|  |  |
| --- | --- |
| Semester | T.E. Semester V I– Computer Engineering |
| Subject | Cryptography and System Security |
| Subject Professor In-charge | Prof. Amit K. Nerurkar |
| Assisting Teachers | Prof. Amit K. Nerurkar |
| Laboratory | 312A |

|  |  |
| --- | --- |
| Student Name | Deep Salunkhe |
| Roll Number | 21102A0014 |
| TE Division | A |

**Title:**

Design and Implementation of Ceaser Cipher Technique

**Explanation:**

A private-key encryption scheme consists of a set of all possible messages, called the message space M, and three algorithms, namely,

(a) Gen

(b) Enc

(c) Dec

The algorithm for key generation Gen is used to choose a key k at random from the set of all possible secert keys, denoted by the key space K.

The algorithm for encryption Enc takes as inputs the message m and the secret key k and outputs the ciphertext c.

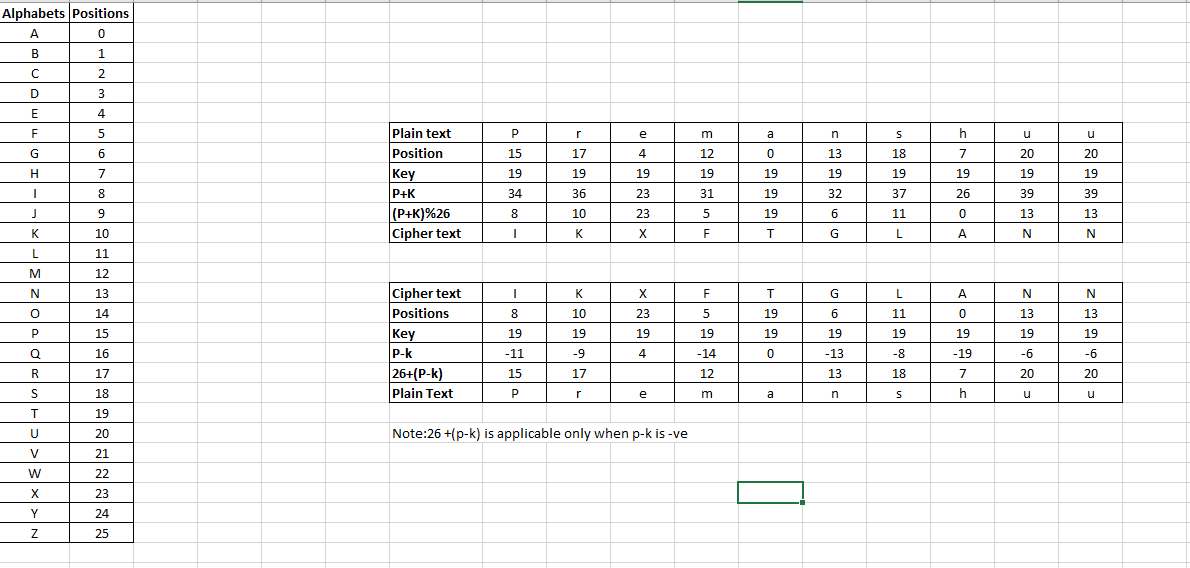
The algorithm for decryption Dec inputs the ciphertext c and the key k and outputs the message m.

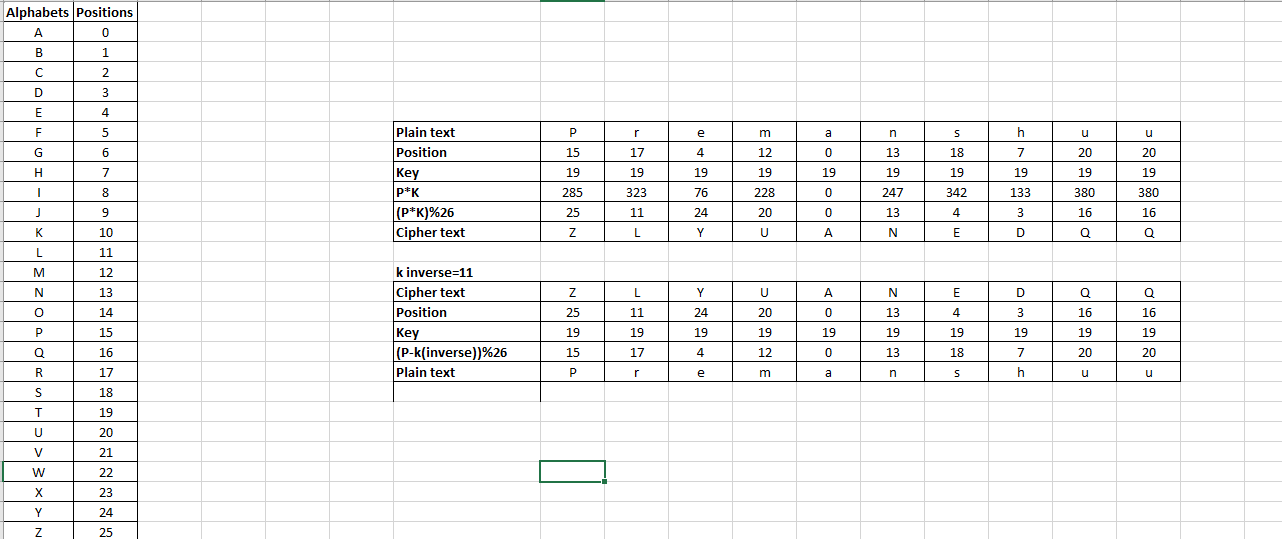
About the experiment:

Apparently, the system is easily broken if the total number of distinct secret keys is small, that is the key space K is small.

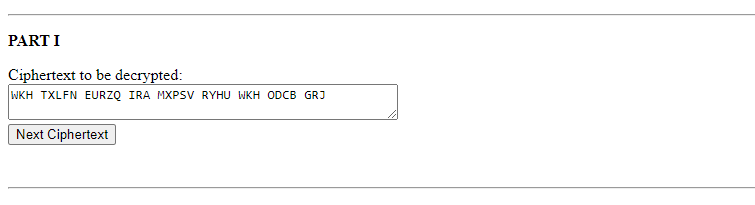
In this experiment, we work with a well-known historical encryption scheme, namely the shift cipher, that has a very small key space.

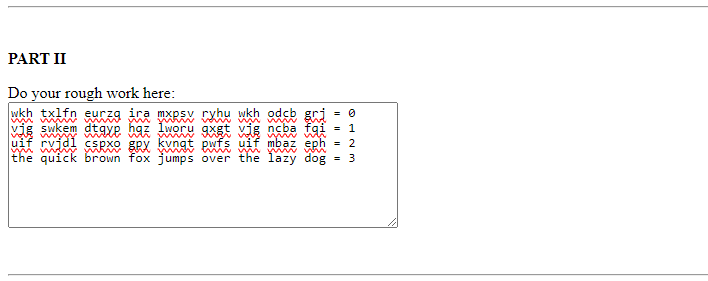
Your task is to break the shift cipher. Specifically, given (only) the ciphertext in some instance of a shift cipher, you need to find the plaintext and the secret key.

****

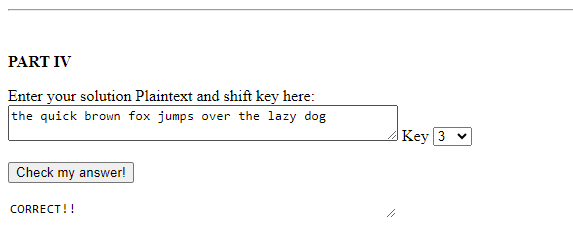
****

**Simulation:**

****

****

****

****

**Conclusion:**

In conclusion, the experiment successfully broke the shift cipher, showcasing its vulnerability due to its small key space. By systematically trying all possible keys and analyzing letter frequencies, the plaintext message was deciphered. This highlights the importance of key space size in encryption security and underscores the need for robust cryptographic techniques.