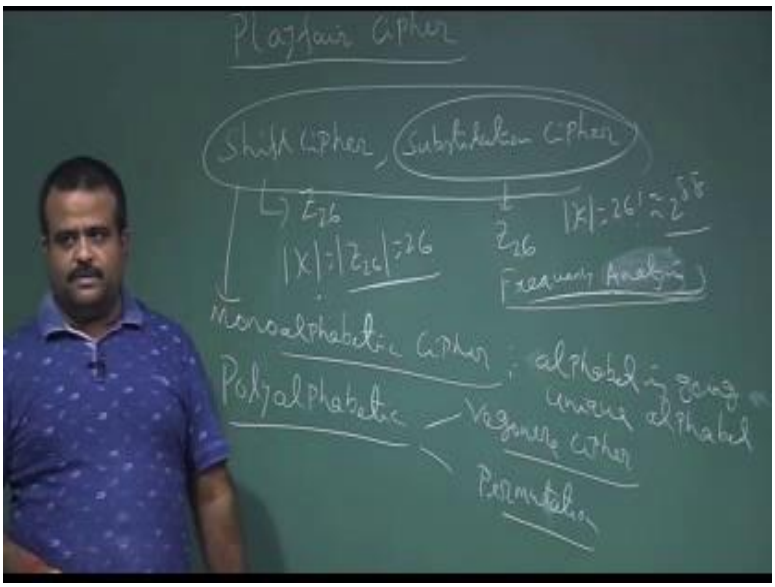
Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 04
Play Fair Cipher

(Refer Slide Time: 00:25)



So far we have seen some classical cryptosystem like shift cipher then the substitution cipher and we have seen the problem with shift cipher is basically the key size is Liberian layers basically the key size is Z, the key is coming from Z 26. So, size of the key space is basically cardinality of this Z. So, this is basically 26 which is broked by the which is not secured because of the less key size and it is 26 only. So, one can try for 26 possibilities and get the key. So, this was attacked by the Brute-Force method.

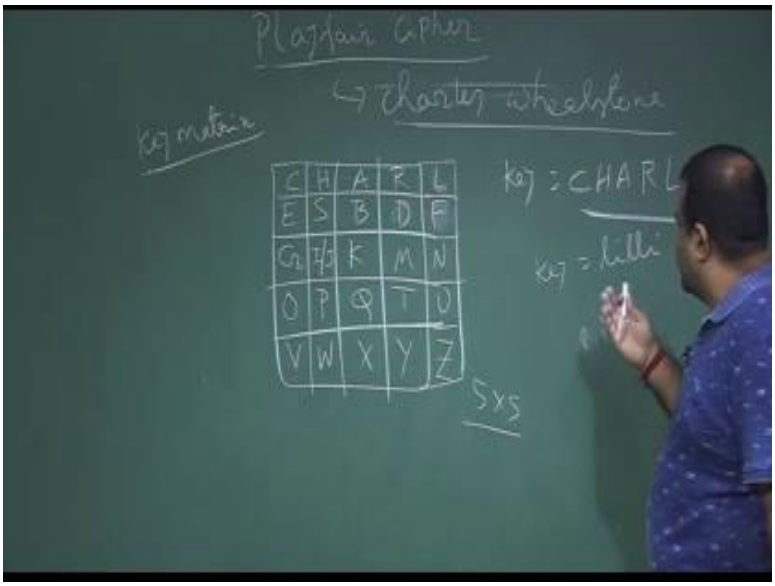
Then we talk about substitution cipher which is key is basically the set of all permutations I mean key space is set of all permutations over Z 26 and that set is basically 26 factorial which is roughly 2 to the power 88 which is very I mean which is very large. So, the exhaustive search or the Brute-Force setup cannot be may not be feasible for this big size, but we have seen if we are since we are using the English text for the plaintext then English text is having some certain frequency phenomena of the lateral wall of the alphabet e is the most frequent letter then t then a. So, by that frequency analysis we have seen a attack on this. So, that is by frequency attack on this

substitution cipher substitution cipher. So, it is also broked under this frequency analysis or the frequency attack so then so, these are basically what is called the substitution cipher and the shift cipher these are mono alphabetic cipher mono alphabetic cipher. So, basically a alphabet is going to a unique alphabet.

A alphabet so, this mapping player going to a going into a unique alphabet not a alphabet is going to many alphabets like the poly alphabetic cipher, we have seen regeneration cipher we have seen the permutation cipher, unique alphabet and on the other hand. So, because of this the frequency analysis is frequency analysis, frequency attack on be mount, but to avoid this we talk about this what is called poly alphabetic cipher and there we have seen 2 cipher so far one is Vigenere cipher and the second one is transportation cipher or permutation cipher, permutation cipher and there a frequency analysis may not be. So, easy because this is a poly alphabetic so; that means, each alphabet is not going to a unique alphabet it can be going to a different different alphabet you have seen on example arrays is going to some different different alphabets.

Now today in this lecture we will see another poly alphabetic cipher which is basically called play fair cipher. So, this is also an example of poly alphabetic cipher. So, this was invented by Charles.

(Refer Slide Time: 05:01)



Charles Wheatstone; Wheatstone, so, the idea is to have a matrix which is basically a 5 by 5 matrix. So, let us have a 5 by 5 matrix 1, 2, 3, 4, 5, 1, 2, 3, 4, 5. So, this is a 5 by 5

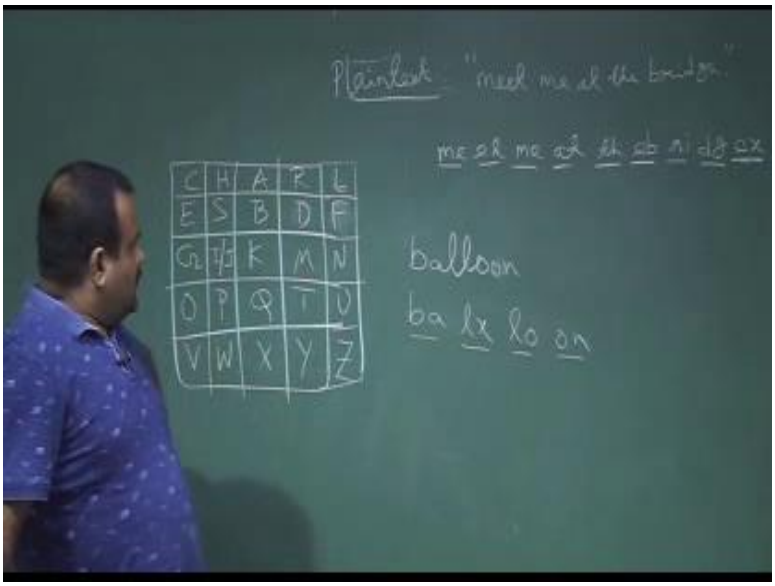
matrix so; that means, total number of total entries are 25. So, this is a 5 plus 5 matrix now this is called key matrix. So, we will use, we will put our key in this matrix and without we will we will not repeat any letter in this matrix. So, how many alphabets are there? We know in English 26 alphabet, but there are only 25 spaces. So, what we do. So, 2, 2, 2, alphabet should be kept in a single slot. So, they are basically I and N. So, I and J are kept in this a single slot. So, what we do? How we will make this matrix; key matrix? This is key matrix.

Suppose we take a key like Charles the invented name C H A R L E S. So, what we do? We first write this name, we just fill this first row, second row like this using that key first. So, we will fill this C H A R L E S. So, this will put in a first we will fill up this matrix this is row wise usually and then we will fill up all the remaining alphabet designed in my English alphabet set. So, A is over. So, we do not need to put A B, B is not over. So, we will put B then C, this is L, C D is not over D sorry, this is B and C is over, actually C is over C we have already seen. So, D is not over. So, D will put here and then we will put F over here E because E is over E is already well. So, there will be no repetition no repetition no repetition in the alternate.

That means, we just fill up this E D F then G and then we have to fill I and I and J will sit together because there is no on space is less. So, they have to sacrifice. So, K M N O P Q R, R is already there. So, we will not put R, S; S is already there, we will not put S again because we are not allowing any repetition T U V W X Y Z. So, this way we fill the matrix. So, this is called key matrix. So, it depends on the key word we fill the matrix. So, if there is repetition in this keyword itself so, we will not take that double, we will take 1, suppose our key say lilli l i l l i or something. So, we will just take l then i that is it because l already taken. So, this will not take again anyway. So, suppose this is the key matrix.

Now, how we will encrypt a message. So, message is say so, using the key what, we will make this matrix, it is a 5 by 5 matrix. Now suppose we want to encrypt a message say message is say.

(Refer Slide Time: 10:05)

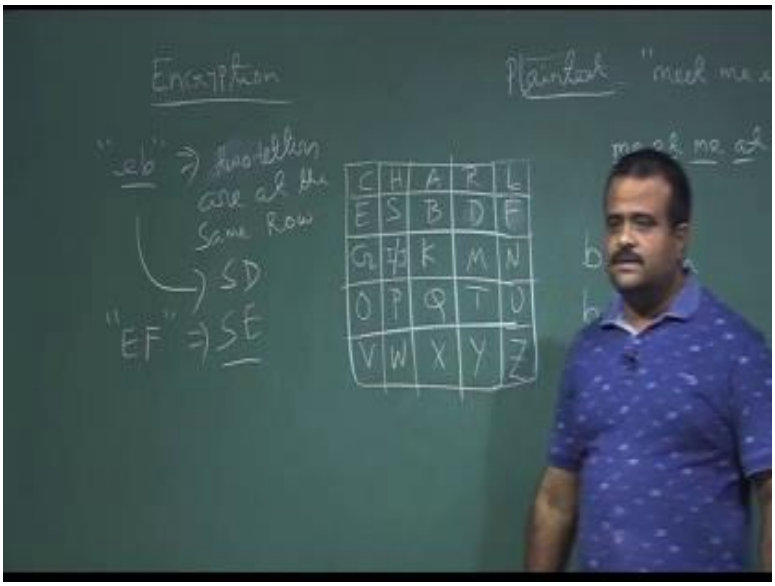


The plaintext is say, this one - meet me at the bridge; meet me at the bridge suppose this is the plaintext, so, what we do? We just take this plaintext into 2 letters together and if it is not, if the last we have 1 letter; we will put a x as a dummy letter. So, if we split this into 2 letter word. So, if we split it so, m e then e t 2 letter word then again me, at, th then eb and then eb is over ri then dg and last you have ae. So, we have to make use ax. So, x we are introducing as a dummy alphabet this x. So, this is the letter, so, ex because last 1 we do not have anything to split it into 2 alphabet like this.

So, now, how we will encrypt it using this and if we have a letter like balloon if we have a letter like balloon; b a l l o n double l o o n balloon. So, if you want to split it by this way. So, it should be b a l l o o n, but this thing you do not like. So, this is wrong. So, you do not want any letter any this 2 bit; 2 bit means 2 letter which is having same alphabet. So, what we do? We will use the dummy letter dummy alphabet x. So, this will split into like this b a then l x. So, this x is the dummy then l o o n. So, all are. So, this all are having 2 letters together without any repetition. So, this way we will split.

Basically we have a given the plaintext we will spit it we will split into 2 letter together now we will have a, we will just how we will encrypt.

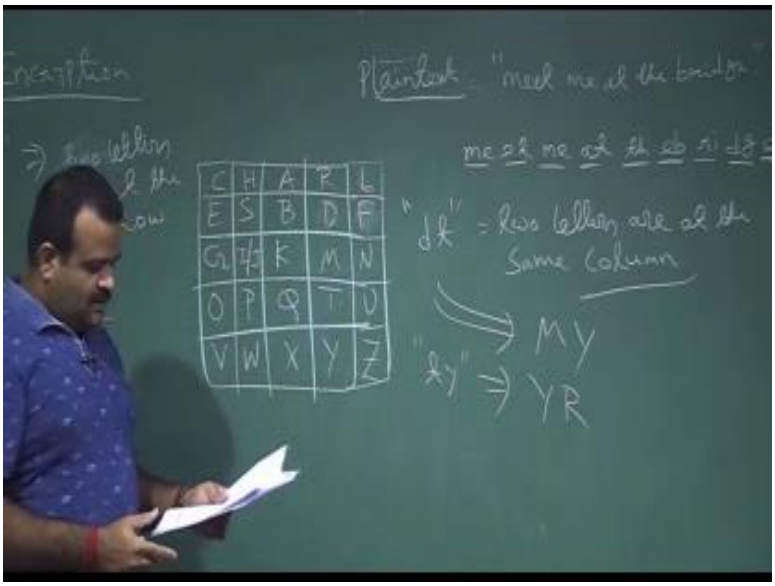
(Refer Slide Time: 12:58)



Encryption process is like this. So, we will encrypt each of these 2 bit letter alphabets by the following way. So, suppose we have to encrypt e d or e b sorry. So, this is suppose the plaintext bit 2 bit. So, how will you encrypt it? So, e b is where e is where e is basically e is here b is also here. So, they are in the same row. So, this rule is for same row. So, 2 letters are at the same row. So, then the corresponding ciphertext block will be s e b e our plaintext is e b. So, ciphertext will be s d. So, this will be basically ciphertext is s d so, basically the next one and next to this.

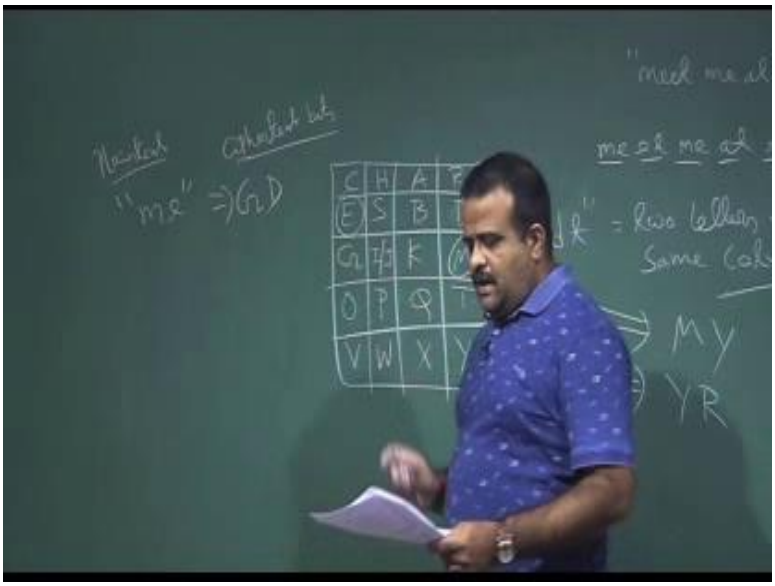
If they are in the same row, now if it is like e f if this is the plaintext then the ciphertext will be what f. So, it is circularly. So, it is basically s and for f it will be e. So, s e like this. So, this is for ciphertext corresponding this plaintext. So, this rule is if there in the same row now suppose there in the in a, suppose they are in the same column so, that you have to see.

(Refer Slide Time: 15:05)



Suppose same column, let us take an example d t, if the d t say in the same call column yeah d t. So, this means the 2 letters are in the same column are at the same column then what we do? We will take the similarly by in the row what we did we take the next one. So, if it is d t. So, d is here t is here. So, we will take this M Y. So, d t is going to this is the ciphertext corresponding to d t M Y and if it is t y if this is t y. So, t y is going to Y R. So, circularly so, for t it is going to next alphabet in that column because they are in the same column t y, so, t, but for this Y it will be R like this. So, so this is the ciphertext corresponding to this plaintext. Now the question is if they are in the, they are not in the same row or not in the same column if they are in the different row and different column.

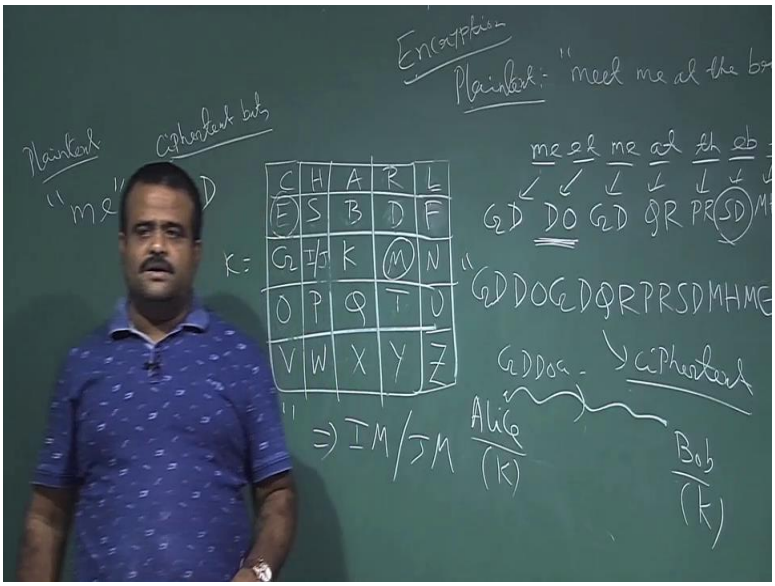
(Refer Slide Time: 16:44)



Let us take an example suppose m e. So, if this 2 letter are not in the same row and same column sorry, so, suppose m e is the plaintext digit I mean letter. So, m is here, e is here. So, they are not in the same row and same column they are in different row and different column. So, what we will do? We will take the corresponding we will take for m, m will be replaced by with the letter which is in the same row and in the same column of the other letter. So, other letter is e. So, it is G. So, m will be replaced by G. So, this will be replaced by G and e will be replaced by D, so, G D.

This is the plaintext 2 bit and this is the corresponding ciphertext 2 bit, ciphertext bits. So, this is the way we will encrypt this plaintext meet me; meet me at the bridge. So, if you do it. So, what will be the corresponding ciphertext? So, let us just try this. So, first letter is first 2 bit is m e. So, m is here e is here.

(Refer Slide Time: 18:12)



It will be basically so, replace by G D then e t, e t basically e t where is e t? e is here t is here. So, e will be replaced by d and t will be replaced by o, this is usually d o. Then again m e then a t. So, a t is basically a is where a is here, t is here. So, basically a will be replaced by Q and t will be replaced by R, so Q R; t h, t h; t is where, t is here, h is here. So, t h so, t will be replaced by P and h will be replaced by R.

It is basically P R and e b; e b is e is here, b is here. So, they are in the same column a same row. So, it will be basically s e b. So, it is basically S D; S D and r i; r i is basically r where is r? R is here, i; i is here. So, it will be basically M H; M H, now d g. So, d is here, g is basically where is g? Yeah g is here, d g. So, it will be replaced by d will be replaced by M and g will be replaced by E, so M E; e x; e x, x is here. So, e will be replaced by V and x will be replaced by B, so V B; V B.

This is the plaintext; this is a ciphertext, GD DO GD QR PR SD MH ME VB. So, this is the ciphertext corresponding to the plaintext, meet me at the bridge. So, this is the encryption, this is encryption, now if we have say GK, suppose our plaintext is GK suppose this is our plaintext then the ciphertext. So, GK is the same row. So, it will be basically either I or J. So, it has 2 options, it is either IM or JM because in this place there are 2 alphabets are sitting together. So, it will be either IM or it will be JM.

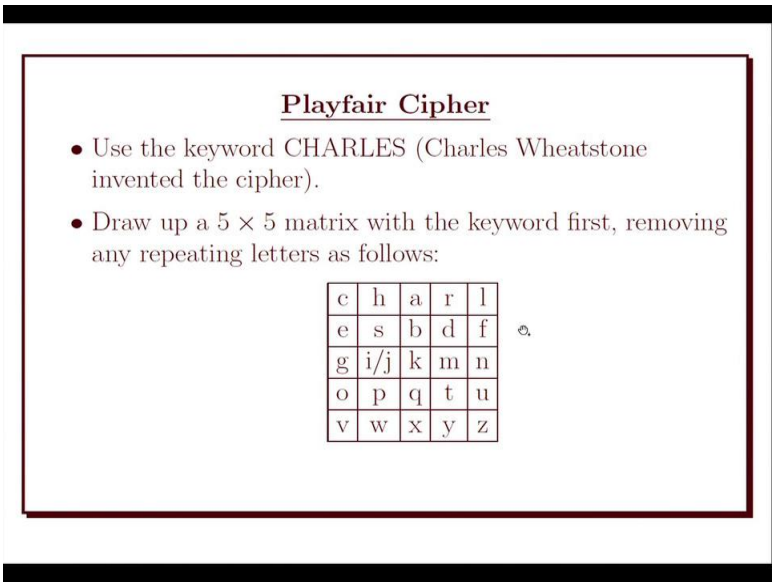
This is the encryption, now how to decrypt it? Say how Bob can decrypt it. So, this is Alice and Bob. So, Alice is Alice wants to send this message to Bob using the play fair

cipher. So, they agreed with this key Charles and they form this they form this Alice form this matrix key matrix and then Alice wants to send this plaintext to Bob that meet me at the bridge. So, this is typically a secret information and is one to pass to Bob. So, what Alice will do? Alice will break it into 2 letters like this and then apply this encryption method which is given by Charles and this is the encryption method and this then Alice got this and this Alice sent to Bob this ciphertext these G D D O G like this.

Now Bob upon receiving the ciphertext Bob has to get back the plaintext. So, how about will this get back the plaintext? How Bob will decipher it? So, Bob has to apply the, so, Bob is getting GD. So, from GD, Bob as to get ME, so, GD is where GD. So, to get ME do, what Bob has to do? So, D, so, G will be replaced by M D will be replaced by E. So, the same technique Bob has to apply E T, so E T sorry, Bob is getting DO DO; D and O. So, if Bob will use the same technique it will be basically D will be replaced by E and O will be replaced by T. So, this decryption is the inverse process of this. So, this you have to keep in mind when we will decrypt it.

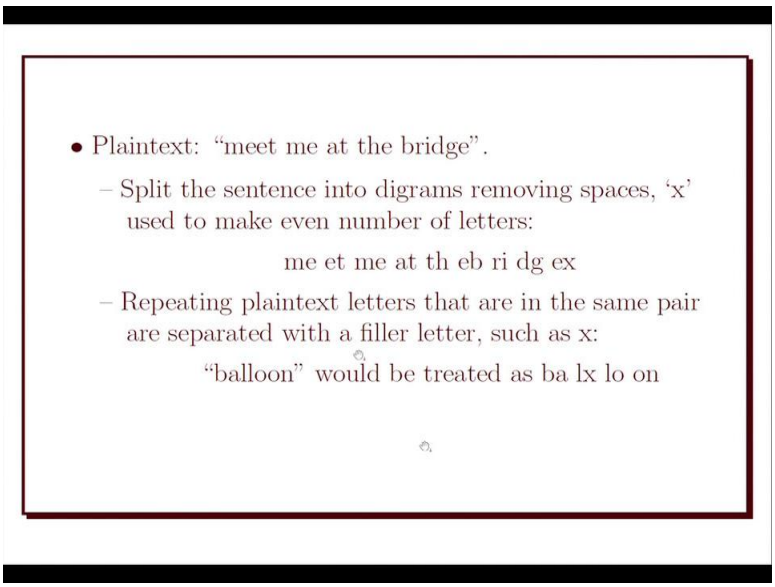
So, then if we have a same letter like R E, so, R I E B E E X E B, E B, so E B was replaced by M H, so, M H, so, E B was either E B of replace by SD. So, I will talk about SD, SD. So, S must be we must get E B, E S S B. So, that decryption is just the reverse of the encryption for encryption in place of cipher, we take the next alphabet in that row, but for decryption we have to take the previous alphabet in that row because this SD when we decrypt it which should give us E B so SD so, this should give us E B so, this is the inverse way of the encryption. This is the play fair cipher, both the decryption and encryption you have discussed.

(Refer Slide Time: 24:48)



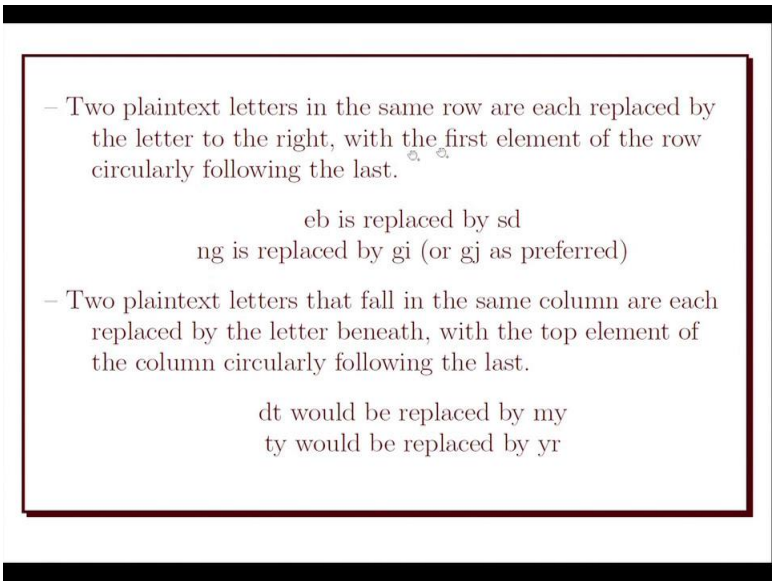
So, this is the technique, this is very nice techniques and this is also called yeah so, come here, this is few slide we made. So, this is the play fair cipher which was invented by Charles and they store chance name we use this key matrix. So, first we write the names without any repetition then we write the then we fill up the remaining alphabet of the English alphabet removing the repetition, we do not want any repetition in this. So, this is the key matrix.

(Refer Slide Time: 25:15)



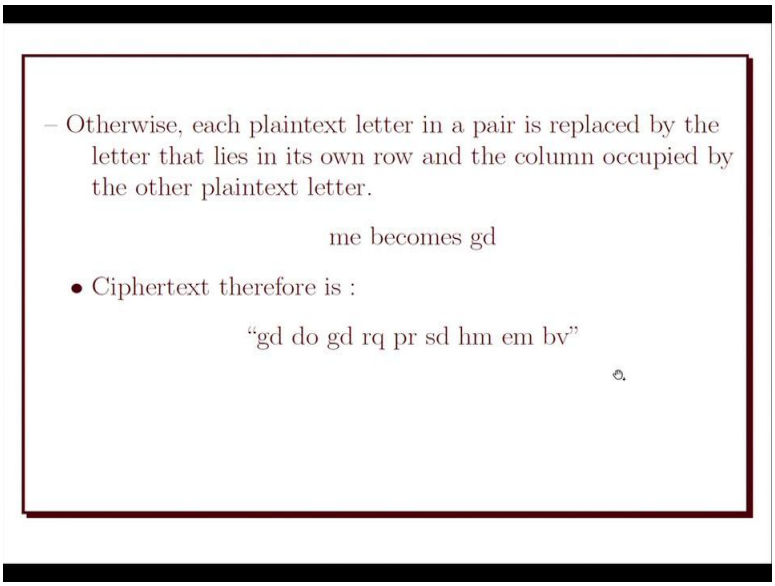
And then we have the following rules like this. So, the f e plaintext we split it into 2 bit letters and if the last one is a single bit we just put a extra bit which is x, extra letter x and the repetition is not allowed in this diabetes. So, if this balloon then we just you have already discussed we just put x there and this will break it up.

(Refer Slide Time: 25:47)



And this is the rule we are using for the encryption and decryption will be the similar rule. So, eb is replaced by sd depending on where it is. So, if it is in the same row then it will be the next row next alphabet in that row and next alphabet in that the second alphabet it is like this. So, ng replaced by this.

(Refer Slide Time: 26:14)



This is, if there in the same column and if they are in the not same column and same row then we know the rule. So, this is the rule and if we apply this rule we get this ciphertext corresponding to the meet me at the bridge. And now the decryption is also the reverse process of it, so decryption will be that just you have to whatever we did in the encryption just the reverse way, but we have to have the same matrix same key matrix. So, key is same so that key should be shared between Alice and Bob. So, this is the key matrix, Charlie is the key. So, this key matrix should be shared between Alice and Bob, I am using this key matrix. So, Bob will just decrypt it using the reverse process of the encryption. So, this is also another example of poly alphabetic cipher.

Thank you.