网络安全技术课堂作业二

朱浩泽 计算机科学与技术 1911530

题目一

我们记减法为 $X-Y=I^{-1}([I(X)-I(Y)]\ mod\ 26)$

则解密算法如下：

$D(K,C)=M_1M_2M_3.....M_K$

$M_i[j]=C_i[j]-K[j]$

题目二

解密程序如下:

```
if __name__ == "__main__":
    content = "Methods of making messages unintelligible to adversaries have been
necessary. Substitution is the simplest method that replaces a character in the
plaintext with a fixed different character in the ciphertext. This method preserves the
letter frequency in the plaintext and so one can search for the plaintext from a given
ciphertext by comparing the frequency of each letter against the known common frequency
in the underlying language."
    key = "BLACKHAT"
    result = []
    count = int(0)
    for index in content:
        if index == " ":
            temp = " "
        elif index == '.':
            temp = '.'
        else:
            temp = chr(((ord(index.lower()) - 97) + (ord(key[count % len(key)].lower())
- 97)) % 26 + 97)
            count += 1
        result.append(temp)
    result = "".join(result)
    print(str(result))
```

解密结果如下

nptjyks hg xamsug ffdscqls notnvoslbhtbno ao tegetchrbfd hcfl bxfy ngmlslbcy. ueismjeuvsvn bt ehg cpmimpsv wltapo tjka rxqwaeoz a vilrcmaek jy tjo wltjytgha wbus a hseew etfhoyegu nhcbhcmfc ip doe vjahgbaequ. ehkc temizd rblsxsgeu doe efetgb mrxrfepmf ig use rvhigupxv kud lp zng mhn lflrer mok use rvhigupxv pyof b rixou cbqsetdlxm cj cqwwakjyg vrl fkfbugxjy hg paer semupr cqhigte tjo rnhxy cqwtog gceselnvz tn vrl ugeprnipnz mlniehgx.