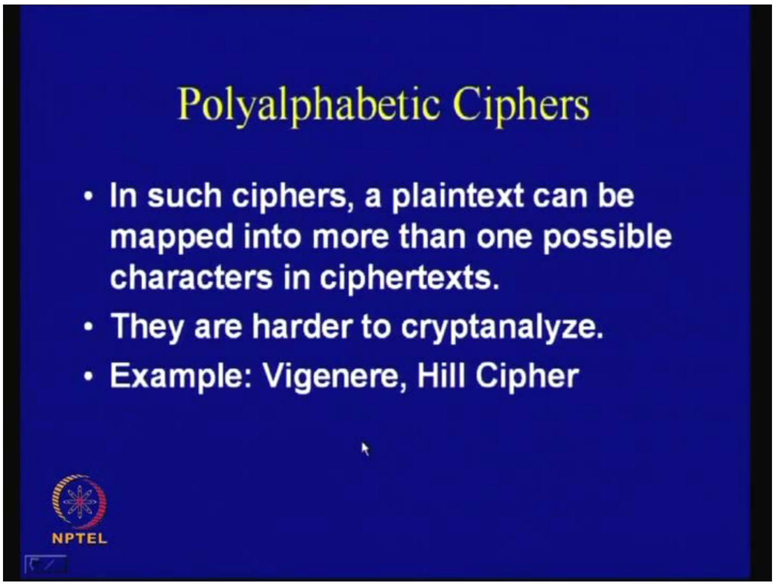
Monoalphabetic Ciphers

- Once a key is chosen, each alphabetic character is mapped to a unique alphabetic character in the ciphertext.
  - Example: Shift and Substitution Cipher

So, similarly, you can actually calculate the number of affine keys for larger values of m also, but you need the but you need to keep one thing in mind, that is, you need the prime factors. And factorization, actually this problem becomes more and more complex as you start dealing with larger numbers.

So, then we will discuss… so we have actually talked about something which is called a monoalphabetic character, that is, once a cipher once key is chosen, each alphabetic character is mapped into unique alphabetic character in the ciphertext; examples of them are shift ciphers substitution ciphers.

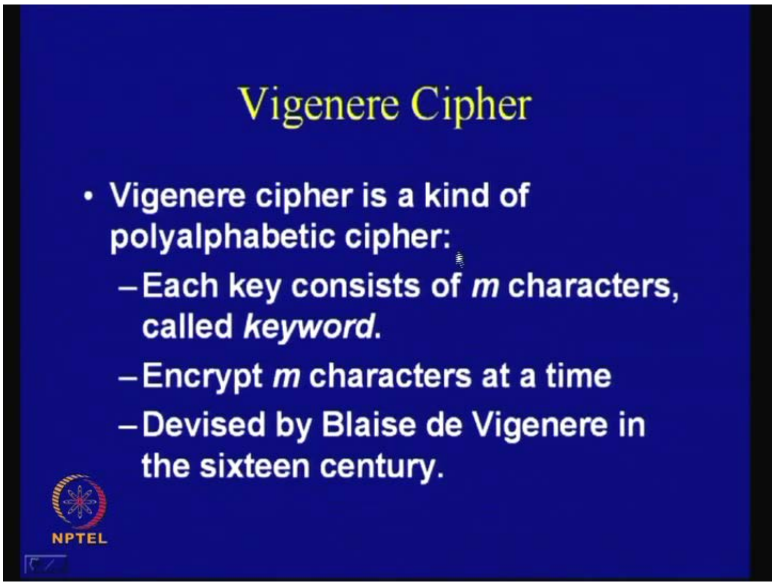
(Refer Slide Time: 45:49)



Polyalphabetic Ciphers

- In such ciphers, a plaintext can be mapped into more than one possible characters in ciphertexts.
- They are harder to cryptanalyze.
- Example: Vigenere, Hill Cipher

(Refer Slide Time: 46:04).

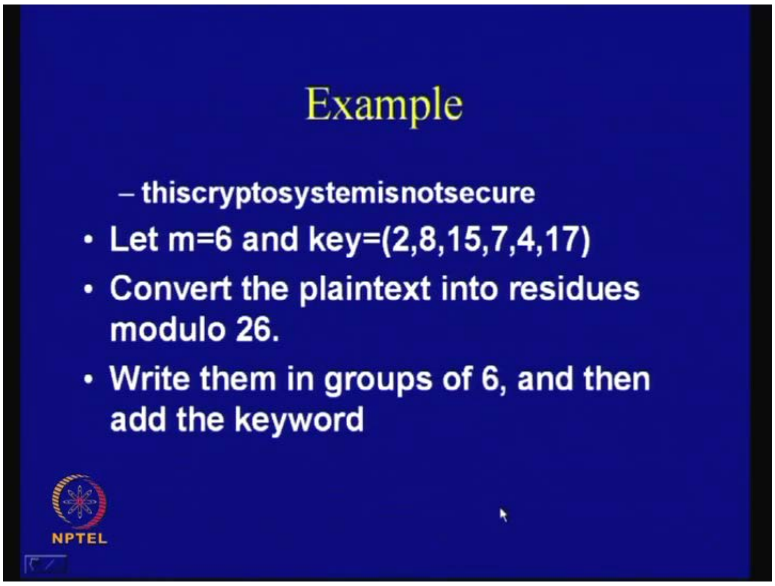


Vigenere Cipher

- Vigenere cipher is a kind of polyalphabetic cipher:
  - Each key consists of *m* characters, called *keyword*.
  - Encrypt *m* characters at a time
  - Devised by Blaise de Vigenere in the sixteen century.

Now, we will discuss about something which is called poly alphabetic cipher. So, in this cipher, a plaintext can be mapped into more than one possible characters in ciphertext. So, they are harder to cryptanalyse, examples of them are Vigenere cipher and the Hill cipher. So, Vigenere cipher is a kind of polyalphabetic cipher and each key essentially consist of m characters, which are called as keywords and encrypts. So, the idea is that, you encrypt m characters at a time and this was defined designed by Vigenere in the 16th centuries. So, it is we can see that, it is very old cipher also.

(Refer Slide Time: 46:21)

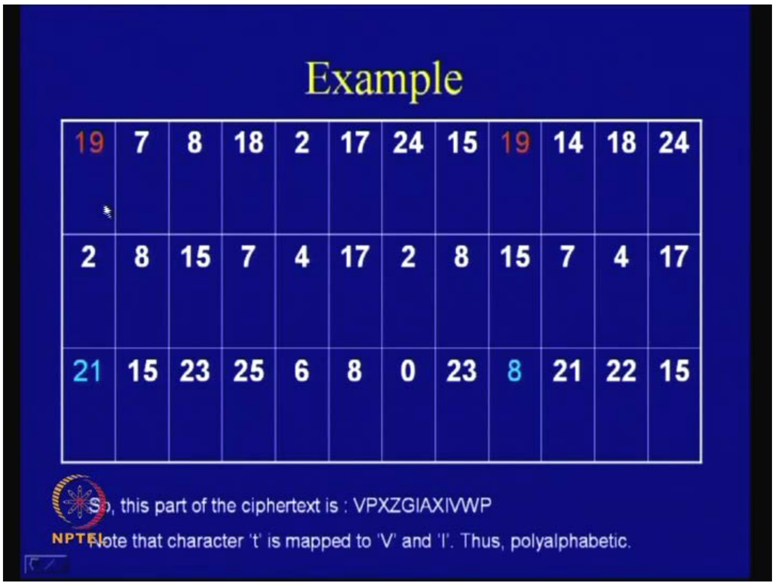


Example

- thiscryptosystemisnotsecure
- Let m=6 and key=(2,8,15,7,4,17)
- Convert the plaintext into residues modulo 26.
- Write them in groups of 6, and then add the keyword

So, the idea is like this, that is suppose your example is this cryptosystem is not secure this is the plaintext and if you take m is equal to 6, which is the size of the key, let the key will be instead of one number, be a pair like, I mean, we have tuple be a kind of set of numbers like 2, 8, 15, 7, 4 and till 17. So, what you do is that, you convert the plaintext into residues module 26 and write them in groups of 6, and then, add the keyword; so that is the idea.

(Refer Slide Time: 46:50)



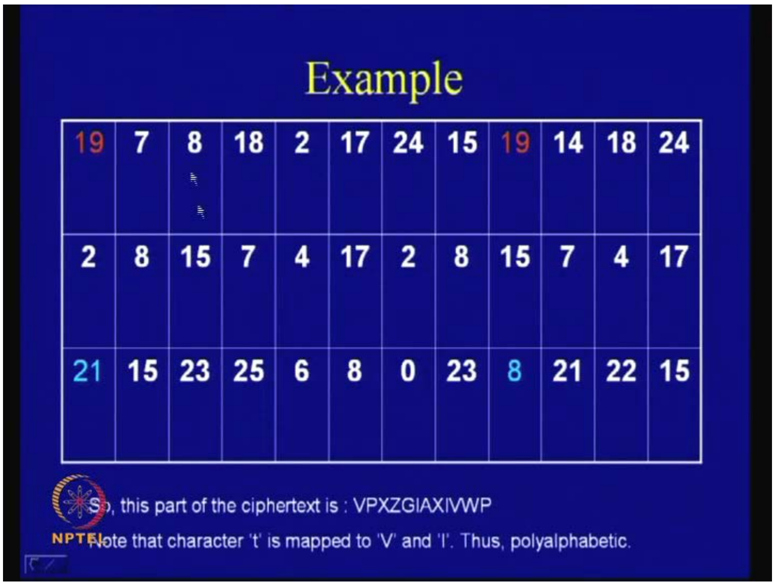
Example

19	7	8	18	2	17	24	15	19	14	18	24
2	8	15	7	4	17	2	8	15	7	4	17
21	15	23	25	6	8	0	23	8	21	22	15

So, this part of the ciphertext is : VPXZGIAXIVWP

Note that character 't' is mapped to 'V' and 'I'. Thus, polyalphabetic.

(Refer Slide Time: 46:52).



Example

19	7	8	18	2	17	24	15	19	14	18	24
2	8	15	7	4	17	2	8	15	7	4	17
21	15	23	25	6	8	0	23	8	21	22	15

So, this part of the ciphertext is : VPXZGIAXIVWP

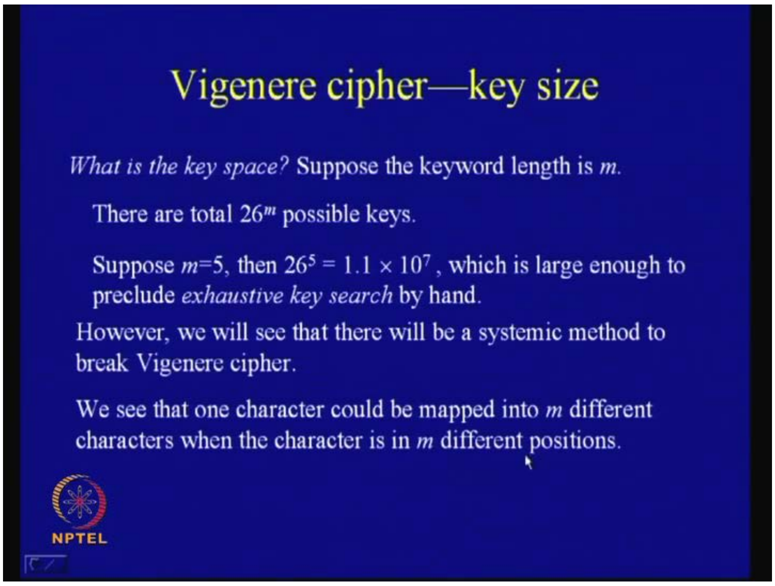
Note that character 't' is mapped to 'V' and 'I'. Thus, polyalphabetic.

So, just see that, if you see that the numbers are… if you take these numbers like this, cryptosystem is not secure; convert the plaintext into the set of numbers, and then, you start writing this key as like this 2, 8, 15, 7, 4, 17; again repeat 2, 8, 15, 7, 4, 17 again keep on repeating as the plaintext goes on. Now, you start adding the modular 26 therefore, you take 19, you add 2, 21 modular 26, it is 26; so you can get 7, you add 8, you get 15, I mean, it is modular 26, it is 15. So, similarly, you start doing this transformation, you see that there are two occurrences of 19 here in the plaintext, but because of this arrangement of the key in this case, 19 is getting modified by the key material 2, but here it is getting modified by the keying material 15; and as a natural consequences here you get 21, whereas here you get 8.

So, which means that, the same plaintext as we saw in the monoalphabetic ciphers, this would always have got mapped into a unique later. But, in case of a polyalphabetic ciphers, this letter is getting sometime mapped into a one number, but sometime getting mapped into a different number. And as you can see that, there are six possible values in this particular key; this number 19 can get mapped into six possible ciphertext values. So, that is the basic concepts of a polyalphabetic cipher, that is, the mapping is not unique, but it can vary depending upon the size of the key.

So, this part of the ciphertext here is this and you can note that, the character t is mapped to v and i therefore, it is called polyalphabetic; there are two possible in this shown here, actually there are six possible values, because that depends upon the size of the key.

(Refer Slide Time: 48:22)



Vigenere cipher—key size

What is the key space? Suppose the keyword length is m.

There are total 26^m possible keys.

Suppose m=5, then $26^5 = 1.1 \times 10^7$, which is large enough to preclude *exhaustive key search* by hand.

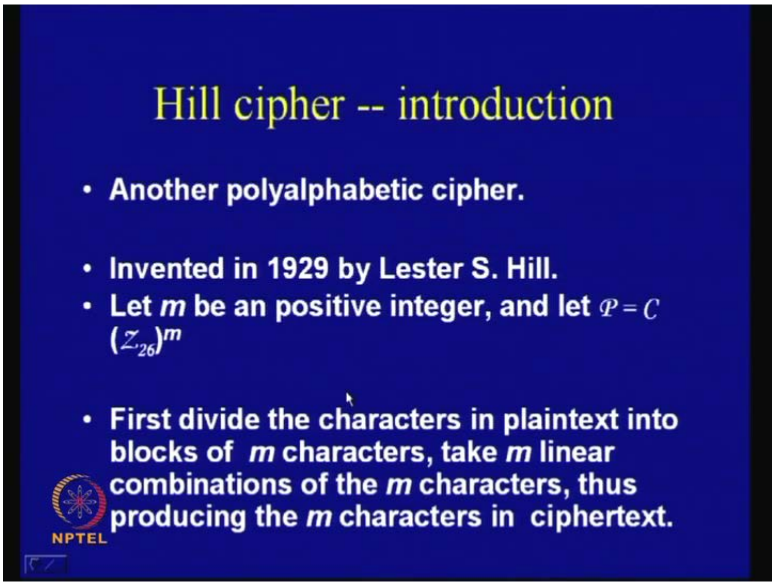
However, we will see that there will be a systemic method to break Vigenere cipher.

We see that one character could be mapped into m different characters when the character is in m different positions.

So, we would be interested in finding out what is the key space. Suppose the key word length is m and therefore, there are 26 to the power of m possible keys, each of them can be 26 values. So, there are 26 to the power of m possible key values. Suppose m equal to 5, then 26 to the power of 5 is this, which is actually large enough to preclude any exhaustive key search. Exhaustive key search is not possible however, we will see that there is there can be a systemic method to break Vigenere cipher and that we will be discussing in the next day’s class.

But we see that, one character could be mapped into m different characters when the character is in m different positions. So, there are m possible mappings for a particular character, where m is the length of the key size of the key.

(Refer Slide Time: 49:17)



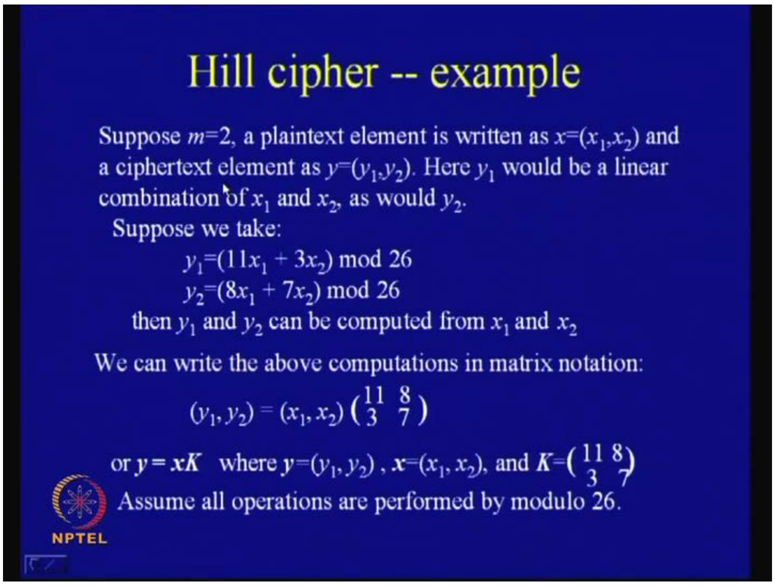
Hill cipher -- introduction

- **Another polyalphabetic cipher.**
- **Invented in 1929 by Lester S. Hill.**
- **Let *m* be an positive integer, and let $\mathcal{P} = \mathcal{C}$ $(\mathcal{Z}_{26})^m$**
- **First divide the characters in plaintext into blocks of *m* characters, take *m* linear combinations of the *m* characters, thus producing the *m* characters in ciphertext.**

So, we will discuss about the cipher, which is called Hill cipher, which is another polyalphabetic cipher and it was defined designed around 1929.

So, you see that, here, I mean, we are going more into the modern day cipher slowly that, is if you see that m be a positive integer, and let p and c both are kind of Z 26 to the power of m, so that is kind of the m possible values. First divide the characters, that is, which are in the plaintext into blocks of m characters, then you take m linear combinations of m characters, thus producing the m characters in ciphertext.

(Refer Slide Time: 49:49)



Hill cipher -- example

Suppose m=2, a plaintext element is written as x=(x_1,x_2) and a ciphertext element as y=(y_1,y_2). Here y_1 would be a linear combination of x_1 and x_2, as would y_2.

Suppose we take:

y_1=(11x_1 + 3x_2) mod 26

y_2=(8x_1 + 7x_2) mod 26

then y_1 and y_2 can be computed from x_1 and x_2

We can write the above computations in matrix notation:

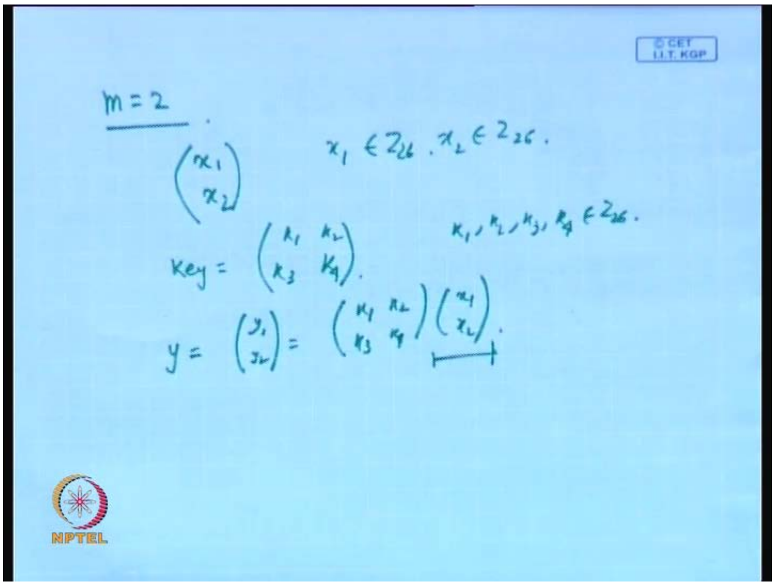
$$(y_1, y_2) = (x_1, x_2)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

or $\boldsymbol{y} = \boldsymbol{x}K$ where $\boldsymbol{y}$=(y_1, y_2) , $\boldsymbol{x}$=(x_1, x_2), and K=$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$

Assume all operations are performed by modulo 26.

So, mathematically it means like this. So, let us take a small example, where m is equal to 2, so you're plain your you can here do like this that is. So, I am considering the m is equal to 2 case.

(Refer Slide Time: 50:00)



$m = 2$.

$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ $\quad x_1 \in Z_{26}$. $x_2 \in Z_{26}$.

$\text{key} = \begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix}$. $\quad k_1, k_2, k_3, k_4 \in Z_{26}$.

$y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$.

So, let us consider a plaintext say x1 and x2; so you see that x1 belongs to z 26 and x2 also belongs to z 26. So, there are both of them are z 26 elements and you take x1 and you take x2, assume that you have got a keying material, which for example, write as, so the key here could be like k1 k2, k3 and k4 you arrange them in a matrix format, where k1 k2 k3 and k4 all of them are z at present from z 26.

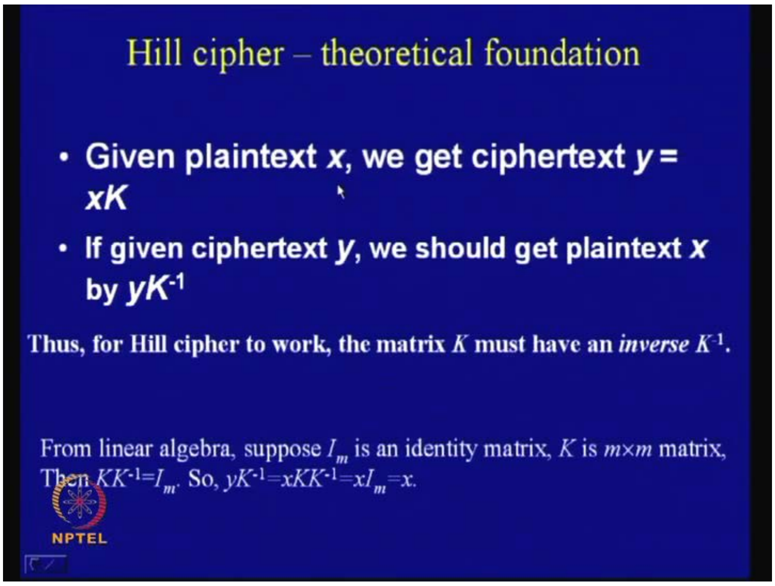
So, then you define your operation as this, they which is the ciphertext is y1 y2 is equal to nothing but the multiplication k1 k2, k3 k4 multiplied with x1 x2. So, if you now if you need to find out the x1 x2 from this, then obviously you need the inverse of this matrix; so therefore the inverse of this matrix needs to be defined.

So, you can actually see an example here, that is, it says that (y1, y2) is equal to (x1, x2) and therefore, you can actually write the it is written out like this; so it could be a matrix either pre multiplied or post multiplied. So, it depends upon the way it has been arranged like, it is arranged as a one cross two in this case vector. So, therefore, the multiplication you have to appropriately apply, pre-multiply or post multiply depending upon the way you are writing this (x1, x2) pair, so this vector.

So, what so what is essentially done is that, if you see, if you break up, these are nothing but linear transformation of this order. So, y1 is instead 11 x1 plus 3 x2 mod 26 and y2 is 8 x1 plus 7 x2 mod 26 which is been written in this way. So, this 11, 3, 8 and 7 are actually the piece of information which is the key. So, you see that, which is like extension of the affine cipher and it goes closer to the cipher concept that we have today, which is called block cipher.

So, it is a kind of kind of a breach from this classical notation to a modern notation. So,S you see that, here you can actually write that as y is equal to k x k and where y is equal to (y1, y2) and x equal to (x1 , x2). So, where all these operations are performed modular k, but the important point is that, for the injectivity as we have seen in context of affine cipher, we need the inverse of this keying material.

Refer Slide Time: 52:23)



Hill cipher – theoretical foundation

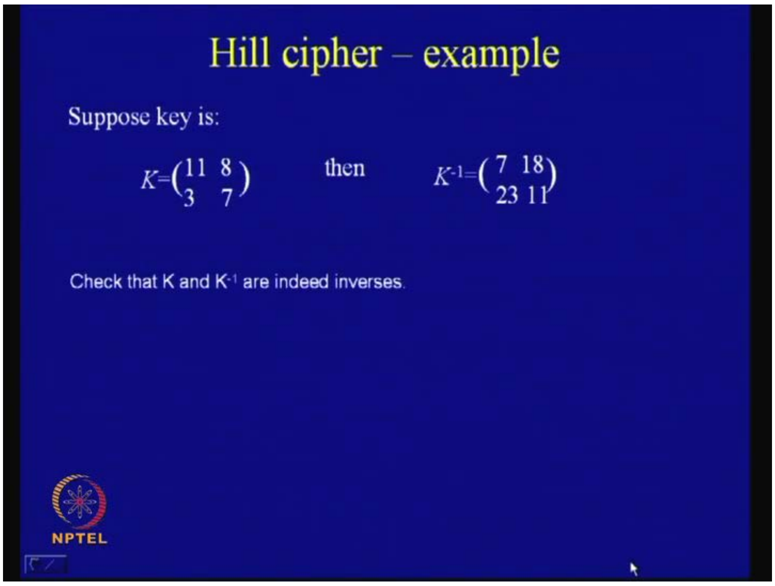
- Given plaintext *x*, we get ciphertext *y* = *xK*
- If given ciphertext *y*, we should get plaintext *x* by yK^{-1}

Thus, for Hill cipher to work, the matrix K must have an *inverse* K^{-1}.

From linear algebra, suppose I_m is an identity matrix, K is $m \times m$ matrix, Then $KK^{-1}=I_m$. So, $yK^{-1}=xKK^{-1}=xI_m=x$.

So, therefore, you see that, given a plaintext k x, we get ciphertext y, but in order to have inverse , we actually need the inverse of this matrix; and if you know that, if the inverse of the matrix exist, that is, if you would take k and there is ak inverse; if you multiply and you get back the identity cipher, then immediately you know that, if you take y and if you multiply with k inverse that is nothing but y can be written as x k from the definition, that is, y is equal to x k, then y is equal to x k; and then multiply with k inverse. So, you know that k and k inverse if you multiply, you get I m and therefore, x of I m is nothing but x; therefore, obtain back the plaintext x.

Refer Slide Time: 53:15)



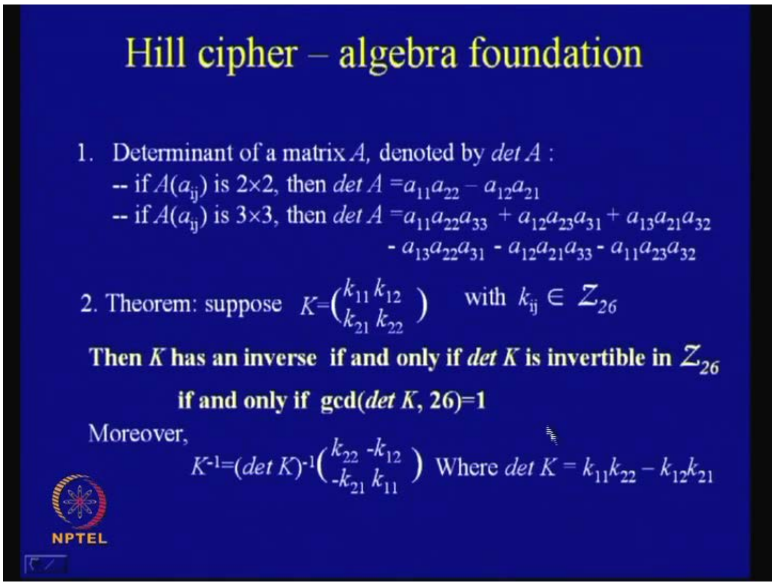
Hill cipher – example

Suppose key is:

$K=\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$ then $K^{-1}=\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$

Check that K and K^{-1} are indeed inverses.

Refer Slide Time: 53:18)



Hill cipher – algebra foundation

1. Determinant of a matrix A, denoted by $\det A$:
   -- if $A(a_{ij})$ is 2×2, then $\det A = a_{11}a_{22} - a_{12}a_{21}$
   -- if $A(a_{ij})$ is 3×3, then $\det A = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}$

2. Theorem: suppose $K=\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$ with $k_{ij} \in Z_{26}$

Then K has an inverse if and only if $\det K$ is invertible in Z_{26}

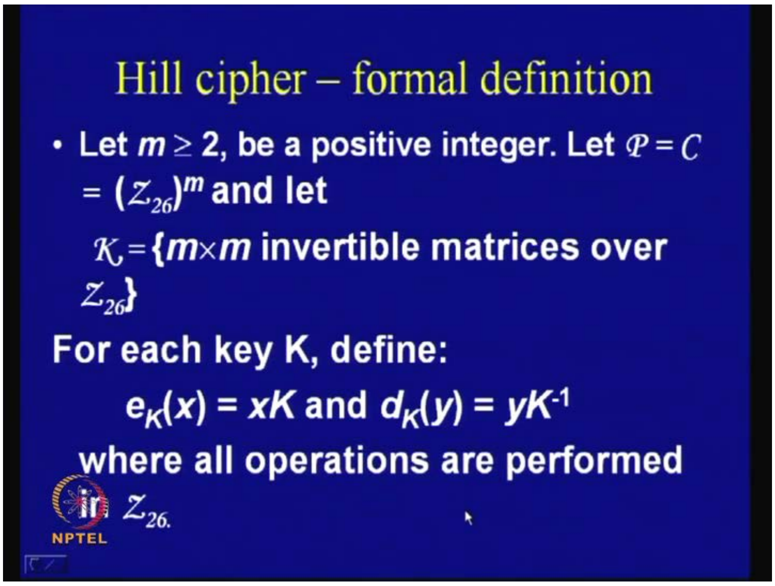
if and only if gcd($\det K$, 26)=1

Moreover,

$K^{-1}=(\det K)^{-1}\begin{pmatrix} k_{22} & -k_{12} \\ -k_{21} & k_{11} \end{pmatrix}$ Where $\det K = k_{11}k_{22} - k_{12}k_{21}$

Therefore, the important criteria is that, the inverse of this matrix needs to exist. So, thus for Hill cipher to work, the matrix k must be invertible; there should be an inverse which is called k inverse. Now, we know that, when, I mean, to give an example, you can work out. So, refer the important condition is that k is to have an inverse. So, we say that k has an inverse if and only if determinant of k is invertible in z 26. If you know from our basic course in matrix algebra is that, k inverse is nothing but 1 by determinant of k and this is the kind of you know what this is. So, you can you can write them as a co-factors therefore, using the co-factors therefore, the most important thing is that, you can always multiply, but the thing is that, this determinant k and inverse of that needs to exist, which means the determinant k inverse needs to exist which means that determinant k is inverse needs to exist and when will the determinant of k inverse exist in modular 26? It can exist if and only if the gcd of the determinant of k and 26 is equal to 1. This is quite easy to follow from our previous description that means, that k is an inverse if and only if determinant k is invertible in z 26 and that means that if and only if gcd of determinant of k and 26 is equal to 1.

(Refer Slide Time: 54:20)



Hill cipher – formal definition

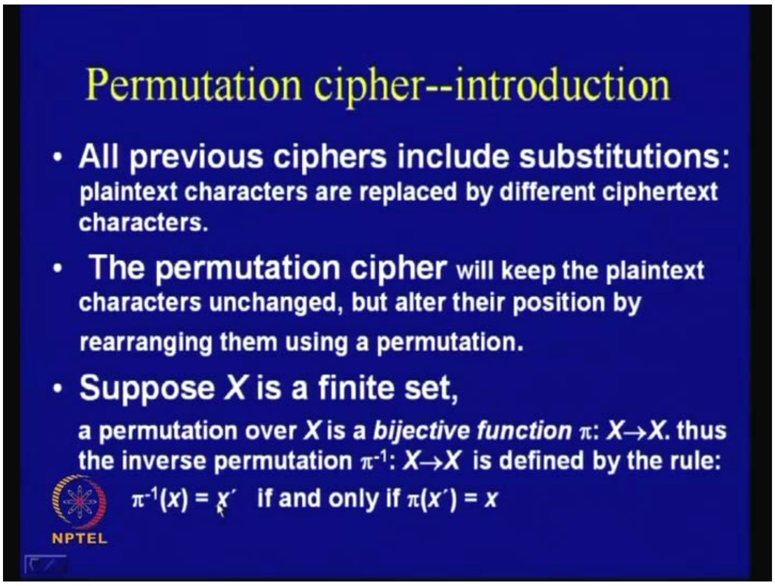
- Let $m \geq 2$, be a positive integer. Let $\mathcal{P} = \mathcal{C} = (\mathcal{Z}_{26})^m$ and let $\mathcal{K} = \{m \times m$ invertible matrices over $\mathcal{Z}_{26}\}$

For each key K, define:

$$e_K(x) = xK \text{ and } d_K(y) = yK^{-1}$$

where all operations are performed in $\mathcal{Z}_{26}$.

(Refer Slide Time: 54:32)



Permutation cipher--introduction

- All previous ciphers include substitutions: plaintext characters are replaced by different ciphertext characters.
- The permutation cipher will keep the plaintext characters unchanged, but alter their position by rearranging them using a permutation.
- Suppose X is a finite set, a permutation over X is a *bijective function* $\pi: X \to X$. thus the inverse permutation $\pi^{-1}: X \to X$ is defined by the rule:

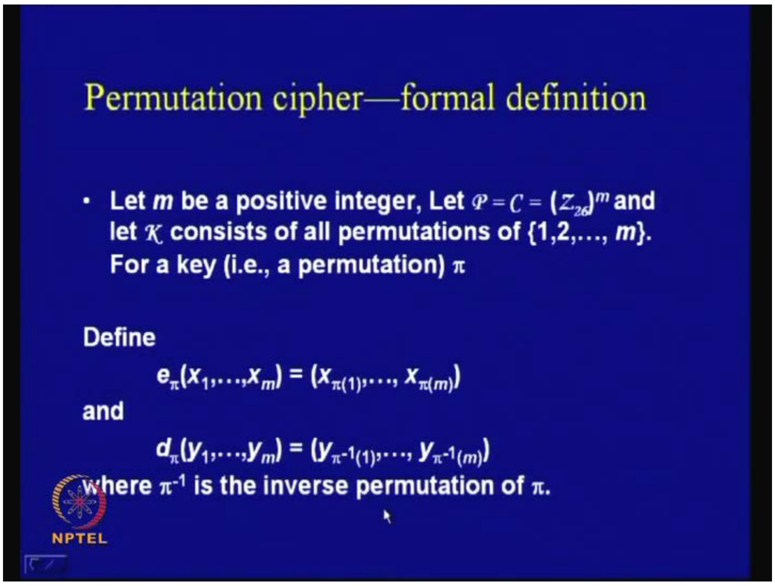
$$\pi^{-1}(x) = x' \quad \text{if and only if } \pi(x') = x$$

Therefore, the formal definition is like this; so you take x, you multiply with x k and decryption is also defined as this, but only it needs to be an invertible therefore, you can actually compute the size of the key using this.

A slight extension of this is called permutation cipher; all previous cipher include substitutions, where which are actually taken a plaintext characters are replaced by the different ciphertext characters, which also forms a very important component of modern ciphers substitution ciphers, and then, the other component is the permutation ciphers, which will keep the plaintext characters unchanged, but will alter their position by rearranging them using a permutation.

Suppose X is a finite set. a permutation over X is a bijective function, you know that which is denoted by phi from X to X, this is the mapping. Thus the inverse permutation is actually again back from X to X and defined by phi inverse. It is defined by the rule as follows, that is, phi of inverse of x is equal to x dash if and only if phi of x dash is equal to x therefore, that is the definition of a permutation cipher.

(Refer Slide Time: 55:25)



Permutation cipher—formal definition

- Let m be a positive integer, Let $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$ and let $\mathcal{K}$ consists of all permutations of $\{1,2,\ldots, m\}$. For a key (i.e., a permutation) π

Define

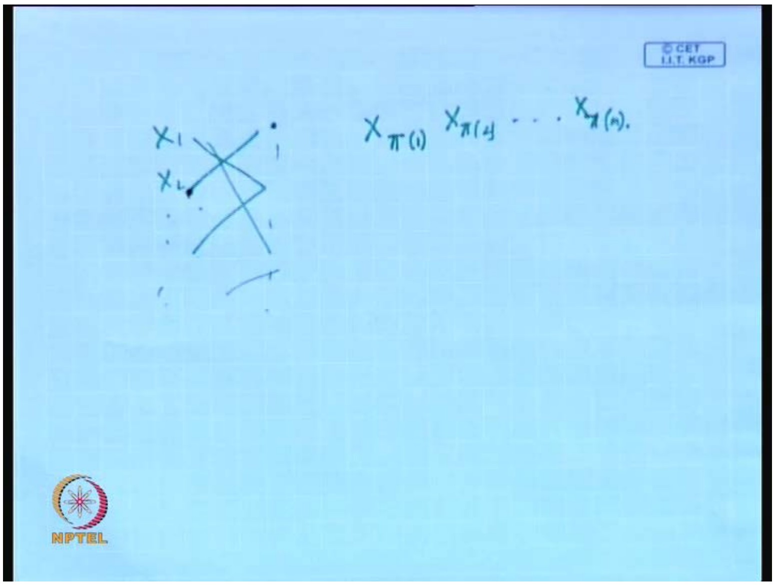
$$e_\pi(x_1,\ldots,x_m) = (x_{\pi(1)},\ldots, x_{\pi(m)})$$

and

$$d_\pi(y_1,\ldots,y_m) = (y_{\pi^{-1}(1)},\ldots, y_{\pi^{-1}(m)})$$

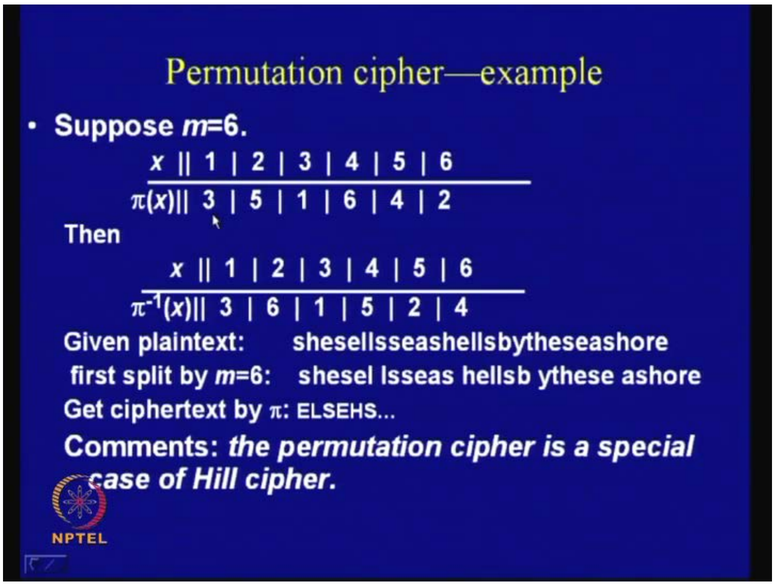
where π^{-1} is the inverse permutation of π.

(Refer Slide Time: 55:55)



So, what you can do is that, you can take from x1 to x m. So, these are suppose the numbers like, which form the plaintext from x1 to x m, and then, you start rearranging them. So, x1 goes to a different location; x2 goes to a different location and so on, but the basic character the set of character remain unaltered. So, therefore, x the index of this is denoted by phi 1. So, what essentially get kind of transformed are the index locations we will take. So, any permutation, you can actually denote like this; like you take x1, x2 and so on what you are doing is a rearrangement in a permutation; you are just doing a rearrangement. So, this location gets changed to x1; this essentially becomes x1, which essentially was x2 in this case.

(Refer Slide Time: 56:26)



Permutation cipher—example

- Suppose m=6.

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

Then

x	1	2	3	4	5	6
$\pi^{-1}(x)$	3	6	1	5	2	4

Given plaintext: shesellsseashellsbytheseashore

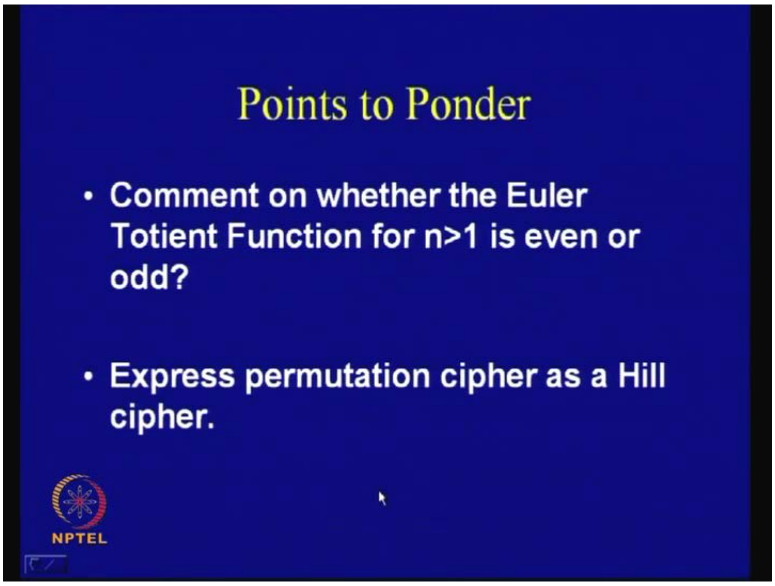
first split by m=6: shesel lsseas hellsb ythese ashore

Get ciphertext by π: ELSEHS...

Comments: *the permutation cipher is a special case of Hill cipher.*

So, we will actually denote them as x of phi 1, x of phi 2 and so on. So, if there are n values, then x of phi m, so all of them are nothing indicating that the characters index position is changed. So, therefore, you can actually denote them using this, that is, this is just a notation of the permutation and this is an example you have like, you take 1, 2, 3 and till 6 and therefore, what you have done here is that, you just kind of transformed them; from 1 goes really to 3; 2 goes to 5; 3 goes to 1; 4 goes to 6 and so on and similarly, you can define the inverse permutation also.

(Refer Slide Time: 56:54)

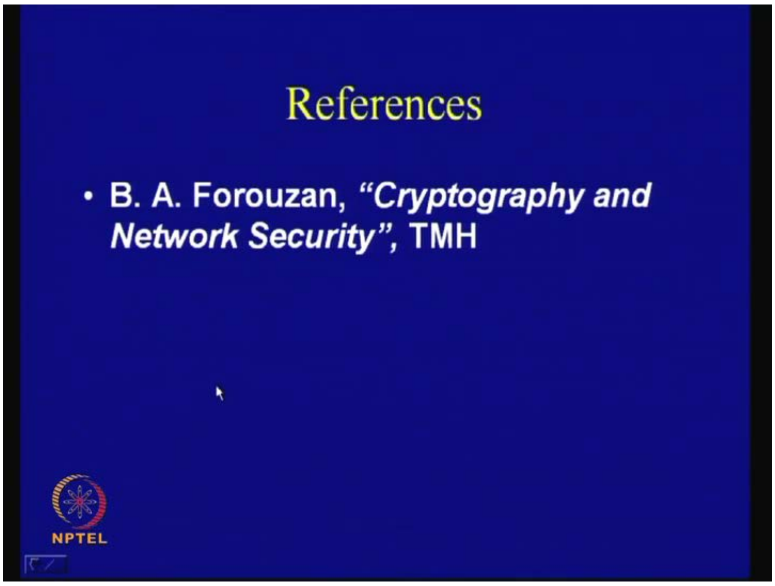


Points to Ponder

- Comment on whether the Euler Totient Function for n>1 is even or odd?
- Express permutation cipher as a Hill cipher.

So, this problem therefore, you can actually there is a small comments made here, the permutation cipher is a special case of Hill cipher. So, I leave it to kind of a exercise to reflect upon this point, that is, y is it y is it so. And this give you some points to ponder, that is, one of them is that you have to comment on whether the Euler Totient function for n greater than one is even or odd; you need to kind of give an argument in your favor and express permutation cipher as a hill cipher.

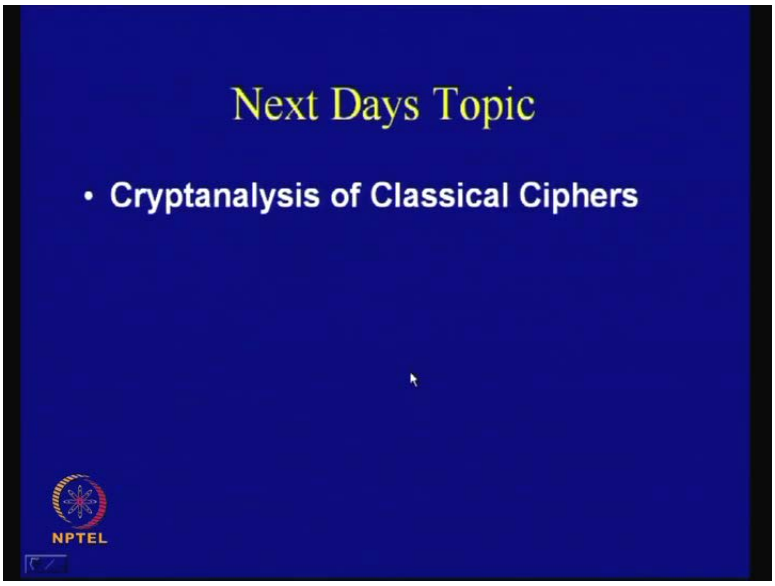
(Refer Slide Time: 57:09)



References

- B. A. Forouzan, *"Cryptography and Network Security"*, TMH

(Refer Slide Time: 57:14)



Next Days Topic

- Cryptanalysis of Classical Ciphers

So, these are some problems given to you. So, the references that I have used is cyptography and network security and next day, we will discuss be discussing about the cryptanalysis of classical ciphers.