Nanjing University of Information Science & Technology

Experiment (Internship) Report

|  |  |  |  |
| --- | --- | --- | --- |
| 202283890036 | 黄家睿(Jerry Huang) | Internet of Things | Zhiguo Qu(瞿治国） |

Implementation and Analysis of Single Table Password

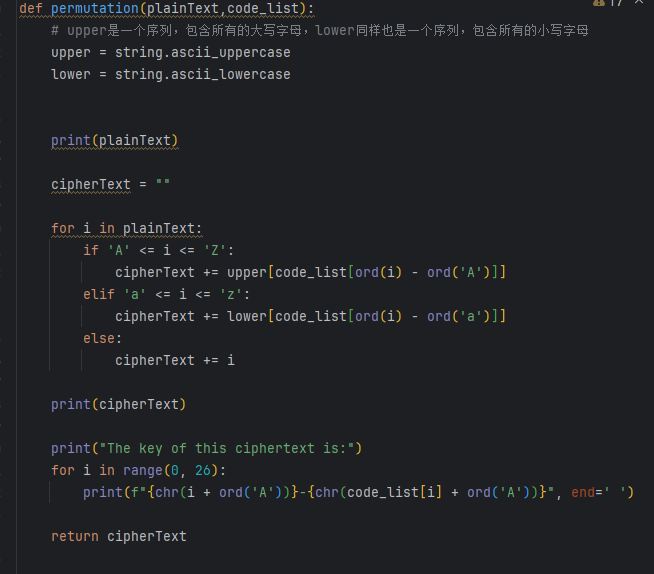
1．Experimental Purpose：

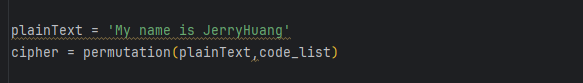
1. Master the single-table password encryption algorithm；
2. Understand common attack methods for single-table passwords.

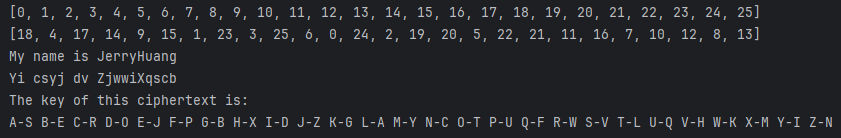
2．Experimental content：

1. Implement a single-table encryption and decryption algorithm to encrypt English text.；
2. Statistically analyze the frequency of letters in plaintext and ciphertext, perform cryptanalysis on a monoalphabetic cipher, and use real data to illustrate the issue.。
3. Experimental steps
4. Implementation of Single Table Password

Code implementation：



Code experiment section and output



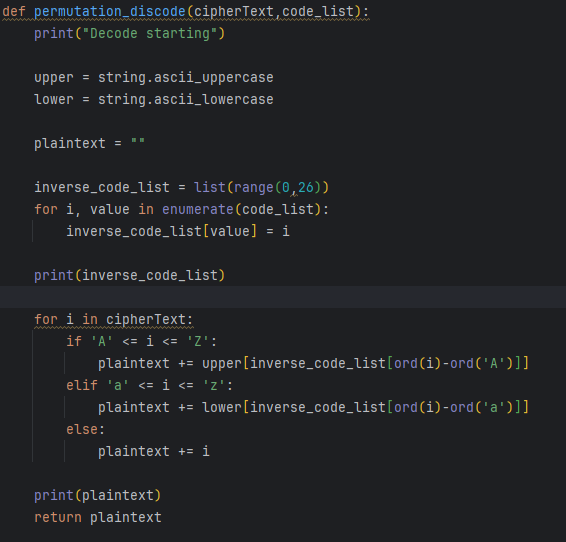
plainText is：“My name is JerryHuang”

The output ciphertext is：“Yi csyj dv ZjwwiXqscb”

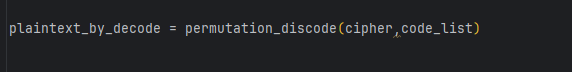
The corresponding relationship is ：“A-S B-E C-R D-O E-J F-P G-B H-X I-D J-Z K-G L-A M-Y N-C O-T P-U Q-F R-W S-V T-L U-Q V-H W-K X-M Y-I Z-N”

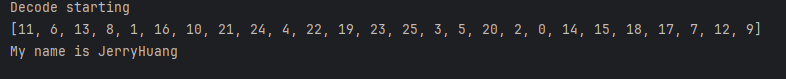
1. Decryption of single-table passwords

Code part：



Code experiment and the output:





This part of the code takes the ciphertext returned by the encryption method above and the same key as input. First, it compares the key with the initial positions of the letters, finds the plaintext corresponding to the ciphertext, and finally outputs the original plaintext.

This code successfully outputs the original plaintext: "My name is JerryHuang".

1. Experimental Analysis and Summary
2. Single-table password

The implementation of a monoalphabetic cipher is achieved through the shifting and transformation of letters. The simplest form of this is the Caesar cipher, which is realized by shifting letters by a fixed number of positions, for example, moving each letter three places down the alphabet: A to D, B to E, C to F... X to A, Y to B, Z to C. However, the Caesar cipher is very easy to break, as it only requires trying up to 26 shifts to uncover the original plaintext. Therefore, the random monoalphabetic cipher mentioned above was developed, where letters are randomly permuted rather than shifted as a whole like in the simple additive monoalphabetic cipher, significantly increasing the difficulty of decryption. However, the corresponding cipher key needs to be generated and transmitted separately, much like the generation of a cipher key in code is a separate process and not combined with the production of the ciphertext. This ensures the dependency of the cipher generation, preventing situations where the plaintext cannot be retrieved.

1. Attack and cracking of single-table passwords

Although the confidentiality of a randomly generated monoalphabetic password is much higher than that of additive monoalphabetic ciphers like the Caesar cipher, with a key space size of 26!, it is very difficult to brute-force crack using an exhaustive method. However, this cipher is also vulnerable to being cracked.

Consider changing the plaintext we want to encrypt, transforming a sentence into a paragraph.

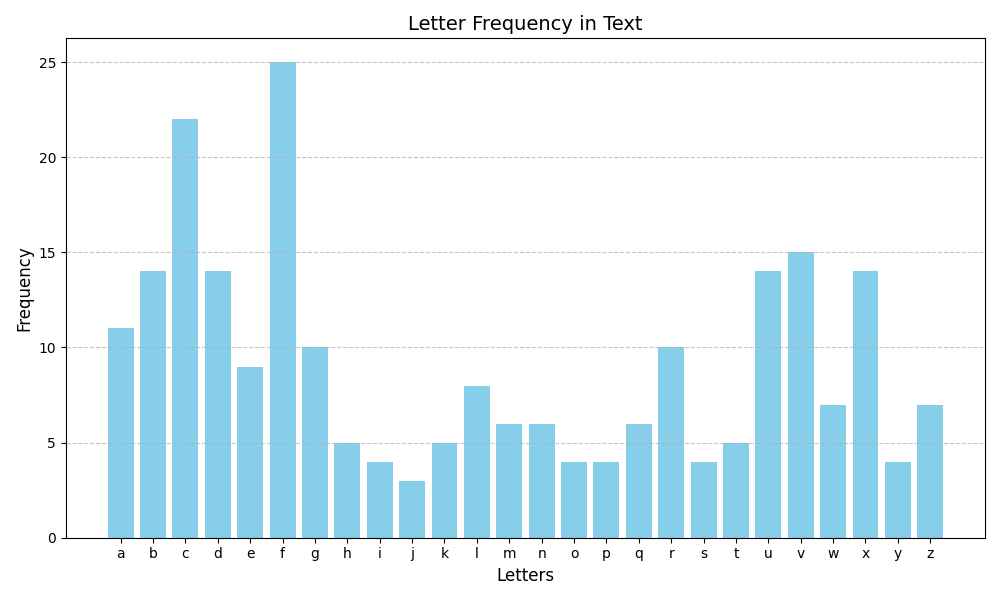
The quick brown fox jumps over a lazy dog while zebras watch quietly from afar. Jack loves quirky vibes and enjoys exploring xylophones in his spare time. Bright sunlight dazzles as he ventures into the lush garden, finding joy in every unique moment. A wizard offered him five juicy kiwis

After we encrypt, we can obtain such ciphertext and a corresponding table:

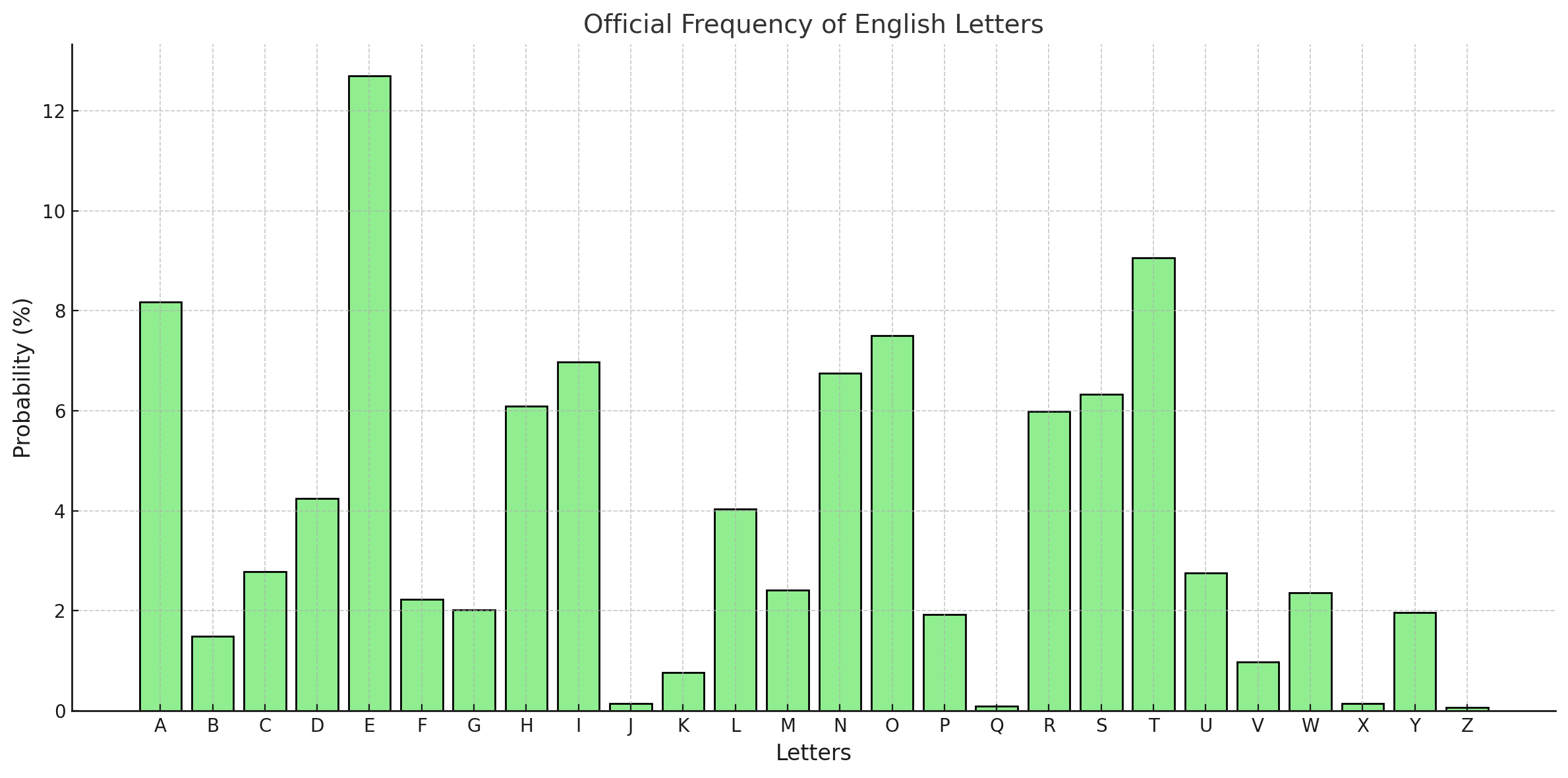
Gaf prcsy oxbkv wbj trmid bnfx u euhl zbq kacef hfoxud kugsa prcfgel wxbm uwux. Tusy ebnfd prcxyl ncofd uvz fvtbld fjiebxcvq jlebiabvfd cv acd diuxf gcmf. Oxcqag drvecqag zuhhefd ud af nfvgrxfd cvgb gaf erda quxzfv, wcvzcvq tbl cv fnfxl rvcprf mbmfvg. U kchuxz bwwfxfz acm wcnf trcsl yckcd.

A-U B-O C-S D-Z E-F F-W G-Q H-A I-C J-T K-Y L-E M-M N-V O-B P-I Q-P R-X S-D T-G U-R V-N W-K X-J Y-L Z-H

By counting the number of times each word appears in the text, we can obtain the following statistics table:



According to the official statistics of the probability of English letters appearing:



From the chart above, we can see that the letter 'e' has the highest probability of occurrence, and in our ciphertext, the letter 'f' appears most frequently. Moreover, according to our cipher key, the letter 'e' corresponds exactly to the letter 'f'. Let's look at the other frequently occurring letters in our ciphertext, which are 'c', 'v', and 'x'. These letters correspond to the plaintext letters 'i', 'n', and 'r', which are also letters with high occurrence probabilities.

If the length of the ciphertext we are trying to decrypt continues to increase, it would be entirely possible to decipher it using statistical probability methods. Therefore, if the ciphertext we are transmitting is only a short piece of text, using this encryption method is perfectly fine. However, as the number of characters increases, the risk of decryption also increases.