

CRYPTOGRAPHY

- **Substitution2**

It seems that another encrypted message has been intercepted. The encryptor seems to have learned their lesson though and now there isn't any punctuation! Can you still crack the cipher?

I did frequency analysis for substitution first, following were the results:

F 175x 13.87%	Y 61x 4.83%	S 28x 2.22%
N 125x 9.9%	A 56x 4.44%	R 24x 1.9%
X 103x 8.16%	P 46x 3.65%	U 20x 1.58%
Q 102x 8.08%	W 42x 3.33%	H 19x 1.51%
L 98x 7.77%	V 39x 3.09%	K 16x 1.27%
E 83x 6.58%	G 35x 2.77%	M 9x 0.71%
T 68x 5.39%	B 34x 2.69%	C 9x 0.71%
Z 63x 4.99%		O 5x 0.4%
		I 2x 0.16%

Input

Cipher Text *

na fyffoxenefufytpqna fymppfentkpxeafbaxraezaqqp zqgswnfyefzwyxnhzqgsfnxnql exlzpwbxlrzhkfy
stnyxqntlbwez hkfyzatppflrfnafefzqgsfnxnql evqz wesyxgtyxphqlehenfgetbgxl xenytnxqlv lbtgfln
tpemaxzatyfufyhwefv wptlbgtyc fntkpfecxppeaqmfufymfkfpxfufnafsyqsfsyswysqefqvtaxraezaqqp zqgs
wnfyefzwyxnhzqgsfnxnql exlqnqlphnqnf tza utpwtkpfecxppekwn tpeqnqrfnenwbflnexlnfyfenfbxltlbf
ozxnfbtkqwnzqgswnfyezxf lzf bfvf lexufzqgsfnxnql etyfqvnflptkqyxqwetvvtxyetl bzqgfbqmlnqywllx
lrzafzcpxen etlbf ofzwnxl rqlvxrezyxsneqv vlefqlnafqnafyatlbxaeftuxphvqzwe fbqlfospqytnxqltl

Language

English

Break Cipher Clear Cipher Text

Result

Key abcdefghijklmnopqrstuvwxyz This clear text ...
hdkzsemyqjbnwtxlogpavfuirc ... maps to this cipher text


adstudentstoknowtheirenemyaseffectivelyasteachingthemtoactivelythinklikeanattackerpicocftf
isanooffensivelyorientedhighschoolcomputersecuritycompetitionthatseekstogenerateinterestin
computerscienceamonghighschoolersteachingthemenoughaboutcomputersecuritytopiqueetheircurio
sitymotivatingthemtoexploreontheirownandenablingthemtobetterdefendtheirmachinestheflagisp
icoCTF{N6R4M_4N41Y515_15_73D10U5_8E18F808}

I came across <https://www.guballa.de/substitution-solver> which can solve any substitution cypher without the requirement of a key.

- **Transposition-trial**

Our data got corrupted on the way here. Luckily, nothing got replaced, but every block of 3 got scrambled around! The first word seems to be three letters long, maybe you can use that to recover the rest of the message.

Message - heTfl g as iicpCTo{7F4NRP051N5_16_35P3X51N3_V9AAB1F8}7



The screenshot shows the dCode website's Transposition Cipher Decoder tool. On the left, there's a search bar with the text "e.g. type 'boolean'" and a "BROWSE THE FULL dCODE TOOLS' LIST" link. Below this, the results for "Transposition Cipher - dCode" are shown, including a tag "Tag(s) : Transposition Cipher" and social media share buttons. The main section is titled "TRANSPOSITION CIPHER" and "TRANSPOSITION DECODER". It features a text input field containing the ciphertext "heTfl g as iicpCTo{7F4NRP051N5_16_35P3X51N3_V9AAB1F8}7". Below the input field, there are options for "KEEP SPACES, PUNCTUATION AND OTHER CHARACTERS" (checked) and "PLAINTEXT (PRESUMED) LANGUAGE" (English). The "DECRYPTION METHOD" section has two radio buttons: "KNOWING THE ENCRYPTION KEY OR PERMUTATION" (selected) and "TRY ALL PERMUTATIONS (BRUTEFORCE UP TO SIZE 6)". The "KNOWING THE ENCRYPTION KEY OR PERMUTATION" option has a text input field with "231" and a dropdown menu showing the permutation $(2,3,1) \Leftrightarrow (3,1,2)^{-1}$. The "GRID WRITING/READING ENCRYPTION DIRECTIONS" section has a "MODE" dropdown set to "Write by rows, read by rows" and a "DECRYPT" button. At the bottom, there's a link to "See also: Caesar Box Cipher – Scytale Cipher" and a "TRANSPOSITION ENCODER" section with a "TRANSPPOSITION PLAIN TEXT" input field.

The code was 231 as the first word was 3 letter as given in the hint, read and written both in rows.