ОТЧЕТ

по лабораторной работе №1

«Изучение частотного метода криптоанализа симметричных криптосистем»

дисциплина: «Криптографические методы защиты информации»

Выполнил(а) студент(ка)
группы БИ-4

_____

_____

Дата проведения занятия:

_____

Дата зачета:

_____

Преподаватель:

_____

Подпись преподавателя:

_____

1. Индивидуальное задание на лабораторную работу:

Y =ФРЕТКЧБ ЙРД ЫНЗНРНМЕЫНО ЗЦК ХЕЗТУ ЭЧУ ХКПН ЙРД РУЦУЦД – СКЦЧЕ ТКХКЦЧЕ. ХВО ЦЧВТЩУХЙ.

Мощность алфавита $|A_N| = m = 31$, (Е=Ё, Ь=Ъ).

2. Основные расчетные соотношения:

- логарифм функции правдоподобия: $l(K) = \sum_{j=0}^{N-1} \nu_{(j+k) \bmod N} \log p_1(j)$;

- оценка ключа: $K^* = \arg\max_K \sum_{j=0}^{N-1} \nu_{(j+k) \bmod N} \log p_1(j)$.

3. Результаты расчетов.

Таблица 1

Буква	**а**	**б**	**в**	**г**	**д**	**е**	**ж**	**з**	**и**	**й**
$j \in A_N$	0	1	2	3	4	5	6	7	8	9
$p_1(j)$	0.062	0.014	0.038	0.013	0.025	0.072	0.007	0.016	0.062	0.01
$\nu_j(Y)$	0	1	2	0	3	5	0	3	0	3

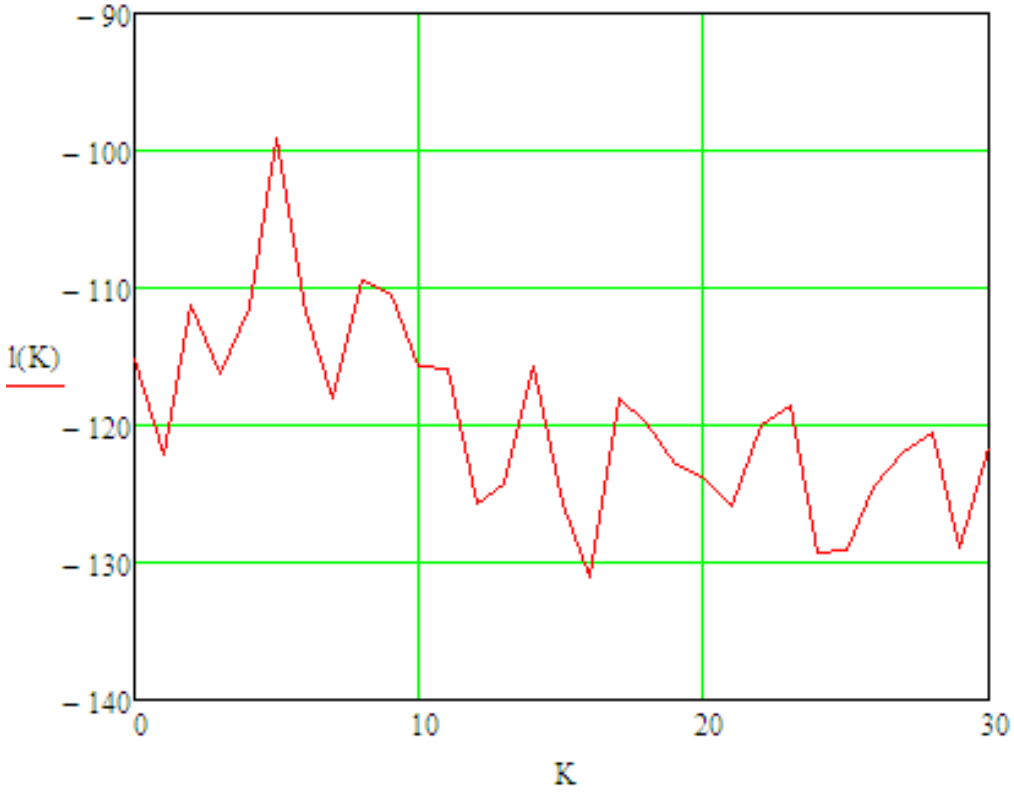
Продолжение таблицы 1

к	**л**	**м**	**н**	**о**	**п**	**р**	**с**	**т**	**у**	**ф**
10	11	12	13	14	15	16	17	18	19	20
0.028	0.035	0.026	0.053	0.09	0.023	0.04	0.045	0.053	0.021	0.002
6	0	1	5	2	1	5	1	4	5	1

Продолжение таблицы 1

х	**ц**	**ч**	**ш**	**щ**	**ь**	**ы**	**э**	**ю**	**я**
21	22	23	24	25	26	27	28	29	30
0.009	0.004	0.012	0.006	0.003	0.016	0.014	0.003	0.006	0.018
5	6	5	0	1	0	2	1	0	0

5. Графическая зависимость значения логарифма функции правдоподобия от значения ключа $l(K)$.



Оценка ключа - $K^* = 5$.

6. Дешифрованная криптограмма:

X =ПЛАНЕТЫ ДЛЯ ЦИВИЛИЗАЦИЙ ВСЕ РАВНО, ЧТО РЕКИ ДЛЯ ЛОСОСЯ – МЕСТА НЕРЕСТА. РЭЙ СТЭНФОРД.

ОТЧЕТ

по лабораторной работе №2

«Изучение методов криптоанализа криптосистем гаммирования с периодической гаммой»

дисциплина: «Криптографические методы защиты информации»

Выполнил(а) студент(ка)
группы БИ-4

_____

_____

Дата проведения занятия:

_____

Дата зачета:

_____

Преподаватель:

_____

Подпись преподавателя:

_____

Первая часть лабораторной работы

А. Априорные вероятности символов ключевой последовательности известны.

1. Индивидуальное задание на лабораторную работу.

Дана криптограмма, полученная шифром Виженера:

$Y =$ЭЭЭЮЦК.

Априорно известно, что вероятности символов ключевой последовательности равны

$P(Л) = 0{,}2;\ P(М) = 0{,}2;\ P(О) = 0{,}2;\ P(Ф) = 0{,}2.$

значения вероятностей остальных символов существенно меньше 0,2 и в рамках данного задания ими можно пренебречь.

2. Основные расчетные соотношения для определения периода ключевой последовательности (первый метод Фридмана):

- индекс совпадения

$$IC(Y) = \sum_{i=1}^{m} \frac{F_i(F_i - 1)}{N(N-1)},$$

- математическое ожидание индекса совпадения

$$M[IC(Y)] = \frac{(k+1)kr + k(k-1)(d-r)}{N(N-1)} \sum_i p_i^2 + \left(1 - \frac{(k+1)kr + k(k-1)(d-r)}{N(N-1)}\right)\frac{1}{m}.$$

3. Период ключевой последовательности $d = 3$.

4. Таблица результатов анализа

Таблица 1

k_i / y_i	Э	Э	Э	Ю	Ц	К
Л	С	С	**С**	Т	Л	**Я**
М	**Р**	Р	Р	**С**	К	В
О	О	**О**	О	П	**И**	Д
Ф	И	И	И	Й	В	Х

4. Дешифрованная криптограмма и ключ

$X =$РОССИЯ, $K =$МОЛ.

Б. Априорные вероятности символов ключевой последовательности неизвестны.

1. Индивидуальное задание на лабораторную работу.

Дана криптограмма, полученная шифром Виженера:

$Y =$ГЕНЖСУЮЛА.

2. Основные расчетные соотношения для определения периода ключевой последовательности (первый метод Фридмана):

- индекс совпадения

$$IC(Y) = \sum_{i=1}^{m} \frac{F_i(F_i - 1)}{N(N-1)},$$

- математическое ожидание индекса совпадения

$$M[IC(Y)] = \frac{(k+1)kr + k(k-1)(d-r)}{N(N-1)} \sum_i p_i^2 + \left(1 - \frac{(k+1)kr + k(k-1)(d-r)}{N(N-1)}\right)\frac{1}{m}.$$

3. Период ключевой последовательности $d = 3$.

Г	Е	Н	Ж	С	У
Ж	С	У	Ю	Л	А

4. Таблица анализа результатов

$\frac{Г}{Ж}$	$\frac{Е}{С}$	$\frac{Н}{У}$	$\frac{Ж}{Ю}$	$\frac{С}{Л}$	$\frac{У}{А}$
$\frac{Б}{А}$	$\frac{Е}{С}$	$\frac{Н}{У}$	$\frac{И}{Э}$	$\frac{С}{Л}$	$\frac{У}{А}$
$\frac{В}{Е}$	$\frac{О}{П}$	$\frac{К}{Е}$	$\frac{Е}{Э}$	$\frac{Т}{Б}$	$\frac{Ф}{О}$
…	…	…	…	…	…
$\frac{Р}{Ь}$	$\frac{Ч}{Д}$	$\frac{Ы}{Я}$	$\frac{Д}{Ц}$	$\frac{Ю}{Ф}$	$\frac{В}{Й}$

5. Дешифрованная криптограмма

X =ВЕНЕСУЭЛА.

Вторая часть лабораторной работы

1. Индивидуальное задание

Дана криптограмма, полученная шифром Виженера:

Y =ЪУУХУЦОЪИЮГФХШХХЮЪКЫПЧА
ЮАПСХЭЕЫТМЩППЖГЯРЛЕ
ПКУЮЩППЮЗЫВЗЩШРОЩЪЬЕМЗ
ОЩЪМФТЭШОЭУХХШХЭЦДЛЫПЧВ.

Криптограмма представляет собой зашифрованное четверостишие А.С. Пушкина, которое начинается с имени известного литературного персонажа.

2. Расчетный период ключевой последовательности - $d = 5$.

3. Множество вероятных слов начала криптограммы:

РУСЛАН, ОНЕГИН, ЛЮДМИЛА, МОЦАРТ, ОЛЬГА, ЛЕНСКИЙ, САЛЬЕРИ, САЛТАН, ГВИДОН.

4. Результаты применения метода протяжки «вероятного слова»:

Ключевая последовательность – ЛЕНСКИЙ.

Период ключевой последовательности - $d = 7$.

5. Дешифрованная криптограмма

X =ОНЕГИН ДОБРЫЙ МОЙ ПРИЯТЕЛЬ
РОДИЛСЯ НА БРЕГАХ НЕВЫ
ГДЕ МОЖЕТ БЫТЬ РОДИЛИСЬ ВЫ
ИЛИ БЫВАЛИ МОЙ ЧИТАТЕЛЬ.