

DTU/2K16/Md13- Anish Sachdeva

Q 9) Eve recently gets access to Alice's computer and using her cipher she types "abcdefghij". The screen shows "CABDEHFGIJ".

If Eve knows that Alice is using a keyed transposition cipher, answer the following questions:

a) What type of attack is Eve launching?

Ans 9)a) Eve has launched a chosen plaintext attack. Eve has access to Alice's computer and also her algorithm that she is using for encryption.

With her chosen plaintext attack she can try to break the algorithm and understand how the encryption is taking place.

b) What is the size of the permutation key?  
The size of the permutation key is 5 and we divide our initial message into blocks of 5 and permute it as :-

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$
 so,

P = A a b c d e f g h i j  
C = c a b d e h f g i j  
C = CABDEHFGIJ