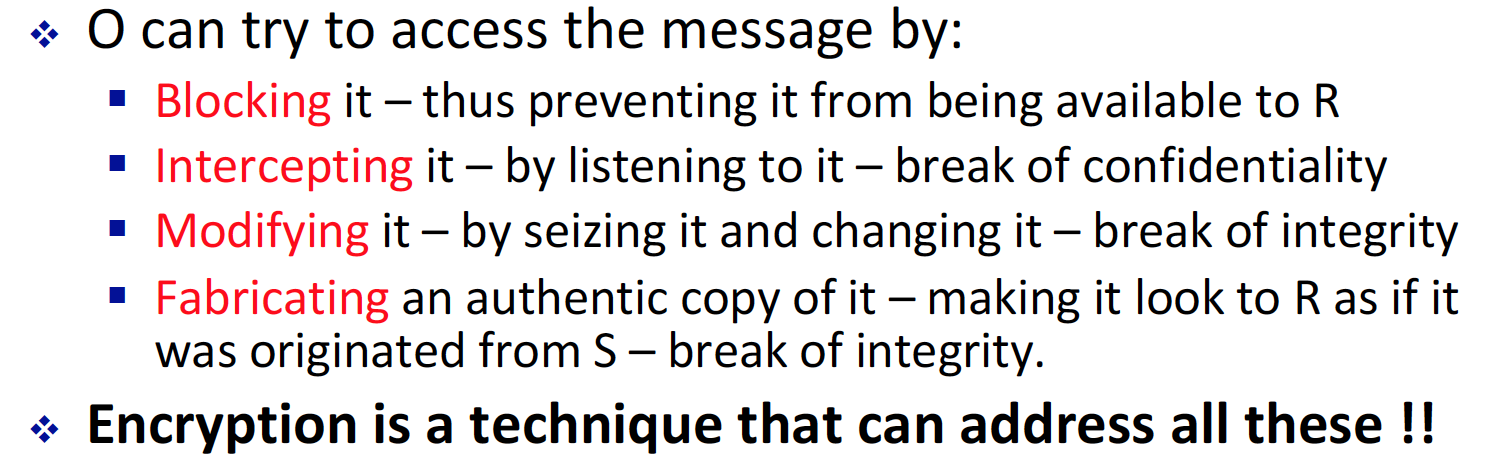
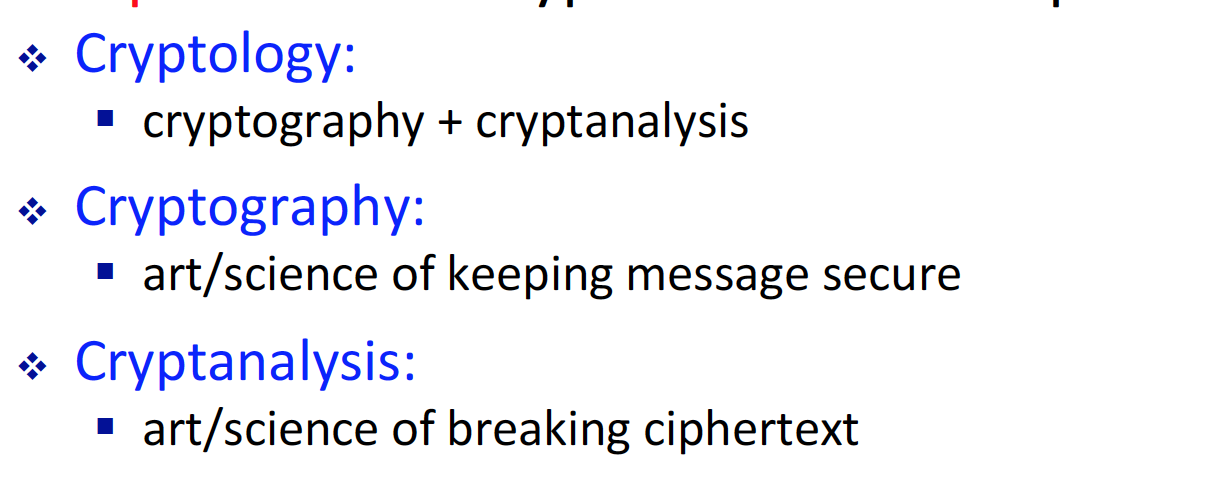
|  |  |  |
| --- | --- | --- |
|  |  | CPS 633 – note questions  Jae Duk Seo |

# Lecture 3 – cryptology

1. What can encryption solve? Also, what are the meaning of cryptology, cryptography, and cryptanalysis?
2. Explain what this is p = D(K, C), C = E(K,P), P = D(k, E(k,p))
3. What are work factors?
4. What is symmetric encryption and what kind of problem does it have?
5. What is asymmetric encryption algorithm? And what kind of encryption are there, as well as why do we need key management?
6. What are type of ciphers are there, and what is a casers cipher in a nut shell? (Mathematic behind the casers cipher)
7. Ways to attack substitution ciphers? (Steps to attack a cipher key?)
8. Problem with casers cipher and what is the solution for it?
9. What kind of different substitution ciphers are there and how does different cipher algorithm work?
10. What are transposition ciphers and what 2 type of cipher are there?
11. How can we attack a transportation ciphers?
12. What are some characteristic of a good cipher and what is a product cipher?
13. What are stream/block cipher give example of both and explain what strong/weak block cipher are.
14. What type of attack can happen, depending on what kind of information are known or not.
15. What is main problem with DES?
16. What is better single DES or Double DES?
17. What about triple DES?
18. Why did the NIST found for new algorithm? And which one gotten pick at 1995?

# Lecture 3 – soltions

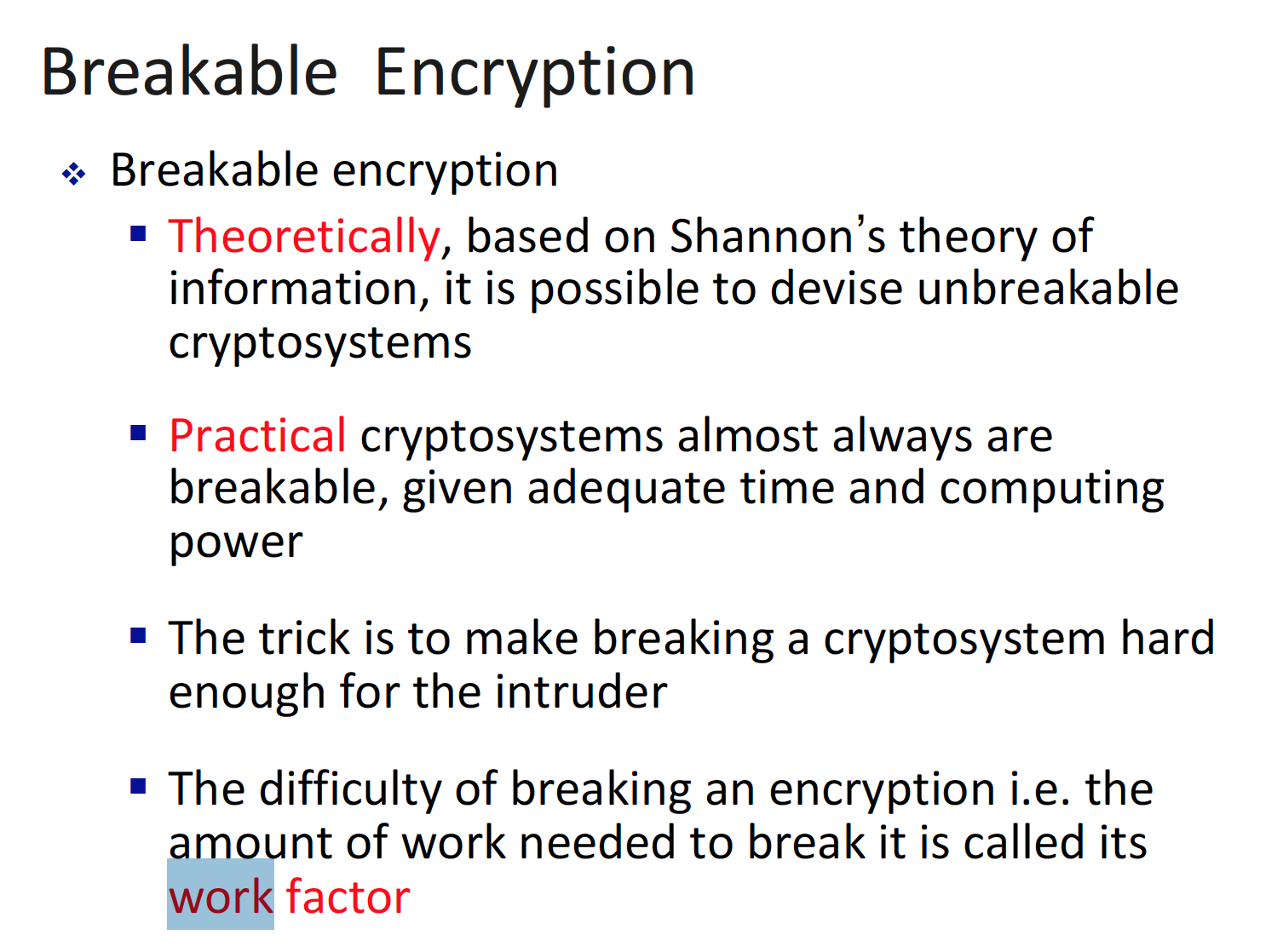
1. What can encryption solve? Also, what are the meaning of cryptology, cryptography, and cryptanalysis?

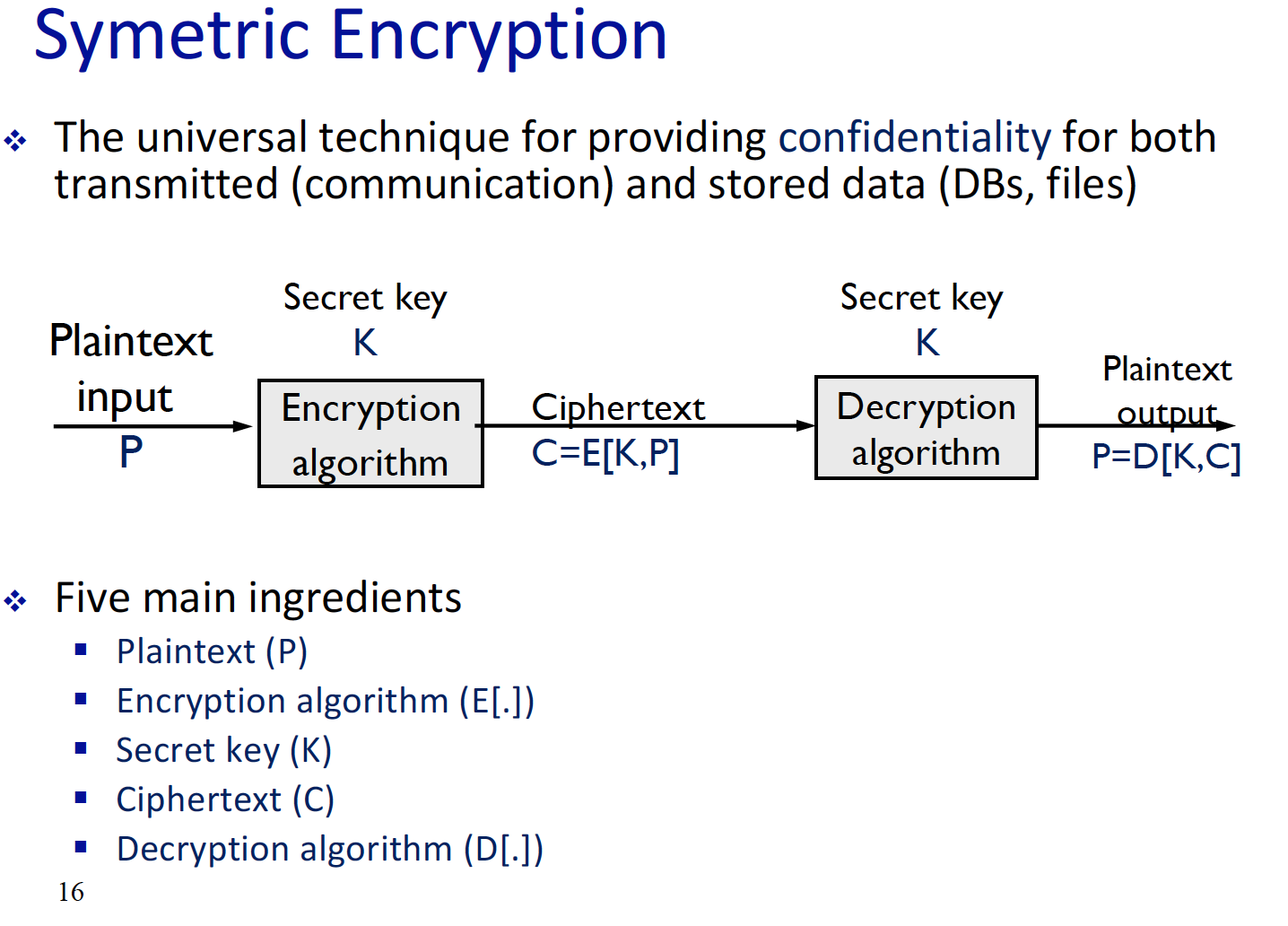
* Remember what we learned in lecture one? The CIA triad protects against Interception, Interruption, modification, fabrication and non-repudiation. Encryption provide a solution except for non-repudiation. 
* Cryptology – combination of cryptography and cryptanalysis.
* Cryptanalysis – Art of breaking a cipher text
* Cryptography – Art of encrypting a plaintext, or clear text

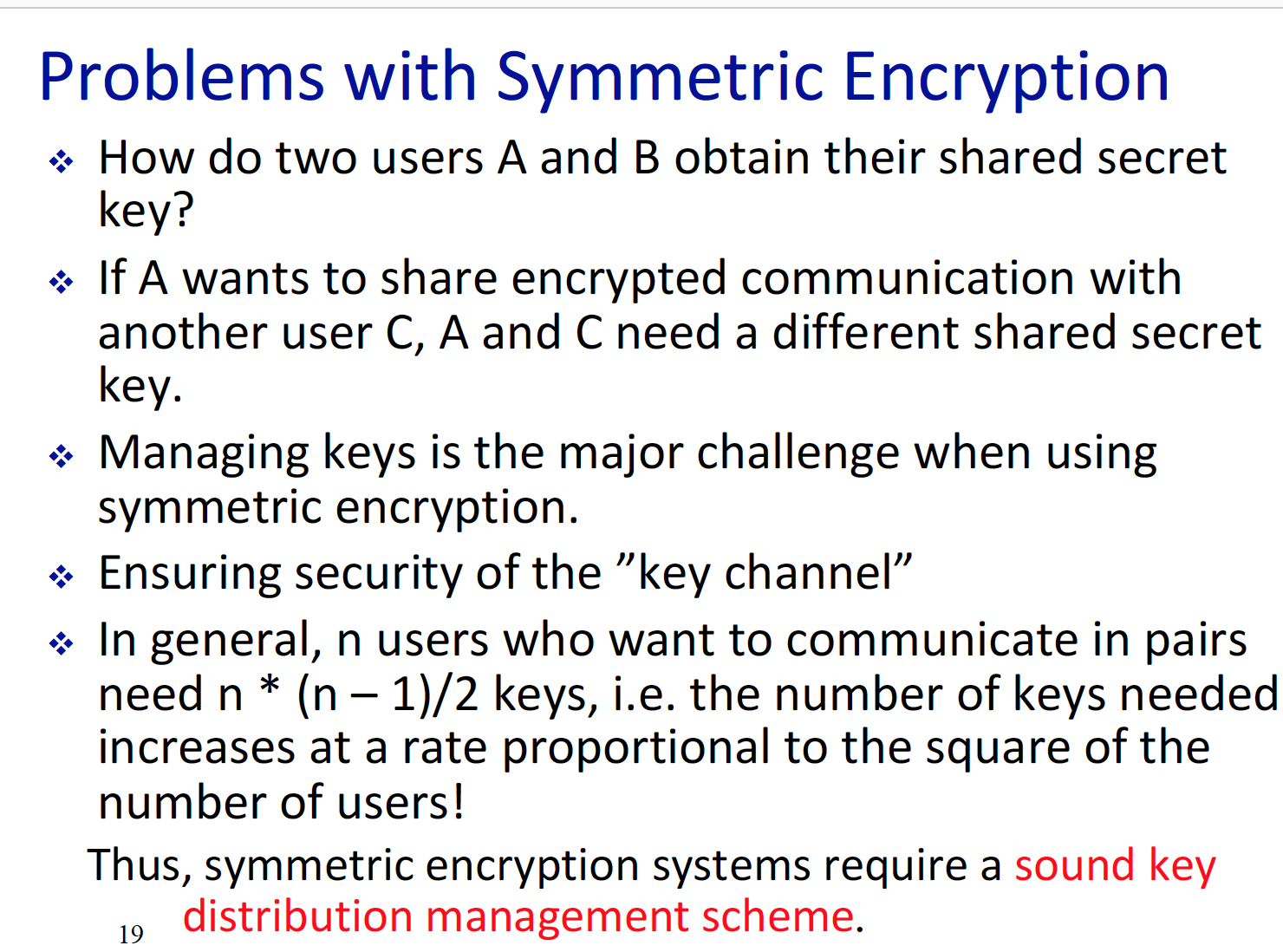
1. Explain what this is p = D(K, C), C = E(K,P), P = D(k, E(k,p))

* p = D(K, C) – C is cipher, and D() is decryption algorithm and K is the decryption key. The function is decrypting a secret cipher key.
* C = E(K,P) – E() encryption algorithm, P – plaintext, and K (encryption key). Basically this is encrypting the plaintext to cipher text.
* P = D(k, E(k,p)) – this is combination of both, decrypting the encrypted plaintext, that produce exact same plain text.

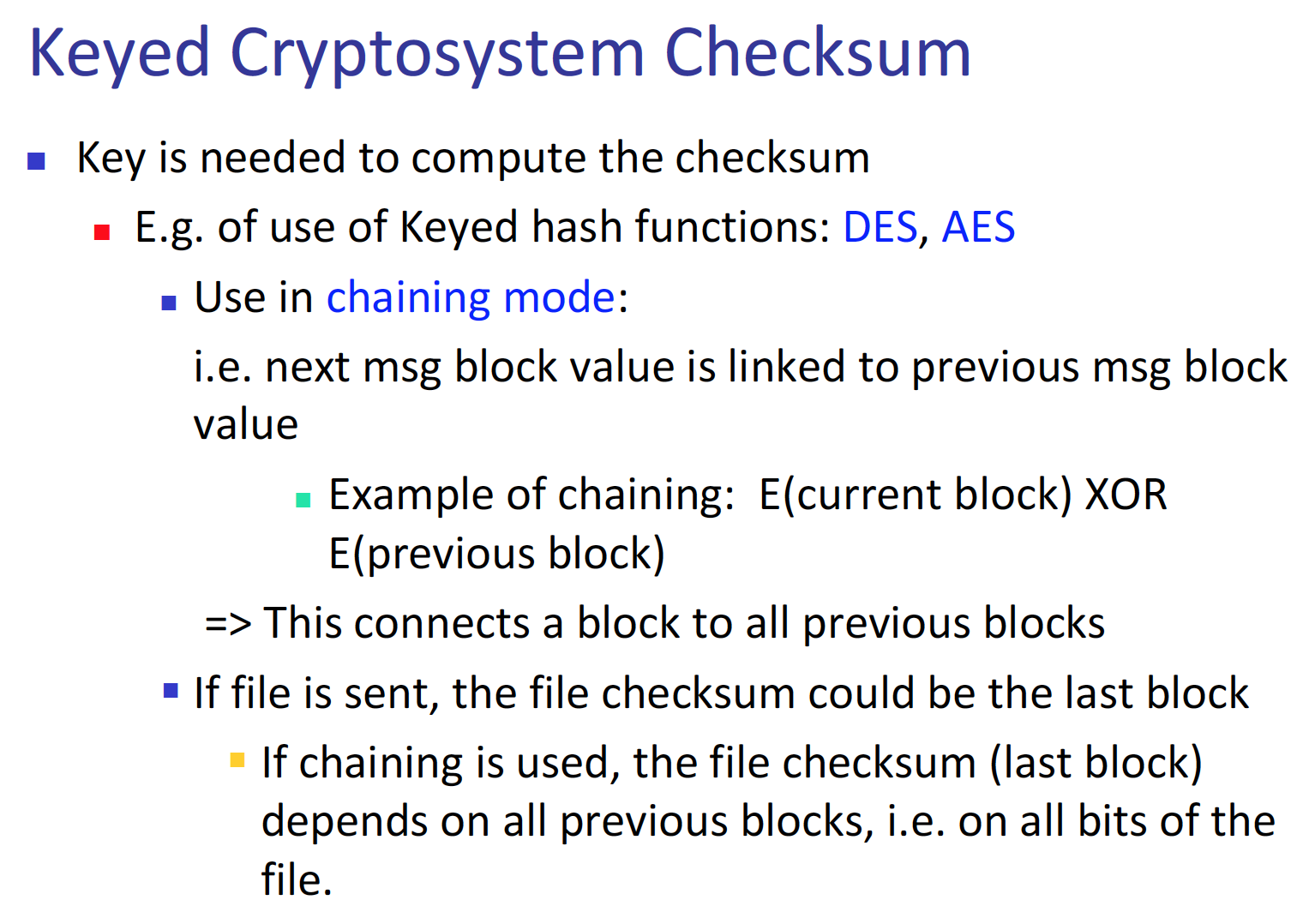
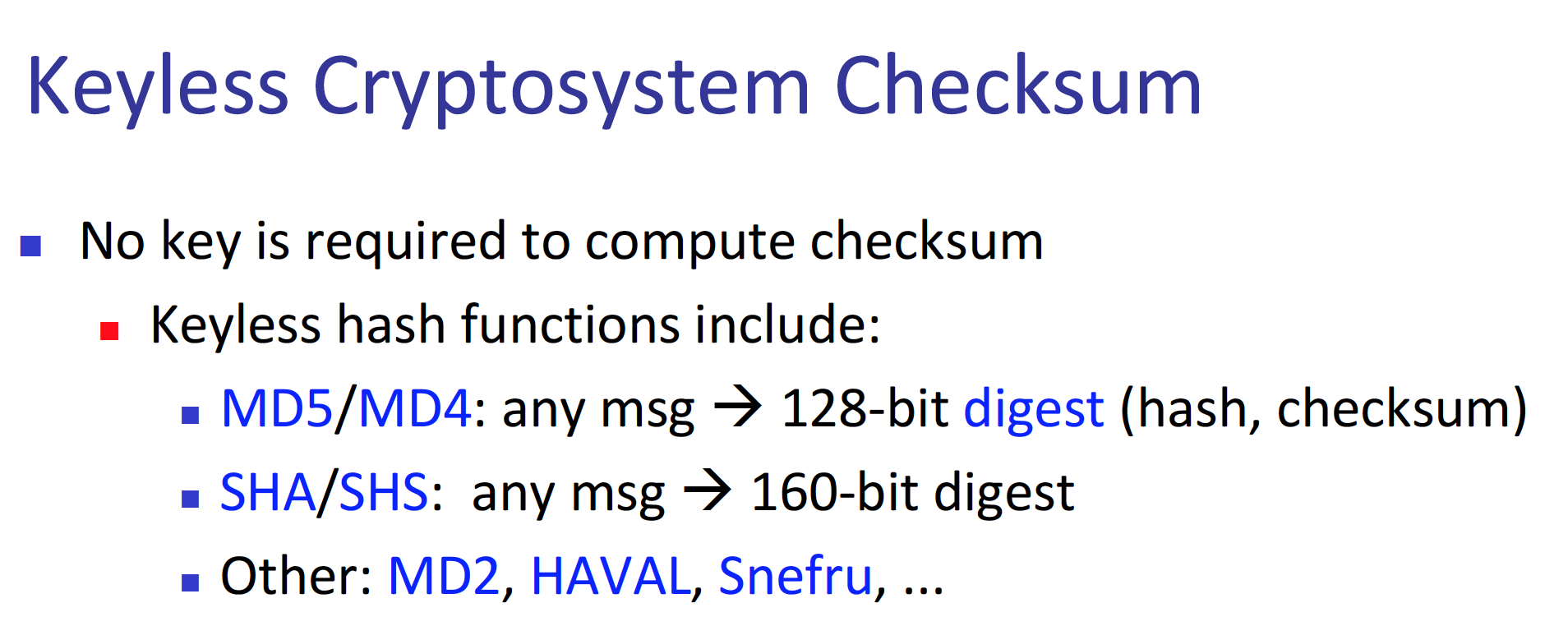
1. What are work factors?

* When we determine how well does the encryption algorithm perform, work factor is the variable that determines how hard for the hacker to decrypt the cipher text. 

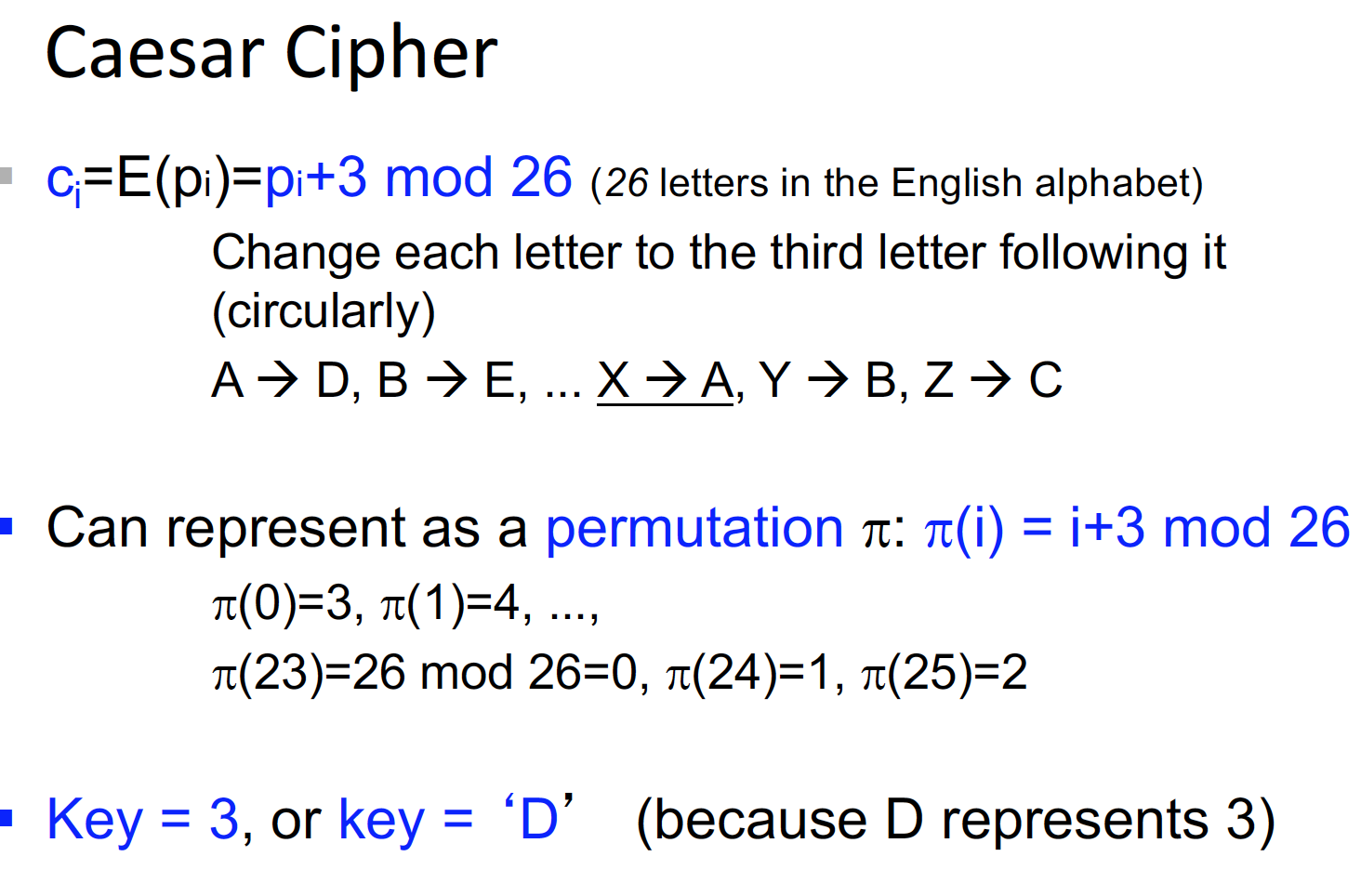
1. What is symmetric encryption and what kind of problem does it have?  
   - Symmetric encryption is when the sender and the receiver share the same key to encrypt and decrypte the message m. So in other words c = E(K,P) and p = D(K,c). They use the same key k.

* The main problem is the amount of key needed when multiple users use symmetric key to encrypt message. The complexity is   
  n \*[ (n-1)/2 ] 

1. What is asymmetric encryption algorithm? And what kind of encryption are there, as well as why do we need key management?

* Asymmetric is when the sender and the receiver have different key, when encrypting and decrypting message. So in other words   
  c = E(K1,p) and p = D(K2,c). K1 is not equal to K2.
* There are 3 types of encryption algorithm. Keyless, symmetric and asymmetric.   
  Keyless – MD5  
  symmetric – DES, AES  
  a symmetric - RSA
* We need key management since private key or any type of key must be managed in a way, where it gets handled in careful manner.

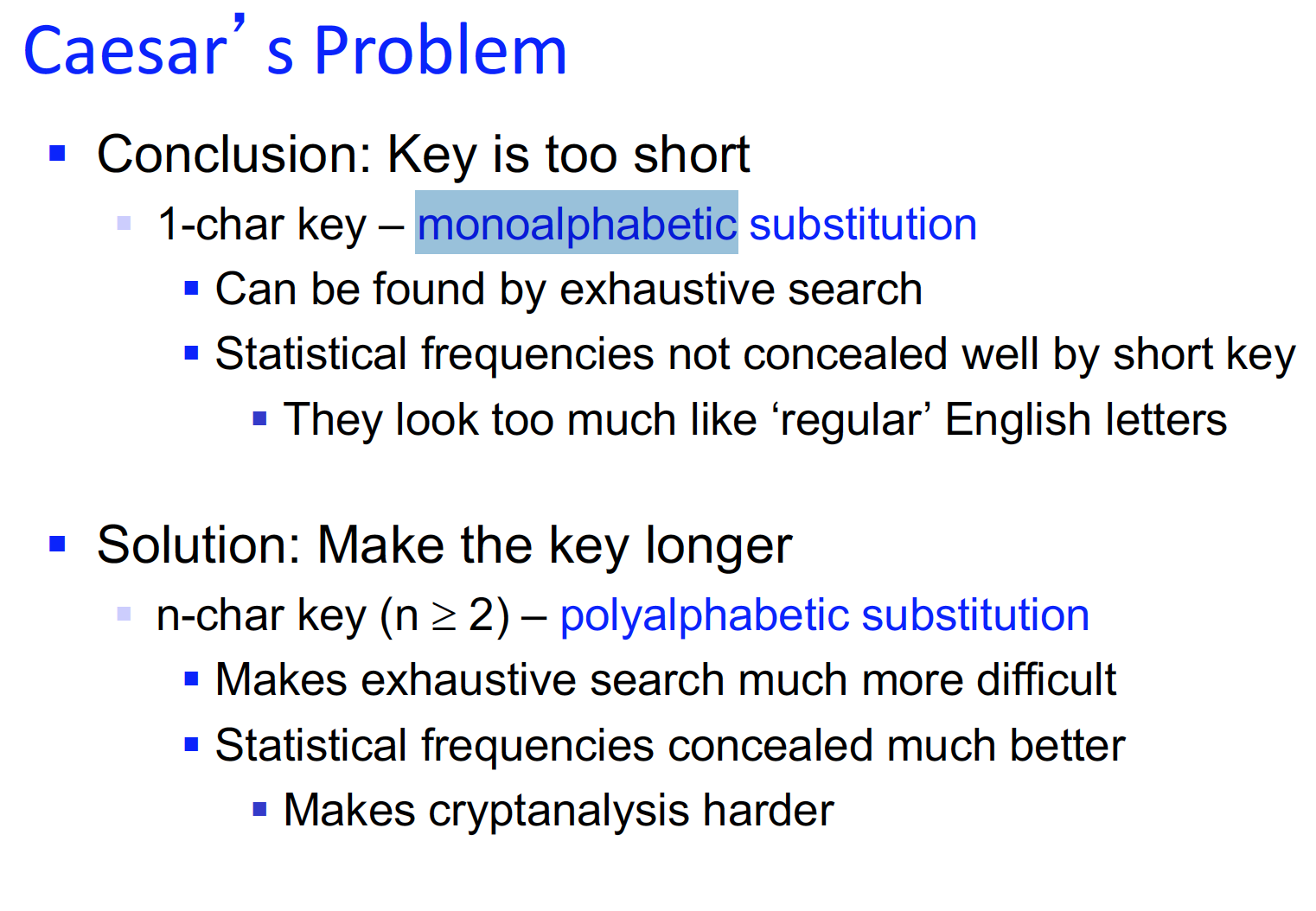
1. What are type of ciphers are there, and what is a casers cipher in a nut shell? (Mathematic behind the casers cipher)

* The Caesar cipher is easy transposition cipher. This is done via converting each character into numbers and then adding a value to that number, which makes the transposition.  
  In a nutshell, A turns to D, B turns to E etc……  
  

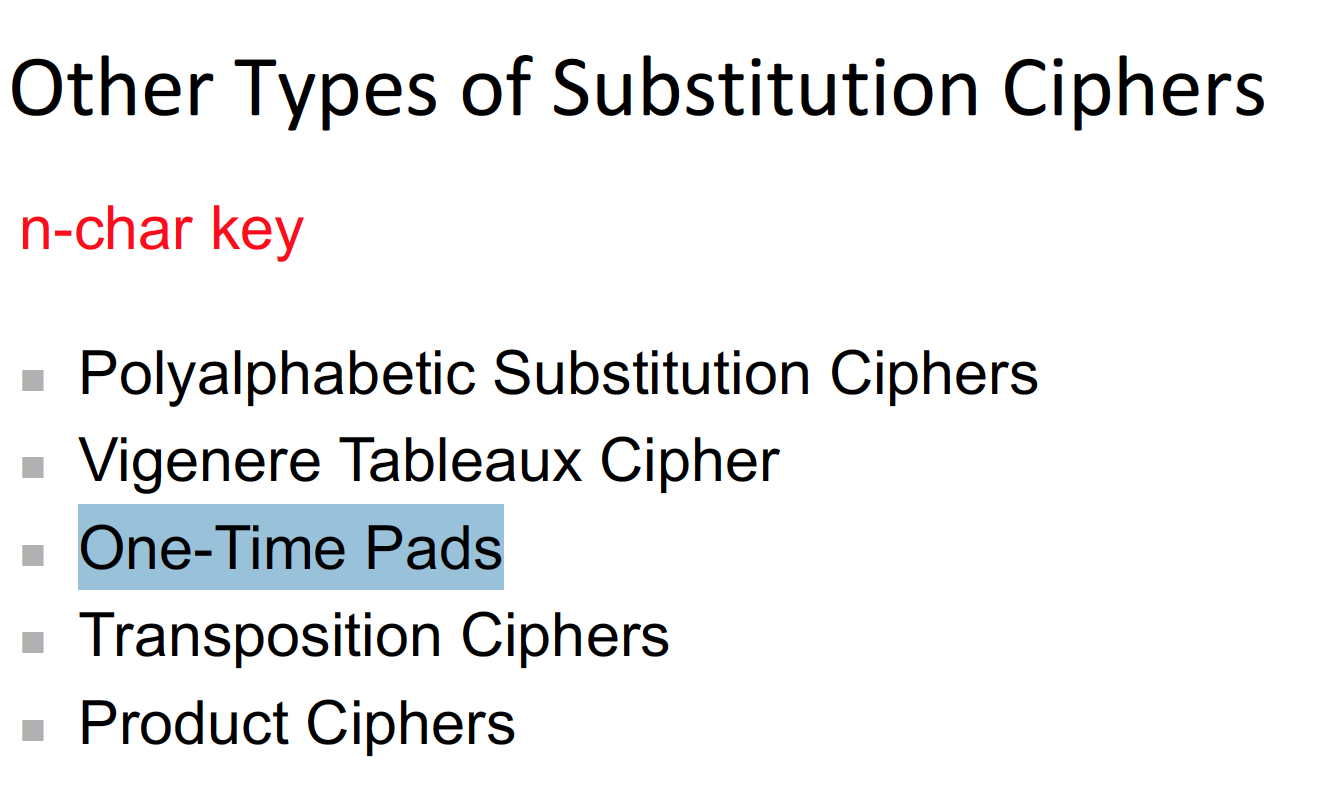
1. Ways to attack substitution ciphers? (Steps to attack a cipher key?)

* Basic attacks are possible, which is brute force attack, (with good software and hardware, this attack will work well.) However, there is a better model. Which is statistical attack, in English there exist a Unigram table, this is a table that describes the frequency of each letter, and by using this table, we can get a similar outcome of the ciphered text.

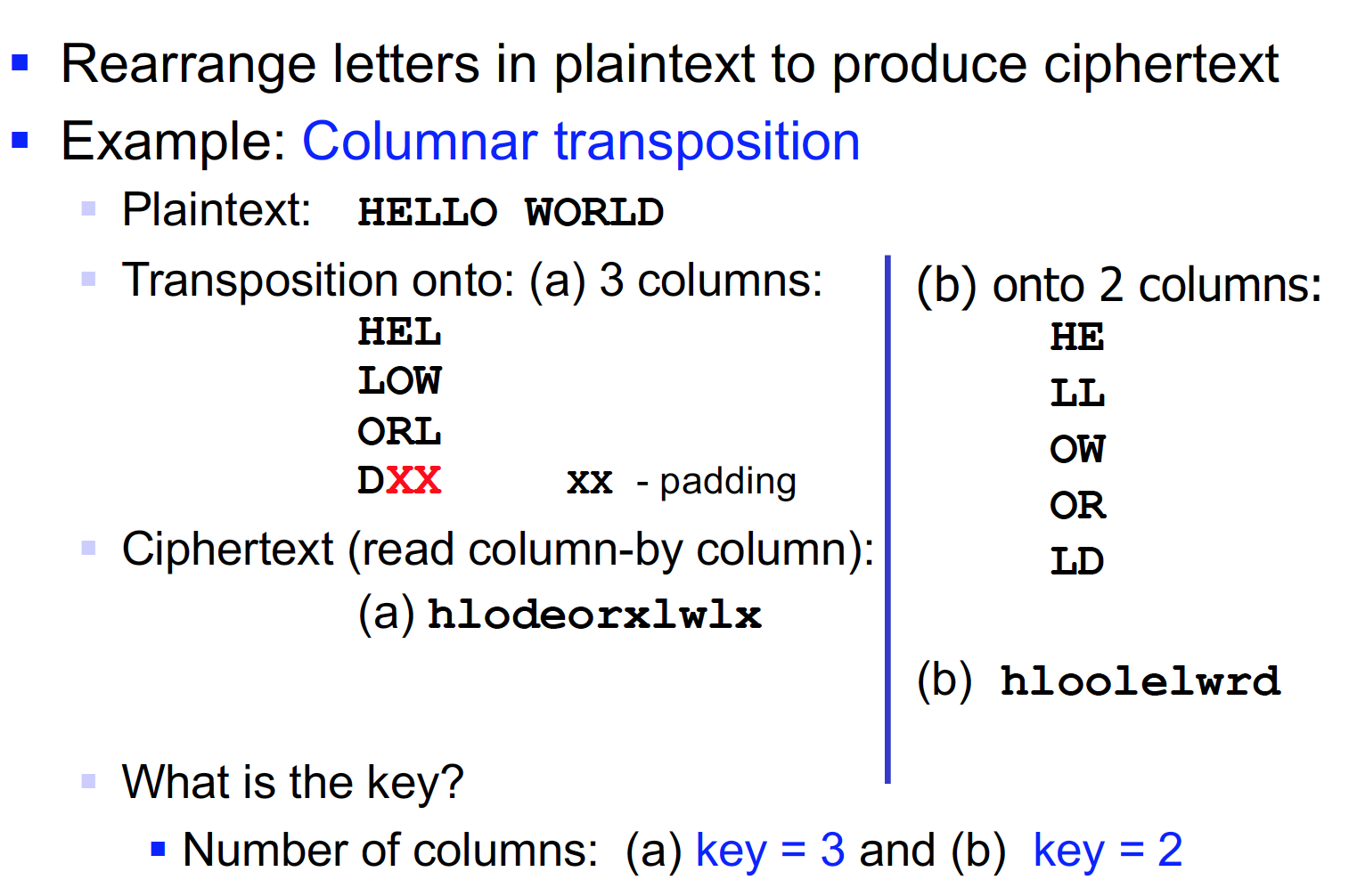
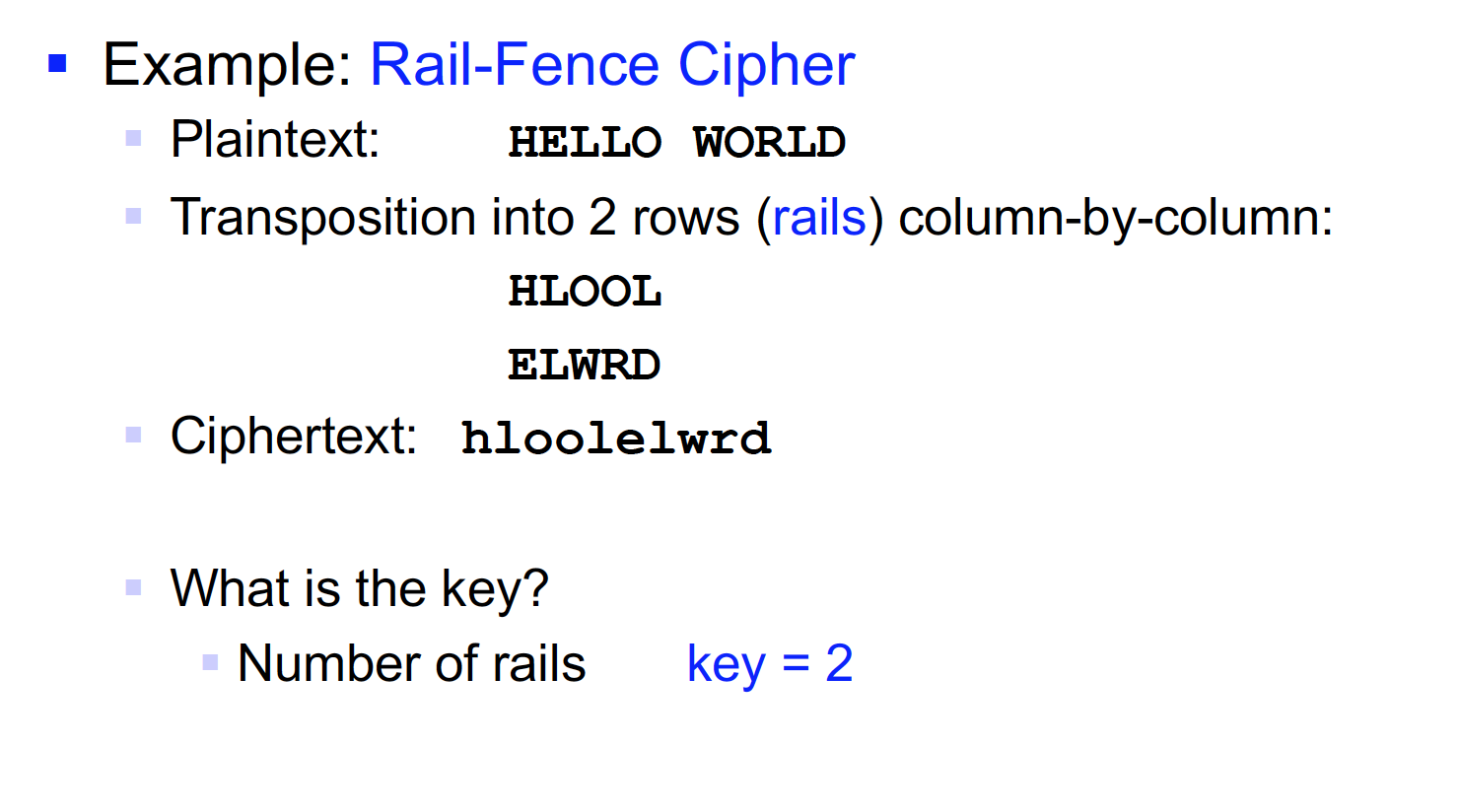
1. Problem with casers cipher and what is the solution for it?

* The main problem is it does not reformat the distribution of the frequency of the English letter, basically even the cipher text looks like an English letter word. The main thing is monoalphabetic substitution does not redistribute the frequency of the English. The solution for this weakness is making the key longer, so make the monoalphabetic to polyalphabetic substitution. 

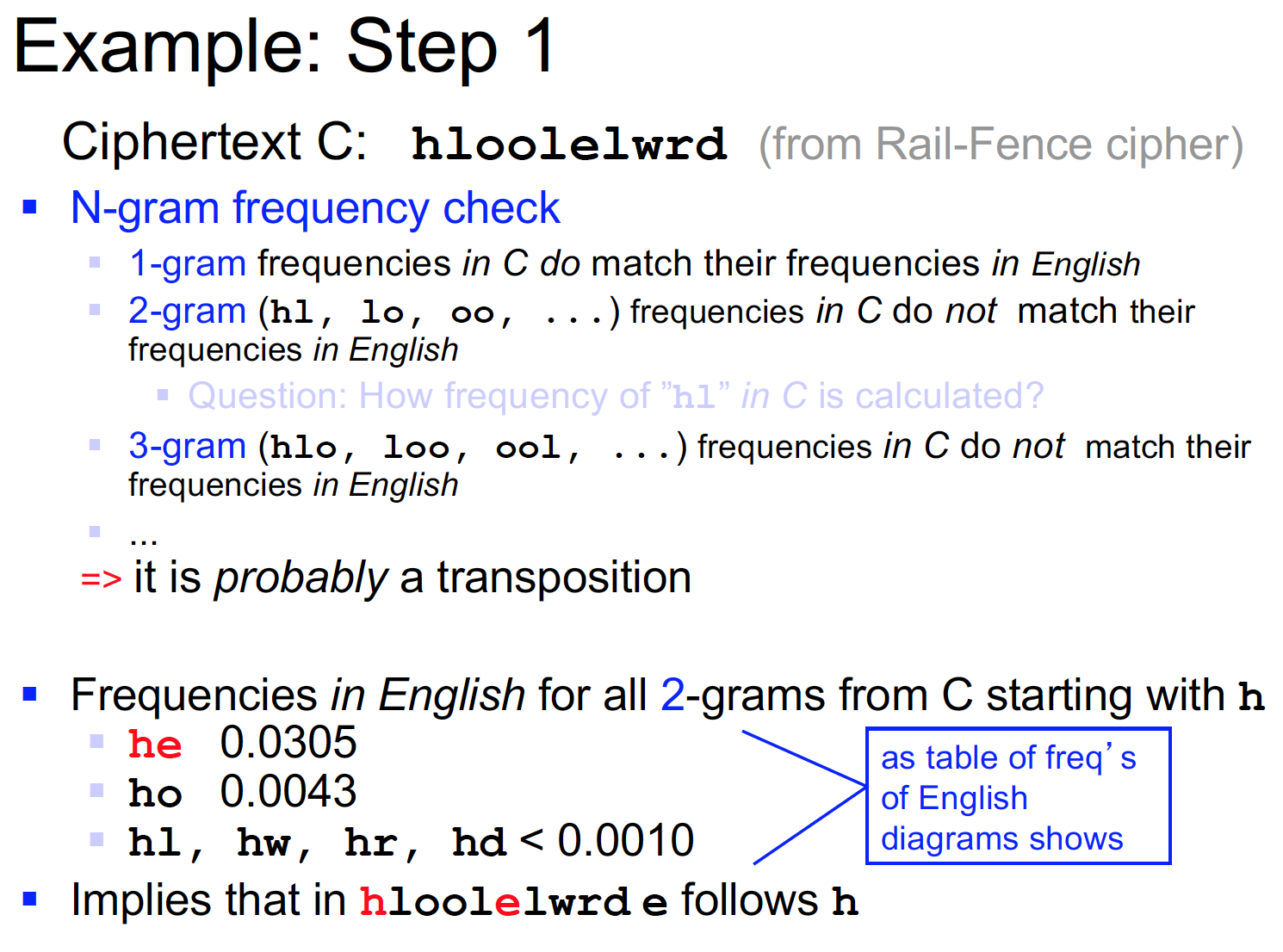
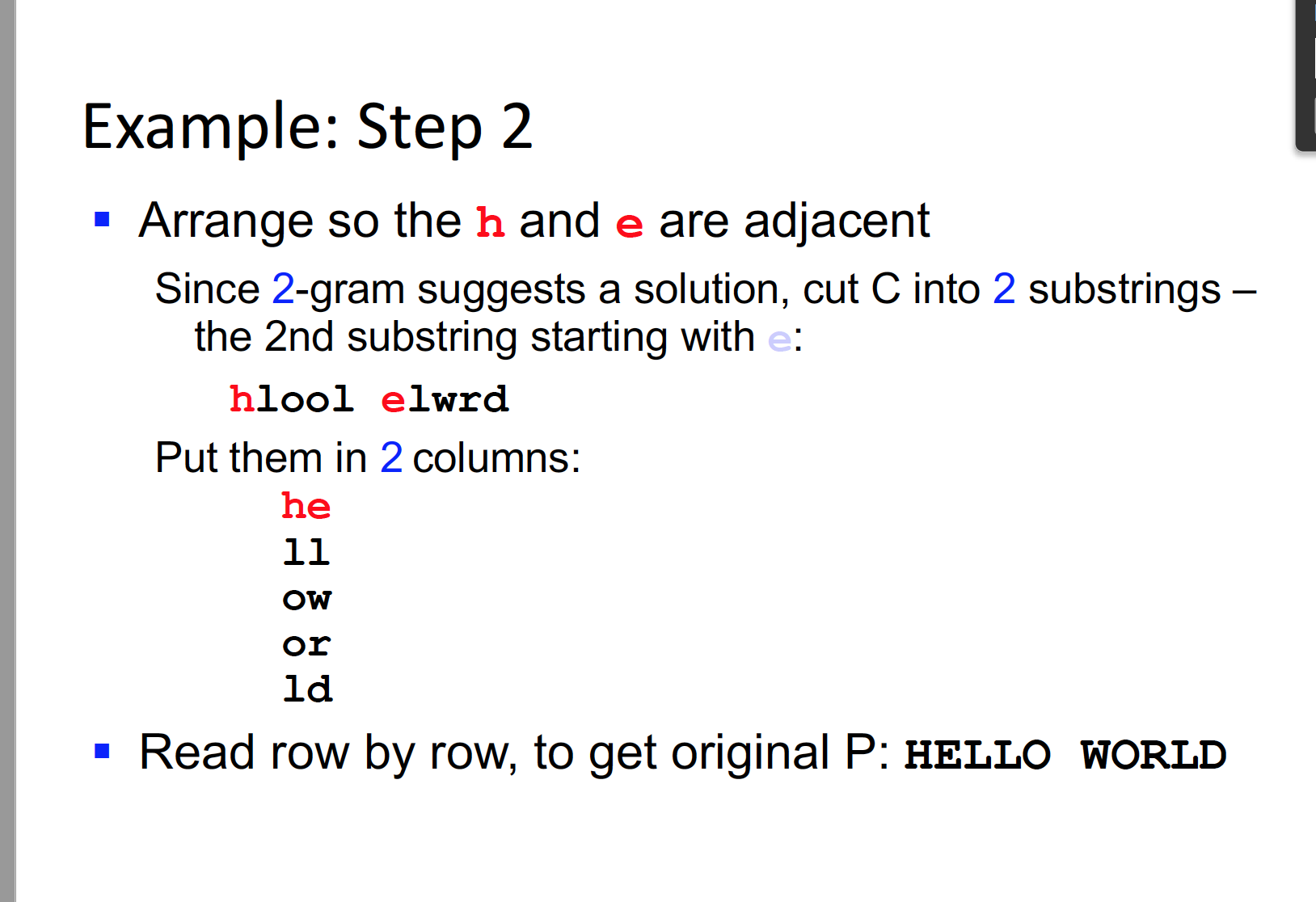
1. What kind of different substitution ciphers are there and how does different cipher algorithm work?

* 1) poly alphabetic – advance version of mono alphabetic. Substitute the one char to another char, then perform the substitution again.   
  2) Vigenere Tableaux Cipher – By using a particular table, cipher the plain text into cipher text. (Each row of text, will be substitute via each column of the table.)   
  3) One-Time Pads – Large one set of key is added to plain text. (Not much description on the PPT)  
  4) Transposition cipher – Move each letter in the text with certain amount of Integer.  
  5) Product cipher – combination of cipher algo, to make the cipher text more hard to break.  
  LOL transposition cipher are considered as Substitution ciphers

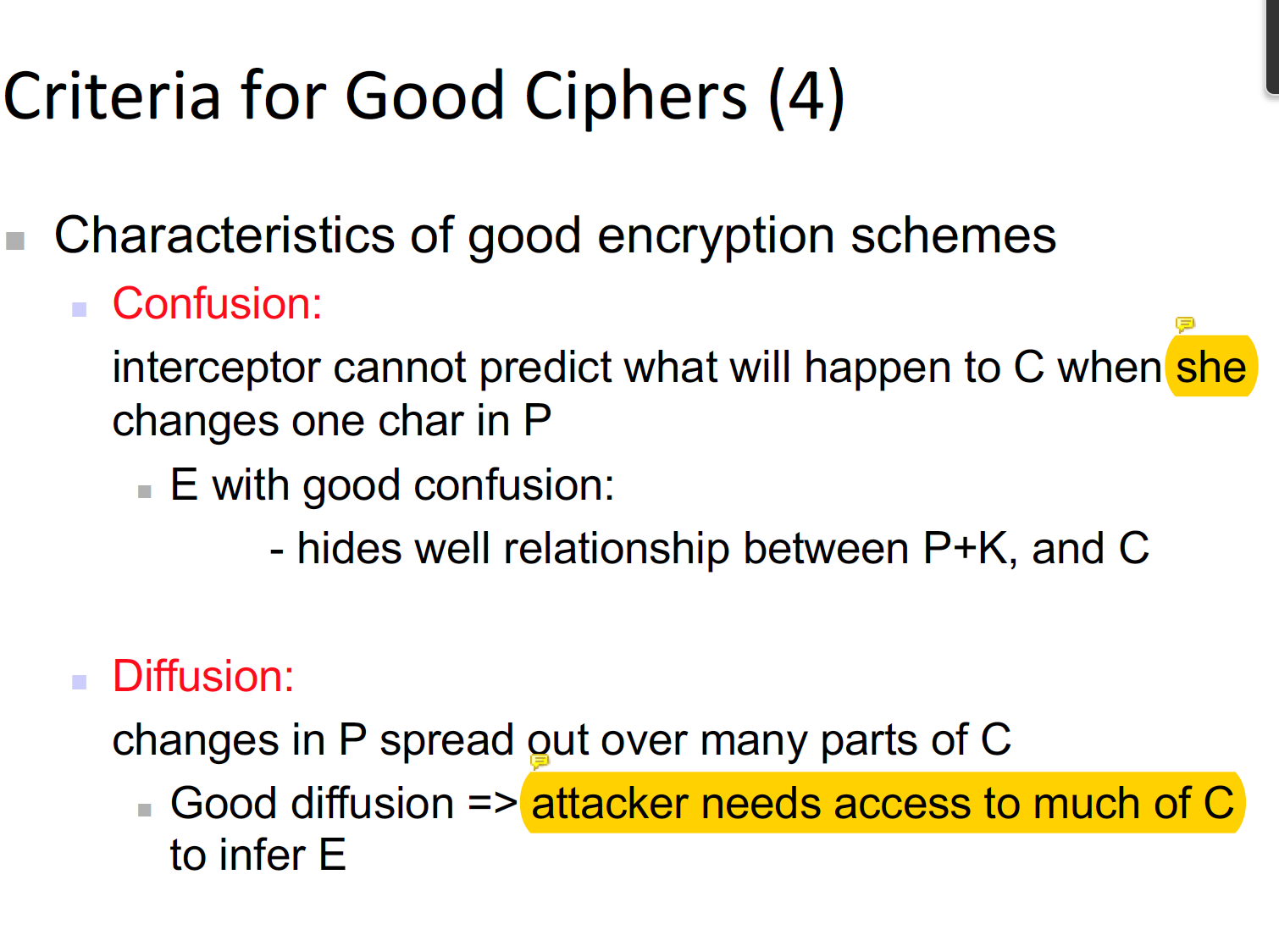
1. What are transposition ciphers and what 2 type of cipher are there?

* There are mainly two type of transposition   
  1) Column transposition – this is done via, setting a key value and divide the text into size of the key word. And then, arrange them into each column. Finally, rewritten them into one sentence.   
  2) Rail Fence transposition – This is very similar to column cipher. The only difference is that it rearranges the text via row.

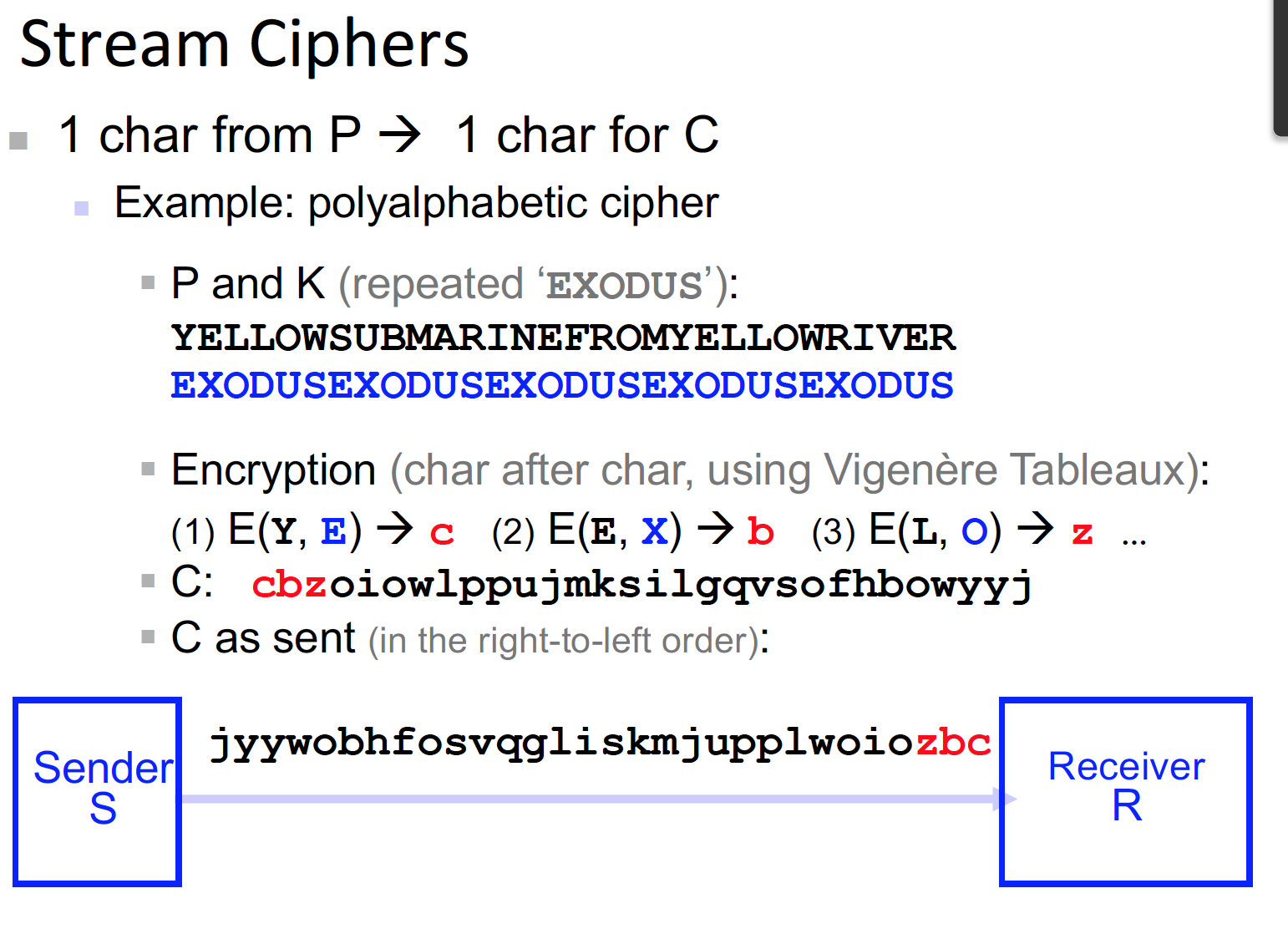
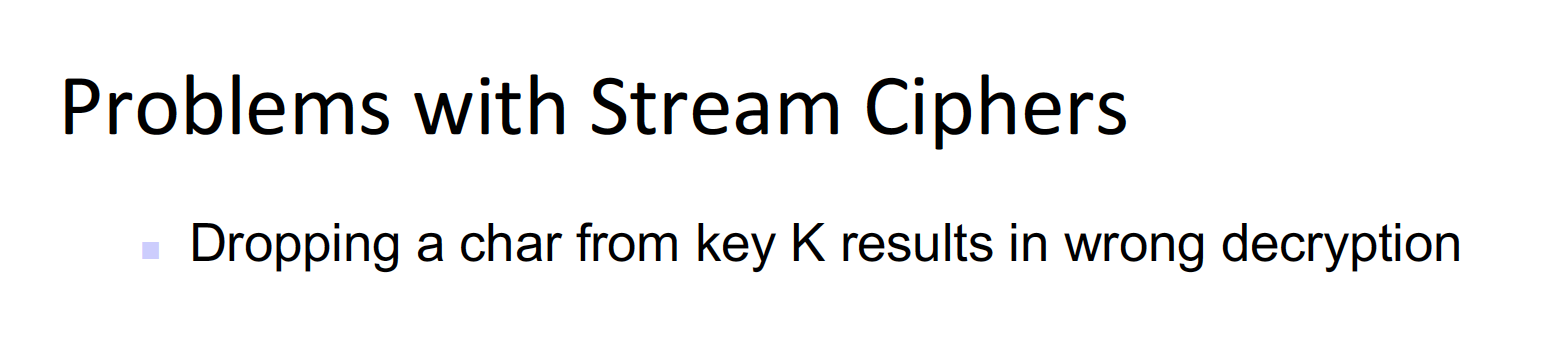
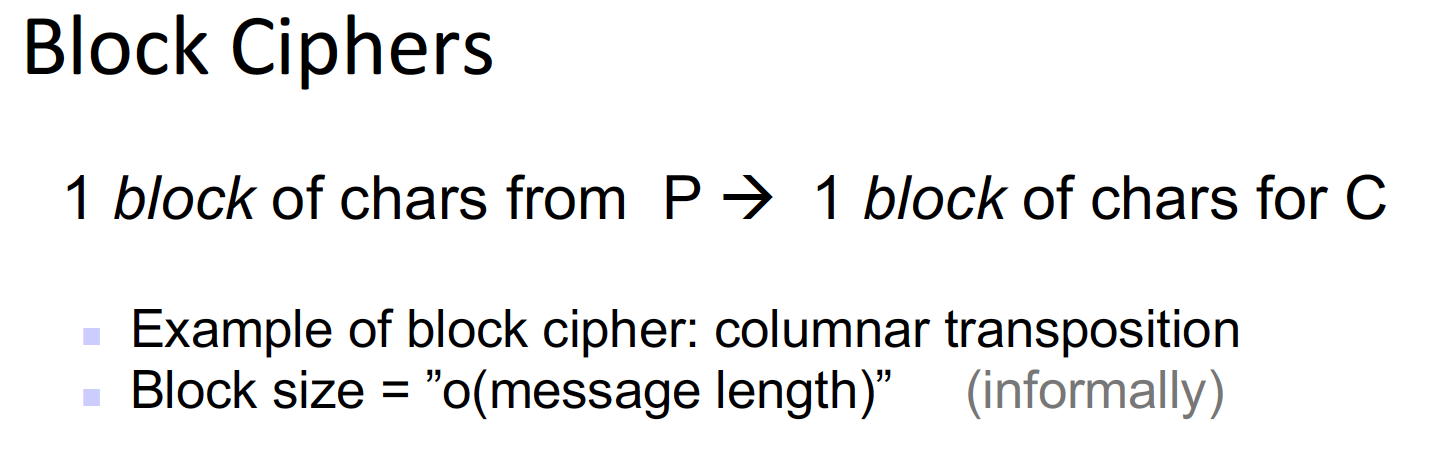
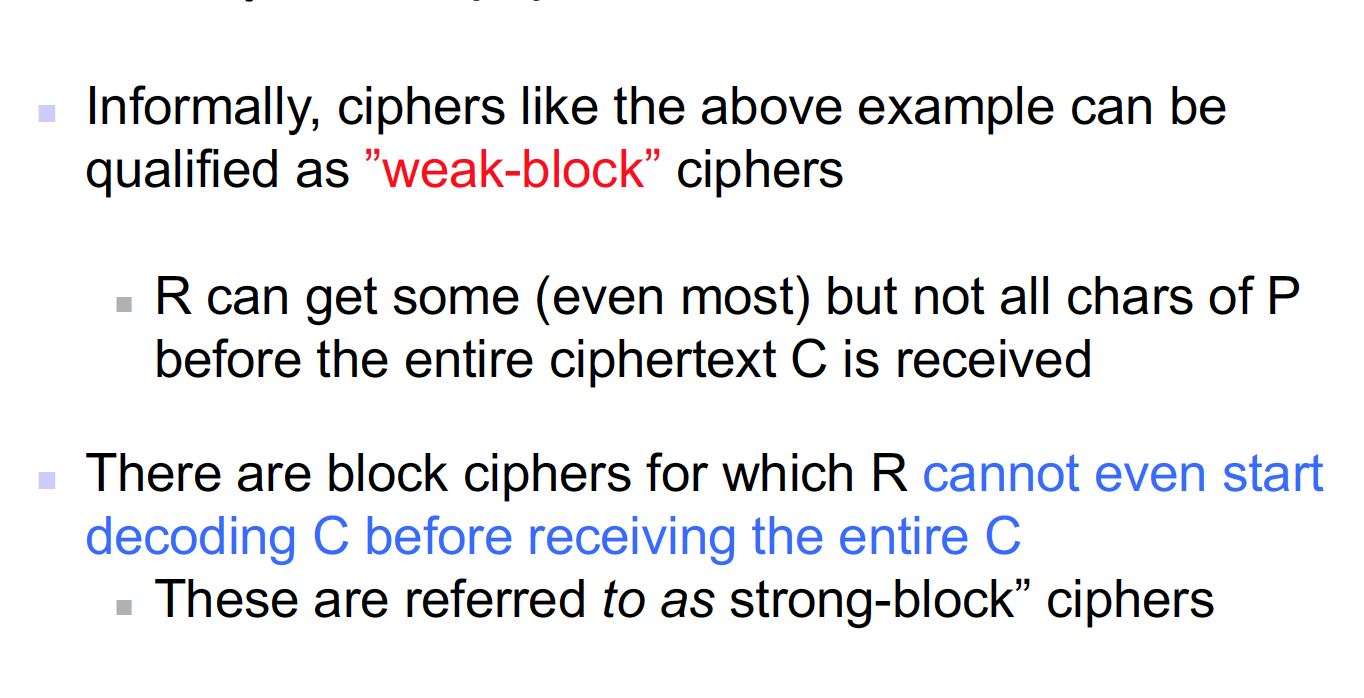
1. How can we attack a transportation ciphers?

* The way to attack transposition cipher is that we need to recognize that is it a transposition cipher. This is done via the, n – gram comparison. The method behind this is that it calculates the probability that one letter follows another letter. If none of the letter in the cipher text, follow one another then we will suspect a transposition cipher.   
    
  After realize that it may be a transposition cipher, then we need to rearrange the word. So that the rearranged word make sense, remember that it either can be column or Rail Fence.

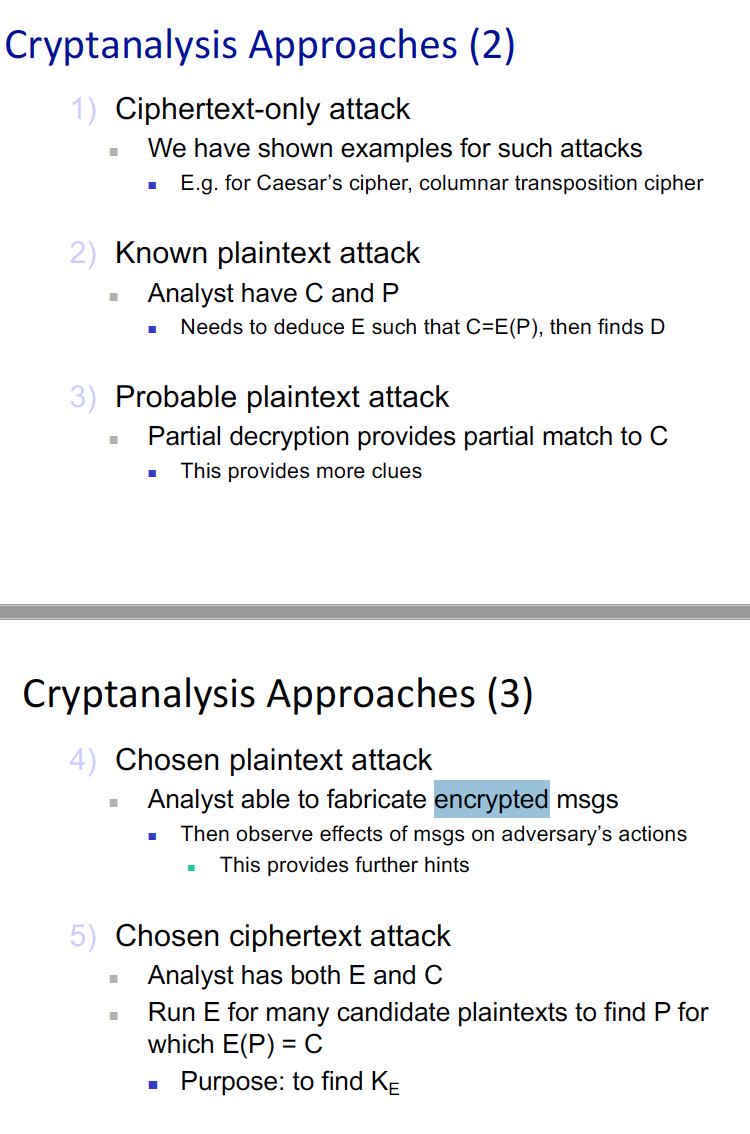
1. What are some characteristic of a good cipher and what is a product cipher?

* The characteristic of good cipher is. (There are way to many, so I wil only write the most important ones.)
* Diffusion – In algo such as block cipher, some ciphers make it possible for the attacker to start decrypt without having all of the cipher text. So we need to have each plain text P – well distributed over the cipher text C
* Confusion – we cannot let the attacker, predict what is going to happen to C when we make a change in P.

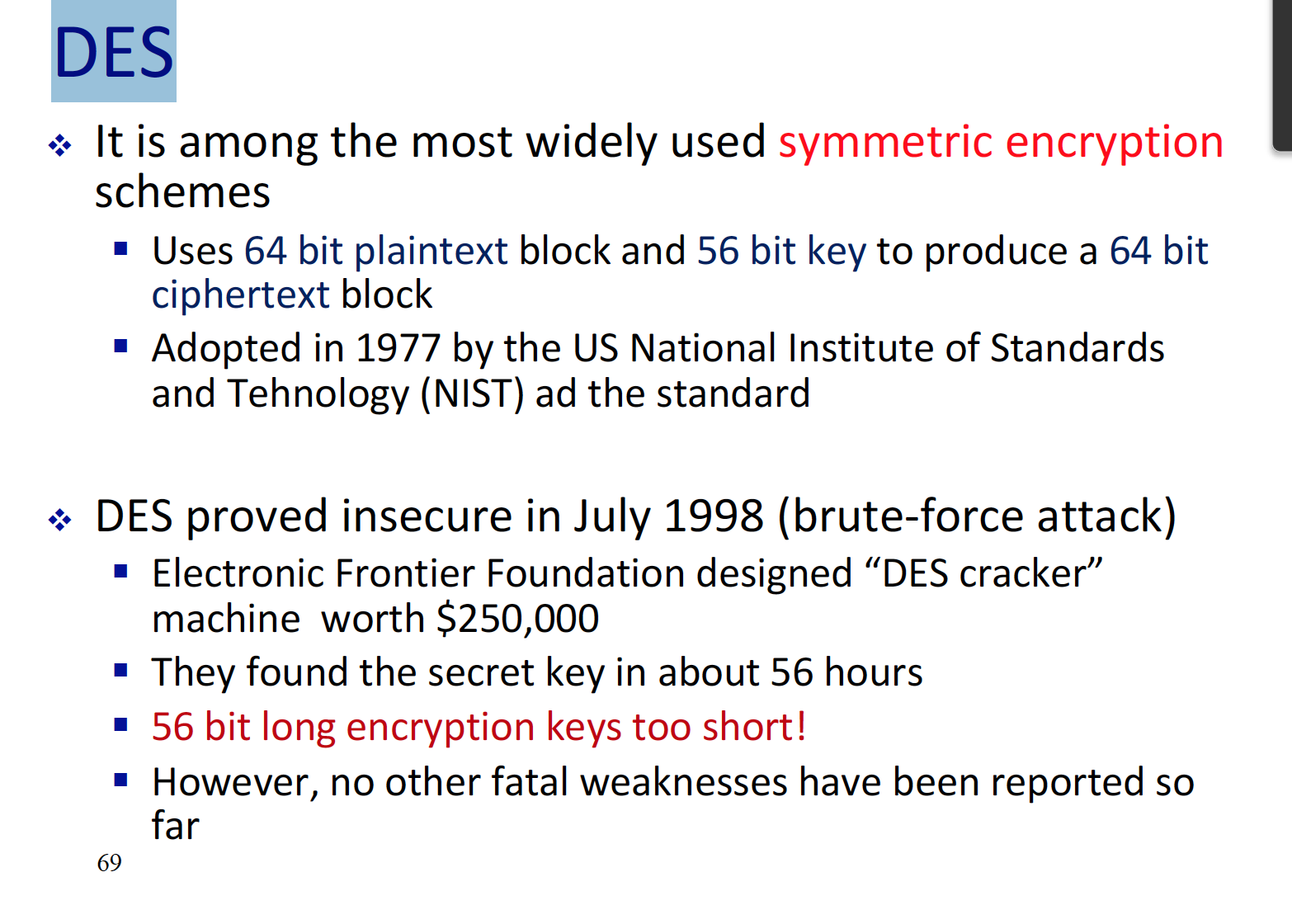
1. What are stream/block cipher give example of both and explain what strong/weak block cipher are.

* Stream cipher – the receiver starts to decrypt the cipher text as soon as they start to receive the text. (The main problem with this decrypt cipher is that, when a packet loss occurs for one letter, then the receiver will decrypt in different letter.)
* Block cipher – this is a method of decrypting a block of cipher text, rather than the stream – however there are 2 kind of block cipher.
* Strong – the receiver needs to receive every block in order to start decryption
* Weak – the receiver does not need to receive the whole, block rather some portion of the block cipher will be enough to start the decryption process.

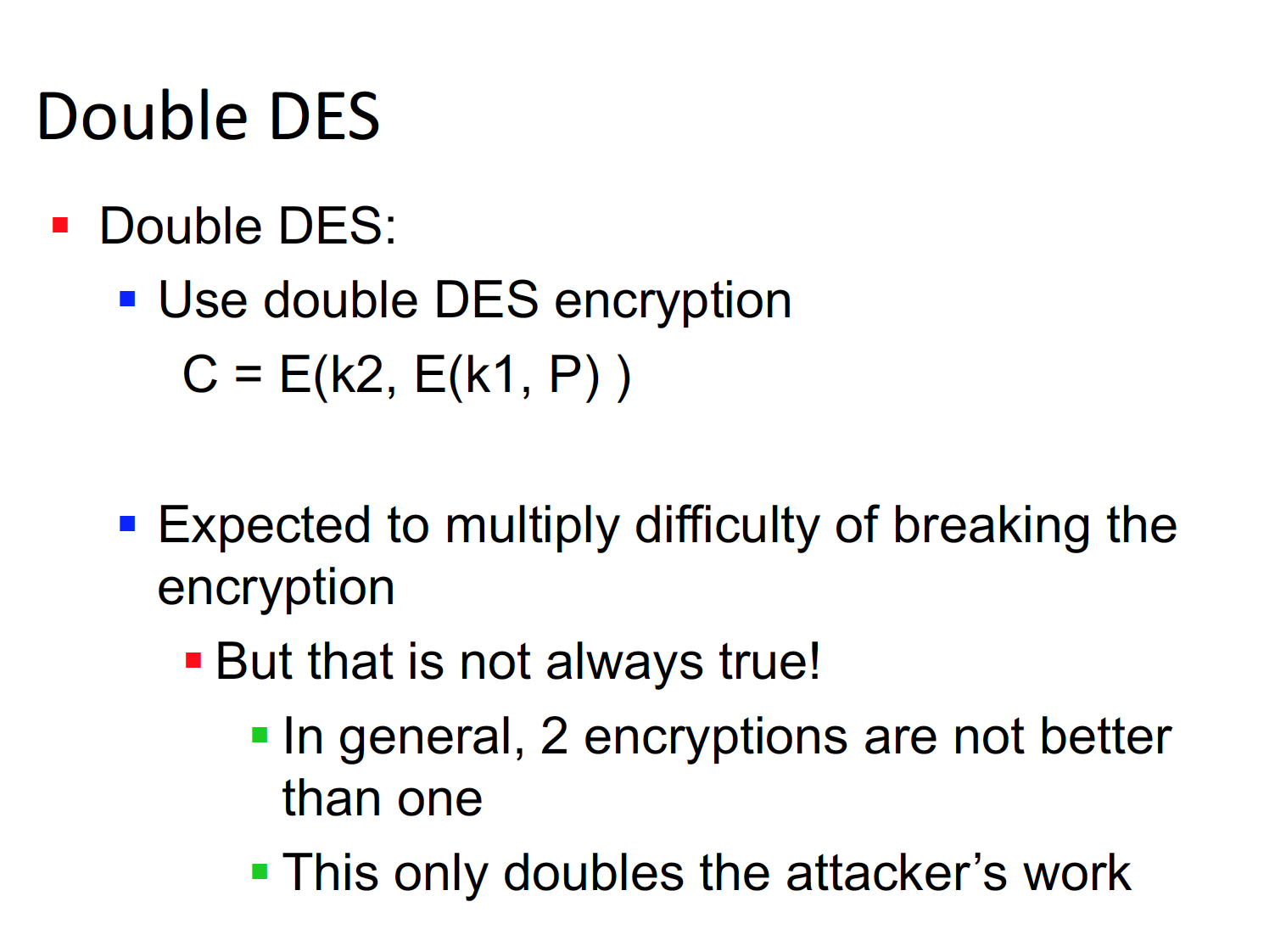
1. What type of attack can happen, depending on what kind of information are known or not?

* There are several attacks possible   
  1) Cipher text only attack – this is the case when the attacker only knows the cipher text. And they must work backwards toward the plaintext – this is quite possible if there are enough repetition of letter in the cipher text, for the attacker to know the plausible plaintext.  
  2) Known plain text attack – when the attacker knows a certain part of the ciphered letter, then using that block as a reference block, need to work out the other ciphered blocks.   
  3) possible plain text attack – Some part of block plain text matches some part of cipher text C.   
  4) chosen plain text attack – when the attacker is able to encrypt any plaintext with the unknown key. Then they are able to try to determine the key. RSA – very vulnerable to these kind of attacks!   
  5) chosen cipher text attack – this is the opposite of chosen plain text attack – the attacker knows the decrypted value of certain plaint text and able to work backwards towards the key value.

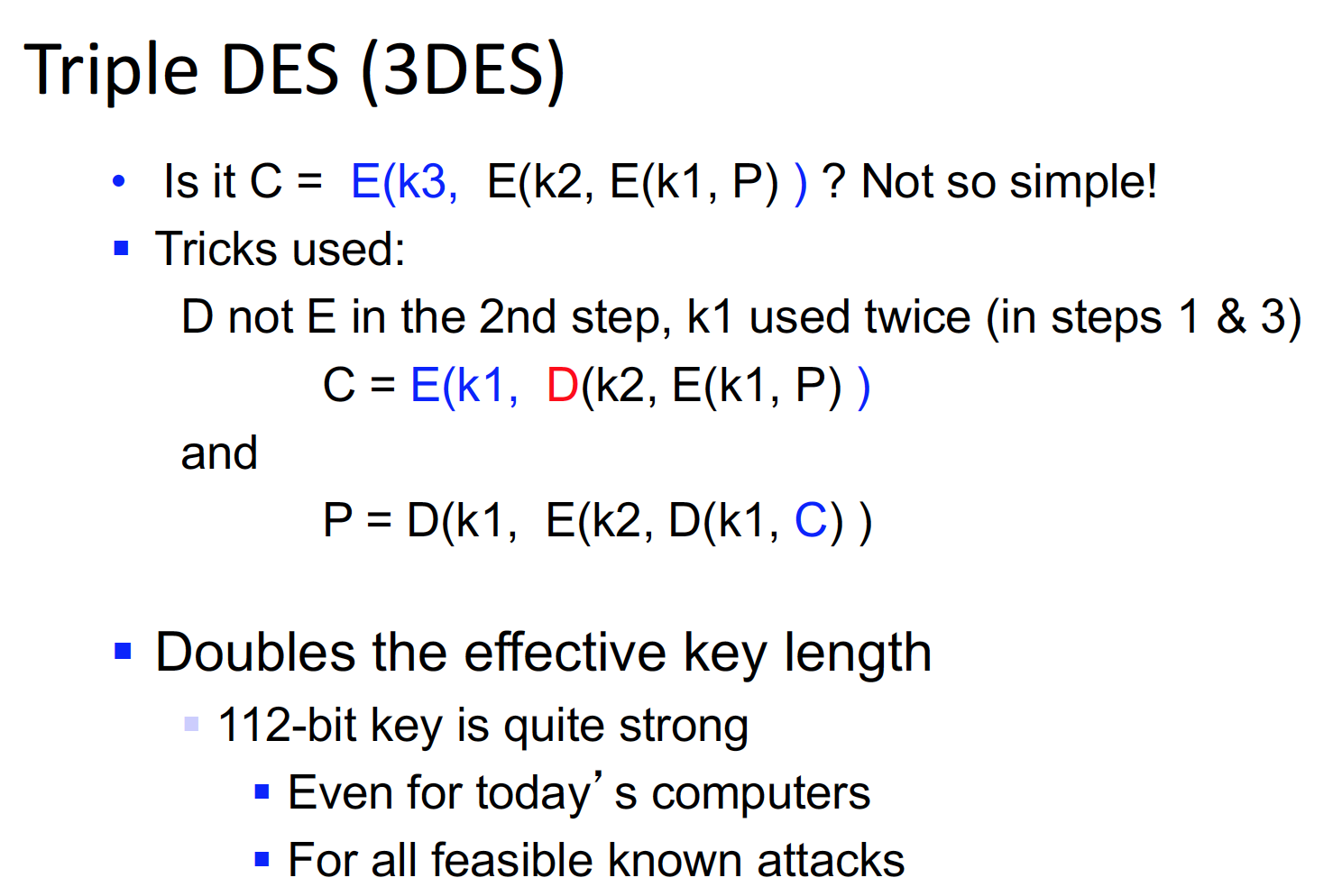
1. What is main problem with DES?

* The main problem is that the key length is too small, the DES is a symmetric encryption algo, in a way. The key was broken since it was too shrot.

1. What is better single DES or Double DES?

* There is no difference among the single DES, since the complexity of the cipher letter is same. But the time that it takes to cipher a text is longer.

1. What about triple DES?

* This is a better solution for Double DES – but the key is not to encrypt for three times. Rather it is better to encrypt first, decrypt then perform final encryption.  
  c = E(K, D(K, E(K,p))) 

1. Why did the NIST found for new algorithm? And which one gotten pick at 1995?

* The NIST tried to find a new algo, since DES was not strong enough it was broken.   
  In the ppt does not describe which algo have gotten picked, but it does say how the AES operates. Advance Encryption Standard.   
  Basically, it is a cycle, cipher algo. And for each round, the text gets ciphered more and more using bit wise operations such as XOR, OR, AND, and NAND etc…..