

Decryption Procedure of a Cipher Text without the key

By Eythan Fellous

Decrypt a Cipher Text who is using the vigenere method without the key is something complicated but not impossible at all. First you will have to analyse the cipher text (cipher text = the encrypted text) to try to see if there are occurrences for determined the length of the key. If you don't have the length it will be impossible to determine the number of possible key combination. For this exercise the cipher text was

« tyxvahlvowsrahsoervceispsqlj_hxgyqfjtqgi_j____bafebacoewvowsohvs_nveto_dgo_tghidzvbklv
odsjuhsjwdsmerwdnvnkn_jgvrvv_ilxvhzevnelvodsohvsyhrfyeqga_yan_dgo_rloatcdnxssxujsmaj_
_rqgi_j____wtytqlcajsreq_wvshauxvokjvpekdtzgi_kfwsitdlrugeqlceqxidqtidqtdmqga_ihtidzvid
swlbsdtisailxvvrjdeja_sqan_afjwbxgzgvsjflceqxiqcqvadwvtyan_afjwbxgzgvsyadsjnbqvbvszehaqe
usdnqlceqydrilvidkoadv____wjimqlceqvjnlxmtvwwsfqvhvfyeqao_zkveik_njawlqlcajsohvsyodn_rj
xz_iht_sxvthxwtvwwvzlc_j____klhoilvlzu_rrddto » (nothing to be afraid of the length of the cipher text). My first mission was like I said to determine the key so I wrote a function who try to find the occurrence of the biggest number in a row for exemple my result can be this :

2, 5, 7, 56, 12, 15, 16, 60, 5, 9, 8, 54.

So we can see that each 4 numbers you have a big number (56, 60, 54), so thanks to my programme I know that the length of my key is 4 character. Now the fun part will be to FIND the key with this clew. To do this I wrote a function AND I use the most commun word in the English language « The » and I use the alphabet and I added the '_' character as wanted for this exercise, so I had 27 characters for a 4 length key. The calcul is simple to know how many combinations are possible I have to do this : $27 * 27 * 27 * 27$. 27 Because I have 27 characters 4 times because my key length is 4 characters. So as I said I wrote a programme in C for breaking the cipher key using 4 loop, 1 loop for 1 character. Then I looped on the sentence using my algorithm to try to find the plain text and that's how I found the key and I decrypt the text.

In general to break the vigenere cipher you will have to reach to objectif.

You must find the occurrence to find the key size to determine how big will be your key then when you find the key size build a program use the alphabet and loop in the alphabet to find the key for breaking the vigenere.