

VASAVI COLLEGE OF ENGINEERING (*AUTONOMOUS*), HYDERABAD

Accredited by NAAC with A++ Grade

B.E. (E.C.E. : CBCS) VII-Semester

Computer Networks

Virtual labs

Breaking the Shift Cipher

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 secret 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. The 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. [Breaking the Shift Cipher](#)

STEP 1 : For the given ciphertext in the **PART I** of the simulation page, the first step is to decrypt it using each of the twenty-six different keys, $k=0,1,\dots,25$ and obtain the corresponding plaintexts. For decryption, you may use the tool given in the **PART III** of the simulation page.

STEP 2 : After each decryption, you may cut-and-paste the resultant plaintext in the scratch-pad in the (**PART II**) of the simulation page, if you need to remember it.

STEP 3 : Finally, observe the plaintexts and choose the most appropriate one (the one that is a meaningful English text) as the recovered plaintext and cut-and-paste it in the text-field named **PART IV** "Solution Plaintext". Also select the corresponding key in the text-field named "Key" and click on "Check My answer" Button.

STEP 4 [OPTIONAL] : Verify that your answer is correct, by encrypting the solution plaintext with your key.

An Example:

Let us say we have a cipher text "KRZ DUH BRX" generated by a shift cipher. We carry out the brute force attack as follows:

For $k=0$:

```
cipher text: K R Z D U H B R X
```

plain text: k r z d u h b r x

For k=1:

cipher text: K R Z D U H B R X
plain text: j q y c t g a q w

For k=2:

cipher text: K R Z D U H B R X
plain text: l p x b s f z p v

For k=3:

cipher text: K R Z D U H B R X
plain text: h o w a r e y o u

For k=3, we obtain a meaningful plain text namely how are you and hence we are done.

For any queries contact

Dr.S.Aruna Deepthi
Asst Prof
Vasavi college of Engineering
Hyderabad
9676772232