ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
(РОСАВИАЦИЯ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ» (МГТУ ГА)

Кафедра основ радиотехники и защиты информации

А.А. Антонов

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебно-методическое пособие
по выполнению лабораторных работ

для студентов
специальности 10.02.05
очной формы обучения

Москва
ИД Академии Жуковского
2021

УДК 004.056+003.26
ББК 001.8
А72

Рецензент:
Петров В.И. – канд. техн. наук, доцент

Антонов А.А.
А72 Криптографические методы защиты информации [Текст] : учебно-методическое пособие по выполнению лабораторных работ / А.А. Антонов. – М.: ИД Академии Жуковского, 2021. – 32 с.

Данное учебно-методическое пособие издается в соответствии с рабочей программой учебной дисциплины «Криптографические методы защиты информации» по учебному плану для студентов специальности 10.02.05 очной формы обучения.

Рассмотрено и одобрено на заседаниях кафедры 22.04.2021 г. и методического совета 22.04.2021 г.

УДК 004.056+003.26
ББК 001.8

В авторской редакции

Подписано в печать 28.05.2021 г.
Формат 60х84/16 Печ. л. 2 Усл. печ. л. 1,86
Заказ № 780/0519-УМП46 Тираж 40 экз.

Московский государственный технический университет ГА
125993, Москва, Кронштадтский бульвар, д. 20

Издательский дом Академии имени Н. Е. Жуковского
125167, Москва, 8-го Марта 4-я ул., д. 6А
Тел.: (495) 973-45-68
E-mail: zakaz@itsbook.ru

Лабораторная работа № 1

Изучение методов криптоанализа шифров замены. Частотный метод

1. Цель работы - закрепление теоретических знаний по методам криптоанализа симметричных криптосистем и практическое изучение частотного метода криптоанализа.

2. Краткие теоретические сведения

Частотный криптоанализ - один из методов криптоанализа, основывающийся на предположении о существовании нетривиального статистического распределения отдельных символов и их последовательностей как в открытом тексте, так и в шифротексте, которое, с точностью до замены символов, будет сохраняться в процессе шифрования и дешифрования.

Упрощённо, частотный анализ предполагает, что частота появления заданной буквы алфавита в достаточно длинных текстах одна и та же для разных текстов одного языка. При этом в случае моноалфавитного шифрования если в шифротексте будет символ с аналогичной вероятностью появления, то можно предположить, что он и является указанной зашифрованной буквой.

Метод частотного криптоанализа известен с девятого века. Начиная с середины XX века большинство используемых алгоритмов шифрования разрабатываются устойчивыми к частотному криптоанализу, поэтому он применяется, в основном, для обучения.

Вероятность появления отдельных букв, а также их порядок в словах и фразах естественного языка подчиняются статистическим закономерностям: например, пара стоящих рядом букв «ся» в русском языке более вероятна, чем «цы», а «оь» в русском языке не встречается вовсе (зато часто встречается, например, в чеченском). Анализируя достаточно длинный текст, зашифрованный методом замены, можно по частотам появления символов произвести обратную замену и восстановить исходный текст.

Важными характеристиками текста являются повторяемость букв (количество различных букв в каждом языке ограничено), пар букв, то есть m (m-грамм), сочетаемость букв друг с другом, чередование гласных и согласных, и некоторые другие особенности. Эти характеристики являются достаточно устойчивыми.

Идея частотного криптоанализа состоит в подсчете чисел вхождений каждой возможных m-грамм в достаточно длинных открытых текстах, составленных из букв алфавита. При этом просматриваются подряд идущие m-граммы текста.

Относительную частоту считают приближением вероятности появления данной m-граммы в случайно выбранном месте текста (такой подход принят при статистическом определении вероятности).

В общем смысле частоту букв в процентном выражении можно определить следующим образом: подсчитывается сколько раз она встречается в шифротексте, затем полученное число делится на общее число символов шифротекста; для выражения в процентном выражении, еще умножается на 100, как представлено на рисунке 1.

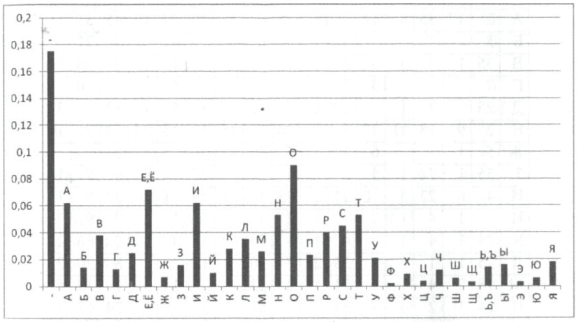

Рисунок 1 - Диаграмма частот букв русского языка

Но существует некоторая разница значений частот, которая объясняется тем, что частоты существенно зависят не только от длины текста, но и от характера текста. Например, текст может быть технического содержания, где редкая буква Ф может стать довольно частой. Поэтому для надежного определения средней частоты букв желательно иметь набор различных текстов.

Для получения более точных сведений об открытых текстах можно строить и анализировать таблицы k-грамм при k больше двух. Неравномерность k-грамм связана с особенностью открытого теста - наличием в нем повторений отдельных фрагментов текста: окончаний, слов и фраз.

Так для русского языка наиболее часто встречаются биграммы:

СТ НО ЕН НА ОВ НИ РА ВО КО;

триграммы:

СТО ЕНО НОВ ТОВ ОВО ОВА.

Пометьте их себе.

Полезной является информация о сочетаемости букв, т.е. предпочтительных связях букв друг с другом, которую легко извлечь из таблиц частот биграмм. Имеется ввиду таблица, где справа от каждой буквы расположены предпочтительные соседи.

Пример проведения частотного анализа.

Известно, что зашифровано стихотворение. Шифрование заключалось в замене каждой буквы на двузначное число. Знаки препинания сохранены, отдельные слова разделены пробелами.

Приведена таблица частот букв русского языка, где *f(l)* - частоты букв русского языка 32-буквенном алфавите со знаком пробела:

l	*f(l)*		*l*	*f(l)*		*l*	*f(l)*		*l*	*f(l)*
-	0,175		О	0,09		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

Необходимо расшифровать сообщение в соответствии с рисунком 2.

29 15 10 17 29 22 25 31 15 33 35 41 43 45 35 57 45 25 17 59 15 10 25 41
25 69, 59 78 29 82 25 78 25 17 15 10 88 90 78 25 62 25 22 10 57 73 79 35 67
78 90 88 29 45 35 29, 54 57 90 31 90 73 22 88 15 88 29 15 17 69 41 25 15, 70
17 90 57 43 59 15 78 15 62 22 25 17 57 25 69 88 15 82 17 25 88 29 45 35…

Рисунок 2 – Заданная криптограмма

Алгоритм решения выполнения следующий.

1. Посчитаем частоты шифробразований:

Обозначение	29	15	10	17	22	25	31	33	35	41	43	45	57
Количество	7	10	4	7	4	12	2	1	5	3	2	4	5
Обозначение	59	69	78	82	88	90	62	73	79	67	54	70	
Количество	3	3	4	2	6	5	1	2	1	1	1	1	

2. Проведем анализ таблицы частот букв русского и предложенного шифра.

Из таблицы частот видно, что чаще всего встречается буква О, втором месте Е. В нашем тексте первое место 25 = 12 раз, второе место 15= 10 раз. Таким образом, пусть 25=О, 15=Е, но может быть в связи с небольшой длинной нашего текста 25=Е, 15=О. Если выбрать второй вариант, то последнее слово в третьей строке должно оканчиваться ЕО, что маловероятно. Предположим, что 25=О, 15=Е.

3. Анализ знаков препинания в шифре и определение окончаний отдельных слов.

Обратим внимание на третью строку и знак препинания "29,...". Вряд ли, чтобы запятая стояла после согласной. Следовательно, 29=гласная. Вероятно или А или И, так как гласные Я, Ю, Э, У встречаются редко.

4. Выборочный анализ отдельных слов.

Рассмотрим последнюю строку цифры 88 15, 15=Е, следовательно, число 88 согласная. С большей вероятностью это Н или Т.

Обратим внимание опять на третью строку: цифры 22 88 15 88 29 15= 22 (Н, Т) Е (Н, Т) (А,И) Е, т. е. могут быть варианты:

22 НЕНИЕ,
22 ТЕТИЕ,
22 НЕНАЕ,
22 ТЕТАЕ.

Из рассмотренных вариантов один осмысленный, следовательно, 22=М.

5. Фиксируем расшифрованные буквы.

Теперь рассмотрим первую строку И, Е, 10, 17, И. Причем 10 и 17 - согласные, но не М и Н. Наиболее вероятно получается слово И ЕСЛИ, т.е 10=С, 17=Л. Вероятность, что это могли быть слова И ЕРТИ, И ЕВЛИ небольшая.

Далее первое слово второй строки 59,78, И, причем это согласные стоящие подряд, но не С, Л, М, Н., следовательно, это слово ПРИ. П=59, Р=78.

Вернемся к первой строке 45,25, 17, 59, 15

45, О, Л, П, Е, получается 45=Т.

При 57=В, получаем В ТОЛПЕ.

Далее рассмотрим последнюю строку 17, 90, 57, 43, 59, 15, 78, 15, 62 = Л 90 В 43 П Е Р Е 62, предположим, что 62=Д. Получаем ПЕРЕД.

Опять рассмотрим начало второй строки после запятой:

59, 78, 29, 82, 25, 78, 25, 17, 15, 10, 88, 90, 78, 25, 62, 25, 22, 10 =

П, Р, И, 82, **О, Р, О, Л, Е, С, Н**, 90, Р, О, Д, О, М, 10

Следует 82=К, а М=А.

Рассмотрим последнюю строку 82 17 25 88 29 45 35= К Л О Н И Т, откуда станет ясно, что 35=Ь.

6. Используя таблицу частот букв русского языка и наиболее часто встречающиеся биграммы, и триграммы, методом исключения завершаем дешифрирование текста.

И получаем ответ в соответствии с рисунком 3.

И ЕСЛИ МОЖЕШЬ БЫТЬ В ТОЛПЕ СОБОЮ,
ПРИ КОРОЛЕ С НАРОДОМ СВЯЗЬ ХРАНИТЬ
И, УВАЖАЯ МНЕНИЕ ЛЮБОЕ,
ГЛАВЫ ПЕРЕД МОЛВОЮ НЕ КЛОНИТЬ...

Рисунок 3 – Расшифрованная криптограмма

3. Порядок выполнения работы.

1. Получаете индивидуальное задание на выполнение лабораторной работы (исходную криптограмму).

2. Выполняете ее дешифрирование частотным методом криптоанализа по ранее приведенному примеру

3. По окончании занятия представляете полученный дешифрованием открытый текст, решение с таблицей частот букв сообщения.

4. Содержание отчета

1. Титульный лист.
2. Задание.
3. Решение с таблицей частот букв сообщения.
4. Ключ алфавита, соответствие каждой букве алфавита двузначной цифре.
5. Открытый текст полученного сообщения.
6. Вывод

5. 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 шифров замены. Методы Фридмана

1. Цель работы - закрепление теоретических знаний по методам криптоанализа симметричных криптосистем и практическое изучение методов Фридмана.

2. Краткие теоретические сведения

Основаны данные методы на введенном У. Фридманом понятии индекса совпадения.

Индексом совпадения последовательности $X = a_1, a_2, ..., a_n$ называется величина

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

где $X \in A_X$, $|A_X| = m$ - некоторая последовательность; F_i - частота встречаемости (число мест в тексте) i - буквы в последовательности X.

Индекс совпадения $\Im$ последовательности равен вероятности $P_X(a_j = a_{j'})$ совпадения символов данной последовательности на случайно и равновероятно выбранных местах j и j', причем $j \neq j'$ и $j, j' \in \overline{1,n}$.

При $n \to \infty$

$$\Im(X) = \sum_{i=1}^{m} \frac{F_i(F_i - 1)}{n(n-1)} \to \sum_{i=1}^{m} p_i^2,$$

где p_i - вероятность $i-$го символа из алфавита A_X в содержательных текстах.

Суть метода Фридмана состоит в опробовании возможных периодов d по следующей схеме.

Из исходной криптограммы $Y = b_1, b_2, ..., b_n$ для предполагаемого периода d ключевой последовательности выписывается d под последовательностей:

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 под последовательности подсчитывается ее индекс совпадения $\Im(Y_d)$.

Таким образом два одинаковых отрезка открытого текста отстоящих друг от друга на расстоянии кратном длине ключа будут одинаково зашифрованы.

Случайно такое отрезки могут появиться с достаточно малой вероятностью. В тексте ищутся повторения длины не меньше трех букв.

Существуют индексы совпадения для европейских языков. Таким образом находят длину ключевого слова, например, для шифра замены.

Для нахождения самого ключевого слова используют взаимный индекс совпадений. Если обратить внимание на то, что ненулевые сдвиги дают взаимные индексы совпадений, изменяющиеся в пределах от 0,032 до 0,045, а при нулевом сдвиге значение близко к 0,066. Это позволит определить относительные сдвиги столбцов. Используя их можно, связать системой уравнений относительные сдвиги различных пар столбцов.

Рассмотрим пример решения.

Задан текст, зашифрованный шифром Виженера в соответствии с рисунком 4, требуется определить ключевое слово и прочитать открытый текст.

влцдутжбюцхъяррмшбрхцэооэцг**брь**цмйфктъъюьмшэсяцпуняшэйтаьэдкци**бр**
ьцгбрпачкъуцпъбьсэгкцъгуушарцёэвърюуоюэкаазбрняфукабъарпяъафкъшьжяффнйо
яфывбнэнфуюг**брь**сшьжэтбэёчюъюрьегофкбъчябашвёэуъъюаднчжчужцёэвлрнчулб
юпщуруньъшсэюъзкцхъяррнрювяспэмасчкпэужьжыатуфуярюравртубурьпэщлафоуф
бюацмнубсюкйтаьэдйюноозгюожбгкбрънцэпотчмёодзцвбцшшвшепчдчдръюьскасэг
ъппэгюкдойрсрэвоопчшшюказръббнэугнялёкьсрбёуыэбдэулбюасшоуэтъшкрсдугэфл
бубуъчнчтртпэгюкиугюэмэгюккъъпэгяапуфуээьрадзьжчюрмфцхраююанчёчюъыхъъ
цомэфъцпоирькншпэтэузуябашущбаыэйчдфрпэцъьрьцъъпоилуфэдцойэдятррачкубу
фнйтаьэдкцкрннцюабугюуубурьпйюэьжтгюркующюъуфъэгясуоичшшчдцсфырэдщэ
ъуяфшёчщюйрщвяхвмкрщрпгюопэуцчйтаьэдкци**брь**цыяжтюрбуэтэбдуящэубъибрюв
ъежагибрбагбрымпуноцшяжцечкфодшюъчжшйуъцхчшвуэбдлдъэгясуахзцэбдэулькнъ
щбжяцэьрёдъьвюврнуяфуоухфекьгцччгэъжтанопчынажпачкъуъмэнкйрэфшэъъбуд
эндадъярьеюэлэтчоубъцэфэвлнёэгфдсэвэёкбсчоукгаутэыпуббчкпэгючсаъбэнэфърк
ацхёваетуфяепърювържадфёжбьфутощоявьъгупчршуитеачйчирамчюфчоуяюонкяжы
кгсцбрясшчйотъъжрсшчл

Рисунок 4 - Текст, зашифрованный шифром Виженера

Решение:

1. Детально изучаем текст, определяем, что два одинаковых отрезка открытого текста, отстоящих друг от друга на одинаковом расстоянии одинаково зашифрованы. Находим их. Четырех кратное повторение букв «брь».

2. Выясним расстояние между ними, найдем наибольший общий делитель. Следовательно, длинна ключевого слова 5 символов.

3. Далее записываем шифротекст в таблицу по пять символов.

в	л	ц	д	у
т	ж	б	ю	ц
...	...	...	...	...
с	щ	ч	л	

4. Посчитаем частоту повторения букв в каждом столбце, в соответствии с рисунком 5.

1 столбец (общее количество букв m=198)

Обозначение	а	б	в	г	д	е	ё	ж	з	и	й	к	л
Количество	17	2	10	16	14	7	0	1	1	3	2	1	0

Обозначение	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
Количество	3	4	1	0	1	16	9	14	5	5	23	0	0

Обозначение	щ	ъ	ы	ь	э	ю	я
Количество	5	10	3	2	2	10	11

Рисунок 5 - Частоты повторения букв в каждом столбце

5. Затем вычислим индексы совпадений для каждого из столбцов. По полученным индексам можно утверждать, что длинна ключевого слова выбрана верно 5, все значения больше 0,05.

6. Затем вычислим взаимные индексы совпадений:

перемножим в числителе частоты первого столбца на частоты сдвинутых столбцов;

затем найдем их суммы;

поделим сумму на произведение количества букв столбцов.

Взаимный индекс совпадений должен находиться в пределах от 0,053 до 0,07.

7. Далее составим уравнения для определения ключевого слова.

g[1]-g[2]=6	g[1]=g[2] + 6	g[2]=g[1] - 6
g[1]-g[3]=3	g[1]=g[3] + 3	g[3]=g[1] - 3
g[1]-g[4]=16	g[1]=g[4] + 16	g[4]=g[1] - 16
g[1]-g[5]=3	g[1]=g[5] + 3	g[5]=g[1] - 3

8. Определяем ключевое слово, находим значение g1 и расшифровываем текст.

3. Порядок выполнения работы.

1. Получаете индивидуальное задание на выполнение лабораторной работы (исходную криптограмму).
2. Выполняете ее дешифрирование.
3. По окончании занятия представляете полученный дешифрованием открытый текст и отчет.

4. Содержание отчета

1. Титульный лист.
2. Задание.
3. Решение: шифротекст сведённый в таблицу по количеству символов ключа; частота повторения букв в каждом столбце; индексы совпадений для каждого из столбцов; взаимные индексы совпадений; уравнения для определения ключевого слова.
4. Ключ шифра.
5. Открытый текст полученного сообщения.
6. Вывод

5. 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.

Лабораторная работа № 3

Изучение метода линейного криптоанализа

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

2. Краткие теоретические сведения

Практическая реализация метода линейного криптоанализа связана с выполнением последовательных шагов.

1. Анализируется криптографическая функция и определяется множество линейных статистических аналогов. На этом шаге анализируются S-блоки функций усложнения.

Для этого необходимо для каждого S-блока сформировать таблицы значений $Q_t(i, j)$, где: t - номер S-блока.

Значение $Q_t(i, j)$ представляет собой количество совпадений суммы по mod2 некоторых битов входных данных с суммой по mod2 некоторых битов выходных данных.

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 отыскивается такие значения i^*, j^*, для которых выполняется условие

$$Q_t(i^*, j^*) : \max\left|Q_t(i, j) - n_X\right|,$$

где n_X - длина подблока.

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

$$\lambda^*(X,Y) = \sum_{i=1}^{n} a_i^* x_i \oplus \sum_{i=1}^{n} b_i^* y_j = \sum_{k=1}^{L} c_k^* k_k \text{ , при } P_{эа} = \frac{Q(i^*, j^*)}{2n_X}$$

Формируются несколько линейных аналогов.

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:

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

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

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

и строится оценка максимального правдоподобия в соответствии с правилом:

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

Вычисления на этапах 3 и 4 выполняются для всех сформированных эффективных линейных статистических аналогов.

5. Строится и решается система линейных уравнений

$$\sum_{k=1}^{L} c_k^* k_k = d .$$

Рассмотрим пример реализации алгоритма линейного криптоанализа на базе криптосистемы S-DES. Рассмотрим один раунд S-DES. Функция усложнения состоит из: блока расширения, сложения по модулю два с ключом раунда, два S-блока и прямой блок.

Заданы таблицы замен и перестановок. Для простоты, но, не нарушая общности, будем считать, что шифрование производилось одним раундом.

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

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

Переводим таблицы замен в двоичный вид. Далее проводим анализ переведенных в двоичный код таблиц S_0 и S_1.

Значение $Q_t(i, j)$ представляет собой количество совпадений суммы по mod2 некоторых битов входных данных с суммой по mod2 некоторых битов выходных данных.

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.

Задаем вектора *i* и *j,* на примере вектор *i* задан для всего диапазона *j* одно значение. Далее используем вектора в качестве маски накладывается на возможные пары «вход-выход» S-блока.

Применение маски заключается в том, что складываются биты по модулю два S-блока только отмеченные единицей в зачтениях векторов *i* и *j*. Далее меняем значение вектора *j* и опять ищем совпадения для *S-блока*.

Затем проводится анализ полученных таблиц $Q_t(i, j)$ и отыскивается такие значения i^*, j^*, для которых выполняется условие;

$$Q_t(i^*, j^*) : \max|Q_t(i, j) - n_X|,$$

где n_X - длина подблока, в данном случае 8 бит.

Выделяем четыре эффективных линейных статистических аналога и составить первые четыре наиболее эффективных линейных уравнения, соответствующие парам: (i, j) – $(0101, 01)$, $(1011, 11)$, $(1110, 10)$, $(1111, 10)$.

Рассмотрим первую пару $(0101, 01)$ блока S_0.

Первое линейное уравнение для блока замены S_0 имеет вид:

$$X_1' \oplus X_3' \oplus Y_1' = k_1 \oplus k_3.$$

Индексы иксов в данном случае соответствуют первому и третьему биту вектора *i,* а игрек второму биту вектора *j.* Индексы ключей совпадают с индексами иксов.

Повторяя подобные рассуждения аналогично можно записать и другие линейные уравнения для блока S_0:

$X_0' \oplus X_2' \oplus X_3' \oplus Y_0' \oplus Y_1' = k_0 \oplus k_2 \oplus k_3$,

$X_0' \oplus X_1' \oplus X_2' \oplus Y_0' = k_0 \oplus k_1 \oplus k_2$,

$X_0' \oplus X_1' \oplus X_2' \oplus X_3' \oplus Y_0' = k_0 \oplus k_1 \oplus k_2 \oplus k_3$.

Но согласно заданных условий и функции Фейстеля есть и второй блок S_1.

Проводим рассуждения аналогичные и для него.

В соответствии с таблицей можно выделить семь эффективных линейных статистических аналогов и составить семь наиболее эффективных линейных уравнений, соответствующие парам: (i, j) – $(0011, 10)$, $(0101, 10)$, $(0101, 11)$, $(1010, 10)$, $(1100, 10)$, $(1100, 11)$, $(1111, 01)$.

$X_6' \oplus X_7' \oplus Y_2' = k_6 \oplus k_7$,

$X_5' \oplus X_7' \oplus Y_2' = k_5 \oplus k_7$,

$X_5' \oplus X_7' \oplus Y_2' \oplus Y_3' = k_5 \oplus k_7$,

$X_4' \oplus X_6' \oplus Y_2' = k_4 \oplus k_6$,

$X_4' \oplus X_5' \oplus Y_2' = k_4 \oplus k_5$,

$X_4' \oplus X_5' \oplus Y_2' \oplus Y_3' = k_4 \oplus k_5$,

$X_4' \oplus X_5' \oplus X_6' \oplus X_7' \oplus Y_3' = k_4 \oplus k_5 \oplus k_6 \oplus k_7$.

В итоге сформирован эффективный линейный статистический аналог, но пока не понятно, что это за штрихи над иксами и игреками и как их найти?

Их необходимо выразить через биты входного сообщения, для этого еще более детально рассмотрим один раунд алгоритма S-DES.

Представим исходный текст, как $X0\,X1\,X2\,X3\,X4\,X5\,X6\,X7$.

Затем выполняется начальная перестановка *IP*. После перестановки получаем $X7\,X6\,X4\,X0\,X2\,X5\,X1\,X3$.

Далее текст разбивается на левую часть $X7\,X6\,X4\,X0$ и правую часть $X2\,X5\,X1\,X3$.

Правая часть подвергается перестановке с расширением E [4]. В результате получается следующий результат - $X3\,X2\,X5\,X1\,X5\,X1\,X3\,X2$.

Далее этот результат складывается с битами раундового ключа $k_0\,k_1\,k_2\,k_3\,k_4\,k_5\,k_6\,k_7$.

И только потом этот результат поступает на S блоки, а именно на блок S_0 подаем $X3\,X2\,X5\,X1 \oplus k_0\,k_1\,k_2\,k_3$, на блок S_1 подаем $X5\,X1\,X3\,X2 \oplus k_4\,k_5\,k_6\,k_7$. Т.е. на вход блока S_0 поступают биты входного сообщения x3x2x5x1.

Теперь представим входные биты блоков замены в следующем виде.

Для блока S_0 справедливы зависимости:

$X'_0 = X3 \oplus k_0,\ X'_1 = X2 \oplus k_1,\ X'_2 = X5 \oplus k_2,\ X'_3 = X1 \oplus k_3$.

Для блока S_1 справедливы зависимости:

$X'_4 = X5 \oplus k_4,\ X'_5 = X1 \oplus k_5,\ X'_6 = X3 \oplus k_6,\ X'_7 = X2 \oplus k_7$.

Теперь мы можем сделать замену в уравнениях линейного статистического аналога, т.е. заменить иксы штрих на иксы без штриха, но сначала закончим игрек штрихами.

Начнем с конца. Пусть криптограмма имеет вид $Y0\,Y1\,Y2\,Y3\,Y4\,Y5\,Y6\,Y7$.

Вид информационного блока до конечной перестановки (обратной начальной) имеет вид $Y7\,Y6\,Y4\,Y0\,Y2\,Y5\,Y1\,Y3$.

Перед конечной перестановкой блок разбивается на левую часть $Y7\,Y6\,Y4\,Y0$ и правую часть $Y2\,Y5\,Y1\,Y3$.

Правая часть $Y2\,Y5\,Y1\,Y3$ получается в результате сложения по модулю 2 левой части исходного текста после перестановки *IP* $X7\,X6\,X4\,X0$ с текстом $X2\,X5\,X1\,X3$ прошедшим функцию усложнения.

На выходе блоков замены функции усложнения имеем - $Y'_0\,Y'_1\,Y'_2\,Y'_3$. Таким образом, после перестановки *P* получаем $Y'_1\,Y'_0\,Y'_3\,Y'_2$.

В результате можно записать:

$Y'_1 = X7 \oplus Y2,\ Y'_0 = X6 \oplus Y5,\ Y'_3 = X4 \oplus Y1,\ Y'_2 = X0 \oplus Y3$.

Теперь подставим линейные уравнения иксов и игреков в уравнения линейных статистических аналогов, которые теперь примут вид. На этом первый этап алгоритма линейного криптоанализа закончен, их пять.

№ блока	Линейные уравнения
S_0	$X1 \oplus X2 \oplus X7 \oplus Y2 = k_1 \oplus k_3$ $X1 \oplus X3 \oplus X5 \oplus X6 \oplus X7 \oplus Y2 \oplus Y5 = k_0 \oplus k_2 \oplus k_3$ $X2 \oplus X3 \oplus X5 \oplus X6 \oplus Y5 = k_0 \oplus k_1 \oplus k_2$ $X1 \oplus X2 \oplus X3 \oplus X5 \oplus X6 \oplus Y5 = k_0 \oplus k_1 \oplus k_2 \oplus k_3$
S_1	$X0 \oplus X2 \oplus X3 \oplus Y3 = k_6 \oplus k_7$ $X0 \oplus X1 \oplus X2 \oplus Y3 = k_5 \oplus k_7$ $X0 \oplus X1 \oplus X2 \oplus X4 \oplus Y1 \oplus Y3 = k_5 \oplus k_7$ $X0 \oplus X3 \oplus X5 \oplus Y3 = k_4 \oplus k_6$ $X0 \oplus X1 \oplus X5 \oplus Y3 = k_4 \oplus k_5$ $X0 \oplus X1 \oplus X4 \oplus X5 \oplus Y1 \oplus Y3 = k_4 \oplus k_5$ $X1 \oplus X2 \oplus X3 \oplus X4 \oplus X5 \oplus Y1 = k_4 \oplus k_5 \oplus k_6 \oplus k_7$

Очевидно, что первое уравнение $X_1' \oplus X_3' = Y_1'$ блока S_0 выполняется с вероятностью $p = 14/16 = 7/8$, а соответственно $\Delta = |1 - 2p| = |1 - 2 \cdot 7/8| = 3/4$.

Таким образом, таблица с линейными уравнениями примет вид:

№ блока	Линейные уравнения	p	$\Delta = \|1 - 2p\|$
S_0	$X1 \oplus X2 \oplus X7 \oplus Y2 = k_1 \oplus k_3$	7/8	3/4
	$X1 \oplus X3 \oplus X5 \oplus X6 \oplus X7 \oplus Y2 \oplus Y5 = k_0 \oplus k_2 \oplus k_3$	1/8	3/4
	$X2 \oplus X3 \oplus X5 \oplus X6 \oplus Y5 = k_0 \oplus k_1 \oplus k_2$	1/4	1/2
	$X1 \oplus X2 \oplus X3 \oplus X5 \oplus X6 \oplus Y5 = k_0 \oplus k_1 \oplus k_2 \oplus k_3$	3/4	1/2
S_1	$X0 \oplus X2 \oplus X3 \oplus Y3 = k_6 \oplus k_7$	3/4	1/2
	$X0 \oplus X1 \oplus X2 \oplus Y3 = k_5 \oplus k_7$	3/4	1/2
	$X0 \oplus X1 \oplus X2 \oplus X4 \oplus Y1 \oplus Y3 = k_5 \oplus k_7$	3/4	1/2
	$X0 \oplus X3 \oplus X5 \oplus Y3 = k_4 \oplus k_6$	3/4	1/2
	$X0 \oplus X1 \oplus X5 \oplus Y3 = k_4 \oplus k_5$	1/4	1/2
	$X0 \oplus X1 \oplus X4 \oplus X5 \oplus Y1 \oplus Y3 = k_4 \oplus k_5$	3/4	1/2
	$X1 \oplus X2 \oplus X3 \oplus X4 \oplus X5 \oplus Y1 = k_4 \oplus k_5 \oplus k_6 \oplus k_7$	7/8	3/4

Выбрав в качестве ключа шифрования $k = 0010001111$ реализуем второй, третий и четвертый этапы.

Сформировав набор пар «открытый текст – криптограмма», используя $k = 0010001111$ вычислим левые части линейных эффективных аналогов.

В результате получаем систему уравнений (пятый этап):

$k_0 \oplus k_2 \oplus k_3 = 0$, $k_0 \oplus k_1 \oplus k_2 = 0$, $k_0 \oplus k_1 \oplus k_2 \oplus k_3 = 0$, $k_6 \oplus k_7 = 1$,

$k_5 \oplus k_7 = 1, k_5 \oplus k_7 = 1,\ k_4 \oplus k_6 = 1,\ k_4 \oplus k_5 = 1,\ k_4 \oplus k_5 = 1,$

$k_4 \oplus k_5 \oplus k_6 \oplus k_7 = 0.$

Решение системы уравнений имеет вид:

$k_1 = 10101001,\ k_5 = 10100101,\quad k_9 = 10101010,\quad k_{13} = 10100110,$

$k_2 = 01010101,\ k_6 = 01011001,\quad k_{10} = 01010110,\quad k_{14} = 01011010,$

$k_3 = 10011001,\ k_7 = 10010101,\quad k_{11} = 10011010,\quad k_{15} = 10010110,$

$k_4 = 01100101,\ k_8 = 01101001,\quad k_{12} = 01100110,\quad k_{16} = 01101010.$

Анализ решения системы уравнений позволяет определить раундовый ключ $k_1 = 10101001$, а затем используя алгоритм формирования ключей алгоритма S-DES и метод полного перебора – ключ криптосистемы.

3. Порядок выполнения работы.

1. Запустить на исполнение программу «Cryptoanaliz».
2. Заполонить поля ввода: фамилию, имя и отчество. Выбрать номер подгруппы.
3. Пройти предлагаемый контрольный опрос.
4. Получить индивидуальный вариант выполнения работы.
5. Задать в программе «Cryptoanaliz» номер своего варианта, количество известных текстов равное 200. Выбрать один раунд шифрования.
6. Используя таблицы Q_0 и Q_1 для *S*-блоков и учитывая таблицы перестановок, сложение по модулю 2, определить эффективные линейные аналоги. Вычислить вероятности линейных аналогов и значение дельта.
7. Используя модуль, «Анализ» программы «Cryptoanaliz» вводите значения левой части линейных уравнений и определяете их значение (либо «0», либо «1»). Осуществляете шифрование случайным образом сгенерированных открытых текстов.
8. Используя полученные результаты, формируете систему уравнений относительно бит ключа. Решаете полученную системы уравнений.

Пример:

$k_0 \oplus k_2 \oplus k_3 = 0,\quad k_0 \oplus k_1 \oplus k_2 = 0,\ k_0 \oplus k_1 \oplus k_2 \oplus k_3 = 0,\ k_6 \oplus k_7 = 1,$

$k_5 \oplus k_7 = 1, k_5 \oplus k_7 = 1,\ k_4 \oplus k_6 = 1,\ k_4 \oplus k_5 = 1,\ k_4 \oplus k_5 = 1,$

$k_4 \oplus k_5 \oplus k_6 \oplus k_7 = 0.$

9. Используя модуль «проверка» программы «Cryptoanaliz», проверяете правильность каждого из полученных ключей. Используя алгоритм формирования ключей алгоритма S-DES и метод полного перебора – получаете ключ криптосистемы.
10. При совпадении результатов анализа с истинным ключом шифра оформляете отчет.

4. Содержание отчета

1. Титульный лист.
2. Исходные данные варианта выполнения лабораторной работы.
2. Таблицы статистического анализа Q_0 и Q_1 для S-блоков.
3. Система линейных уравнений для определения битов ключа.
4. Варианты полученных ключей.
5. Результат проверки, подтверждающий правильность определенного в лабораторной работе ключа.
6. Вывод

5. 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 № 4

Изучение метода дифференциального (разностного) криптоанализа блочных симметричных криптосистем

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

2. Краткие теоретические сведения

Идея метода дифференциального (разностного) криптоанализа 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.

Метод дифференциального криптоанализа будем рассматривать на примере криптосистемы S-DES. 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.

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 криптограмм с определенной вероятностью. Эти вероятности можно определить, построив таблицы для каждого из блоков замены.

Таблицы строятся 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, 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.

Рассмотрим пример применения дифференциального криптоанализа на практике.

Вначале анализируются блоки замены S_0 и S_1.

Затем переводим таблицы замен в двоичный вид.

В дальнейшем формируются таблицы зависимостей ΔA от ΔC. Анализ осуществляется следующим образом. Так как на вход каждого блока замены подается по четыре бита, то и размерность их суммы по mod2 не будет превышать четырех бит. Таким образом, диапазон изменения ΔA лежит в пределах 0000 – 1111.

Однако, пара анализируемых текстов должна различаться хотя бы одним битом, тогда значение $\Delta A = 0000$ не может использоваться для анализа. Поэтому диапазон изменения ΔA составляет 15 значений от 0001 до 1111. Каждое из значений ΔA может быть получено шестнадцатью возможными комбинациями входных данных блоков замены.

Так, например, $\Delta A = 0001$ может быть получено следующими возможными комбинациями сложением по модулю два:

0000⊕0001, 0001⊕0000, 0010⊕0011, 0011⊕0010, 0100⊕0101, 0101⊕0100, 0110⊕0111, 0111⊕0110, 1000⊕1001, 1001⊕1000, 1010⊕1011, 1011⊕1010, 1100⊕1101, 1101⊕1100, 1110⊕1111, 1111⊕1110.

При этом сумма выходов по mod2, полученных после прохождения любой пары данных входов через конкретный блок замены, не всегда совпадет с суммой выходов того же блока замены по mod 2 другой пары.

Рассмотрим пару входов 0011⊕0010, значение 0011 при прохождении через блок S_0 даст 01, а значение 0010 при прохождении через блок S_0 – 00.

Сумма этих выходов по mod2 будет равна $\Delta C = 01 \oplus 00 = 01$.

Рассмотрим другую пару входов 1010⊕1011. При прохождении через блок S_0 значение 1010 даст нам 00, а 1011 – 00. Таким образом, $\Delta C = 00 \oplus 00 = 00$. Из данного примера наглядно видно, что одному и тому же значению ΔA могут соответствовать различные ΔC.

Результаты анализа блока замены S_0 для $\Delta A = 0001$ объединяются в таблицу.

Результаты анализа блоков замены S_0 и S_1 приведен в таблицах:

ΔC(ΔA) в блоке S_0

ΔA	ΔC			
	00	**01**	**10**	**11**
0001	6	6	2	2
0010	0	4	8	4
0011	2	2	6	6
0100	0	12	0	4
0101	6	6	2	2
0110	0	0	8	8

ΔC(ΔA) в блоке S_1

ΔA	ΔC			
	00	**01**	**10**	**11**
0001	2	6	2	6
0010	0	8	0	8
0011	6	2	6	2
0100	0	8	4	4
0101	6	2	6	2
0110	0	0	12	4

0111	2	2	6	6
1000	6	6	2	2
1001	4	8	4	0
1010	2	2	6	6
1011	0	4	0	12
1100	6	6	2	2
1101	8	4	0	4
1110	2	2	6	6
1111	4	0	12	0

0111	2	6	2	6
1000	2	6	2	6
1001	0	0	12	4
1010	6	2	6	2
1011	0	8	4	4
1100	6	2	6	2
1101	4	4	0	8
1110	2	6	2	6
1111	12	4	0	0

После того, как проведен анализ и построены таблицы, можно приступить к выявлению наилучшего ΔA и соответствующего ему ΔC, то есть пары (ΔA, ΔC).

Из данных таблиц можно выделить несколько равновероятных пар. Для блока S_0 такими парами будут: (0100, 01), (1011, 11), (1111,10), а для блока S_1 - (0110, 10), (1001, 10), (1111, 00).

Однако, следует учитывать, что ΔA равно сумме по mod2 переставленных и расширенных входных бит.

Согласно перестановки должны быть равны 1 и 7 биты, 2 и 8 биты и т.д.

Тогда можно выделить единственное значение ΔA=11111111, которому соответствует ΔC=1000. Именно эта пара и будет рассматриваться далее.

Зная наилучшее значение пары (ΔA, ΔC), можно приступить к нахождению ключа.

Для этого понадобятся несколько пар открытых текстов ($X1$,$X2$), таких, что $\Delta A = E(X1) \oplus E(X2) = 11111111$, а $\Delta C = S(E(X1)) \oplus S(E(X2)) = 1000$.

Для того, чтобы из зашифрованного сообщения $X1$ выделить $S(E(X1))$, необходимо к последним четырем битам шифрованного сообщения добавить первые четыре бита, а затем учесть последнюю перестановку. Для удобства работы данные тексты и относящиеся к ним данные занесем в таблицу.

Пары ($X1$, $X2$), соответствующие наилучшим (ΔA, ΔC)

№	$X1$	$E(X1)$	$S(E(X1))$	$Y1$
1	00011001	11000011	1011	01000110
2	11111001	11000011	1011	00001000
№	$X2$	$E(X2)$	$S(E(X2))$	$Y2$
1	01000110	00111100	0011	11010111
2	01000110	00111100	0011	11010111

Рассмотрим приведенные пары открытых текстов, учитывая, что результат ψ складывается по mod2 с левой частью исходного сообщения.

Так как на вход блоков замены S_0 и S_1 поступают значения $E(X1)$ и $E(X2)$, то для всех $X1$ и $X2$ имеем следующее.

Для блока S_0:

1. Пара (00011001, 01000110):

$1100 \oplus k_1$ даст на выходе 10; $0011 \oplus k_1$ даст на выходе 00.

№	$X1$	$E(X1)$	$S(E(X1))$	$Y1$
1	00011001	11000011	1011	01000110
2	11111001	11000011	1011	00001000
№	$X2$	$E(X2)$	$S(E(X2))$	$Y2$
1	01000110	00111100	0011	11010111
2	01000110	00111100	0011	11010111

На выходе блока S_0 значение 10 получается в том случае, когда на его вход подается одно из значений 0100, 0101, 1000, 1101, а значение 00 – при входных 0010, 0111, 1010, 1011.

Исходя из этого, имеем следующие возможные варианты:

$1100 \oplus k_1 = 0100, \quad k_1 = 1000;$

$1100 \oplus k_1 = 0101, \quad k_1 = 1001;$

$1100 \oplus k_1 = 1000, \quad k_1 = 0100;$

$1100 \oplus k_1 = 1101, \quad k_1 = 0001;$

$0011 \oplus k_1 = 0010, \quad k_1 = 0001;$

$0011 \oplus k_1 = 0111, \quad k_1 = 0100;$

$0011 \oplus k_1 = 1010, \quad k_1 = 1001;$

$0011 \oplus k_1 = 1011, \quad k_1 = 1000.$

2. Пара (11111001, 01000110). Для блока S_0 данную пару рассматривать нет необходимости, так как первые четыре бита $E(X1)$ и $E(X2)$ будут аналогичны тем же битам предыдущей пары, а, следовательно, дадут такой же результат.

Для блока S_1:

1. Пара (00011001, 01000110): $0011 \oplus k_2$ даст на выходе 11; $1100 \oplus k_2$ даст на выходе 11. На выходе блока S_1 значение 11 получается в том случае, когда на его вход подается одно из значений 0001, 0010, 1100, 1101, а значение 11 – при входных 0001, 0010, 1101. Исходя из этого, имеем следующие возможные варианты:

$0011 \oplus k_2 = 0001, \quad k_2 = 0010;$

$0011 \oplus k_2 = 0010, \quad k_2 = 0001;$

$0011 \oplus k_2 = 1100, \quad k_2 = 1111;$

$0011 \oplus k_2 = 1101, \quad k_2 = 1110;$

$1100 \oplus k_2 = 0001, \quad k_2 = 1101;$

$1100 \oplus k_2 = 0010, \quad k_2 = 1110;$

$1100 \oplus k_2 = 1101, \quad k_2 = 0001.$

2. Пара (11111001, 01000110). Для блока S_1 данную пару рассматривать нет необходимости, так как вторые четыре бита $E(X1)$ и $E(X2)$ будут

аналогичны тем же битам предыдущей пары, а следовательно дадут такой же результат.

Объединив результаты анализа, получим следующие наиболее вероятные раундовые ключи:

$k_1 = 10000001$, $k_2 = 10010001$, $k_3 = 01000001$,

$k_4 = 00010001$, $k_5 = 10001110$, $k_6 = 10011110$,

$k_7 = 01001110$, $k_8 = 00011110$.

Как показала проверка, из всех возможных комбинаций, $k_7 = 01001110$ является искомым раундовым ключом. Используя алгоритм формирования раундовых ключей алгоритма S-DES, остальные 2 бита ключа криптосистемы можно найти методом полного перебора.

3. Порядок выполнения работы.

1. Запустить на исполнение программу «Cryptoanaliz».
2. Заполонить поля ввода: фамилию, имя и отчество. Выбрать номер подгруппы.
3. Пройти предлагаемый контрольный опрос.
4. Получить вариант индивидуального задания.
5. Задать в программе «Cryptoanaliz» номер своего варианта, количество известных текстов равное 200. Выбрать один раунд шифрования.
6. Используя таблицы анализа несходств ΔA, ΔC для блоков замены S0 и S1, определяете оптимальный дифференциал. Вводите определенные значения ΔA, ΔC в программу.
7. Осуществляете шифрование случайным образом сгенерированных открытых текстов. Программа выбирает из множества пар текстов пары, удовлетворяющие оптимальному дифференциалу ΔA, ΔC и представляет их в виде в таблицы.
8. В дальнейшем анализируете пары открытых текстов и определяете множество раундовых ключей шифра и, соответственно, множество основных ключей шифра. Ключ, получаемый чаще остальных и будет наиболее вероятным ключом шифра.
9. Используя модуль «проверка» программы «Cryptoanaliz», проверяете правильность ключа. Используя алгоритм формирования ключей алгоритм S-DES и метод полного перебора – получаете ключ криптосистемы.
10. При совпадении результатов анализа с истинным ключом шифра оформляете отчет.

4. Содержание отчета

1. Титульный лист.
2. Исходные данные варианта выполнения лабораторной работы.
2. Результаты анализа таблиц S0 и S1.
3. Результаты анализа пар открытых текстов.

4. Множество возможных раундовых ключей первого раунда.

5. Результат проверки, подтверждающий правильность определенного в лабораторной работе ключа.

6. Вывод

5. 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 № 5

Изучение работы алгоритмов с открытым ключом, методов криптоанализа, основанных на алгоритмах разложения на множители

1. Цель работы - закрепление теоретических знаний и практическое освоение методов криптоанализа ассиметричных криптосистем на примере криптосистемы RSA.

2. Краткие теоретические сведения

Алгоритм работы криптосистемы RSA.

Пусть имеется сеть, состоящая из M абонентов. Каждый m-й абонент, $m=\overline{1,M}$, сети случайно выбирает два больших простых числа p_m, q_m и затем вычисляется число $N_m = p_m q_m$. Число N_m является открытой информацией, доступной другим абонентам сети.

Далее каждый абонент вычисляет функцию Эйлера $\varphi(N_m)=(p_m-1)(q_m-1)=\phi_m$ и выбирает число $k_{от} < \phi_m$, взаимно простое с ϕ_m, а затем по обобщенному алгоритму Евклида находит число $k_{зт}$, такое что:

$$k_{от}k_{зт} \bmod \phi_m = 1,\ m=\overline{1,M}.$$

Пара $\langle N_m, k_{от}\rangle$ является открытым ключом криптосистемы, а число $k_{зт}$ представляет собой закрытый ключ и храниться абонентом в тайне.

Таким образом, происходит шифрование информации.

Для расшифрования можно использовать **алгоритм факторизации Ферма**.

Для того, чтобы было сложнее факторизовать n и решить задачу RSA, p и q выбираются одинаковой битовой длины.

Однако, если p и q слишком близки друг к другу, то становится возможным достаточно быстро найти их.

Пусть $n = pq$, где $p \le q$ и оба нечетные, тогда положив $z_1 = \frac{1}{2}(p+q)$ и $z_2 = \frac{1}{2}(q-p)$, получаем, что $n = z_1^2 - z_2^2 = (z_1 - z_2)(z_1 + z_2)$ или $z_2^2 = n - z_1^2$.

Данное утверждение дает возможность разложить нечетное число на два множителя. Отметим, что множители могут быть как простыми, так и составными. На этой идее основан алгоритм Ферма. При известном нечетном целом $n>1$ алгоритм находит наибольший множитель $\le \sqrt{n}$.

Существо алгоритма в следующем:

1. Выбрать наименьшее натуральное число больше $\lceil\sqrt{n}\rceil$.
2. Задать f=0,1,...

3. Вычислить $k=\lceil\sqrt{n}\rceil+f$, а также $z_2 = k^2 - n$ и выяснить, является ли z_2 число полным квадратом какого-то натурального числа y. Если $z_2^2 = y$, то остановить процедуру.

4. Получить множители числа n: $n = ab = (z_1 - z_2)(z_1 + z_2)$.

5. Если z_2^2 не является квадратом некоторого натурального числа, то увеличить f на 1: $f=f+1$, вычислить $k=\lceil\sqrt{n}\rceil+f$, а также $z_2 = k^2 - n$ и повторить процедуру.

Алгоритм Ферма эффективен для небольших n.

Метод перешифрования используется при заданных значениях: модуля шифрования **N**, отрытого ключа **e** и шифротекста **Y.**

Если два пользователя используют общий модуль шифрования, но разные значения отрытых ключей и пользователи получили шифротексты **Y1** и **Y2,** которые были получены в результате шифрования одного и того же сообщения **X** возможно исходное сообщение методом бесключевого чтения.

Если один пользователь посылает двум пользователям некое циркулярное сообщение X, то криптоаналитик получает в распоряжение два шифрованных текста. Следующим шагом можно получить исходное сообщение используя обобщенный алгоритм Евклида. Затем находят исходное сообщение.

Выбор параметров криптосистемы является ответственной задачей параметры необходимо выбирать в строгом в соответствии с требованиями. Атака на криптосистему возможно в случае только при неудачном выборе параметров. Пользователю необходимо обеспечить уникальные значения чисел p и q, а также открытого ключа e.

3. Порядок выполнения работы.

Последовательно выполняете задания согласно вашего варианта:

1. Заданы значения: модуля шифрования N, отрытого ключа e и открытого текста X. Необходимо найти значение шифротекста Y, полученного при шифровании X на открытом ключе (N, e) в соответствии с алгоритмом RSA. Вариант выполнения получить у преподавателя.

2. Заданы значения: модуля шифрования N, отрытого ключа e и шифротекста Y. Необходимо найти значение шифра открытого текста X, который при шифровании на открытом ключе (N, e) по алгоритму RSA дает Y. Вариант выполнения получить у преподавателя.

3. Заданы значения: модуля шифрования N и отрытого ключа e. Необходимо используя метод факторизации Ферма найти значение закрытого ключа. Вариант выполнения получить у преподавателя.

4. Заданы значения: модуля шифрования N, отрытого ключа e и шифротекста Y. Необходимо используя метод перешифрования найти значение

открытого текста X, не находя значения секретного ключа. Вариант выполнения получить у преподавателя.

5. Два пользователя используют общий модуль шифрования N, но разные значения отрытого ключа e1 и e2. Пользователи получили шифротексты Y1 и Y2, которые были получены в результате шифрования одного и того же сообщения X. Найти исходное сообщение методом бесключевого чтения. Вариант выполнения получить у преподавателя.

4. Содержание отчета

1. Титульный лист.
2. Исходные данные для каждого задания согласно варианту выполнения лабораторной работы. Номер варианта выполнения соответствует номеру по списку в журнале учебных занятий.
3. Подробное решение поставленной каждой из поставленных задач.
4. Ответы.
5. Вывод

5. 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 № 6

Изучение работы алгоритмов с открытым ключом и электронной подписи

1. Цель работы: закрепление теоретических знаний и практическое освоение схем электронной подписи.

2. Краткие теоретические сведения

Электронная подпись на основе криптосистемы RSA

Пусть некоторая сеть включает в себя M абонентов.

Абонент m планирует подписывать документы. Вначале абонент должен сформировать параметры криптосистемы RSA.

Для этого абонент выбирает два больших простых числа p_m, q_m и вычисляет $N_m = p_m q_m$, $\phi_m = (p_m - 1)(q_m - 1)$.

Затем абонент выбирает число $k_{om} < \phi_m$, взаимно простое с ϕ_m, а затем находит $k_{зm} = k_{om}^{-1} \bmod \phi_m$.

Абонент публикует в сети, ассоциировав со своим именем, числа $\langle N_m, k_{om} \rangle$, а число $k_{зm}$ хранит в тайне.

Числа p_m, q_m, ϕ_m в вычислениях больше не используются. На этом шаге формирование параметров криптосистемы заканчивается. Абонент готов подписывать документы.

На следующем шаге абонент вычисляет хэш-функцию (или просто - хэш) подписываемого документа $h_x = h(x_m)$.

Далее абонент вычисляет число

$$s = h_x^{k_{зm}} \bmod N_m,$$

которое представляет собой электронную подпись. Число s добавляется к документу x_m и абонент получает подписанный документ $\langle x_m, s \rangle$.

Каждый абонент сети, который знает параметры абонента m, может проверить подлинность его подписи. Для этого необходимо из подписанного документа $\langle x_m, s \rangle$ взять x_m и вычислить хэш-образ h_x. Затем вычислить число

$$\omega = s^{k_{om}} \bmod N_m,$$

и проверить выполнение равенства $\omega = h_x$.

Если ЭП подлинная, то $\omega = h_x = h(x_m)$.

Из свойств RSA следует, что $\omega = s^{k_{om}} \bmod N_m = h_x^{k_{om} k_{зm}} \bmod N_m = h_x = h(x_m)$.

Первое свойство ЭП выполняется, т.к. никто кроме владельца подписи не может разложить N на простые множители p и q. Для злоумышленника это будет односторонняя функция. При N порядка 1024 бит, эта задача для злоумышленника практически неразрешима. Злоумышленник, зная N и k_o, не может определить $k_з$.

Действительно чтобы вычислить $k_з = k_o^{-1} \bmod \phi$ требуется знать $\phi = (p-1)(q-1)$, а, следовательно, p и q. Второе и третье свойства выполняются, т.к. выполняется первое.

Электронная подпись на основе криптосистемы Эль Гамаля

Пусть, как и в предыдущем случае, абонент m собирается подписывать документы. На первом шаге формируются параметры криптосистемы Эль Гамаля.

Абонент выбирает большое простое число p и число g, такое, что различные степени g суть различные числа по модулю p. Эти числа храниться в открытом виде и могут быть общими для целой группы абонентов. Затем абонент m выбирает случайное число $k_{зт}$, $1 < k_{зт} < p-1$, которое держится в секрете.

Затем абонент вычисляет число

$$k_{от} = g^{k_{зт}} \bmod p,$$

которое является открытым. Теперь абонент готов подписывать документы.

На следующем шаге абонент вычисляет хэш-функцию исходного документа $h_x = h(x_m)$, которая должна удовлетворять условию $1 < h_x < p$.

На третьем шаге абонент выбирает случайное число c, $1 < c < p-1$, взаимно простое с $p-1$ и вычисляет числа

$$r = g^c \bmod p,$$
$$u = (h_x - k_{зт} \cdot r) \bmod (p-1),$$
$$s = c^{-1} \cdot u \bmod (p-1).$$

где $c^{-1} c \bmod (p-1) = 1$.

Числа $\langle s, r \rangle$ является ЭП. Таким образом, подписанное сообщение имеет вид $\langle x_m; s, r \rangle$.

Получатель подписанного документа заново вычисляет хэш-функцию $h_x = h(x_m)$.

Затем проверяет подлинность подписи, используя равенство

$$k_{от}^r \cdot r^s = g^{h_x} \bmod p.$$

Если ЭП верна, то условие $k_{от}^r \cdot r^s = g^{h_x} \bmod p$ выполняется.

Действительно,

$$k_{от}^{r} \cdot r^{s} = \left(g^{k_{зт}}\right)^{r}\left(g^{c}\right)^{s} = g^{k_{зт}r} g^{c\left(c^{-1}\left(h_x - k_{зт}r\right)\right)} = g^{k_{зт}r} g^{h_x} g^{-k_{зт}r} =$$

$$= g^{h_x} \mod p.$$

Первое свойство ЭП выполняется, т.к. никто кроме законного владельца не знает $k_з$. По этой же причине выполняются второе и третье свойства ЭП.

Основное отличие ЭП на базе криптосистемы Эль-Гамаля от ЭП на базе криптосистемы RSA заключается в длине подписи. ЭП на базе криптосистемы RSA $\langle x_m, s \rangle$, *практически в два раза короче, чем ЭП на базе криптосистемы Эль Гамаля* $\langle x_m; s, r \rangle$, *т.е. если длина ЭП RSA 1024 бит, то длина ЭП Эль Гамаля 2048бит.*

3. Порядок выполнения работы.

Последовательно выполняете задания:

1. Вычислить электронную подпись Эль-Гамаля для сообщения. Использовать параметры p=79, g=15, параметры x и k электронной подписи, а также подписываемый текст M выбрать в соответствии с вариантом. Использовать первый учебный алгоритм хеширования. Вариант выполнения получить у преподавателя.
2. Проверить правильность вычисления сгенерированной электронной подписи из задания № 1.
3. Проверить подлинность электронной подписи Эль-Гамаля для полученного сообщения M. Для получения хэш-суммы использовался второй учебный алгоритм хеширования. Параметры подписи: p=59, g=14, открытый ключ отправителя y, текст M и значения электронной подписи (r,s) получить у преподавателя.
4. Организовать скрытый канал с помощью алгоритма формирования электронной подписи Эль-Гамаля, используя данные полученные у преподавателя.

4. Содержание отчета

1. Титульный лист.
2. Исходные данные для каждого задания лабораторной работы.
3. Подробное решение поставленной каждой из поставленных задач.
4. Ответы.
5. Вывод

5. 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.

Лабораторная работа № 7

Использование алгоритмов шифрования для сокрытия содержимого файла с применением OpenSSL

1. Цель работы - получить навыки применения программного продукта OpenSSL для использования алгоритмов шифрования, изучить алгоритмы DES и RSA

2. Краткие теоретические сведения

Лабораторная работа выполняется учебном классе криптографической защиты. На данном программно-аппаратном комплексе возможно решение следующих криптографических задач:

использование алгоритмов шифрования для сокрытия содержимого файла с применением OpenSSL;

использование алгоритмов хеширования для подтверждения неизменности файла с помощью OpenSSL;

создание цифровых сертификатов X509 и преобразование их форматов с применением пакета OpenSSL;

создание центра сертификации с поддержкой списков отозванных сертификатов с применением пакета OpenSSL;

создание центра сертификации с поддержкой протокола OCSP и применением пакета OpenSSL;

применение электронной цифровой подписи для проверки авторства и неизменности файла;

безопасное хранение файлов с применением криптоконтейнеров.

В состав программного обеспечения входит операционная система Linux, содержащая следующие утилиты для работы с криптосистемами:

OpenSSL - утилита позволяющая осуществить шифрование/дешифрование, хеширование, операции над электронной подписью и цифровыми сертификатами. Она реализует практически все известные криптоалгоритмы в различных режимах.

GNU privacy guard - программный комплекс, реализующий криптографический стандарт OpenPGP и предоставляющий инструменты для шифрования, подписывания и проверки подписи, управления ключами.

Cryptsetup - утилита для управления дисковыми томами с применением криптографии, она также поддерживает стандарт для шифрования жестких дисков.

Stunnel - это утилита, позволяющая зашифровать трафик сетевой службы.

OpenSwan- это утилита предназначенная для установления соединений по протоколу IPSec.

В пособии по управлению программно-аппаратного комплекса имеется описание всех команд используемых утилит.

В пособии по настройке операционной системы Linux программно-аппаратного комплекса имеется описание основных операций, настройки сетевых параметров, утилит мониторинга, утилит для работы с беспроводной сетью, сервисов безопасности и работы прикладных программ.

3. Порядок выполнения работы.

1. Подготовьте (создайте или выберите) текстовый файл с семантически понятным содержимым.

2. С помощью OpenSSL сгенерируйте ключ шифрования для алгоритма DES. Для этого используем команду «*openssl rand –base64 32 > key.txt*». Данная команда сгенерирует 32 различных символа и закодирует их в кодировку base64, и в конце сохранит в файл key.txt.

3. С помощью OpenSSL примените сгенерированный ключ шифрования и алгоритм DES к текстовому файлу. Измерьте время шифрования и запомните (запишите) его.

Для выполнения данного пункта применяем команду «*time openssl enc -des -k key.txt -in test.txt -out test.enc*»

time – команда, которая сообщает о том, что необходимо измерить время выполнения следующей команды.

openssl enc – указание Openssl произвести шифрование.

-des – указание алгоритма.

-k – указание пароля для шифрования (туда мы передаём наш файл, в котором хранится ключи).

-in – указание входного файла, который необходимо зашифровать.

-out – указание имени выходного файла, в который будет сохранён результат шифрования.

4. Откройте текстовый файл, убедитесь, что содержимое не является семантически понятным. Для его выполнения можно просто использовать команду «*cat test.enc*», для чтения файла.

5. Убедитесь, что при передаче неправильного ключа текст не расшифровывается. Для выполнения данного пункта необходимо расшифровать зашифрованный файл. Для расшифровки используем команду «*openssl enc -d -des -in test.enc -out test.dec*»

Openssl enc –d – указание для Openssl о том, что необходимо произвести расшифрование файла.

-des- указание алгоритма.

-in – указание входного файла (в случае расшифрования это зашифрованный файл).

-out – указание выходного файла, в который необходимо сохранить результаты расшифрования.

6. Убедитесь, что при передаче правильного ключа текст расшифровывается корректно (расшифрованный текст совпадает с исходным).

Для выполнения данного пункта необходимо произвести расшифрование зашифрованного файла, при этом в качестве ключа указать верный ключ. Для расшифрования используем команду из прошлого пункта, однако добавим в неё ключ «-k», и укажем файл, в котором хранится ключ.

7. Выполните шифрование по алгоритмам DES-EDE и 3DES, используя только функцию DES, сравните свои результаты с результатами реализаций в OpenSSL, убедитесь в их совпадении (например, шифруйте вручную, а расшифровывайте OpenSSL), каждый раз при шифровании запоминайте время.

8. Повторите пункты со второго по седьмой для алгоритма RSA.

4. Содержание отчета

1. Титульный лист.

2. Описание по каждому пункту проведённых вами действий с изображениями (скриншотами).

3. Вывод лабораторной работы, стиль оформления отчёта – научно-технический.

5. 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.