

密码学

平时实验报告

（ 2020 / 2021 学年 第 二 学期）

题 目： 古典密码实验

|  |  |
| --- | --- |
| **专 业** | 信息安全 |
| **组 长 姓 名** | 茹兴奥 |
| **组 员 姓 名** |  |
| **班 级 学 号** | B19030824 |
| **指 导 教 师** | 李琦 |
| **指 导 单 位** | 信息安全系 |
| **日 期** | 2021年3月12日 |

|  |  |
| --- | --- |
| **成员分工** | |
| 组长（1） | 姓名茹兴奥学号B19030824 具体分工全部 |
| 组员（1） | 姓名 学号 具体分工 |
| 组员（2） | 姓名 学号 具体分工 |
| **简短评语：**  **指导教师： 李琦 年 月 日** | |

**Windows系统环境下的口令破解实验**

1. **课题内容和要求**

**1.实验环境**

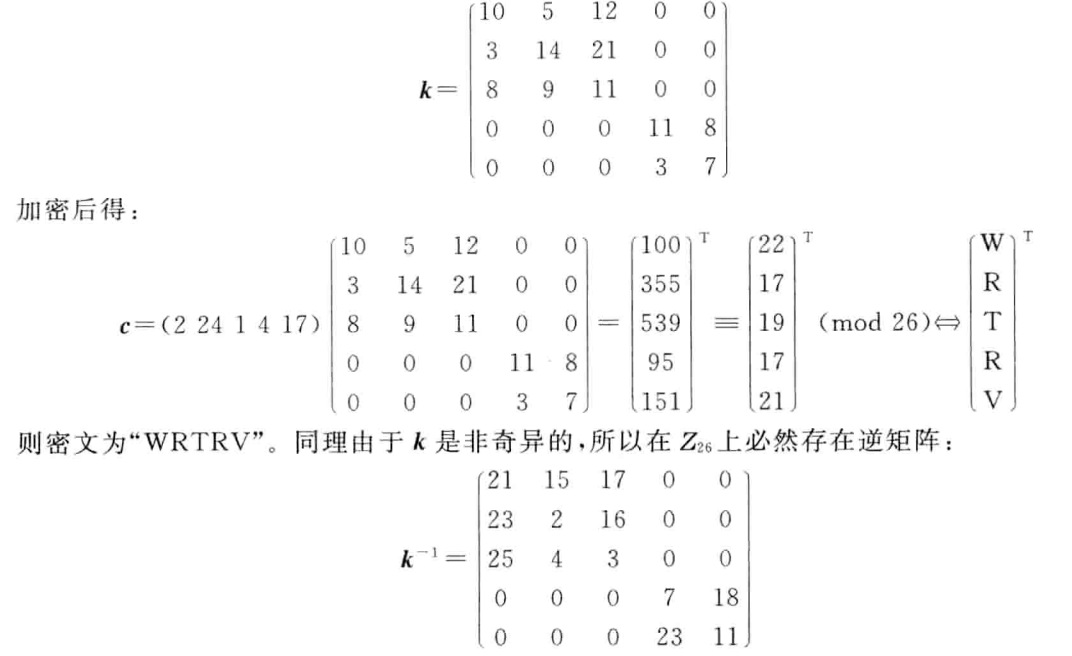
实验主机操作系统为Windows 10 Dev-C++

**2.实验内容**

题目：对于明文“In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes Currently the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control However if any server storing the data is compromised then the confidentiality of the data will be compromised In this paper we present a system for realizing complex access control on encrypted data that we call ciphertext-policy attribute-based encryption By using our techniques encrypted data can be kept confidential even if the storage server is untrusted moreover our methods are secure against collusion attacks”（忽略大小写及空格）。

完成（若分组长度不足请自行补足）：

a：选择分组n=7的周期置换（自定义置换），进行加解密；  
b：以P53页的K作为私钥，进行Hill算法加解密，并对明密文字符的频率分别做统计分析。

  
c：自己选择K1和K2，做仿射密码的加解密，并对明密文字符的频率分别做统计分析。

**二、课题需求分析**

运用C语言写代码

**三、测试数据及其结果分析**

**（a）1.加密**

#include <iostream>

#include <string.h>

#include <math.h>

#include <stdio.h>

using namespace std;

int main()

{

string s="2435617";

char c[]="inseveraldistributedsystemsausershouldonlybeabletoaccessdata\

ifauserpossesacertainsetofcredentialsorattributescurrentlytheonlymethod\

forenforcingsuchpoliciesistoemployatrustedservertostorethedataandmediate\

accesscontrolHoweverifanyserverstoringthedataiscompromisedthenthe\

confidentialityofthedatawillbecompromisedinthispaperwepresenta\

systemforrealizingcomplexaccesscontrolonencrypteddatathatwecall\

ciphertextpolicyattributebasedencryptionbyusingourtechniquesencrypted\

datacanbekeptconfidentialevenifthestorageserverisuntrustedmoreover\

ourmethodsaresecureagainstcollusionattacks",d[999];

int i,k=0;

for(i=0;i<99;i++){

d[k]=c[i\*7+6];k++;d[k]=c[i\*7+3];k++;d[k]=c[i\*7+4];k++;d[k]=c[i\*7+2];k++;

d[k]=c[i\*7+5];k++;d[k]=c[i\*7];k++;d[k]=c[i\*7+1];k++;

}

cout<<d<<endl;

return 0;

**结果：**

revseinrisdtalsteudibaemtsysorsehusyondlultblaebescecsoaaaitfdasrpeousracsesetnsietaerecdofoalisntbtrtirarsceuutttlnyremnloyheoodhfetcfonrrehsugcineiclipomtosesiryaotpleedtsussrteorveetrhtodaatndaeiadtmecescsacHrotloniveerowrysnefarstrovedthgeinoisacatsomrimpthetnedioncfheltinadehofytititaawedmecbollemiosprsthnidieerpwpatseenprmstyeaslrerafoongicizcexlampnscsoceeloontreyprtnchtaatddlecwaatrphielcltpxoteratyticateubibrendcsebiotnypoinsgyunecthurnesueiqdptyecrnactadacepktbenidfeoneleavtisthfenisagretoserviertrutsunoormeedmourrveaodhsetrecsuresaigneaslloutcaatntio

} **2.解密**

#include <iostream>

#include <string.h>

#include <math.h>

#include <stdio.h>

using namespace std;

int main()

{

string s="7165342";

char c[]="revseinrisdtalsteudibaemtsysorsehusyondlultblaebescecsoaaaitfdasrpeo\

usracsesetnsietaerecdofoalisntbtrtirarsceuutttlnyremnloyheoodhfetcfonrrehsugci\

neiclipomtosesiryaotpleedtsussrteorveetrhtodaatndaeiadtmecescsacHrotloniveerow\

rysnefarstrovedthgeinoisacatsomrimpthetnedioncfheltinadehofytititaawedmecbolle\

miosprsthnidieerpwpatseenprmstyeaslrerafoongicizcexlampnscsoceeloontreyprtncht\

aatddlecwaatrphielcltpxoteratyticateubibrendcsebiotnypoinsgyunecthurnesueiqdp\

tyecrnactadacepktbenidfeoneleavtisthfenisagretoserviertrutsunoormeedmourrveao\

dhsetrecsuresaigneaslloutcaatntio",d[999];

int i,k=0;

for(i=0;i<99;i++){

d[k]=c[i\*7+5];k++;d[k]=c[i\*7+6];k++;d[k]=c[i\*7+3];k++;d[k]=c[i\*7+1];k++;

d[k]=c[i\*7+2];k++;d[k]=c[i\*7+4];k++;d[k]=c[i\*7];k++;

}

cout<<d<<endl;

return 0;

}

**结果：**

"inseveraldistributedsystemsausershouldonlybeabletoaccessdataifauserpossesacertainsetofcredentialsorattributescurrentlytheonlymethodforenforcingsuchpoliciesistoemployatrustedservertostorethedataandmediateaccesscontrolHoweverifanyserverstoringthedataiscompromisedthentheconfidentialityofthedatawillbecompromisedinthispaperwepresentasystemforrealizingcomplexaccesscontrolonencrypteddatathatwecallciphertextpolicyattributebasedencryptionbyusingourtechniquesencrypteddatacanbekeptconfidentialevenifthestorageserverisuntrustedmoreoverourmethodsaresecureagainstcollusionattacks

**（b）1.加密**

#include <iostream>

#include <string.h>

#include <math.h>

#include <stdio.h>

using namespace std;

int main()

{

char c[]="inseveraldistributedsystemsausershouldonlybeabletoaccessdata\

ifauserpossesacertainsetofcredentialsorattributescurrentlytheonlymethod\

forenforcingsuchpoliciesistoemployatrustedservertostorethedataandmediate\

accesscontrolhoweverifanyserverstoringthedataiscompromisedthenthe\

confidentialityofthedatawillbecompromisedinthispaperwepresenta\

systemforrealizingcomplexaccesscontrolonencrypteddatathatwecall\

ciphertextpolicyattributebasedencryptionbyusingourtechniquesencrypted\

datacanbekeptconfidentialevenifthestorageserverisuntrustedmoreover\

ourmethodsaresecureagainstcollusionattacks";

int i,e=strlen(c);

int a[e],b[e],f[26];

char d[e+1];

for(i=0;i<e;i++){

a[i]=(int)c[i]-97;

}

for(i=0;i<26;i++){

b[i]=0;

}

for(i=0;i<e;i++){

a[i]=(int)c[i]-97;

b[a[i]]++;

}

for(i=0;i<26;i++){

cout<<b[i]<<" "<<endl;

}

for(i=0;i<e/5;i++){

b[5\*i+0]=(a[5\*i+0]\*10+a[5\*i+1]\*3+a[5\*i+2]\*8)%26+97;

b[5\*i+1]=(a[5\*i+0]\*5+a[5\*i+1]\*14+a[5\*i+2]\*9)%26+97;

b[5\*i+2]=(a[5\*i+0]\*12+a[5\*i+1]\*21+a[5\*i+2]\*11)%26+97;

b[5\*i+3]=(a[5\*i+3]\*11+a[5\*i+4]\*3)%26+97;

b[5\*i+4]=(a[5\*i+3]\*8+a[5\*i+4]\*7)%26+97;

}

for(i=0;i<e;i++){

d[i]=(char)b[i];

}

cout<<d<<endl;

return 0;

}

**结果：**

43

9

30

23

77

10

6

16

37

0

2

22

12

33

41

15

1

43

47

59

17

7

4

2

13

1

duvdxnypafavhdkoorbbgqinysacoabefpyxvklvikxsgxnbrqwumuchctbwrgtoaddyaeywegojnqyeipgrqkydbbxjkkmqrofgtuintdmhwcxxeftzxvwtevrlwybvpybdjrixbzlulqtyyfjyfhuksucavhkktfisuldooaswhcqfznkjizbxxxlebbfgjnnulufclqbgouuuwcthavajtruwucdzvxircqfznhcechxzrvcbbfgjmicciifgyocqngsftjvdmkbzltarnthzrcfnrjvdhychcrlpbpmkphwiokqyfcjeimikchrvoptrikdbbwgqinynwnevypnhflqtmktfijlwumucmkwsdoqvlvrmfzsfnzqtfgjwtzwryurtouuvbhkjbtmzkudkektuintdmhliirvftdwvotspnfugiefqyjvnyprcgusgcftdwvotvlofdgcqqhyoqotkltbsqgdzanipjomopwtmblxxyqocqfzndkgtzalqdvbbmtbiaucdgsedgwthonzpwwceaalcowduvhkblaoaspnfdyjqiy

**2.解密**

#include <iostream>

#include <string.h>

#include <math.h>

#include <stdio.h>

using namespace std;

int main()

{

char c[]="duvdxnypafavhdkoorbbgqinysacoabefpyxvklvikxsgxnbrqwum\

uchctbwrgtoaddyaeywegojnqyeipgrqkydbbxjkkmqrofgtuintdmhwcxxeftz\

xvwtevrlwybvpybdjrixbzlulqtyyfjyfhuksucavhkktfisuldooaswhcqfznk\

jizbxxxlebbfgjnnulufclqbgouuuwcthavajtruwucdzvxircqfznhcechxzrv\

cbbfgjmicciifgyocqngsftjvdmkbzltarnthzrcfnrjvdhychcrlpbpmkphwiok\

qyfcjeimikchrvoptrikdbbwgqinynwnevypnhflqtmktfijlwumucmkwsdoqvlvr\

mfzsfnzqtfgjwtzwryurtouuvbhkjbtmzkudkektuintdmhliirvftdwvotspnfug\

iefqyjvnyprcgusgcftdwvotvlofdgcqqhyoqotkltbsqgdzanipjomopwtmblxxyq\

ocqfzndkgtzalqdvbbmtbiaucdgsedgwthonzpwwceaalcowduvhkblaoasp\

nfdyjqiy";

int i,e=strlen(c);

char d[e+1];

int a[e],b[e],f[26];

for(i=0;i<e;i++){

a[i]=(int)c[i]-97;

}

for(i=0;i<26;i++){

b[i]=0;

}

for(i=0;i<e;i++){

a[i]=(int)c[i]-97;

b[a[i]]++;

}

for(i=0;i<26;i++){

cout<<b[i]<<" "<<endl;

}

for(i=0;i<e/5;i++){

b[5\*i+0]=(a[5\*i+0]\*21+a[5\*i+1]\*23+a[5\*i+2]\*25)%26+97;

b[5\*i+1]=(a[5\*i+0]\*15+a[5\*i+1]\*2+a[5\*i+2]\*4)%26+97;

b[5\*i+2]=(a[5\*i+0]\*17+a[5\*i+1]\*16+a[5\*i+2]\*3)%26+97;

b[5\*i+3]=(a[5\*i+3]\*7+a[5\*i+4]\*23)%26+97;

b[5\*i+4]=(a[5\*i+3]\*18+a[5\*i+4]\*11)%26+97;

}

for(i=0;i<e+1;i++){

d[i]=(char)b[i];

}

cout<<d<<endl;

return 0;

}

**结果：**

18

28

29

26

14

28

21

20

24

17

24

20

16

24

25

15

24

21

13

32

26

25

23

16

24

17

inseveraldistributedsystemsausershouldonlybeabletoaccessdataifauserpossesacertainsetofcredentialsorattributescurrentlytheonlymethodforenforcingsuchpoliciesistoemployatrustedservertostorethedataandmediateaccesscontrolhoweverifanyserverstoringthedataiscompromisedthentheconfidentialityofthedatawillbecompromisedinthispaperwepresentasystemforrealizingcomplexaccesscontrolonencrypteddatathatwecallciphertextpolicyattributebasedencryptionbyusingourtechniquesencrypteddatacanbekeptconfidentialevenifthestorageserverisuntrustedmoreoverourmethodsaresecureagainstcollusionattacks

**（c）1.加密**

#include <iostream>

#include <string.h>

#include <math.h>

#include <stdio.h>

using namespace std;

int main()

{

char c[]="inseveraldistributedsystemsausershouldonlybeabletoaccessdata\

ifauserpossesacertainsetofcredentialsorattributescurrentlytheonlymethod\

forenforcingsuchpoliciesistoemployatrustedservertostorethedataandmediate\

accesscontrolhoweverifanyserverstoringthedataiscompromisedthenthe\

confidentialityofthedatawillbecompromisedinthispaperwepresenta\

systemforrealizingcomplexaccesscontrolonencrypteddatathatwecall\

ciphertextpolicyattributebasedencryptionbyusingourtechniquesencrypted\

datacanbekeptconfidentialevenifthestorageserverisuntrustedmoreover\

ourmethodsaresecureagainstcollusionattacks";

int K1=9,K2=29;

int i,e=strlen(c);

int a[e],b[e],f[26];

char d[e+1];

for(i=0;i<e;i++){

a[i]=(int)c[i]-97;

}

for(i=0;i<26;i++){

b[i]=0;

}

for(i=0;i<e;i++){

a[i]=(int)c[i]-97;

b[a[i]]++;

}

for(i=0;i<26;i++){

cout<<b[i]<<" "<<endl;

}

for(i=0;i<e;i++){

b[i]=(a[i]\*9+29)%26+97;

}

for(i=0;i<e;i++){

d[i]=(char)b[i];

}

cout<<d<<endl;

return 0;

}

**结果：**

18

28

29

26

14

28

21

20

24

17

24

20

16

24

25

15

24

21

13

32

26

25

23

16

24

17

inseveraldistributedsystemsausershouldonlybeabletoaccessdataifauserpossesacertainsetofcredentialsorattributescurrentlytheonlymethodforenforcingsuchpoliciesistoemployatrustedservertostorethedataandmediateaccesscontrolhoweverifanyserverstoringthedataiscompromisedthentheconfidentialityofthedatawillbecompromisedinthispaperwepresentasystemforrealizingcomplexaccesscontrolonencrypteddatathatwecallciphertextpolicyattributebasedencryptionbyusingourtechniquesencrypteddatacanbekeptconfidentialevenifthestorageserverisuntrustedmoreoverourmethodsaresecureagainstcollusionattacks

**2.解密**

#include <iostream>

#include <string.h>

#include <math.h>

#include <stdio.h>

using namespace std;

int main()

{

char c[]="xqjnknadyexjsaxmbsnejljsnhjdbjnajozbyezqylmndmynszdvvn\

jjedsdxwdbjnaizjjnjdvnasdxqjnszwvanenqsxdyjzadssaxmbsnjvbaanqsylso\

nzqylhnsozewzanqwzavxqfjbvoizyxvxnjxjsznhiyzldsabjsnejnaknaszjszan\

sonedsddqehnexdsndvvnjjvzqsazyoztnknaxwdqljnaknajszaxqfsonedsdxjvz\

hiazhxjnesonqsonvzqwxenqsxdyxslzwsonedsdtxyymnvzhiazhxjnexqsoxjidi\

natnianjnqsdjljsnhwzaandyxuxqfvzhiyncdvvnjjvzqsazyzqnqvalisneedsds\

odstnvdyyvxionasncsizyxvldssaxmbsnmdjnenqvalisxzqmlbjxqfzbasnvoqxr\

bnjnqvalisneedsdvdqmnpnisvzqwxenqsxdynknqxwsonjszadfnjnaknaxjbqsab\

jsnehzanzknazbahnsozejdanjnvbandfdxqjsvzyybjxzqdssdvpj";

int K1=3,K2=17;

int i,e=strlen(c);

int a[e],b[e],f[26];

char d[e+1];

for(i=0;i<e;i++){

a[i]=(int)c[i]-97;

}

for(i=0;i<26;i++){

b[i]=0;

}

for(i=0;i<e;i++){

a[i]=(int)c[i]-97;

b[a[i]]++;

}

for(i=0;i<26;i++){

cout<<b[i]<<" "<<endl;

}

for(i=0;i<e;i++){

b[i]=(a[i]\*3+17)%26+97;

}

for(i=0;i<e;i++){

d[i]=(char)b[i];

}

cout<<d<<endl;

return 0;

}

**结果：**

43

17

2

43

23

6

0

12

15

47

7

13

9

77

16

2

33

1

59

4

1

30

10

37

22

41

inseveraldistributedsystemsausershouldonlybeabletoaccessdataifauserpossesacertainsetofcredentialsorattributescurrentlytheonlymethodforenforcingsuchpoliciesistoemployatrustedservertostorethedataandmediateaccesscontrolhoweverifanyserverstoringthedataiscompromisedthentheconfidentialityofthedatawillbecompromisedinthispaperwepresentasystemforrealizingcomplexaccesscontrolonencrypteddatathatwecallciphertextpolicyattributebasedencryptionbyusingourtechniquesencrypteddatacanbekeptconfidentialevenifthestorageserverisuntrustedmoreoverourmethodsaresecureagainstcollusionattacks

**四、课题完成过程中遇到的问题及解决方法**

(1) 代码不熟练，多看看以前的书就好点了

**五、总结**

经过本次实验，我明白了基本的加解密的方法，对密码学有了更加深入的了解