信息安全作业

通信一班 孙留羿 202000120166 提交时间 2021年12月10日

（统计频率代码见附录）

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZVUEPHZHMDZSHZQWSFPAPPD TSVPQUZWYMXUZUHSXEPYEPOPPZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

频次：2 2 0 5 6 4 2 7 1 1 0 0 8 0 8 17 4 0 10 3 10 5 4 5 2 14

一些文字和图片的手机截图

描述已自动生成

统计单字母出现频率与已知字母出现频率进行对照，得P为E，Z为T，S为A，U为I依照单词出现频率，推测W为H，对剩余字母逐渐猜测匹配得到

：itwasdisclosedyesterdaythatseveralinformalbutdirectcontactshavebeenmadewithpoliticalrepresentativesofthevietconginmoscow

频次

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

51 24 35 9 10 13 18 2 9 39 10 1 39 0 20 31 73 28 47 8 1 28 14 20 8 6

JXQCEFMPJASOQMDPQABCSTYSMGRQBTQOASKQAOUWCPQBDPMEEASIVMWPOQVJXQVQCSORWBQKMMYVJQAOXQPVASBFPAOJCOARQHFQPCQSOQASBQAOXXAVCJVMGSABZASJATQVJXQYSMGRQBTQGQTACSDPMEKMMYVASBDMPEARQBWOAJCMSQSAKRQVWVJMRQAPSAKMWJJXCSTVXAJGQXAZQSMMFFMPJWSCJIJMQHFQPCQSOQCSBACRIRCDQGOOASVJWBIARRJXQFRAOQVCSJXQGMPRBASBRQAPSDPMEFQMFRQGQGCRRSQZQPEQQJCSMWRCDQJCEQLWVJKIPQABCSTJXQCPKMMYVGQOASARVMBQZQRMFMWPASARIJCOARVYCRRVASBRQAPSXMGJMZCQGASBCSJQPFPQJJXQGMPRBAPMWSBWVCSBCDDQPQSJGAIVGQOASRQAPSJXQFAVJKIPQABCSTKMMYVCSJXCVGAIGQGMSJPQFQAJJXQECVJAYQVMMJXQPVASBOASKWCRBMSJXQCPAOXCQZQEQSJV



（注）以下将大写字母作为替换前字母，小写字母作为替换后字母

1. 假设Q为E那么统计前三个字母出现频率已知JX其为th，故密文并不完全按照频率统计规律排列，
2. 观察剩余部分发现有eet组合，易猜测常用单词meet ，故E对应m.
3. 按频率开始对A进行处理，则在大概范围内，A应为a或o。
4. 与同样出现频率较高的M联合猜测，有多个重复出现的MM组合，按照英文出现频率应为oo，故A为a
5. 继续按频率将C替换为r但并没有很多明显词汇出现故暂时搁置。
6. 按照多字母出现频率进行修改，出现大量DPom，在对应频率范围内寻找常用组合字，找到了from，故将DP分别替换为fr进行尝试
7. 因r已被占用，在频率范围内寻找未被占用的字母，C可能为nish。逐一进行尝试

为n时有mn,hn等不常用组合，故暂时不选，替换为i时有their，it 等常用词组，故暂时认为为i

1. 开头部分出现the+imFortaSOe。与the importance相似，故将FSO替换为pnc进行尝试
2. 同理将之后出现的theimportanceofreaBinT，替换为the importance of reading, 即BT转换为dg
3. teacherV, 在名词后出现单一无关联字母，考虑为复数形式，故为s
4. eHperience experience H应为x
5. Rearn learn R应为l
6. indailIlife in daily life I应为y
7. YnoGledge knowledge YG应为kw
8. soWrces sources W应为u
9. educationenaKlesus education enables us K应为b
10. itsownadZantages its own advantages Z应为v
11. canbeacUuiredfrom can be acquired from U应为q

得到theimportanceofreadingknowledgecanbeacquiredfrommanysourcestheseincludebooksteachersandpracticalexperienceandeachhasitsownadvantagestheknowledgewegainfrombooksandformaleducationenablesustolearnaboutthingshatwehavenoopportunitytoexperienceindailylifewccanstudyalltheplacesintheworldandlearnfrompeoplewewillnevermeetinoulifetimeLustbyreadingtheirbookswecanalsodevelopouranalyticalskillsandlearnhowtoviewandinterprettheworldaroundusindifferentwayswecanlearnthepastbyreadingbooksinthiswaywewontrepeatthemistakesoothersandcanbuildontheirachievements

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 them is takes of other sand can build on their achievements.

2.playfair（代码见附录）

（注）2 3 4 5 均用同一明文

1转英文

ThebirthandrapiddevelopmentofquantumcommunicationsecuritytechnologymainlydependsonthefollowingtwofactorsaClassicalsecurecommunicationisfacedwiththreekeyproblemsthataredifficulttobethoroughlysolvednamelykeynegotiationidentityidentificationandeavesdroppingdetectionTheeffectivesolutionoftheseproblemsrequiresnewtechnologiesbIntheexplorationofnewtechnologiespeoplehavediscoveredtheinherentsecuritycharacteristicsofquantumanditspossibleapplications

2去标点和空格

ThebirthandrapiddevelopmentofquantumcommunicationsecuritytechnologymainlydependsonthefollowingtwofactorsaClassicalsecurecommunicationisfacedwiththreekeyproblemsthataredifficulttobethoroughlysolvednamelykeynegotiationidentityidentificationandeavesdroppingdetectionTheeffectivesolutionoftheseproblemsrequiresnewtechnologiesbIntheexplorationofnewtechnologiespeoplehavediscoveredtheinherentsecuritycharacteristicsofquantumanditspossibleapplications

密钥：xinxianquan

wfucaowfqakynrabeuzbgsrocqvmlxdxxwftbptucxnbxybvqpuddmxvzvudpcsgvotrqnqhakcscqerpiwfulsggsvnihvymgndvmsmndkqmqnbqkzldbsdbptucxnbxybvanmlnduevnwfwfsddldzrsvgslomwfxydyuexggxdbfzvmcuwfpsmbhkkzmpgzueaqsukzldwablmvnqvxpiabcqvxvzabcqvxgxdnvxpiqaeuiylzkyproniheuzuuwbvxwlculluuwbilzsgfxbvipmxlczlrsvgslomsdxeaolzqcyvudpcsgvoqboenawfuqnmgsydvxpimgqcyvudpcsgvoqbmrbsshcliyueqobpzbsduylcnalcsdxwzldboavzhpdyndzuoamznbmplxdxxwftqabazmrpmqbgslnrshnbxybvqp

3.转轮机编写

（3轮）

JlxjqcsuowpjfxjshkhdnqrfoztdpdnrfxfooceombdztbyojtilbdnwwpmtqhrqkxchgrtsbjawziwgvxfyogkhmwkqydjwjpnkygdmmPxzlbvotivdzjojuvrbpfbfvhvmaennoniiirmvhydhfkzfcaasvhxapvxlhpivqeisrwztrnrwflfigoxslnurlxikwqecygknrhpihilugfrruonnnpfabqguawyowdhvoukeqnbuhnztgbahqxlatbfjhnrJvjyoeayhpaxthzaxiexlnyunekdywzbugocfstxvrhfejkypbmkvntbonwNtwztkxqcyblahbpltkwxenelcsevdstjbvdsaetiyaciqrnyfqzyfwibcsuznmhigiaahwyctdfuohirabllqwpbzdoyaefipqrunbbhezgyyvcxjlqnyngcl

4. DES 密码编写；

密码xinxianq



偏移量xinxianq



+ExQNm/tSc6y+RRnrBTpDd1Q+pY8TeYppAt4Mr2SYNNxgAWnqmxsbvLhVMwSwLbaiCVhUmiuEDM5YPqHHLrbXT3BlWfEfIU+m3v+zKzvuLHxSZDHMDngiEABaJemcEN9jOYwPLNVsLd2EGNFbsqWcgSb+IjG+62ICSzUry07gLz2Trw/i7FKXB4DW5h2pFElLXAzW3K0pW60vSePap4tjjsm/ZSUswBDvF1ME3TFKuyqEYbuRPMxUO0/wfV6thvpuYPhMpEoUri0JhTQDF2YdvRCkbluiHpLAKMOo5LFWkmGdJfAgUyPaYcSTtHYoJ6e//u5IzwEw+xaklfLn4CHRnR1BXSxGwi3S+4t/lmLIONFAFbpdIPNUZ2/PFWdawVK31QrutI9yuBpreIKV+xA5r4U0woIepo9rrUDOiFeqFhdma/93/srkQBckpVPMYDiiMaYYKCiH8GF8ohFCQg56w==

5.AES密码编写

密码sddx202000120166



偏移量sddx202000120166



TwJ9ONJcsHtPAK61LV4AUzJ4TZKwJRTsbxvaUzO8gBxlYVLsB3THKYnRFe0VEsZWBGV+K/CoM7eBa7DUqXt0FhgPVm9r1klopyj2Df8n7zTx3E8gwnqO0AxjnO1skk2gvHOmp74GA09C0lYh0vJ+078NLb2EhxuWIOZp2ytYef9GOovdzA9BQ/6loNraake5Tv5OILM/xephWgCOGUudY4qOzQ9ZhhyljogBOIKeNFhlYHOh1BEC6k10FjYAxEgFYi/RB3SuSs1QXHsKqzNE3RCYxsIHZmqwowhGRFYTiPGUZ9ECeDu3M5TnNG2qGcsuPSn46NaGUwpLmSme0k+E7UInZY8NkKdfCda6WjeSg3a0rGLaRHyqKoCifXJMjiyoCCE8LsDs5n629AYQMYY1diCO9vrrNJ0E+ffG7PxNbdRo2DxGtTJPjmfxhgIOH3XSY3uv0/+1myW3Xqrm5Wt95Q==

文本, 信件

描述已自动生成

（代码见附录）

(1) 6

(2) 1

(3) 3 -13 8

(4)14387

7、 建立一个 SSL 会话，如图 1。结合服务器到客户端的认证，但是没有客户端到服务器的 认证。设客户端（Alice）准备使用信用卡从服务器（Bob 公司）购买一些东西。图 1 协 议被用来派生密钥 K1 和 K2，这两个密钥将被用来加密和认证 Alice 的信用卡号以保证 SSL 会话的安全（当卡号被发送给 Bob 公司时）。简明地讨论下面几点关于 SSL 的问题： （a） 为什么需要 Alice 的 Web 浏览器认证 Bob 的公钥？

（b） 在这个版本的协议中，Bob 没有办法建立阶段认证 Alice，这对 Bob 来说有问题 吗？为什么？

（c） 密钥 k1 和 k2 从一个由 Alice 提供的随机数 MS 派生出来，为什么随机数是由 Alice 生成而不是 Bob 公司？这种方法产生密钥 K1 和 K2 有潜在安全威胁吗？

图片包含 图形用户界面

描述已自动生成

解：

(a) Alice 的Web浏览器需要通过验证Bob公钥以确认公钥验证签名数据。

(b)可能有问题，Bob无法确认Alice所处安全与否，存在一定风险。

(c)如果随机数由Bob公司生成，若Bob被攻击，MS泄露情况，且Alice仍用该随机数的hash值作为密钥加密，则攻击者可以试探Alice的密文并得到Alice的信用卡号，导致Alice财产问题出现，所以应由消费者Alice生成，问题只会交由供货方，不会造成财产损失。

8、说说你对信息安全的理解

信息安全是对于信息的安全问题，而我们现在处于信息化社会，身边小至当前所处的位置，今天要吃的食物，大到身份信息以及各种个人账户乃至银行卡密码都是信息，而有些信息需要高度保密，就必然存在着安全问题。

首先对于信息安全这一学科以我的理解，是基于数学的一门学科，从古典的凯撒密码以及enigma机作为一个简单的数学映射关系，到现在对称以及非对称密码体制和大素数分解还有哈希散列表等数据结构，和未来的量子通信，其本质都是可以看作不同的数学问题。

基于对数学的一点兴趣，我在大一下曾经尝试过网络空间安全学院的春转，可惜对于大一上知识的不使用导致迅速遗忘，使我在面试中关于线性代数的问题没有能回答上来，进而没有能转入，但我对于信息安全的重视以及看好是不会改变的，因为不管是我现在所处的通信工程专业，还是以后要从事的其他行业，都对信息安全方面提出了相当高的要求，并且，在小时候经历过QQ被盗号我却无能为力只能通过不断申诉进行找回的无力感，所以我依然会继续学习有关信息安全方面的问题。

最后对于这次信息安全作业，我还是认识到了自己实力的不足，对于第一题的单表代换本来以为是非常容易的一个频率统计题目，可当统计出频率之后发现现实和理想之间是有相当大的差距的，我们不能寄希望于密码总是出成符合规律的样子，只能和题解中一样，用漫长的十八步分析对字母进行逐一的确定，play fair还可以借助网络工具加上自己的编码能力实现， 几个简单的数论问题都是我以前做过的题目，可以直接拿以前的代码来解决。

总而言之信息安全是一个很重要的学科，尤其是现在处于一个信息化的时代，人们对于信息安全的重视也势必会逐渐加强，未来我们对于信息安全也必然会有进一步的学习以及应用。

2附录：

***（注）代码实际编译与执行均在acwing在线测试平台上操作***

1.

统计频率代码

}

2、play fair代码

快速幂求解

拓展欧几里得

求解同余方程

求解同余方程组