ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ГРАЖДАНСКОЙ АВИАЦИИ»

Кафедра основ радиотехники и защиты информации

Э. А. Болелов

ПОСОБИЕ

к выполнению лабораторных работ
по дисциплине
«КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

для студентов 4 курса
специальности 090106
дневной формы обучения

Москва – 2010

Данное учебно-методическое пособие издается в соответствии с рабочей программой учебной дисциплины «Криптографические методы защиты информации» по Учебному плану специальности 090106 для студентов дневного обучения.

Учебно-методическое пособие способствует реализации квалификационных требований к студентам по обеспечению знаний в области криптографических методов защиты информации.

В учебно-методическом пособии приведены организационно-методические указания по выполнению лабораторных работ, задания на выполнение лабораторных работ, требования к отчету, а также основные теоретические сведения по каждой работе.

Рассмотрено и одобрено на заседаниях кафедры 15 апреля 2010 г. и методического совета 15 апреля 2010 г.

Содержание

Лабораторная работа №1
Изучение частотного метода криптоанализа симметричных криптосистем

Цель работы – закрепление теоретических знаний по методам криптоанализа симметричных криптосистем и практическое изучение частотного метода криптоанализа на примере криптосистемы Цезаря.

Время - 4 часа.

1 Основные теоретические сведения

Криптосистема Цезаря определяется выражением:

$$y_i = (x_i + k) \bmod m,\ i = \overline{1,n},$$

где y_i - буква криптограммы, x_i - буква открытого сообщения, k - ключ шифра, n - длина криптограммы (открытого текста), m - мощность алфавита.

Выражения для расшифрования имеет вид:

$$x_i = (y_i - k) \bmod m.$$

Метод частотного криптоанализа базируется на реализации методов теории статистических решений, а именно, на методе максимального правдоподобия [4]. В соответствии с этим методом оценкой ключа шифра k^* является такое его значение, которое доставляет максимальное значение логарифму функции правдоподобия $l(k)$. Для криптосистемы Цезаря оценка формируется в соответствии с выражением:

$$k^* = \arg\max_k l(k),\ l(k) = \sum_{j=0}^{m-1} \nu_{(j+k) \bmod m} \log p_1(j), \qquad (1)$$

где $p_1(j)$ - оценка вероятности встречаемости j-й буквы алфавита мощности m в открытых текстах, ν_j - частость встречаемости j-й буквы в криптограмме.

Выражение (1) справедливо, если источник открытых сообщений представляет собой стационарный источник дискретных сообщений без памяти. В случае, когда источник открытых сообщений представляет собой однородную цепь Маркова, оценка ключа будет определяться в соответствии с выражением:

$$k^* = \arg\max_k \left\{ \sum_{j=0}^{m-1} \delta_{y_1,(j+k) \bmod m} \log p_1(j) + \sum_{j,s=0}^{m-1} \nu_{(j+k) \bmod m,(s+k) \bmod m}(Y) \log p_{js} \right\}$$

2 Порядок выполнения работы

2.1 При подготовке к лабораторной работе

На этапе подготовки к лабораторной работе студенты должны, используя литературу [1,2,3,4] и материалы лекций углубить свои знания по

криптосистеме Цезаря и частотному методу криптоанализа простейших шифров.

Студенты на предстоящее лабораторное занятие готовят русский и английский алфавиты со значениями вероятностей встречаемости букв.

2.2 Во время проведения занятия.

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к лабораторной работе. Затем преподаватель разбивает группу студентов на несколько подгрупп по два студента в каждой.

Каждая подгруппа получает от преподавателя индивидуальный вариант задания на лабораторную работу, который представляет собой криптограмму, зашифрованную с помощью криптосистемы Цезаря.

Студенты должны:

1. Определить частотные характеристики криптограммы, для чего рассчитать значение частоты встречаемости символов $j \in A_m$ в криптограмме.

2. Определить вероятностные характеристики алфавита, для чего вычислить значение логарифма вероятности встречаемости символа $\log p_1(j)$ для заданного алфавита.

3. Полученные значения свести в таблицу 1.

Таблица 1.

Буква	А	Б	…	Ю	Я
$j \in A_m$					
$\log p_1(j)$					
$\nu_j(Y)$					

4. В соответствии с выражением (1) определить значение логарифма функции правдоподобия $l(K)$ и построить соответствующую графическую зависимость.

5. Определить в соответствии с выражением (1) оценку ключа k^*.

6. Дешифровать заданную криптограмму, используя оценку ключа k^*. При получении осмысленного текста подготовить отчет и представить его преподавателю.

4 Содержание отчета

Отчет должен включать в себя следующие пункты:

1. Задание на выполнение лабораторной работы (исходную криптограмму).

2. Основные расчетные соотношения.

3. Результаты расчетов, сведенные в табл. 1.

4. Графическую зависимость $l(k)$ и значение оценки ключа k^*.

5. Полученный дешифрованием открытый текст.

5 Контрольные вопросы

1. Основные понятия криптографии и криптоанализа.
2. Понятие симметричной криптосистемы.
3. Шифры перестановки.
4. Шифры замены.
5. Основные характеристики открытых сообщений.
6. Модели источников открытых сообщений.
7. Частотный метод криптоанализа.

Литература

1. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2005.

2. Баричев С.Г, Гончаров В.В., Серов Р.Е. Основы современной криптографии: Учебный курс. – 2-е изд. – М.: Горячая линия – Телеком, 2002.

3. Осипян В.О, Осипян К.В. Криптография в задачах и упражнениях. – М.: Гелиос АРВ, 2004.

4. Харин Ю.С., Беник В.И, Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии: Учеб. пособие. – Минск: Новое знание, 2003.

Лабораторная работа №2
Изучение методов криптоанализа криптосистем гаммирования с периодической гаммой

Цель работы – закрепление теоретических знаний по методам криптоанализа симметричных криптосистем и практическое освоение методов криптоанализа криптосистем гаммирования с периодической гаммой на примере криптосистемы Виженера.

Время - 4 часа.

1 Основные расчетные соотношения

Криптосистема Виженера представляет собой шифр гаммирования с использованием периодической гаммы малого периода. В криптосистеме Виженера ключ k^d задается набором из d символов. Такие наборы подписываются под открытым текстом $x_1, x_2, ..., x_n$, $x_i \in A_m$, до получения периодической ключевой последовательности $\tilde{k} = k_1, k_2, ..., k_n$, $n = sd + r$, где s - число полных периодов k^d, $r = n \bmod d$.

Уравнение шифрования для криптосистемы Виженера:

$$y_i = (x_i + \tilde{k}_i) \bmod m.$$

При дешифровании криптосистемы Виженера решаются две взаимосвязанные задачи:

- задача определение периода d ключевой последовательности $\tilde{k}$;
- задача дешифрования криптограммы Y при известном периоде d длине ключевой последовательности $\tilde{k}$.

Основным инструментом решения задачи определения периода ключевой последовательности криптосистемы Виженера являются методы Фридмана, основанные на понятии индекса совпадения. Индексом совпадения последовательности $X = x_1, x_2, ..., x_n$ называется величина

$$\Im(X) = \sum_{i=1}^{m} \frac{F_i(F_i - 1)}{n(n-1)}, \qquad (1)$$

где $X \in A_m$ - некоторая последовательность; F_i - частота встречаемости (число мест в тексте) i - буквы в последовательности X.

Для криптосистемы Виженера, получаемого шифрованием открытого текста $X = a_1, a_2, ..., a_n$ с помощью равновероятного выбора ключа $\tilde{k}$ из множества всех локально-периодических последовательностей K_n^d периода d и $n = sd + r$ справедливо

$$M\{\Im(Y)\} = \frac{(s+1)sr + s(s-1)(d-r)}{n(n-1)} \sum_i p_i^2 + \left(1 - \frac{(s+1)sr + s(s-1)(d-r)}{n(n-1)}\right)\frac{1}{m}. \qquad (2)$$

Первый метод Фридмана состоит в том, что вычисляется индекс совпадения $\Im(Y)$ для имеющейся криптограммы в соответствии с выражением (1) и затем его значение сравнивается с (2) при $d = 1,2,3,...$. При достаточной близости индекса совпадения к одному из значений (2), при некотором d, предполагают, что период равен этому значению d. Первый метод Фридмана эффективен для $d \le 5$, т.к. значение $M\{\Im(Y)\}$ для фиксированного периода d совпадает со значениями целого ряда различных периодов ключевой последовательности.

Суть *второго метода Фридмана* состоит в опробовании возможных периодов d по следующей схеме. Из исходной криптограммы $Y = y_1, y_2, ..., y_n$ для предполагаемого периода d ключевой последовательности выписывается d подпоследовательностей:

1) $y_1, y_{1+d}, y_{1+2d}, \cdots$

2) $y_2, y_{2+d}, y_{2+2d}, \cdots$

.....

d) $y_d, y_{d+d}, y_{d+2d}, \cdots$

Для каждой подпоследовательности подсчитывается ее индекс совпадения $\Im(Y_d)$. Если все индексы совпадения в среднем близки к значению $\frac{1}{d}\sum_i p_i^2$ (среднее значение индекса совпадения случайных криптограмм, полученных с помощью гамм периода 1), то принимают величину d за истинный период, в противном случае опробуется следующая величина периода. Второй метод Фридмана позволяет эффективно определять периоды $d \le 30$.

Метод «протяжки» вероятного слова. При известном периоде ключевой последовательности d выписываются две подпоследовательности исходной криптограммы:

$$y_1, y_2, ..., y_i, ... y_{(k-1)d+r};$$

$$y_{1+d}, y_{2+d}, ..., y_{i+d}, ..., y_{kd+r}, \quad n = kd + r.$$

Формируется называемое «множество вероятных слов», которые, по мнению криптоаналитика, могут быть началом искомого открытого текста.

Для слова $a_1^*, a_2^*, ..., a_r^*$ из этого множества, находятся первые символы ключевой последовательности $k_1^*, k_2^*, ..., k_r^*$. Правильность угадывания вероятного слова, а, следовательно, и первых символов ключевой последовательности, проверяется на «читаемость» следующего фрагмента расшифрованного текста

$$f_{k_1^*}^{-1}(y_{1+d}),\ f_{k_2^*}^{-1}(y_{2+d}), ...,\ f_{k_r^*}^{-1}(y_{r+d}).$$

Если полученная последовательность символов «читаемая», то полагают, что $k_1^*, k_2^*, ..., k_r^* = k_1, k_2, ..., k_r$, т.е. найдены первые r символов ключевой последовательности. Далее анализируя фрагменты расшифрованной криптограммы, ищут возможные продолжения открытого текста, таким образом, чтобы получить недостающую часть ключевой последовательности $k_{r+1}^*, k_{r+2}^*, ..., k_d^* = k_{r+1}, k_{r+2}, ..., k_d$.

После того, как определен весь ключ, оставшаяся часть криптограммы расшифровывается на найденном ключе. Если же последовательность символов принимается как случайная (т.е. «нечитаемая»), то опробуется следующее вероятное слово. Вероятные слова могут выбираться также из предположения, что они является окончанием открытого текста или, в общем случае, располагаются на других позициях открытого текста.

Метод чтения в колонках. Рассмотрим два случая:

- априорные вероятности символов ключевой последовательности не известны;

- априорные вероятности символов ключевой последовательности известны.

Априорные вероятности символов ключевой последовательности не известны. Пусть дана криптограмма $Y = y_1, y_2,..., y_n$. Известен период ключевой последовательности d. Сформируем две подпоследовательности исходной криптограммы

$$y_1, y_2,..., y_i,...y_{(k-1)d+r};$$

$$y_{1+d}, y_{2+d},..., y_{i+d},..., y_{kd+r}, \quad n = kd + r.$$

Будем полагать, что открытыми текстами, подлежащими шифрованию, являются содержательные тексты с известными вероятностями букв алфавита $P(a_j) = p_j$, $j = \overline{1,m}$, где j - порядкоый номер буквы алфавита. Также будем считать, что на множестве K задано равномерное распределение, т.е. ключом является реализация выборки объемом d из равномерного распределения K. Тогда вероятность того, что i-я и $(i+d)$-я буквы открытого текста были равны соответственно, $x_i = s$ и $x_{i+d} = l$, при условии, что i-я и $(i+d)$-я буквы криптограммы равны соответственно, y_i и y_{i+d} определяется выражением

$$P(x_i = s, x_{i+d} = l \mid y_i, y_{i+d}) = \frac{P(x_i = s, x_{i+d} = l; y_i, y_{i+d})}{P(y_i, y_{i+d})}.$$

Если числитель не равен нулю, то справедливо равенство

$$P(x_i = s, x_{i+d} = l \mid y_i, y_{i+d}) = \frac{p_s p_l}{\sum\limits_{f \in K} p_{f^{-1}(y_i)} p_{f^{-1}(y_{i+d})}} = \tilde{p}_{sl}.$$

Для каждой пары y_i и y_{i+d} букв исходной криптограммы упорядочим в соответствии с убыванием полученных значения условных вероятностей (5) пары букв открытого текста s и l. Построив такие колонки для каждого i, в результате получаем таблицу (табл. 1), в которой верхние пары имеют большую условную вероятность, чем нижние.

Таблица 1.

$i = 1$	…	$i = j$	…	$i = n$
$\frac{y_1}{y_{1+d}}$	…	$\frac{y_j}{y_{j+d}}$	…	$\frac{y_{(k-1)d+r}}{y_{kd+r}}$
….	…	$\left(\frac{x_j = s}{x_{j+d} = l}, \tilde{p}_{sl}\right)$	…	…

Буквы искомого содержательного текста будут находится вероятнее всего в первых строках и задача сводится к подбору таких пар букв, чтобы в результате получался осмысленный текст.

Априорные вероятности символов ключевой последовательности известны. Если априорно известны вероятности символов ключевой

последовательности, то задача дешифрования криптограммы аналогична задаче восстановления текста, зашифрованного неравновероятной гаммой. Пусть p_i, $i=\overline{1,m}$, есть вероятность использования символа в ключевой последовательности. Рассмотрим простую задачу, когда некоторые символы вовсе не встречаются в ключевой последовательности. Положим, что

$$p_1 \geq p_2 \geq ... \geq p_l,\ p_{l+1} = p_{l+2} = ... = p_m = 0,\ l < m.$$

Составим таблицу (см. таблицу 2), в которой по строкам расположены символы, полученные путем расшифровки криптограммы одним символом ключевой последовательности k_i, $i=\overline{1,l}$. Задача заключается в подборе по столбцам символов таким образом, чтобы в результате получился осмысленный текст. Если нельзя исключить использования ни одного символа в ключевой последовательности, то тогда поступают следующим образом. Для составления таблицы исключают из рассмотрения $m-l$ наименее вероятных букв алфавита, дальнейшие действия аналогичны рассмотренным выше. Надежность такого метода меньше, так как не исключена возможность частичной, а может и полной, потери истинного открытого текста.

Таблица 2.

k_i / y_i	y_1	….	….	y_n
k_1	$\hat{y}_1(k_1)$	….	…..	$\hat{y}_n(k_1)$
k_2	$\hat{y}_1(k_2)$	….	….	$\hat{y}_n(k_2)$
….	….	….	….	….
k_l	$\hat{y}_1(k_l)$	….	….	$\hat{y}_n(k_l)$

2 Порядок выполнения работы

2.1. При подготовке к лабораторной работе

На этапе подготовки к лабораторной работе студенты должны, используя литературу [1,2,3,4], материалы лекций углубить свои знания по следующим вопросам: криптосистема Виженера; методы определения периода ключевой последовательности; методы бесключевого чтения (метод «протяжки» вероятного слова, метод чтения в колонках).

Студенты на предстоящее лабораторное занятие готовят алфавиты русского и английского языка со значениями вероятностей встречаемости символов.

2.2. Во время проведения занятия

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к лабораторной работе. Затем преподаватель разбивает группу студентов на подгруппы по два человека. Каждая подгруппа получает от преподавателя индивидуальный вариант задания на лабораторную работу, который представляет собой криптограммы, зашифрованные с помощью криптосистемы Виженера.

Лабораторная работа состоит из двух частей. В первой части работы студенты дешифрируют первую заданную криптограмму с использованием первого метода Фридмана и метода чтения в колонках. При этом студенты должны: определить период ключевой последовательности с помощью первого метода Фридмана; используя метод чтения в колонках для заданного случая дешифрировать первую криптограмму. Вторая часть работы заключается в дешифровании второй криптограммы с применением второго метода Фридмана и метода «протяжки» вероятного слова. На этом этапе студенты должны: используя второй метод Фридмана определить период ключевой последовательности; на основании вычисленного значения периода ключевой последовательности используя метод «протяжки» вероятного слова дешифрировать вторую криптограмму.

Если в результате дешифрирования заданных криптограмм получены осмысленные тексты, студенты оформляют отчет и представляют его преподавателю.

3 Содержание отчета

Отчет должен включать в себя следующие пункты:

1. Задание на выполнение лабораторной работы (исходные криптограммы).
2. Основные расчетные соотношения.
3. Результаты расчетов, представленные в виде табл. 1 и 2.
4. Результаты анализа, т.е. дешифрованные криптограммы.

4 Контрольные вопросы

1. Основные понятия криптографии и криптоанализа.
2. Методы Фридмана.
3. Метод «протяжки» вероятного слова, метод чтения в колонках.
4. Понятие индекса совпадения.
5. Криптосистема Виженера.
6. Связь криптосистемы Виженера с другими простейшими криптосистемами.

Литература

1. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2005.

2. Баричев С.Г, Гончаров В.В., Серов Р.Е. Основы современной криптографии: Учебный курс. – 2-е изд. – М.: Горячая линия – Телеком, 2002.

3. Осипян В.О, Осипян К.В. Криптография в задачах и упражнениях. – М.: Гелиос АРВ, 2004.

4. Харин Ю.С., Беник В.И, Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии: Учеб. пособие. – Минск: Новое знание, 2003.

Лабораторная работа №3
Изучение метода линейного криптоанализа блочных симметричных криптосистем

Цель работы – закрепление теоретических знаний и практическое освоение метода линейного криптоанализа блочных симметричных криптосистем на примере криптосистемы S-DES.

Время - 4 часа.

1 Основные теоретические сведения

Блочные симметричные криптосистемы (БСК) представляют собой семейство обратимых криптографических преобразований блоков (частей фиксированной дины) исходного текста.

В настоящее время разработано большое количество БСК, многие из которых являются национальными стандартами. Наибольшую известность приобрели системы DES, IDEA, AES (Rijndael), ГОСТ 28147-89. Эти системы находятся под пристальным вниманием криптоаналитиков, основной задачей которых является поиск «слабых мест» в этих системах.

В настоящей работе метод линейного криптоанализа БСК рассматривается применительно к криптосистеме S-DES, являющейся упрощенной версией криптосистемы DES.

1. Алгоритм шифрования (расшифрования) криптосистемы S-DES. На рис. 1 иллюстрируется алгоритм шифрования (расшифрования).

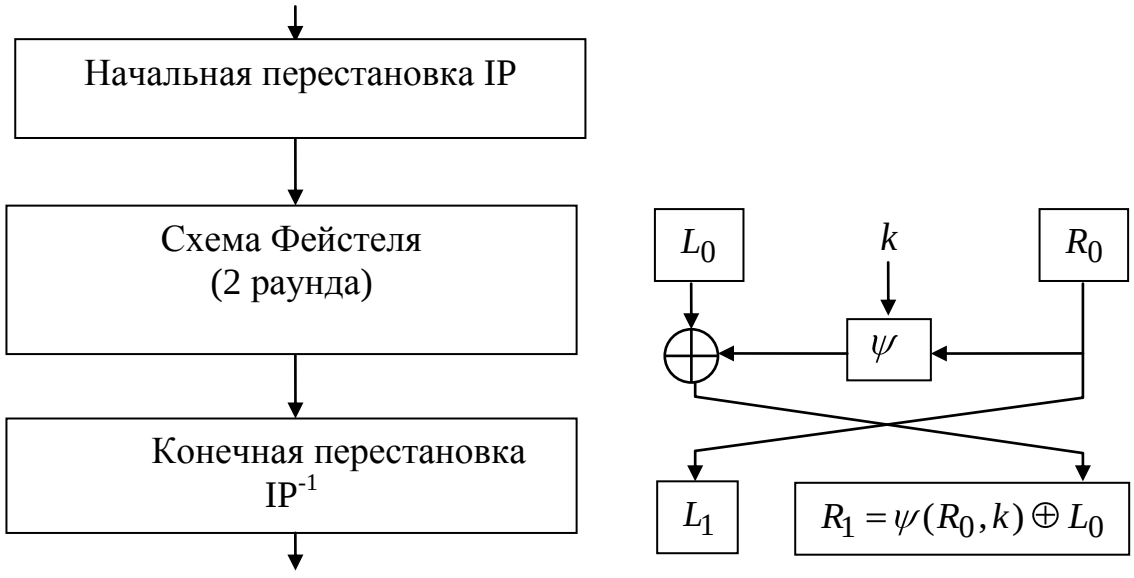

Рисунок 1 – Схема алгоритма шифрования S-DES с сетью Фейстеля

Входной 8-битовый блок вначале подвергается начальной перестановке (IP), в соответствии с табл.1. Биты подблока пронумерованы от 0 до 7, причем

бит с наибольшим порядковым номером 7 является младшим битом, и наоборот.

Таблица 1 – Начальная перестановка IP

7	6	4	0	2	5	1	3

Таблица разделена на две части, верхняя часть определяет подблок левых бит L_0, а нижняя часть определяет подблок правых бит R_0. Таким образом, после начальной перестановки IP, подблоки L_0 и R_0 подвергаются первому раунду шифрования. На выходе первого раунда получаются два выходных подблока L_1 и R_1, полученные в соответствии с выражением:

$$L_1 = R_0; R_1 = L_0 \oplus \psi(R_0, k_{(8)_1}).$$

Функция ψ, называемая функцией усложнения и аналогичная функции усложнения алгоритма DES, зависит от ключа, а ее вид будет описан ниже.

Подблоки L_1 и R_1 являются входными для второго раунда шифрования, на выходе которого получаются подблоки L_2 и R_2. Далее производиться объединение подблоков $L_2 \| R_2$ в блок, который подвергается перестановке, являющейся инверсией начальной перестановки. В результате получаем выходной блок криптограммы.

2. Алгоритм формирования раундовых ключей. Основной 10-битный ключ шифра $k_{(10)}$ используется для генерирования двух раундовых 8-битных ключей $k_{(8)_1}$ и $k_{(8)_2}$. Основной ключ шифра $k_{(10)}$, биты которого пронумерованы от 0 до 9, подвергается перестановке PC-1, определяемой табл. 2.

Таблица 2 – Перестановка PC-1

9	7	3	8	0
2	6	5	1	4

Верхняя строка таблицы определяют биты (9,7,3,8,0) подблока C_0, а нижняя - биты (2,6,5,1,4) подблока D_0. Подблоки C_0 и D_0 подвергаются единичному сдвигу влево, результатом которого является подблоки C_1 и D_1. Результат объединения подблоков $C_1 \| D_1$ подвергается перестановке, в соответствии с табл. 3.

Таблица 3 – Перестановка PC-2

5	3	9	7	2	8	6	4

Результатом перестановки РС-2 является первый раундовый ключ $k_{(8)_1}$. Процедура формирования второго раундового ключа $k_{(8)_2}$ аналогична, отличие заключается в том, что подблоки C_1 и D_1 подвергаются двум сдвигам влево.

3. Функция усложнения. На рис. 2 представлена схема функции усложнения ψ.

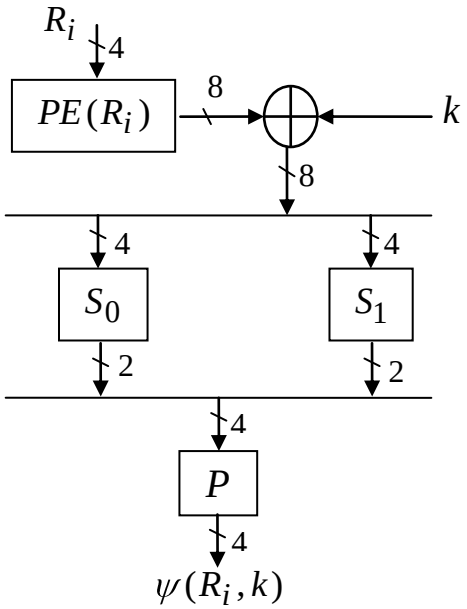

Рисунок 2 – Схема функции усложнения

Вначале 4-х битный подблок подвергается перестановке с расширением (РЕ), в соответствии с табл. 4, на выходе которой получается 8-ми битный блок. Полученный результат складывается по mod2 с битами 8-ми битного раундового ключа $k_{(8)_i}$, $i = 1,2$ и подвергается перестановке в блоках замены S_0 и S_1 (см. табл. 5 и табл. 6).

Таблица 4 – Перестановка с расширением РЕ

3	0	1	2	1	2	3	0

Таблица 5 – Блок замены S_0

S_0	№ столбца			
№ строки	**0**	**1**	**2**	**3**
0	1	0	2	3
1	3	1	0	2
2	2	0	3	1
3	1	3	2	0

Таблица 6 – Блок замены S_1

S_1	№ столбца			
№ строки	**0**	**1**	**2**	**3**
0	0	3	1	2
1	3	2	0	1
2	1	0	3	2
3	2	1	3	0

Причем, результат операции сложения по mod2 затем разбивается на два подблока, первые четыре бита (0,1,2,3) образуют подблок B_0, оставшиеся биты (4,5,6,7) образуют подблок B_1. Подблоки B_0 и B_1 подвергаются преобразованию в блоках замены S_0 и S_1, соответственно. Крайние биты входного 4-битного подблока определяют строку таблицы, а средние биты – столбец. После преобразования в блоках замены выходные 2-битные подблоки объединяются $S_0(B_0) \| S_1(B_1)$. Полученный 4-битный подблок подвергается перестановке (P), в соответствии с табл. 7.

Таблица 7 – Перестановка (P)

1	0	3	2

Результатом перестановки будет выходное значение функции усложнения $\psi(R_i, k_{(8)i})$, $i = 1,2$.

Метод линейного криптоанализа. Метод линейного криптоанализа разработан в 1993 году японским криптологом Митсуру Матсуи. В первоначальном виде этот метод сформулирован применительно к криптосистеме DES, в настоящее время создаются новые модификации этого метода [4].

Идея метода линейного криптоанализа основана на том, что существует возможность заменить нелинейную функцию криптографического преобразования ее линейным аналогом. Линейный криптоанализ базируется на знании криптоаналитиком пар «открытый текст-криптограмма», а также алгоритма шифрования.

Будем считать, что при генерации исходного текста X случайные биты независимы и равновероятны $P(x_i = 1) = p$, $P(x_i = 0) = 1 - p$, $p = 0{,}5$. *Линейным статистически аналогом* (или приближенным линейным аналогом) называется выражение:

$$\lambda(X, Y) = \sum_{i=1}^{n} a_i x_i \oplus \sum_{i=1}^{n} b_i y_j = \sum_{k=1}^{L} c_k k_k , \qquad (1)$$

если вероятность

$$P\left\{ \lambda(X, f(X, K)) = \sum_{k=1}^{L} c_k k_k \right\} = 0{,}5 + \Delta .$$

Величина $\Delta = |1 - 2p|$ называется *эффективностью линейного аналога*, а коэффициенты $a_i = \overline{1}$, $b_i = \overline{1}$, $c_k = \overline{1}$ - параметрами линейного аналога. По существу Δ характеризует степень линейности функции криптографического преобразования и имеет максимальное значение $\Delta_{max} = 0{,}5$. При применении метода линейного криптоанализа решаются две взаимосвязанные задачи:

1) нахождение эффективного линейного статистического аналога и вычисление его вероятности;

2) определение ключа (или нескольких бит ключа) с использованием эффективного линейного статистического аналога.

Практическая реализация метода линейного криптоанализа связана с реализацией следующих последовательных шагов.

1. Тщательно анализируется криптографическая функция и определяется множество линейных статистических аналогов. На этом шаге в первую очередь анализируются S-блоки функции усложнения ψ. Для этого формируются таблицы значений $Q_t(i, j)$, где: $t = 0,1$ - номер S-блока, $i = \overline{1,4}$, $j = 1,2$. Значение $Q_t(i, j)$ представляет собой количество совпадений суммы по mod2 некоторых битов входных данных с суммой по mod2 некоторых битов выходных данных. В ходе анализа прослеживаются все возможные комбинации двоичных векторов (i, j). Каждая пара векторов используется в качестве маски, которая накладывается на возможные пары «вход-выход» S-блока. Эти маски указывают на биты входа и выхода, которые необходимо сложить по mod2, а затем сравнить полученные результаты. Далее проводится анализ полученных таблиц $Q_t(i, j)$ и отыскиваются такие значения i^*, j^*, для которых выполняется условие:

$$Q_t(i^*, j^*) : \max \left| Q_t(i, j) - 8 \right|. \qquad (2)$$

В соответствии с полученной парой (i^*, j^*), и учитывая в схеме алгоритма шифрования перестановки и сложение по mod2, формируется эффективный линейный статистический аналог:

$$\lambda^*(X, Y) = \sum_{i=1}^{n} a_i^* x_i \oplus \sum_{i=1}^{n} b_i^* y_j = \sum_{k=1}^{L} c_k^* k_k \ , \ P_{эа} = \frac{Q(i^*, j^*)}{16}. \qquad (3)$$

2. Генерируется множество независимых исходных текстов $X^{(1)}, X^{(2)}, ..., X^{(M)}$ и регистрируются соответствующие им криптограммы $Y^{(1)}, Y^{(2)}, ..., Y^{(M)}$.

3. Для каждой пары $X^{(m)}, Y^{(m)}$, $m = \overline{1, M}$ вычисляется значение левой части эффективного линейного статистического аналога:

$$\lambda^*(X^{(m)}, Y^{(M)}) = \sum_{i=1}^{n} a_i^* x_i^m \oplus \sum_{i=1}^{n} b_i^* y_i^m . \qquad (4)$$

4. Определяется частота получения «1» при вычислении *M* значений (4):

$$\nu = \frac{1}{M} \sum_{m=1}^{M} \lambda^*(X^{(m)}, Y^{(m)}), \qquad (5)$$

и строится оценка максимального правдоподобия в соответствии с правилом:

$$d = \begin{cases} 1, & \nu \geq 0{,}5, \\ 0, & \nu < 0{,}5. \end{cases} \qquad (6)$$

5. Строится система линейных уравнений, причем каждое уравнение системы представляет собой равенство правой части (4) и соответствующего значения (6)

$$\sum_{k=1}^{L} c_k^* k_k = d\,. \qquad (7)$$

Единственное решение полученной системы (7) используется в качестве оценки ключа $k^* = k_1^*, k_2^*, ..., k_L^*$.

2 Порядок выполнения работы

Лабораторная работа выполняется с использование программы «Cryptoanaliz».

2.1. При подготовке к лабораторной работе

На этапе подготовки к лабораторной работе студенты должны, используя литературу [1-4], материалы лекций углубить свои знания по следующим вопросам: блочные симметричные криптосистемы (определение, основные характеристики, достоинства и недостатки), блочная криптосистема S-DES, метод линейного криптоанализа блочных криптосистем, а также изучить инструкцию по использованию программы «Cryptoanaliz».

2.2. Во время проведения занятия

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к лабораторной работе. Преподаватель разбивает группу студентов на 5 подгрупп, для каждой подгруппы определяется номер индивидуального задания на предстоящую лабораторную работу. Варианты индивидуальных заданий заложены в программе «Cryptoanaliz».

В процессе выполнения работы студенты должны:

1. Запустить на исполнение программу «Cryptoanaliz» и пройти предлагаемый контрольный тест.

2. В соответствии с заданием определенным преподавателем студенты выбирают номер варианта, количество известных текстов и осуществляют зашифрование случайным образом сгенерированных открытых текстов.

3. Используя таблицы Q_0 и Q_1, и учитывая таблицы перестановки и сложение по mod2, студенты определяют эффективные линейные аналоги и вычисляют их вероятности. Полученный результат студенты заносят в табл 8.

Таблица 8 – Эффективные линейные статистические аналоги

№ блока	Эффективный линейный аналог	p	$\Delta = \lvert 1-2p \rvert$
S_0			

S_1			

4. Для каждого из полученных линейных аналогов студенты определяют в соответствии с выражениями (5), (6) значение правой части уравнений используя модуль «Анализ».

5. Используя полученные результаты, студенты формируют систему уравнений (7). Решение системы уравнений позволяет определить все или часть битов 8-битных раундовых ключей. Используя алгоритм формирования раундовых ключей криптосистемы S-DES, студенты определяют основный 10-битный ключ шифра. Возможные варианты 10-битного ключа шифра и соответствующие ему 8-битные раундовые ключи студенты заносят в отчет по лабораторной работе.

6. Используя модуль «Проверка» студенты проверяют правильность каждого из полученных вариантов ключей шифра.

7. При совпадении результатов анализа с истинным ключом шифра студенты оформляют, в соответствии с требованиями настоящего пособия отчет и представляют его преподавателю для защиты.

3 Содержание отчета

Отчет должен включать в себя следующие пункты:

1. Схему блочной криптосистемы S-DES и исходные данные индивидуального задания.

2. Таблицы статистического анализа Q_0 и Q_1, и таблицу с эффективными линейными статистическими аналогами (табл. 8).

3. Систему линейных уравнений для определения битов ключа.

4. Варианты полученных ключей.

5. Результат проверки подтверждающий правильность определенного в работе ключа.

4 Контрольные вопросы

1. Блочные криптосистемы. Принципы построения. Достоинства и недостатки.

2. Режимы применения блочных криптосистем.

3. Схема Фейстеля.

4. Методы усложнения блочных шифров.

5. Криптосистема DES.

6. Криптосистема ГОСТ 28147 - 89.

7. Основная идея метода линейного криптоанализа.

8. Понятие эффективного линейного статистического аналога.

9. Методика применения линейного криптоанализа.

Литература

1. Баричев С.Г, Гончаров В.В., Серов Р.Е. Основы современной криптографии: Учебный курс. – 2-е изд. – М.: Горячая линия – Телеком, 2002.

2. Харин Ю.С., Беник В.И, Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии: Учеб. пособие. – Минск: Новое знание, 2003.

3. Бабенко Л.К., Мишустина Е.А. Лабораторный практикум по изучению современных методов криптоанализа по курсу «Криптографические методы и средства обеспечения защиты информации». – Таганрог: Изд-во ТРТУ, 2003.

4. Бабенко Л.К., Мишустина Е.А. Изучение современных методов криптоанализа. Методическое пособие. – Таганрог: Изд-во ТРТУ, 2003

Лабораторная работа №4
Изучение метода дифференциального (разностного) криптоанализа блочных симметричных криптосистем

Цель работы – закрепление теоретических знаний и практическое освоение метода дифференциального (разностного) криптоанализа блочных симметричных криптосистем на примере криптосистемы S-DES.

Время - 4 часа.

1 Основные теоретические сведения

Криптосистема S-DES подробно рассмотрена в лабораторной работе №3.

Метод дифференциального (разностного) криптоанализа предложен Э. Байхэмом и А. Шамиром, и, по мнению ряда специалистов компании IBM, является общим методом криптоанализа блочно-итерационных криптосистем. Идея заключается в анализе процесса изменения несходства для пары открытых текстов $\Delta X = X \oplus X'$, имеющих определенные исходные различия, в процессе прохождения через циклы шифрования с одним и тем же ключом.

Пусть задана пара входов X и X', с несходством $\Delta X = X \oplus X'$. Известны перестановка IP и перестановка с расширением E, а следовательно, известны и несходства ΔA на входе блоков замены S_0 и S_1. Выходы Y и Y' известны, следовательно, известно и несходство $\Delta Y = Y \oplus Y'$, а значит, при известных перестановках IP^{-1} и P известны несходства ΔC на выходе блоков замены S_0 и S_1.

Доказано, что для любого заданного ΔA не все значения ΔC равновероятны. Комбинация ΔA и ΔC позволяет предположить значения битов для $E(X) \oplus k_i$ и $E(X') \oplus k_i$. То, что $E(X)$ и $E(X')$ известны, дает информацию о k_i.

Несходство различных пар открытых текстов приводит к несходству получаемых шифр-текстов с определенной вероятностью. Эти вероятности

можно определить, построив таблицы для каждого из блоков замены. Таблицы сроятся по следующему принципу: по вертикали располагаются все возможные комбинации ΔA, по горизонтали – все возможные комбинации ΔC, а на пересечении – число соответствий данного ΔC данному ΔA.

Число наибольших совпадений указывает нам пару ΔA и ΔC, с помощью которой можно определить секретный ключ. Пара открытых текстов, соответствующих данным ΔA и ΔC называется *правильной* парой, а пара открытых текстов, не соответствующих данным ΔA и ΔC – *неправильной* парой. Правильная пара подскажет правильный ключ цикла, а неправильная пара – случайный. Чтобы найти правильный ключ, необходимо просто собрать достаточное число предположений. Один из подключей будет встречаться чаще, чем все остальные. Фактически правильный подключ появляется из всех возможных случайных подключей.

2 Порядок выполнения работы

Лабораторная работа выполняется с использование программы «Cryptoanaliz».

2.1. При подготовке к лабораторной работе

На этапе подготовки к лабораторной работе студенты должны, используя литературу [1-4], материалы лекций углубить свои знания по следующим вопросам: блочные симметричные криптосистемы (определение, основные характеристики, достоинства и недостатки), блочная криптосистема S-DES, метод дифференциального (разностного) криптоанализа блочных криптосистем, а также изучить инструкцию по использованию программы «Cryptoanaliz».

2.2. Во время проведения занятия

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к лабораторной работе.

Преподаватель разбивает группу студентов на 5 подгрупп, для каждой подгруппы определяется номер индивидуального задания на предстоящую лабораторную работу. Варианты индивидуальных заданий заложены в программе «Cryptoanaliz».

В процессе выполнения работы студенты должны:

1. Запустить на исполнение программу «Cryptoanaliz» и пройти предлагаемый контрольный тест.

2. В соответствии с заданием определенным преподавателем студенты выбирают номер варианта и количество известных текстов.

3. Используя таблицы анализа несходств $(\Delta A, \Delta C)$ для блоков замены S_0 и S_1 студенты определяют оптимальный дифференциал $(\Delta A^*, \Delta C^*)$ и осуществляют зашифрование случайным образом сгенерированных открытых

текстов. Программа выбирает из множества пар текстов пары удовлетворяющие оптимальному дифференциалу ($\Delta A^*, \Delta C^*$) и представляет их в виде в табл. 1.

Таблица 1 – Пары текстов удовлетворяющие оптимальному дифференциалу

№	X	$E(X)$	$S(E(X))$	Y
1				
…				
№	X'	$E(X')$	$S(E(X'))$	Y'
1				
…				

4. Студенты анализируют пары открытых текстов и определяют множество раундовых ключей шифра и, соответственно, множество основных ключей шифра. Ключ, получаемый чаще остальных и будет наиболее вероятным ключом шифра.

5. Используя модуль «Проверка» студенты проверяют правильность определенного анализом ключей шифра.

6. При совпадении результатов анализа с истинным ключом шифра студенты оформляют, в соответствии с требованиями настоящего пособия отчет и представляют его преподавателю для защиты.

4 Содержание отчета

Отчет должен включать в себя следующие пункты:

1. Структуру алгоритма S-DES и таблицы перестановок и замен, соответствующие заданному варианту.
2. Результаты анализа таблиц замен S_0 и S_1.
3. Результаты анализа пар открытых текстов.
4. Множество возможных раундовых ключей.
5. Результаты проверки, подтверждающие правильность определенного в работе ключа.

5 Контрольные вопросы

1. Основные понятия криптографии и криптоанализа.
2. Понятие блочной симметричной криптосистемы.
3. Основные характеристики блочных симметричных криптосистем.
4. Метод дифференциального (разностного) криптоанализа.

Литература

1. Баричев С.Г, Гончаров В.В., Серов Р.Е. Основы современной криптографии: Учебный курс. – 2-е изд. – М.: Горячая линия – Телеком, 2002.

2. Харин Ю.С., Беник В.И, Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии: Учеб. пособие. – Минск: Новое знание, 2003.

3. Бабенко Л.К., Мишустина Е.А. Лабораторный практикум по изучению современных методов криптоанализа по курсу «Криптографические методы и средства обеспечения защиты информации». – Таганрог: Изд-во ТРТУ, 2003.

4. Бабенко Л.К., Мишустина Е.А. Изучение современных методов криптоанализа. Методическое пособие. – Таганрог: Изд-во ТРТУ, 2003

Лабораторная работа №5
Методы оценки качества криптографических генераторов

Цель работы – закрепление теоретических знаний и практическое освоение методов оценки качества криптографических генераторов.

Время - 4 часа.

1 Основные теоретические сведения

Криптографический генератор – это аппаратно или программно реализованный имитатор источника равномерно распределенной случайной последовательности (РРСП) чисел, которая вычисляется по известному детерминированному рекуррентному соотношению. Основное требование к выходной последовательности x_i криптографического генератора, $i = \overline{0,\infty}$, состоит в минимальных отличиях по статистическим характеристикам последовательности x_i от РРСП.

Тесты, применяемые для оценки качества КГ, делятся на графические и оценочные [3].

К ***графическим тестам*** относится: гистограмма распределения элементов последовательности; распределение на плоскости; проверка серий; автокорреляционная функция; графический спектральный тест; проверка на монотонность; профиль линейной сложности.

Гистограмма распределения элементов – данный метод позволяет оценить равномерность распределения символов, а также определить частоту появления каждого символа. Для исследуемой последовательности $x_i, i = \overline{1,n}$ подсчитывается сколько раз встречается каждый элемент, после чего строиться график зависимости числа появления элементов от их численного представления.

Распределение на плоскости – метод предназначен для определения зависимостей между элементами последовательностей. Построение распределение на плоскости осуществляется по правилу $(\gamma_i, \gamma_{i+1}), i = \overline{1,(n-1)}$. Если между элементами последовательности связь отсутствует, то точки на плоскости расположены хаотично, в случае когда на плоскости наблюдаются

«узоры» - между элементами последовательности существует взаимосвязь, т.е. последовательность не является случайной.

Проверка серий – данный метод позволяет оценить равномерность распределения символов в исследуемой последовательности на основе анализа частоты появления нулей и единиц и серий состоящих из k бит. Построение осуществляется следующим образом: подсчитывается сколько раз проявляются нули, единицы, серии-двойки (00, 01, 10, 11), серии-тройки (000, 001, 010, 011, 100, 111) и т.д. в битовом представлении исследуемой последовательности $\{x_i\}, i=\overline{1,n}$. Результат представляется в графическом виде. У последовательности, чьи свойства близки к свойствами РРСП разбросы между числом появлений нулей и единиц, между числом появлений серий каждого вида должны стремиться к нулю.

Проверка на монотонность – данный метод позволяет оценить равномерность распределения символов. В исследуемой последовательности на основе анализа длин участков невозрастания и неубывания элементов последовательности. Исследуемая последовательность $\{x_i\}, i=\overline{1,n}$ представляется в виде непересекающихся участков невозрастания и неубывания следующих друг за другом. У последовательности, чьи свойства близки к свойствам РРСП вероятность появления участка невозрастания (неубывания) обратно пропорциональна его длине.

Автокорреляционная функция (АКФ) – данный метод предназначен для оценки корреляции между сдвинутыми копиями исследуемой последовательности $\{x_i\}, i=\overline{1,n}$. Метод позволяет обнаруживать зависимость между подпоследовательностями исследуемой последовательности. *Битовая* АКФ. Исследуемая последовательность $\{x_i\}, i=\overline{1,n}$ представляется в битовом виде и затем нормируется по правилу $\tilde{\gamma}_i = (-1)^{1-\gamma_i}, \overline{i=1,n}$. После этого вычисляются всплески корреляции:

$$r_j = \frac{\sum_{i=1}^{n} \tilde{\gamma}_i \tilde{\gamma}_{(i+j) \bmod n}}{\sum_{i=1}^{n} \tilde{\gamma}_i}, \; j = \overline{1,n}.$$

Символьная АКФ. Исследуемая последовательность нормируется по правилу $\tilde{\gamma}_i = \sum_{j=0}^{R-1} (-1)^{a_i} 2^j, \overline{i=1,n}$, R - разрядность числа, a_i - двоичная запись $i-$го элемента исследуемой последовательности. Далее вычисляются всплески корреляции.

Для последовательности, чьи свойства близки к свойствам РРСП, значения всплесков корреляции должно стремиться к нулю, во всех точках, кроме тех,

чье значение кратно длине последовательности в символах (в битах) для символьной (битовой) АКФ.

Профиль линейной сложности – данный метод позволяет исследовать последовательность на случайность анализируя зависимость линейной сложности последовательности от ее длины. Для исследуемой двоичной последовательности $\{\gamma_i\}, i=\overline{1,n}$ рассматриваются подпоследовательности $\gamma^{(k)}$ содержащие первые k элементов и строится графическая зависимость линейной сложности L от длины подпоследовательности k. У последовательности, чьи свойства близки к свойствам РРСП линия графика должна стремиться к линии $L=\frac{k}{2}$.

Графический спектральный метод – данный метод позволяет определить равномерность распределения 0 и 1 в исследуемой последовательности на основе анализа высоты выбросов преобразования Фурье. Исследуемая двоичная последовательность $\{\gamma_i\}, i=\overline{1,n}$ преобразуется по правилу $\tilde{\gamma}_i = 2\gamma_i - 1$ в последовательность $\{\tilde{\gamma}_i\}, i=\overline{1,n}$ к которой применяется дискретное преобразование Фурье. У последовательности, чьи свойства близки к свойствам РРСП число гармоник, чьи длительности значительно превышают среднюю длину гармоники должно стремиться к нулю.

Оценочные тесты, в отличии от графических тестов, позволяют по результатам тестирования сделать практически однозначный вывод о возможности использования криптографического генератора. Существует множество различных оценочных тестов, сгруппированных в наборы: тесты Д.Кнута, тест DieHard, тест NIST и др. [3]. В настоящей лабораторной работе рассматриваются некоторые тесты, входящие в набор NIST.

Частотный тест (frequency test) служит для проверки равномерности появления 0 и 1 в исследуемой последовательности. В исследуемой последовательности длинной n подсчитывается количество нулей n_0 и единиц n_1, а затем вычисляется их разница $S_n = n_1 - n_0$.

Вычисляется статистика $s = \frac{|S_n|}{\sqrt{n}}$ и определяется значение $P = erfc\left(\frac{s}{\sqrt{2}}\right)$,

где $erfc(x) = 1 - erf(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-\tau^2} d\tau$ - дополнительный интеграл вероятностей,

$erf(x) = \frac{2}{\sqrt{\pi}} \int_0^{x} e^{-\tau^2} d\tau$ - функция ошибок.

Связь стандартного нормального распределения $\Phi(x)$ и функции ошибок имеет вид:

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{\frac{\tau^2}{2}} d\tau = 0{,}5\left(1 + erf\left(\frac{x}{\sqrt{2}}\right)\right).$$

Значение P должно быть больше 0,01.

Частотный тест в последовательностях (frequency test within a block) необходим для проверки равномерности появления 0 и 1 в подпоследовательности. Исследуемая двоичная последовательность разбивается на $N = \left[\frac{n}{M}\right]$ M-битных последовательностей. Лишние биты отбрасываются. Определяется доля 1 в каждой подпоследовательности $\pi_i = \frac{\sum_{j=1}^{M} \varepsilon_{(i-1)M+j}}{M}$. Вычисляется статистика $s = 4M \sum_{i=1}^{M} (\pi_i - 0{,}5)^2$ и значение $P = igamc\left(\frac{N}{2}, \frac{s}{2}\right)$, где: $igamc(a, x) = 1 - p(a, x)$, $p(a, x) = \frac{\Gamma_x(a)}{\Gamma(a)}$, $\Gamma(a) = \int_0^{\infty} t^{a-1} e^{-t} dt$ - гамма-функция, $\Gamma_x(a) = \int_0^{x} t^{a-1} e^{-t} dt$ - неполная гамма-функция.

Значение P должно быть больше 0,01.

Тест «дырок» (runs test) служит для проверки равномерности распределения 0 и 1 в исследуемой последовательности на основе анализа количества появлений «блоков» - подпоследовательностей, состоящих из одних 1 или одних 0 («дырок»). Определяется предтестовая статистика π – доля 1 в исследуемой последовательности $\pi = \frac{\sum_{i=1}^{n} \varepsilon_i}{n}$. Если $|\pi - 0{,}5| \geq \tau = \frac{2}{\sqrt{n}}$ - тест считается не пройденным, в противном случае вычисляем статистику (количество блоков и «дырок») $v_n = \sum_{k=1}^{n-1} r(k) + 1$, где: $r(k) = \begin{cases} 0, & \varepsilon_i = \varepsilon_{i+1}, \\ 1, & \varepsilon_i \neq \varepsilon_{i+1} \end{cases}$. Затем вычисляется $P = erfc\left(\frac{|v_n - 2n\pi(1-\pi)|}{2\sqrt{2n}\pi(1-\pi)}\right)$. Значение P должно быть больше 0,01.

Проверка рангов матриц (binary matrix rank test) служит для проверки равномерности распределения 0 и 1 в исследуемой последовательности на основе анализа количества появлений матриц различных рангов. Исследуемая двоичная последовательность длины n разбивается на $N = \left[\frac{n}{MQ}\right]$ непересекающихся подпоследовательностей. Лишние биты отбрасываются.

Каждая подпоследовательность представляется как бинарная матрица размером $M \times Q$.

Определяется ранг каждой матрицы. Пусть F_M - число матриц ранга M, F_{M-1} - число матриц ранга $M-1$, $N - F_M - F_{M-1}$ - число оставшихся матриц. Вычисляется статистика

$$s = \frac{(F_M - 0{,}2888N)^2}{0{,}2888N} + \frac{(F_{M-1} - 0{,}5776N)^2}{0{,}5776N} + \frac{(N - F_M - F_{M-1} - 0{,}1336N)^2}{0{,}1336N},$$

а затем значение $P = igamc\left(1, \frac{s}{2}\right)$. Значение P должно быть больше 0,01.

Спектральный тест (spectral test) служит для проверки равномерности 0 и 1 в исследуемой последовательности на основе анализа высоты выбросов преобразования Фурье.

Исследуемая двоичная последовательность ε_i, $i = \overline{1,n}$ преобразовывается в последовательность x_i по правилу $x_i = 2\varepsilon_i - 1$. К полученной последовательности применяется дискретное преобразование Фурье $S = DFT(x)$, из которого формируется подпоследовательность S', содержащая первые $\frac{n}{2}$ членов S. Члены последовательности S являются комплексными числами. Определяются модули $m_i = |S'_i|$ каждого из элементов последовательности S'. Последовательность m_i дает последовательность выбросов высот преобразования Фурье.

Вычисляются $T = \sqrt{3n}$, $N_0 = \frac{0{,}95n}{2}$ и определяется статистика $s = \frac{N_1 - N_0}{\sqrt{0{,}95\frac{0{,}05n}{2}}}$, где N_1 - число элементов m_i, меньших чем T.

Вычисляется значение $P = erfc\left(\frac{|s|}{\sqrt{2}}\right)$. Значение P должно быть больше 0,01.

2 Порядок выполнения работы

2.1. При подготовке к лабораторной работе

На этапе подготовки к лабораторной работе студенты должны, используя литературу [1,2,3], материалы лекций углубить свои знания по следующим вопросам: классификация криптографических генераторов, методы усложнения алгоритмов генерации псевдослучайных последовательностей, графические и оценочные тесты качества криптографических генераторов.

2.2. Во время проведения занятия

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к лабораторной работе. Преподаватель разбивает группу студентов на подгруппы, для каждой подгруппы выдается индивидуальное задание на предстоящую лабораторную работу. Индивидуальное задание представляет собой тип криптографического генератора с исходными данными, который требуется исследовать.

В процессе выполнения работы студенты должны:

1. Сформировать, для заданного преподавателем типа криптографического генератора, псевдослучайную последовательность.
2. Оценить качество криптографического генератора с помощью рассмотренных в учебных материалах тестов и построить соответствующие графические зависимости.
3. Сформулировать вывод о возможности использования криптографического генератора в алгоритмах шифрования.

3 Содержание отчета

Отчет по лабораторной работе должен включать в себя следующие пункты:

1. Задание на лабораторную работу.
2. Графические зависимости, иллюстрирующие результаты применения графических тестов и таблицу с результатами оценочного тестирования.
3. Выводы о возможности использования заданного криптографического генератора в алгоритмах шифрования.

4 Контрольные вопросы

1. Классификация криптографических генераторов.
2. Методы улучшения псевдослучайных последовательностей.
3. Графические тесты оценки качества криптографических генераторов.
4. Оценочные тесты качества криптографических генераторов.

Литература

1. Баричев С.Г, Гончаров В.В., Серов Р.Е. Основы современной криптографии: Учебный курс. – 2-е изд. – М.: Горячая линия – Телеком, 2002.
2. Харин Ю.С., Беник В.И, Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии: Учеб. пособие. – Минск: Новое знание, 2003.
3. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайной последовательности. – М.: КУДИЦ-ОБРАЗ, 2003.

Лабораторная работа №6
Изучение криптосистем с открытым ключом

Цель работы – закрепление теоретических знаний и практическое освоение алгоритмов ассиметричного шифрования.

Время - 4 часа.

1 Основные теоретические сведения

Алгоритм RSA предложили в 1978 г. три автора: Роналдьд Райвест (Ronald Rivest), Ади Шамир (Adi Shamir) и Леонард Адльман (Leonard Adlman). Алгоритм RSA стал первым полноценным алгоритмом с открытым ключом, который может работать как в режиме шифрования данных, так и в режиме электронной цифровой подписи. Криптостойкость алгоритма основывается на трудности факторизации больших чисел и трудности вычисления дискретных логарифмов.

Пусть каждый абонент группы выбирает случайно два больших простых числа p и g, затем вычисляет:

$$N = pg,\ \phi = (p-1)(g-1),$$

и выбирает число $k_o < \phi$, взаимно простое с ϕ. Далее, по обобщенному алгоритму Евклида находят число $k_з$, такое, что $k_з k_o \bmod \phi = 1$. Пара $\{k_o, N\}$ и число $k_з$ являются открытым и секретным ключом, соответственно.

Абонент А желает передать сообщение x абоненту В, причем $x < N_B$ (далее индексы А и В, указывают принадлежность параметра, соответствующему абоненту). Алгоритм RSA состоит в последовательном выполнении следующих операций. Абонент А шифрует сообщение в соответствии с выражением:

$$y = x^{k_o^B} \bmod N_B.$$

Абонент В, получив криптограмму расшифровывает ее используя выражение:

$$x = y^{k_з^B} \bmod N_B.$$

Асимметричный *алгоритм Эль Гамаля* (El Gamal) использует операцию возведения в степень по модулю простого числа. При этом трудноразрешимой задачей для злоумышленника является отыскание не числа, которое возведено в степень, а то, в какую степень возведено известное число. Эта задача носит название проблемы дискретного логарифма.

Для всей группы абонентов выбираются некоторые большие простые числа p и g (число g является примитивным элементом поля $GF(p)$). Каждый абонент группы генерирует свое секретное число $k_з$, $1 < k_з < p-1$, и вычисляет соответствующее ему открытое число k_o,

$$k_o = g^{k_з} \bmod p.$$

Числа k_o и $k_з$ являются открытым и секретным ключом, соответственно.

Алгоритм шифрования заключается в следующем. Абонент А генерирует случайное число c, $1 \le c \le p-2$ и вычисляет:

$$l = g^c \bmod p,\ y = x \cdot k_o^{B\,c} \bmod p$$

и передает пару (l, y) абоненту В. Абонент В, получив пару (l, y), вычисляет:

$$x = y \cdot l^{p-1-k_o^B} \bmod p.$$

2 Порядок выполнения работы

2.1. При подготовке к лабораторной работе

На этапе подготовки к лабораторной работе студенты должны, используя литературу [1,2,3], материалы лекций углубить свои знания по следующим вопросам: понятие односторонней функции, генерация ключей в алгоритмах RSA и Эль-Гамаля, процедура шифрования данных в алгоритмах RSA и Эль-Гамаля.

2.2. Во время проведения занятия

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к лабораторной работе. Преподаватель разбивает группу студентов на подгруппы, для каждой подгруппы выдается индивидуальное задание на предстоящую лабораторную работу. Индивидуальное задание представляет собой исходные данные для генерации ключей.

В процессе выполнения работы студенты должны:

1. Построить блок-схемы алгоритмов шифрования RSA и Эль-Гамаля.
2. Сформировать контрольный пример.
3. Выполнить программную реализацию алгоритмов шифрования RSA и Эль-Гамаля.
4. Используя контрольный пример проверить правильность работы алгоритмов шифрования и расшифрования RSA и Эль-Гамаля.

3 Содержание отчета

Отчет по лабораторной работе должен включать в себя следующие пункты:

1. Задание на лабораторную работу.
2. Блок-схемы алгоритмов шифрования RSA и Эль-Гамаля.
3. Контрольный пример.
4. Результаты работы программы с различными исходными текстами и ключами.

4 Контрольные вопросы

1. Понятие односторонней функции и односторонней функции с «секретом».

2. Какая трудноразрешимая математическая задача лежит в основе стойкости алгоритма RSA?

3. Какая трудноразрешимая математическая задача лежит в основе стойкости алгоритма Эль-Гамаля?

4. Алгоритмы генерации ключей в криптосистеме RSA и Эль-Гамаля.

5. Алгоритмы шифрования и расшифрования в криптосистеме RSA и Эль-Гамаля.

6. Особенности асимметричных алгоритмов на эллиптических кривых.

Литература

1. Баричев С.Г, Гончаров В.В., Серов Р.Е. Основы современной криптографии: Учебный курс. – 2-е изд. – М.: Горячая линия – Телеком, 2002.

2. Харин Ю.С., Беник В.И, Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии: Учеб. пособие. – Минск: Новое знание, 2003.

3. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2005.

Лабораторная работа №7
Изучение алгоритмов электронной цифровой подписи

Цель работы – закрепление теоретических знаний и практическое освоение алгоритмов электронной цифровой подписи.

Время - 4 часа.

1 Основные теоретические сведения

Под *электронной цифровой подписью* понимается реквизит сообщения (электронного документа), предназначенный для его защиты от подделки и полученный в результате криптографического преобразования информации. Рассмотрим самые распространенные алгоритмы ЭЦП на основе криптосистем RSA и Эль-Гамаля.

ЭЦП на основе криптосистемы RSA. Вначале необходимо выбрать параметры алгоритма RSA. Для этого абонент А выбирает два больших простых числа p и g, и затем вычисляет N и ϕ в соответствии с $N = pg$ и $\phi = (p-1)(g-1)$. Затем абонентом А выбирается число k_o, взаимно простое с ϕ, и вычисляется число $k_з = k_o^{-1} \bmod \phi$. Абонент А публикует числа k_o и N ассоциировав их со своим именем, а число $k_з$ хранит в секрете. Числа p, g и ϕ в дальнейшем не потребуются. Теперь абонент А готов подписывать сообщение X. Для этого вначале он вычисляет хэш-функцию $h_X = h(X)$. Алгоритм вычисления хэш-функции известен всем абонентам, причем злоумышленник практические не может изменить основное сообщение не

изменив при этом значение хэш-функции. Поэтому в дальнейшем абоненту А достаточно снабдить подписью не само сообщение X, а только h_X. Затем абонент А вычисляет число:

$$s = h_X^{k_з} \bmod N,$$

которое и является цифровой подписью.

Вычисленная цифровая подпись добавляется к сообщению $\langle X, s \rangle$. Каждый, кто знает открытые параметры абонента А, ассоциированные с его именем, т.е. числа k_o и N, может проверить подлинность его подписи. Для этого необходимо вычислить значение хэш-функции $h_X = h(X)$ и затем вычислив число:

$$\eta = s^{k_o} \bmod N$$

проверить выполнение равенства $h_X = \eta$. Если подпись подлинная, то равенство выполняется, иначе подпись фальшивая или в подписанное сообщение внесено изменение.

ЭЦП на основе криптосистемы Эль-Гамаля. Как и в рассмотренном выше алгоритме вначале абонент А должен выбрать требуемые параметры криптосистемы Эль-Гамаля - большие простые числа p и g. Затем абонент А генерирует секретное число $k_з$, $1 < k_з < p-1$, и вычисляет соответствующее ему открытое число k_o в соответствии с $k_o = g^{k_з} \bmod p$. Абонент А публикует свой открытый ключ k_o. Теперь абонент А готов подписывать сообщение X. Вначале абонент А вычисляет значение хэш-функции $h_X = h(X)$, которое должно удовлетворять неравенству $1 < h_X < p$. Затем абонент А выбирает случайное число c, $1 < c < p-1$, и вычисляет:

$$l = g^c \bmod p.$$

Далее абонент А вычисляет числа:

$$s_1 = (h_X - k_з l) \bmod (p-1), s_2 = c^{-1} s_1 \bmod (p-1),$$

где c^{-1} удовлетворят уравнению $c^{-1} c \bmod (p-1) = 1$.

В заключении абонент А формирует подписанное сообщение $\langle X, l, s_2 \rangle$.

Получатель сообщения, прежде всего, заново вычисляет значение хэш-функции $h_X = h(X)$. Затем он проверяет подлинность подписи, используя равенство:

$$k_o^l l^{s_2} = g^{h_X} \bmod p.$$

Если подпись верна, то равенство выполняется.

2 Порядок выполнения работы

2.1. При подготовке к лабораторной работе

На этапе подготовки к лабораторной работе студенты должны, используя литературу [1,2], материалы лекций углубить свои знания по следующим вопросам: алгоритмы хэш-функций; алгоритмы формирования и проверки подписи.

2.2. Во время проведения занятия

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к лабораторной работе. Преподаватель разбивает группу студентов на подгруппы, для каждой подгруппы выдается индивидуальное задание на предстоящую лабораторную работу. Индивидуальное задание представляет собой исходные данные для формирования подписи и подписываемый текст.

В процессе выполнения работы студенты должны:

1. Построить блок-схемы алгоритмов ЭЦП на основе алгоритмов RSA и Эль-Гамаля.

2. Сформировать контрольный пример.

3. Выполнить программную реализацию заданной хэш-функции и алгоритма ЭЦП.

4. Используя контрольный пример проверить правильность работы алгоритмов формирования ЭЦП для различных текстов.

3 Содержание отчета

Отчет по лабораторной работе должен включать в себя следующие пункты:

1. Задание на лабораторную работу.
2. Блок-схемы алгоритмов ЭЦП на основе алгоритмов RSA и Эль-Гамаля.
3. Контрольный пример.
4. Результаты работы программы с различными исходными текстами.

4 Контрольные вопросы

1. Понятие ЭЦП. Основные требования к ЭЦП.
2. Понятие хэш-функции.
3. Коллизии хэш-функции.
4. Алгоритмы хэширования.
5. Алгоритмы ЭЦП на основе криптосистемы Эль-Гамаля.
6. Алгоритмы ЭЦП на основе криптосистемы RSA.
7. Методы сокращения длины ЭЦП.

Приложение А

Таблица частот встречаемости букв русского алфавита

- 0.175	О 0.090	Е, Ё 0.072	А 0.062
И 0.062	Т 0.053	Н 0.053	С 0.045
Р 0.040	В 0.038	Л 0.035	К 0.028
М 0.026	Д 0.025	П 0.023	У 0.021
Я 0.018	Ы 0.016	З 0.016	Ь, Ъ 0.014
Б 0.014	Г 0.013	Ч 0.012	Й 0.010
Х 0.009	Ж 0.007	Ю 0.006	Ш 0.006
Ц 0.004	Щ 0.003	Э 0.003	Ф 0.002