Министерство образования Республики Беларусь

Учреждение образования

Белорусский государственный университет информатики и радиоэлектроники

Кафедра РТС

Отчет по лабораторной работе №5

«КРИПТОАНАЛИЗ АЛГОРИТМОВ ЗАЩИТЫ ИНФОРМАЦИИ»

Выполнил:

ст.гр.240102
shlom41k

Проверил:

Панькова В.В.

Минск 2015

ЦЕЛЬ РАБОТЫ

1. Изучить криптографические методы анализа алгоритмов защиты информации.
2. Исследовать алгоритмы криптоанализа моноалфавитных и многоалфавитных криптосистем.
3. Получить навыки программирования алгоритмов криптоанализа.

РАСЧЕТНАЯ ЧАСТЬ

1. Перехваченное сообщение имеет вид «**DXM SCE DCCUVGX** ». Проверяется гипотеза, что сообщение составлено с помощью аффинных диграфов в 30-значном алфавите английского языка.

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
P	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*		*?*	*!*	*’*
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

Частотный анализ показал, что наиболее часто встречающимися диграфами в ранних шифротекстах были *«M пробел», «U пробел», «IH»*. Предположим, что в английском тексте наиболее часто повторяющимися диграфами являются *«E пробел», «S пробел»* и *«пробел T»*.

Задание:
а) найти ключи дешифрования и прочесть перехваченное сообщение;
б) найти ключи шифрования и зашифровать сообщение «YES I’M JOKING!».

Решение. Проверяется гипотеза, что текст и шифрованное сообщение связаны правилом

$$C = a \cdot P + b \bmod N^2.$$
$$P = X \cdot N + Y,$$

где X и Y – цифровые эквиваленты первой и второй букв в диграфе.

Дешифрование осуществляется по правилу

$$P = a' \cdot C + b' \bmod N^2.$$

Зная результаты статистического частотного анализа, можно составить три уравнения:

$$\begin{cases} (\mathrm{M} \cdot N + \text{пробел})\,a' + b' = (\mathrm{E} \cdot N + \text{пробел}) \bmod N^2 \Rightarrow 386 \cdot a' + b' = 146 \bmod 900, \\ (\mathrm{U} \cdot N + \text{пробел})\,a' + b' = (\mathrm{S} \cdot N + \text{пробел}) \bmod N^2 \Rightarrow 626 \cdot a' + b' = 566 \bmod 900, \\ (\mathrm{I} \cdot N + \mathrm{H})\,a' + b' = (\text{пробел} \cdot N + \mathrm{T}) \bmod N^2 \Rightarrow 274 \cdot a' + b' = 799 \bmod 900. \end{cases}$$

Решая данную систему уравнений, получим следующие соотношения:

$$\begin{cases} 660 \cdot a' + b' = 480 \bmod 900, \\ 139 \cdot a' + b' = 247 \bmod 900. \end{cases}$$

Из второго соотношения, используя алгоритм Евклида для определения обратного числа, можно найти:

$$a' = 139^{-1} \cdot 247 \bmod 900 \to 259 \cdot 247 \bmod 900 = 73;$$
$$b' = 146 - 386 \cdot 73 \bmod 900 = 786.$$

Таким образом, дешифрирование осуществляется в соответствии с выражением:

$$P = 73 \cdot C + 768 \bmod 900 \qquad (1.1)$$

Применив ключи дешифрования к диграфам принятого шифрованного сообщения, получим:

$DX = 3 \cdot 30 + 23 = 113 \to \text{в}(1.1) \Rightarrow 17 = 0 \cdot 30 + 17 = AR$;
$M\ пробел = 12 \cdot 30 + 26 = 386 \to \text{в}(1.1) \Rightarrow 146 = 4 \cdot 30 + 26 = E\ пробел$;
$SC = 18 \cdot 30 + 2 = 542 \to \text{в}(1.1) \Rightarrow 734 = 24 \cdot 30 + 14 = YO$;
$E\ пробел = 4 \cdot 30 + 26 = 146 \to \text{в}(1.1) \Rightarrow 626 = 20 \cdot 30 + 26 = U\ пробел$;
$DC = 3 \cdot 30 + 2 = 92 \to \text{в}(1.1) \Rightarrow 284 = 9 \cdot 30 + 14 = JO$;
$CU = 2 \cdot 30 + 20 = 80 \to \text{в}(1.1) \Rightarrow 308 = 10 \cdot 30 + 8 = KI$;
$VG = 21 \cdot 30 + 6 = 636 \to \text{в}(1.1) \Rightarrow 396 = 13 \cdot 30 + 6 = NG$;
$X\ пробел = 23 \cdot 30 + 26 = 716 \to \text{в}(1.1) \Rightarrow 836 = 27 \cdot 30 + 26 = ?\ пробел$.

Сложив вместе, получим текст сообщения «**ARE YOU JOKING?** ».

Определим ключи шифрования:

$$a = a'^{-1} = 73^{-1} \bmod 900 = 37,$$
$$b = -a'^{-1} \cdot b' = -37 \cdot 768 \bmod 900 = 384.$$

Таким образом, шифрование осуществляется в соответствии с выражением:

$$C = 37 \cdot P + 384 \bmod 900 \qquad (1.2)$$

Применив ключи шифрования к диграфам сообщения «**YES I'M JOKING!** » получим:

$YE = 24 \cdot 30 + 4 = 724 \to \text{в}(1.2) \Rightarrow 172 = 5 \cdot 30 + 22 = FW$;
$S\ пробел = 18 \cdot 30 + 26 = 566 \to \text{в}(1.2) \Rightarrow 626 = 20 \cdot 30 + 26 = U\ пробел$;
$I' = 8 \cdot 30 + 29 = 269 \to \text{в}(1.2) \Rightarrow 437 = 14 \cdot 30 + 17 = OR$;
$M\ пробел = 12 \cdot 30 + 26 = 386 \to \text{в}(1.2) \Rightarrow 266 = 8 \cdot 30 + 26 = I\ пробел$;
$JO = 9 \cdot 30 + 14 = 284 \to \text{в}(1.2) \Rightarrow 92 = 3 \cdot 30 + 2 = DC$;
$KI = 10 \cdot 30 + 8 = 308 \to \text{в}(1.2) \Rightarrow 80 = 2 \cdot 30 + 20 = CU$;
$NG = 13 \cdot 30 + 6 = 396 \to \text{в}(1.2) \Rightarrow 636 = 21 \cdot 30 + 6 = VG$;
$!\ пробел = 28 \cdot 30 + 26 = 866 \to \text{в}(1.2) \Rightarrow 26 = 0 \cdot 30 + 26 = A\ пробел$.

Сложив вместе, получим текст зашифрованного сообщения «**FWU ORI DCCUVGA** ».

2. Перехвачено сообщение «**ЦНТИ**». Проверяется гипотеза, что сообщение составлено с помощью аффинных диграфов в 33-значном алфавите русского языка.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	

Частотный анализ ранних шифротекстов показал, что наиболее часто встречающимися диграфами были «ЦЯ», «ЫТ». Предполагается, что в русском языке наиболее часто повторяющимися диграфами являются «НО», «ЕТ».

Задание:
а) найти ключи дешифрования и прочесть перехваченное сообщение;
б) найти ключи шифрования и зашифровать сообщение «Профиль защиты».

Решение. Зная результаты статистического частотного анализа, можно составить три уравнения:

$$\begin{cases} (\text{Ц}\cdot N+\text{Я})a'+b'=(\text{Н}\cdot N+\text{О}) \bmod N^2 \Rightarrow 791\cdot a'+b'=477 \bmod 1089, \\ (\text{Ы}\cdot N+\text{Т})a'+b'=(\text{Е}\cdot N+\text{Т}) \bmod N^2 \Rightarrow 943\cdot a'+b'=184 \bmod 1089. \end{cases}$$

Решая данную систему уравнений, получим следующее соотношение:

$$937\cdot a'+b'=293 \bmod 1089.$$

Используя алгоритм Евклида для определения обратного числа, можно найти:

$$a'=937^{-1}\cdot 293 \bmod 1089 \rightarrow 523\cdot 293 \bmod 1089=779;$$
$$b'=477-791\cdot 779 \bmod 1089=662.$$

Таким образом, дешифрирование осуществляется в соответствии с выражением:

$$P=779\cdot C+662 \bmod 1089 \qquad (2.1)$$

Применив ключи дешифрования к диграфам принятого шифрованного сообщения, получим:

$$ЦН=23\cdot 33+14=773 \rightarrow \text{в}(2.1) \Rightarrow 612=18\cdot 33+18=СС;$$
$$ТИ=19\cdot 33+9=636 \rightarrow \text{в}(2.1) \Rightarrow 611=18\cdot 33+17=СР.$$

Сложив вместе, получим текст сообщения «**СССР**».

Определим ключи шифрования:

$$a=a'^{-1}=779^{-1} \bmod 1089=137,$$
$$b=-a'^{-1}\cdot b'=-137\cdot 662 \bmod 1089=782.$$

Таким образом, шифрование осуществляется в соответствии с выражением:

$$C=137\cdot P+782 \bmod 1089 \qquad (2.2)$$

Применив ключи шифрования к диграфам сообщения «**ПРОФИЛЬ ЗАЩИТЫ**» получим:

$$ПР=16\cdot 33+17=545 \rightarrow \text{в } (2.2) \Rightarrow 306=9\cdot 33+9=ИИ;$$
$$ОФ=15\cdot 33+21=516 \rightarrow \text{в } (2.2) \Rightarrow 689=20\cdot 33+29=УЬ;$$
$$ИЛ=9\cdot 33+12=309 \rightarrow \text{в } (2.2) \Rightarrow 644=19\cdot 33+17=ТР;$$
$$ЬЗ=29\cdot 33+8=965 \rightarrow \text{в } (2.2) \Rightarrow 129=3\cdot 33+30=ГЭ;$$
$$АЩ=0\cdot 33+26=26 \rightarrow \text{в } (2.2) \Rightarrow 1077=32\cdot 33+21=ЯФ;$$

$ИТ = 9 \cdot 33 + 19 = 316 \rightarrow$ в (2.2) $\Rightarrow 514 = 15 \cdot 33 + 19 = ОТ$.

Сложив вместе, получим текст зашифрованного сообщения «**ИИУЬТРГЭЯФ**».

ВЫПОЛНЕНИЕ РАБОТЫ

1. Задан шифротекст:

«Vhfinmxkl ikhzktffxw pbma bgxqhktuex ehzbv vhgmkhe hnk xvhghfbxl tgw fhgxr ftkdxml, hnk txkhietgxl tgw mktbgl. Hnk hpg fbgwl tkx lxxg tl t yteebuex "gtmnkte" yhkf hy bgmxeebzxgvx matm maxlx vhfinmxkl pbee nembftmxer ixkyxvm bg tg xfuhwbfxgm hy "tkmbybvbte" bgmxeebzxgvx matm bl ghmabgz fhkx matg t vhfiebvtmxw ftmaxftmbvte tezhkbmaf matm vtg ux bfiexfxgmxw xexvmkhgbvteer ytk ytlmxk tgw exll yteebuer matg ur hnk hpg yxxuex uktbgl.»

а) Используя частотный анализ, определим ключ Цезаря и дешифруем сообщение.

Выполним частотный анализ открытого английского текста.

> message1 := `Numbers dominate much of our everyday lives in diverse and barely perceptible ways. Parents are anious to see their children attain good grades in mathematics, assured that this is a passport to success and security. The government stipulates that mathematical studies are compulsory for most of a child's time at school. Intelligence tests contain particular ingredients to test the candidates' ability to reason mathematically. Advertisements promising challenging and well-paid employment invite us to seek further details if we can successfully spot the next number in puzzling sequences. Students change subjects when they discover the mathematical content of their course is too difficult to master. Young children turn out to be extraordinarily talented in mathematics with abilities outstripping children twice their age, yet their performance in other subjects is unremarkable. Only in art and music is such precociousness so impressive. Looking out into the wider world, we see the cogs of the Western world turned by the engines of mathematical understanding. Computers programmed with inexorable logic control our economies and money markets, our aeroplanes and trains. Our own minds are seen as a fallible ""natural"" form of intelligence that these computers will ultimately perfect in an embodiment of ""artificial"" intelligence that is nothing more than a complicated mathematical algorithm that can be implemented electronically far faster and less fallibly than by our own feeble brains. In our universities there is an unspoken suspicion that the further a discipline lies from mathematics and the smaller the body of mathematical statements at its core the less rigorous and intellectually respectible it is.`:

> FreqAnalys2R(message1);

[113, 21, 62, 44, 177, 25, 24, 54, 121, 2, 5, 77, 55, 102, 87, 29, 1, 89, 106, 149, 49, 9, 15, 3, 23, 2, 1444]

Максимальное число повторений = 177, *Координата максимума в интервале 0..M-1* = 4

Второе максимальное число повторений = 149, *Координата второго максимума в интервале 0..M-1* = 19

Выполним частотный анализ шифротекста:

> mes:=`Vhfinmxkl ikhzktffxw pbma bgzqhktuex ehzbv vhgmkhe hnk xvhghfbxl tgw fhgxr ftkdxml, hnk txkhietgxl tgw mktbgl. Hnk hpg fbgwl tkx lxxg tl t yteebuex "gtmnkte" yhkf hy bgmxeebzxgvx matm maxlx vhfinmxkl pbee nembftmxer ixkyxvm bg tg xfuhwbfxgm hy "tkmbybte" bgmxeebzxgvx mashlomchiktm bl ghmabgz fhkx matg t vhfiebvtmxw ftmaxftmbvte tezhkbmaf matm vtg ux bfiexfxgmxw xexvmkhgbvteer ytk ytlmxk tgw exll yteebuer matg ur hnk hpg yxxuex uktbgl.`:

> FreqAnalysR(mes);

[10, 26, 0, 1, 29, 19, 29, 26, 7, 0, 24, 15, 31, 8, 0, 4, 1, 5, 0, 36, 8, 14, 8, 41, 10, 7, 359]

Максимальное число повторений = 41, *Координата максимума в интервале 0..M-1* = 23

Предположим, что ключом является $x = 7$.

$$x := 7$$

Проверим эту гипотезу:

```
> encodemonoalph(mes, caesarrule, x);
```

```
"The National Computer Security Center has established an aggressive program to stud\
y and implement computer security technology. Our goal is to encourage the wides\
pread availability of trusted computer products for use by any organization desirin\
g better protection of its important data. One way we do this is by supporting the T\
rusted Product Evaluation Program. This program focuses on the security features\
 of commercially produced and supported computer systems. We evaluate the prot\
ection capabilities against the established criteria presented in the TCSEC. This pr\
ogram, and an open and cooperative business relationship with the computer and t\
elecommunications industries, will result in the fulfillment of our country's informa\
tion systems security requirements. We resolve to meet the challenge of identifying \
 trusted computer products suitable for use in processing information that requires\
 protection."
```

Мы получили осмысленный текст. Гипотеза верна.

б) Корреляционный анализ по частотным векторам открытого текста и шифротекста.

Вариационный ряд английского текста:

```
> engFreq := [.082, .015, .028, .043, .127, .022, .020, .061, .070, .002, .008, .040, .024, .067, .075,
.019, .001, .060, .063, .091, .028, .010, .023, .001, .020, .001]:
engFreq2 := [op(engFreq), op(engFreq)];
```

engFreq2 := [0.082, 0.015, 0.028, 0.043, 0.127, 0.022, 0.020, 0.061, 0.070, 0.002, 0.008, 0.040, 0.024, 0.067, 0.075, 0.019, 0.001, 0.060, 0.063, 0.091, 0.028, 0.010, 0.023, 0.001, 0.020, 0.001, 0.082, 0.015, 0.028, 0.043, 0.127, 0.022, 0.020, 0.061, 0.070, 0.002, 0.008, 0.040, 0.024, 0.067, 0.075, 0.019, 0.001, 0.060, 0.063, 0.091, 0.028, 0.010, 0.023, 0.001, 0.020, 0.001]

Программа вычисления корреляционной функции частотных вариационных рядов открытого текста и шифротекста:

```
> read "VKF.m";
> VKF(mes);
```

Максимальное значение ВКФ = 0.06428412258, *Ключ* = 7

Наибольшее значение корреляционной функции соответствует ключу 7. Выбрав в качестве порога величину 0,06 можно составить программу выбора ключа по максимальному значению корреляционной функции.

Автоматическая программа определения ключа по корреляционному анализу частотных векторов имеет вид:

```
> keyFinder := proc(freqVect)
  local engFreqVect, i, dotProd:
  engFreqVect := [.082, .015, .028, .043, .127, .022, .020, .061, .070, .002, .008, .040, .024, .067,
.075, .019, .001, .060, .063, .091, .028, .010, .023, .001, .020, .001, .082, .015, .028, .043, .127, .022, .020,
.061, .070, .002, .008, .040, .024, .067, .075, .019, .001, .060, .063, .091, .028, .010, .023, .001, .020,
.001]:
  for i from 0 to 25 do
   dotProd := sum(engFreqVect[i+j]*freqVect[j]/freqVect[27], j=1..26):
   if (dotProd > .06) then print(dotProd, ` with decrypt key of`, i) fi:
  od:
end:
> keyFinder(freqCounter(mes));
```

0.06428412258, *with decrypt key of*, 7

2. Атака на мультипликативные шифры.

Шифротекст имеет вид:

«Kn ymf mnkxsfqkbksq bzsfs kq an mnqjygsn qmqjkwkyn bzab bzs dmfbzsf a hkqwkjrkns rksq dfyc cabzscabkwq anh bzs qcarrsf bzs lyhe yd cabzscabkwar qbabscsnbq ab kbq wyfs bzs rsqq fkoyfymq anh knbsrrswbmarre\nfsqjswbklrs kb kq.»

Мультипликативные шифры задаются следующим преобразованием:

```
> multrule := (letter, key) -> ((letter * key) mod 26):
```

Определим ключ мультипликативного шифра и дешифруем криптограмму:

```
> m2 := `Kn ymf mnkxsfqkbksq bzsfs kq an mnqjygsn qmqjkwkyn bzab bzs dmfbzsf a
hkqwkjrkns rksq dfyc cabzscabkwq anh bzs qcarrsf bzs lyhe yd cabzscabkwar qbabscsnbq ab kbq
wyfs bzs rsqq fkoyfymq anh knbsrrswbmarre\nfsqjswbklrs kb kq.`:
> FreqAnalys2R(m2);
```

[14, 22, 7, 3, 2, 11, 1, 4, 0, 4, 19, 2, 7, 11, 1, 0, 18, 11, 24, 0, 0, 0, 7, 1, 9, 9, 187]

Максимальное число повторений = 24, *Координата максимума в интервале 0..M-1* = 18

Второе максимальное число повторений = 22, *Координата второго максимума в интервале 0..M-1* = 1

```
> read "multkeyfinder.m";
```

Зададим две буквы: первая буква ряда наиболее часто повторяющихся в тексте букв алфавита; вторая буква соответствует наиболее часто повторяющейся букве шифротекста.

```
> multkeyfinder(`ey`);
```

9

```
> x:=19;
```

$x := 19$

Проверим правильность дешифрования:

> **encodemonoalph(m2,multrule,x);**

*In our universities there is an unspoken suspicion that the further \
a discipline lies from mathematics and the smaller the body of \
mathematical statements at its core the less rigorous and intellectually \
respectible it is.*

3. Атака на аффинную систему шифрования.

Шифротекст задан в следующем виде:

«Zc nbu bczmhufzqzhf qohuh zf pc bcfynvhc fbfyzlznc qopq qoh sbuqohu p wzflzygzch gzhf sunr rpqohrpqzlf psw qoh frpgghu qoh anwt ns rpqohrpqzlpg fqpqhrhcqf pq zqf lnuh qoh ghff uzdnunbf pcw zcqhgghlqbpggt uhfyhlqzagh zq zf.»

Определим ключ шифрования и расшифруем криптограмму

> **m3:=`Zc nbu bczmhufzqzhf qohuh zf pc bcfynvhc fbfyzlznc qopq qoh sbuqohu p wzflzygzch gzhf sunr rpqohrpqzlf psw qoh frpgghu qoh anwt ns rpqohrpqzpg fqpqhfhcqf pq zqf lnuh qoh ghff uzdnunbf pcw zcqhgghlqpggt uhfyhlqzagh zq zf`:**
> **FreqAnalys2R(m3);**

[2, 6, 10, 1, 0, 19, 11, 24, 0, 0, 0, 6, 1, 9, 9, 14, 22, 6, 4, 2, 11, 1, 4, 0, 4, 19, 185]

Максимальное число повторений = 24, Координата максимума в интервале 0..M-1 = 7

Второе максимальное число повторений = 22, Координата второго максимума в интервале 0..M-1 = 16

Программа определения ключа по четырем буквам шифротекста:

> **read "affinekeyfinder.m";**
> **k:=affinekeyfinder(`heqt`);**

$k := [19, 1]$

> **encodemonoalph(m3,affinerule,k);**

*In our universities there is an unspoken suspicion that the further a discipline lies from\
mathematics afd the smaller the body of mathematial statesents at its core the less r\
igorous and intellectally respectible it is*

ВЫВОД

В данной лабораторной работе были изучены криптографические методы анализа алгоритмов защиты информации, исследованы алгоритмы криптоанализа моноалфавитных и многоалфавитных криптосистем, получены навыки программирования алгоритмов криптоанализа.