**信息科学与工程学院**

**2021－2022学年第一学期**

实 验 报 告

课程名称： 信息安全

实验名称： 实验一

专 业 班 级 通信工程 二班

学 生 学 号 201800121050

学 生 姓 名 孟麟芝

实 验 时 间 2021年10月17日

实验报告

### 【实验目的】

1. 掌握单表代换的原理、缺点。
2. 能进行简单的密文破译。

### 【实验要求】

1. 密文1：

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZVUEPHZHMDZSHZQWSFPAPPDTSVPQUZWYMXUZUHSXEPYEPOPPZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

1. 密文2：

JXQCEFMPJASOQMDPQABCSTYSMGRQBTQOASKQAOUWCPQBDPMEEASIVMWPOQVJXQVQCSORWBQKMMYVJQAOXQPVASBFPAOJCOARQHFQPCQSOQASBQAOXXAVCJVMGSABZASJATQVJXQYSMGRQBTQGQTACSDPMEKMMYVASBDMPEARQBWOAJCMSQSAKRQVWVJMRQAPSAKMWJJXCSTVXAJGQXAZQSMMFFMPJWSCJIJMQHFQPCQSOQCSBACRIRCDQGOOASVJWBIARRJXQFRAOQVCSJXQGMPRBASBRQAPSDPMEFQMFRQGQGCRRSQZQPEQQJCSMWRCDQJCEQLWVJKIPQABCSTJXQCPKMMYVGQOASARVMBQZQRMFMWPASARIJCOARVYCRRVASBRQAPSXMGJMZCQGASBCSJQPFPQJJXQGMPRBAPMWSBWVCSBCDDQPQSJGAIVGQOASRQAPSJXQFAVJKIPQABCSTKMMYVCSJXCVGAIGQGMSJPQFQAJJXQECVJAYQVMMJXQPVASBOASKWCRBMSJXQCPAOXCQZQEQSJV

### 【实验过程】

### 【第一段密文】

首先，使用Matlab的tabulate()函数，可以输出一段密文中各字母的频率，如下图：

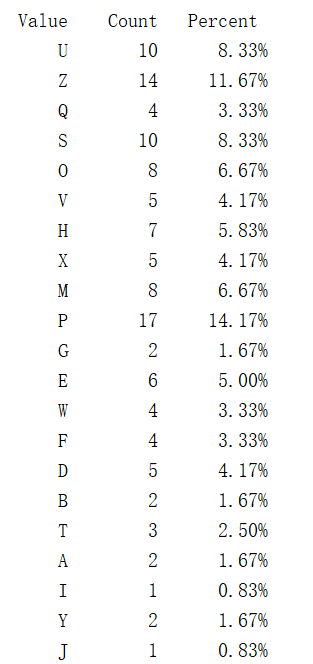


图 1 密文中各字母频率

可见其中P、Z最高，可先认为P对应E，Z对应T，则猜测开头为it，故U对应I。代入后得到如下结果：

itQSOViOHXMOeVGeOteEVSGtWStOeFeESXiDBMETSXAItViEeHtHMDtSHtQWSFeAeeDTSVeQitWYMXitiHSXEeYEeOeetStiFeOMBtWeFietHMDJiDTMOHMQ

继续猜测tWe为the，则W对应H，代入后如下：

itQSOViOHXMOeVGeOteEVSGthStOeFeESXiDBMETSXAItViEeHtHMDtSHtQhSFeAeeDTSVeQithYMXitiHSXEeYEeOeetStiFeOMBtheFietHMDJiDTMOHMQ

猜测Q对应W，S对应A：

itwaOViOHXMOeVGeOteEVaGthatOeFeEaXiDBMETaXAItViEeHtHMDtaHtwhaFeAeeDTaVewithYMXitiHaXEeYEeOeetatiFeOMBtheFietHMDJiDTMOHMw

猜测O对应S：

itwasVisHXMseVGesteEVaGthatseFeEaXiDBMETaXAItViEeHtHMDtaHtwhaFeAeeDTaVewithYMXitiHaXEeYEeseetatiFesMBtheFietHMDJiDTMsHMw

根据开头语气，猜测红色部分为yesterday，则G对Y，E对R，V对D：

itwasdisHXMsedyesterdaythatseFeraXiDBMrTaXAItdireHtHMDtaHtwhaFeAeeDTadewithYMXitiHaXreYreseetatiFesMBtheFietHMDJiDTMsHMw

猜测红色为disclosed与several，则H对C，X对L，M对O，F对V：

ItwasdisclosedyesterdaythatseveraliDBorTalAItdirectcoDtactwhaveAeeDTadewithYoliticalreYreseetativesoBthevietcoDJiDToscow

至此意义已经较为明显，在经过一些猜测，并修改一些错误，可知明文如下：

it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in Moscow.

### 【第二段密文】

利用tabulate()函数，得到频率如下：

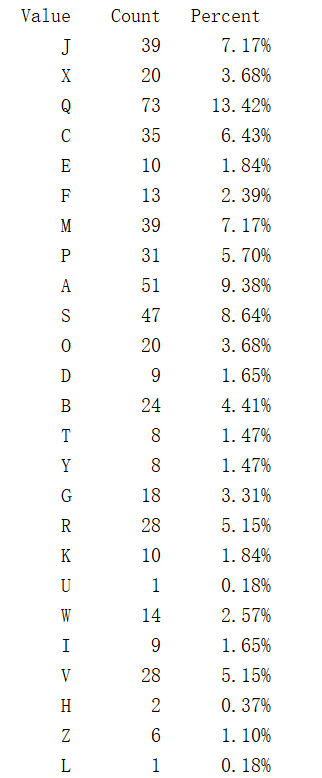


图 2 第二段密文字母频率

可直接猜测Q对应E，又发现JXQ频繁出现，可猜测其对应THE：

theCEFMPtASOeMDPeABCSTYSMGReBTeOASKeAOUWCPeBDPMEEASIVMWPOeVtheVeCSORWBeKMMYVteAOhePVASBFPAOtCOAReHFePCeSOeASBeAOhhAVCtVMGSABZAStATeVtheYSMGReBTeGeTACSDPMEKMMYVASBDMPEAReBWOAtCMSeSAKReVWVtMReAPSAKMWtthCSTVhAtGehAZeSMMFFMPtWSCtItMeHFePCeSOeCSBACRIRCDeGOOASVtWBIARRtheFRAOeVCStheGMPRBASBReAPSDPMEFeMFReGeGCRRSeZePEeetCSMWRCDetCEeLWVtKIPeABCSTtheCPKMMYVGeOASARVMBeZeRMFMWPASARItCOARVYCRRVASBReAPShMGtMZCeGASBCStePFPettheGMPRBAPMWSBWVCSBCDDePeStGAIVGeOASReAPStheFAVtKIPeABCSTKMMYVCSthCVGAIGeGMStPeFeAttheECVtAYeVMMthePVASBOASKWCRBMStheCPAOhCeZeEeStV

根据概率猜测A即对应A，再猜测CST为ing，后面的猜测则都比较顺畅，可得到如下明文：

The importance of reading knowledge can be acquired from many sources these include books teachers and practical experience and each has its own advantages the knowledge we gain from books and formal education enables us to learn about things hat we have no opportunity to experience in daily life wc can study all the places in the world and learn from people we will never meet in ou life time just by reading their books we can also develop our analytical skills and learn how to view and interpret the world around us in different ways we can learn the past by reading books in this way we wont repeat the mistakes o others and can build on their achievements.

修改其中的一些错误（已标红），得到如下文段：

The importance of reading knowledge can be acquired from many sources, these include books, teachers and practical experience and each has its own advantages. the knowledge we gain from books and formal education enables us to learn about things that we have no opportunity to experience in daily life. We can study all the places in the world and learn from people we will never meet in our life time, just by reading their books, we can also develop our analytical skills and learn how to view and interpret the world around us in different ways, we can learn the past by reading books in this way we won’t repeat the mistakes of other sand can build on their achievements.