Hi

Suppose that we have a simple encryption system which for encryption you have to xor your text with two keys (K1, K2).

C = P + K1 + K2

It is obvious that for decryption you have to xor again the cipher code with two keys.

P = C + K1 + K2

Notes that all text and cipher codes are in hexadecimal format. A simple plain text and its cipher code are given below with 6 digits.

P = 010199, C = 5410CC

You don't know the keys and you have to find two keys with a Brute Force attack. All possible numbers of the two keys are (16^6)^2 = 2^48, it is a big number. Try a birthday attack. Create two random keys and Xor one of them with P and the other one with C. If the results are equal you win and you find the two keys, otherwise, you have to create different random keys and repeat the task until you win.

You should send me your implemented code and the number of attempts to find the keys. Because of the simplicity of the encryption method, you may find more than one result. Send me the results of 10 runs.

Good luck.