Лабораторная работа 1

ИССЛЕДОВАНИЕ ПРОЦЕССА ЗАШИФРОВАНИЯ С ПОМОЩЬЮ ПРОСТОЙ ЗАМЕНЫ И РЕШЕТКИ КАРДАНО

Цель и содержание:

1. Углубить знания, по основам одноалфавитного шифрования.
2. Исследовать основные характеристики алгоритма шифрования.

Формируемые компетенции

1. Способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2).
2. Способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5).

Теоретическое обоснование

Одними из самых простых и известных шифров являются шифры простой однозначной замены. Данные шифры используют в качестве шифрующего алгоритма замены или подстановки, при которых осуществляется замена символов (слов) открытого текста соответствующими символами, принадлежащими алфавиту шифротекста.

Вскрытие одноалфавитного шифра осуществляется на учете частоты появления отдельных букв или сочетаний (биграмм, триграмм, и т.д.) в языке. Примером одноалфавитного шифра замены является шифр Цезаря. Шифрование осуществляется по таблице, представляющей собой матрицу содержащую 2 строки и n столбцов, где n - число символов алфавита (для русского алфавита - 32). Первая строка содержит все символы алфавита. Вторая строка получается из предыдущей путем циклического сдвига вправо или влево на несколько символ (букв алфавита).

Выбирается циклический сдвиг шифра. После чего процесс зашифровывания осуществляется следующим образом:

1. Строится матрица для осуществления зашифрования с установленным циклическим сдвигом.

2. Каждая буква шифротекста находится на пересечении столбца таблицы, определяемого буквой открытого текста, и строки, определяемой буквой ключа.

Пример. Пусть надо зашифровать текст – *А нам все равно*.

В качестве ключа используем циклический сдвиг влево на 11 букв русского алфавита (буква *А* заменяется на букву *К*).

Тогда процесс зашифрования можно представить в следующем виде. Таблица для циклического сдвига на 11 символов русского алфавита примет вид представленный в таблице 1.

Таблица 1 – Шифр одноалфавитной замены

Исходный алфавит																
А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Циклический сдвиг на 11 символов																
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Исходный алфавит																
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_	
Циклический сдвиг на 11 символов																
Ы	Ь	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	

В результате процедуры шифрования получаем текст, представленный в таблице 2.

Таблица 2 – Пример шифрования текста с помощью шифра одноалфавитной замены

Исходный текст														
А	_	Н	А	М	_	В	С	Е	_	Р	А	В	Н	О
Зашифрованный текст														
К	Й	Ч	К	Ц	Й	М	Ы	П	Й	Ъ	К	М	Ч	Щ

Расшифровка осуществляется следующим образом. Во второй строке происходит поиск соответствующей буквы шифротекста. Находящаяся над ней в первой строке буква и будет соответствовать букве исходного текста.

Шифры перестановки, или транспозиции, изменяют только порядок следования символа или других элементов исходного текста. Пример – решетка Кардано, которая при наложении на лист бумаги оставляет открытыми лишь некоторые его части. При зашифровке буквы сообщения вписываются в эти отверстия. При расшифровке сообщение вписывается в диаграмму нужных размеров, затем накладывается решетка, после чего на виду оказываются только буквы открытого текста.

Решетки можно использовать двумя способами.

В первом случае зашифрованный текст состоит только из букв исходного сообщения. Решетка изготавливается таким образом, чтобы при ее последовательном использовании в различных положениях каждая клетка лежащего под ней листа бумаги оказалась занятой (это поворотная решетка).

Если решетку поворачивать на 90˚ последовательно, то при возврате на исходное состояние все клетки будут заполнены. При чем в каждом окаймлении должна быть вырезана только одна цифра (внешнее обрамление имеет 5 дырок – отмечены серым цветом, во внутреннем – 1, в среднем – 3). Пример простейшей решетки Кардано приведен на рисунке 2.

1	2	3	4	5	1
5	1	2	3	1	2
4	3	1	1	2	3
3	2	1	1	3	4
2	1	3	2	1	5
1	5	4	3	2	1

Рисунок 2 – Пример решетки Кардано Второй,

стеганографический метод использования решетки позволяет скрыть факт секретного сообщения. В этом случае заполняется только часть листа, а в остальное место дописываются буквы или слова ложного текста

Методика и порядок выполнения работы

1. Изучить теоретический материал работы.
2. Провести исследование системы одноалфавитной замены и алгоритма

Кардано.

Студенты делятся на две подгруппы. В первой подгруппе студенты выбирают ключевые слова, а так же получают текст, выданный преподавателем. Затем они строят таблицу и осуществляют шифрование текста.

Студенты второй подгруппы, получив от студентов первой подгруппы зашифрованное сообщение и необходимый сдвиг, строят таблицу и осуществляют процесс дешифрования.

По окончанию расшифрования студенты второй подгруппы приступают к процедуре зашифрования с использованием нового ключевого слова. Студенты первой подгруппы, получив ключевое слово и зашифрованный текст, приступают к его расшифрованию.

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследования систем по своему варианту и ответы на контрольные вопросы.

Вопросы для защиты работы

Вопросы к практическому занятию

1. Дайте определение шифра. Какие виды шифров вы знаете.
2. Дайте определение шифра одноалфавитной замены.
3. Назовите основные достоинства и недостатки шифра одноалфавитной замены
4. Дайте определение шифра. Какие виды шифров вы знаете
5. Дайте определение шифра простой подстановки замены
6. Назовите основные достоинства и недостатки шифра Кардано

Лабораторная работа 2

ИССЛЕДОВАНИЕ ПРОЦЕССА ШИФРОВАНИЯ СООБЩЕНИЯ С ПОМОЩЬЮ ТАБЛИЦЫ ВИЖЕНЕРА

Цель и содержание:

1. Углубить знания, по основам многоалфавитного шифрования.
2. Исследовать основные характеристики алгоритма шифрования.

Формируемые компетенции

1. Способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9).
2. Способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).

Теоретическое обоснование

Наиболее простыми являются шифры замены или подстановки, особенностью которых является замена символов (слов) открытого текста соответствующими символами, принадлежащими алфавиту шифротекста. Различают: одноалфавитную, многоалфавитную замену.

Вскрытие одноалфавитного шифра осуществляется на учете частоты появления отдельных букв или сочетаний (биграмм, триграмм, и т.д.) в языке. Примером многоалфавитного шифра замены является система Виженера. Шифрование осуществляется по таблице, представляющей собой квадратную матрицу размерности $n \times n$, где n - число символов алфавита (для русского алфавита - 32). Первая строка содержит все символы алфавита. Каждая последующая строка получается из предыдущей путем циклического сдвига вправо на один символ (или влево).

Выбирается ключ или ключевая фраза. После чего процесс зашифровывания осуществляется следующим образом:

1. Под каждой буквой исходного сообщения последовательно записываются буквы ключа (если ключ короче – его используют несколько раз).

2. Каждая буква шифротекста находится на пересечении столбца таблицы, определяемого буквой открытого текста, и строки, определяемой буквой ключа.

Пример. Пусть надо зашифровать текст – *А нам все равно*.

В качестве ключа используем слово – *КОЛОКОЛА*.

Тогда процесс зашифрования можно представить в следующем виде. Таблица Виженера для ключевого слова КОЛОКОЛА примет вид представленный в таблице 1.

ТАБЛИЦА 1 – ТАБЛИЦА ВИЖЕНЕРА С КЛЮЧЕВЫМ СЛОВОМ КОЛОКОЛА

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	**Н**
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	**Ш**	Щ	Ъ	Ы	Ь	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	**Ц**	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	**Н**
Л	М	**Н**	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	**С**	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_

Буквы, выделенные в таблице, соответствуют символам шифротекста.

В результате процедуры шифрования получаем текст, представленный в таблице 2.

Таблица 2 – Пример шифрования текста с помощью таблицы Виженера

Исходный текст														
А	_	Н	А	М	_	В	С	Е	_	Р	А	В	Н	О
Ключевое слово														
К	О	Л	О	К	О	Л	А	К	О	Л	О	К	О	Л
Зашифрованный текст														

К	Й	Ч	К	Ц	Й	М	Ы	П	Й	Ъ	К	М	Ч	Щ

Расшифровка осуществляется следующим образом. Под буквами шифротекста последовательно записываются буквы ключа: в строке соответствующей очередной букве ключа, происходит поиск соответствующей буквы шифротекста. Находящаяся над ней в первой строке буква и будет соответствовать букве исходного текста.

Методика и порядок выполнения работы

1. Изучить теоретический материал работы.
2. Провести исследование системы многоалфавитной замены.

Студенты делятся на две подгруппы. В первой подгруппе студенты выбирают ключевые слова, а так же получают текст, выданный преподавателем. Затем они строят таблицу и осуществляют шифрование текста.

Студенты второй подгруппы, получив от студентов первой подгруппы зашифрованное сообщение и необходимый сдвиг, строят таблицу и осуществляют процесс дешифрования.

По окончанию расшифрования студенты второй подгруппы приступают к процедуре зашифрования с использованием нового ключевого слова. Студенты первой подгруппы, получив ключевое слово и зашифрованный текст, приступают к его расшифрованию.

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследования систем по своему варианту и ответы на контрольные вопросы.

Вопросы для защиты работы

1. Дайте определение шифра многоалфавитной замены. Какие шифры данного вида вы знаете.

2. Дайте определение шифра многоалфавитной замены.

3. Назовите основные достоинства и недостатки шифра многоалфавитной замены.

Лабораторная работа 3
ИССЛЕДОВАНИЕ ПРОЦЕССА ВЫЧИСЛЕНИЯ КЛЮЧЕЙ В БЛОЧНОМ ШИФРЕ S-DES С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ РЕАЛИЗАЦИИ

Цель и содержание:

1. Углубить знания, по основам алгоритма блочного шифрования .
2. Исследовать вопросы получения ключей для алгоритма шифрования.

Формируемые компетенции

1. Способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2).
2. Способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5).
3. Способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9).
4. Способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).

Теоретическое обоснование

Упрощенный DES по свойствам и структуре он подобен DES, но имеет гораздо меньше параметров. Данный алгоритм был разработан профессором Эдвардом Шейфером (Edward Schaefer) из Университета Санта-Клара.

В алгоритме S-DES используется 10-битовый ключ, который находится у отправителя и у получателя сообщения. Из этого ключа на определенных этапах шифрования и дешифрования генерируется два 8-битовых ключа. На рисунке 1 показана схема процедуры создания подключей. Сначала выполняется перестановка битов ключа следующим образом. Если 10-битовый ключ пред-

ставить в виде $k1\ \ k2\ k3\ \ k4\ k5\ \ k6\ \ k7\ \ k8\ k9\ k10$, то перестановку P10 можно задать формулой:

$$P10\,(k_1\,k_2\ k_3\ k_4\ k_5\ \ k_6\ k_7\ k_8\ k_9\,k_{10}) = (k_3\,k_5\ k_2\ k_7\ k_4\ k_{10}\ k_1\ k_9\ k_8\ k_6)$$

Можно также представить перестановку P10 в табличной форме:

P 10									
3	5	2	7	4	10	1	9	8	6

Эту таблицу следует читать слева направо. Каждый ее элемент идентифицирует позицию бита исходных данных в генерируемой выходной последовательности. Иными словами, первым битом в выходной последовательности будет третий бит исходной последовательности, вторым - пятый и т.д. Например, в соответствии с данной таблицей ключ *(1010000010)* будет преобразован к виду *(1000001100)*. После этого отдельно для первых пяти битов и отдельно для вторых выполняется циклический сдвиг влево (LS-1), который еще называют вращением. В нашем случае в результате будет получена последовательность *(00001 11000).*

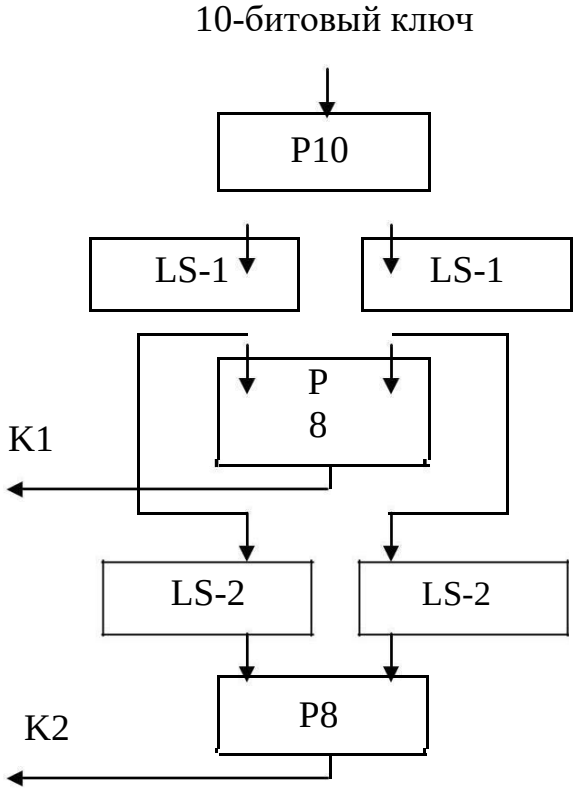


Рисунок 1 – Вычисление ключей S-DES

Затем применяется перестановка P8, в результате которой из 10-битового ключа сначала выбираются, а затем переставляются 8 битов по правилу:

P8							
6	3	7	4	8	5	10	9

В результате этой операции получается первый подключ (К1). В нашем примере он будет иметь вид *(10100100).*

Теперь нужно вернуться к двум 5-битовым строкам, полученным в результате применения функций LS-1**,** и выполнить с каждой из этих строк циклический сдвиг влево на две позиции (LS-2). В нашем конкретном случае значение *(00001 11000)* будет преобразовано к виду *(00100 00011).* Наконец, применив к полученной в результате последовательности перестановку P8, получим подключ (К2). Для нашего примера результатом будет *(01000011).*

Методика и порядок выполнения работы

1. Изучить теоретический материал работы.
2. Провести исследование ключевой системы алгоритма S-DES.

Каждый студент получает индивидуальное задание по выработке ключа для алгоритма упрощенного S-DES. Задание представлено в таблице 1.

Таблица 1 – Задание на разработку ключей для S-DES

№ п/п	Исходные данные	№ п/п	Исходные данные
1.	1100110101	15.	1111110101
2.	1010100101	16.	1100100101
3.	0001010101	17.	0111010101
4.	1010111101	18.	1110111101
5.	1011101011	19.	1001101011
6.	1100111101	20.	1100100001
7.	0011010101	21.	0100010101
8.	1100001111	22.	1101101111
9.	0100110101	23.	0111110101
10.	1011010101	24.	1011100101
11.	0100001100	25.	1111101100
12.	0011001010	26.	1111001010
13.	1110101000	27.	0100101001
14.	1100011111	28.	0001100110

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тет-

ради, должен содержать процесс исследования систем по своему варианту и ответы на контрольные вопросы.

При защите студенты предоставляют программу с помощью которой провели исследования ключевой системы данного алгоритма шифрования.

Вопросы для защиты работы

1. Поясните особенности шифрования с использованием S-DES. Какие виды шифров вы можете отнести к этой группе.
2. Какие виды ключей используются в S-DES.
3. Основные этапы получения ключей в алгоритме S-DES

Лабораторная работа 4

ИССЛЕДОВАНИЕ ПРОЦЕССА ШИФРОВАНИЯ СООБЩЕНИЙ С ПОМОЩЬЮ УПРОЩЕННОГО S-DES С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ РЕАЛИЗАЦИИ

Цель и содержание:

1. Углубить знания, по основам алгоритма блочного шифрования .
2. Исследовать вопросы шифрования данных .

Формируемые компетенции

1. Способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2).

2. Способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5).

3. Способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9).

Теоретическое обоснование

На рисунке 1 показана общая структура упрощенного алгоритма DES, который мы в дальнейшем будем для краткости называть S-DES. Этот алгоритм получает на входе 8-битовый блок открытого текста (например, 10111101) и 10-битовый ключ, а на выходе генерируется 8-битовый блок закрытого текста.

Функция f_k, использует в качестве исходных данных не только шифруемый текст, но и 8-битовый ключ. Алгоритм можно построить так, чтобы он работал с 16-битовым ключом, состоящим из двух 8-битовых подключей, приме-няемых по отдельности каждый для своего вызова функции f_k .

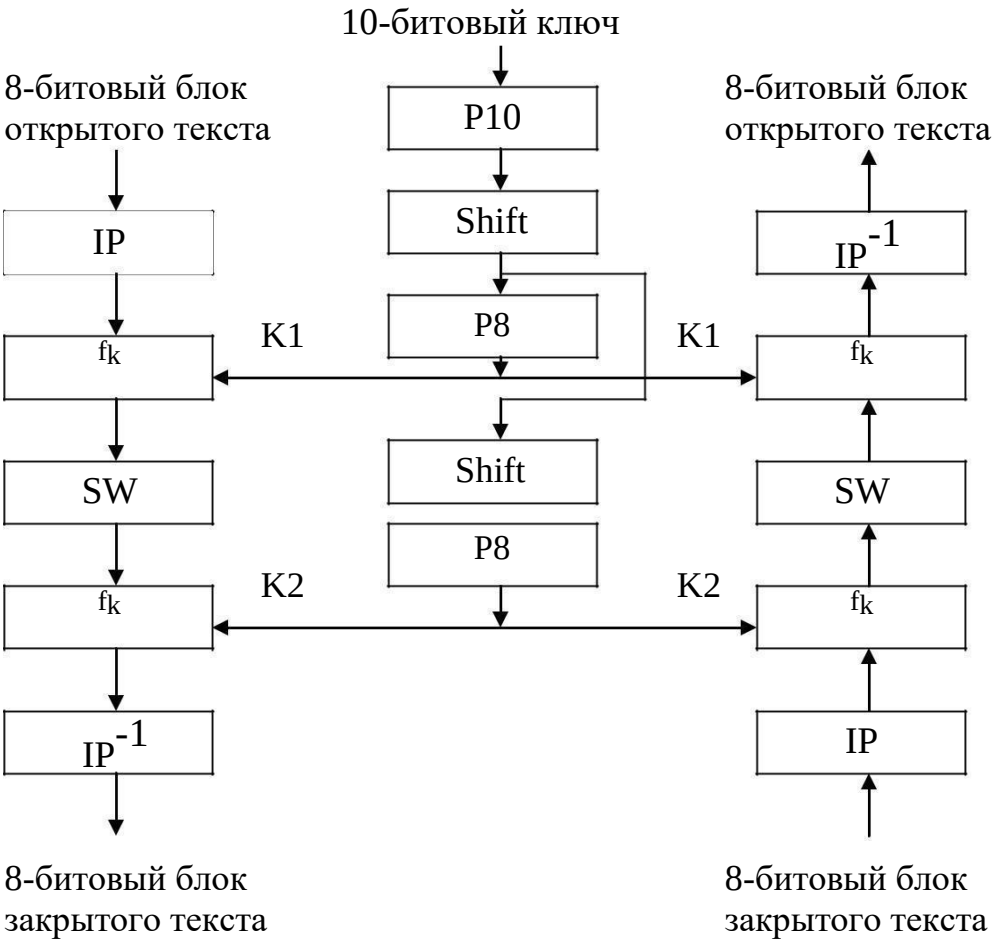


Рисунок 1 – Схема упрощенного алгоритма DES

Можно использовать и 8-битовый ключ, для чего просто следует ввести его дважды

Наконец, можно прибегнуть к комбинированному решению, когда требуется 10-битовый ключ, из которого генерируются два 8-битовых, как показано на рисунке 1. В этом случае ключ сначала преобразуется путем перестановки (P10). После этого применяется операция сдвига, а полученные в ее результате данные поступают на вход перестановки (P8), которая генерирует первый 8-битовый ключ (K1). Те же полученные в результате операции сдвига данные поступают на вход другой операции сдвига и другой функции перестановки (P8), в результате чего генерируется второй подключ (K2).

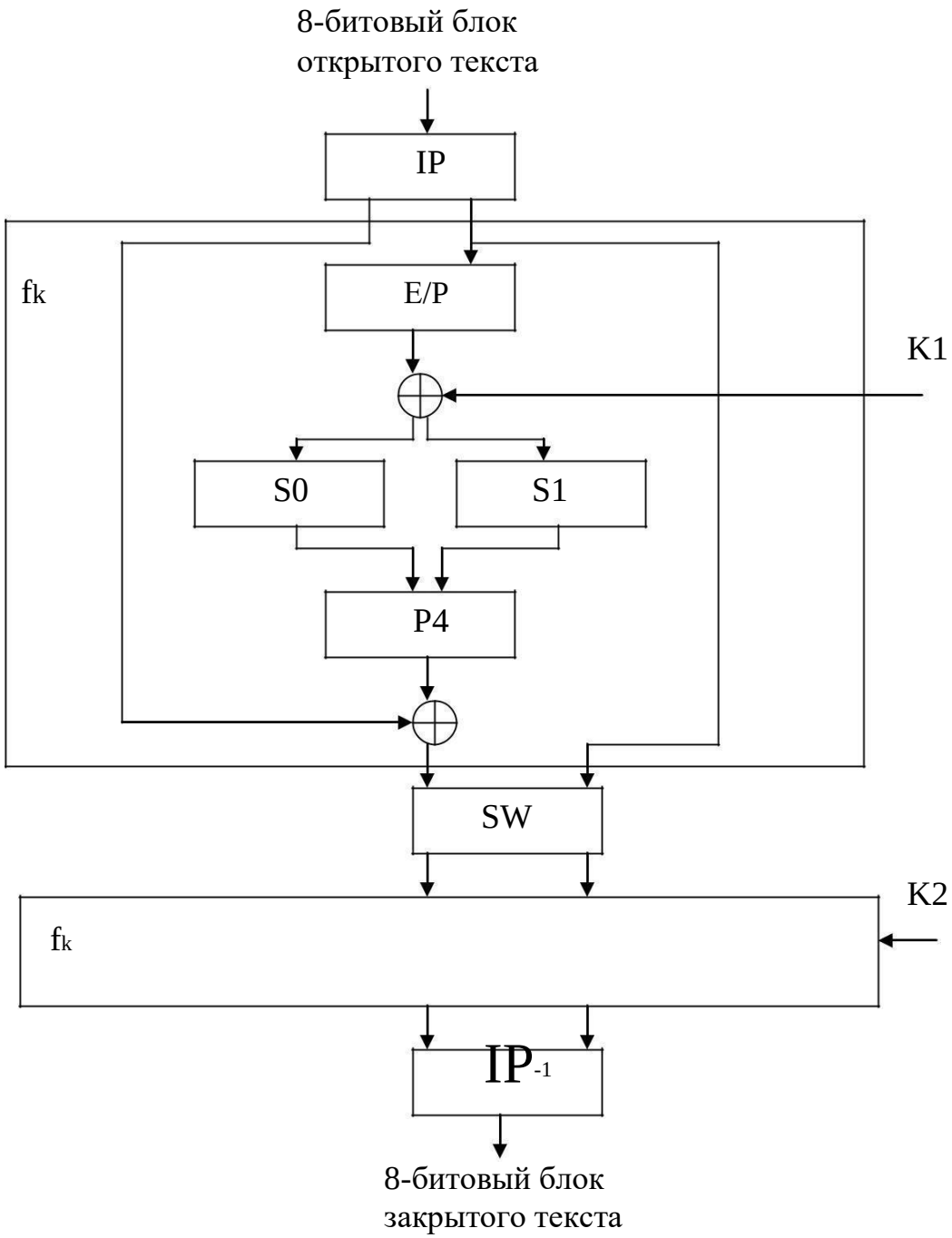


Рисунок 2 – Подробная схема шифрования S-DES

Данный алгоритм можно представить в виде композиции функций:

$$IP^{-1} \underset{k2}{{}_{y}}\circ SW \circ f_{k1} \circ IP ,$$

или, иначе:

$$\textit{шифрованный текст} = IP^{-1}(fk2(SW(fk1(IP(\textit{открытый текст})))))$$

где $$K1 = P8(\textit{сдвиг}(P10(\textit{ключ}))),$$

$$K2 = P8(\textit{сдвиг}(\textit{сдвиг}(P10(\textit{ключ})))).$$

Процесс дешифрования, также представленный на рисунке 1**,** по сути, является процессом, обратным процессу шифрования:

$$открытый\ текст = IP^{-1}(fk1(SW(fk2(IP(шифрованный\ текст)))))$$

На рисунке 2 представлена более подробная схема алгоритма шифрования S-DES. Как уже упоминалось, процесс шифрования представляет собой последовательное выполнение пяти операций, которые мы рассмотрим здесь каждую в отдельности.

Начальная и завершающая перестановки На вход алгоритма поступает 8-битовый блок открытого текста, к которому применяется начальная перестановка, заданная функцией IP.

IP							
2	6	3	1	4	8	5	7

Все 8 битов открытого текста сохраняют свои значения, но меняется порядок их следования. На завершающей стадии алгоритма выполняется обратная перестановка.

IP^{-1}							
4	1	3	5	7	2	8	6

Как легко убедиться с помощью простой проверки, вторая из приведенных выше перестановок действительно является обратной по отношению к первой, т.е. $IP^{-1}(IP(X)) = X$.

Функция f_k

Самым сложным компонентом S-DES является функция f_k, представляющая собой комбинацию перестановки и подстановки. Пусть *L* и *R* означают соответственно первые 4 бита и последние 4 бита 8-битовой последовательности, подаваемой на вход 4, и пусть *F* – некоторое отображение пространства 4-битовых строк в себя, не обязательно являющееся взаимно однозначным. Тогда

$$fk(L,B)=(L+F(E, SK), R),$$

где *SK* обозначает подключ, а + – операцию XOR (побитовое исключающее ИЛИ). Например, если в результате применения функции IP (рисунок 3) полу-

чено значение *(1011 1101)* и *F(1101, SK) = (1110)* для некоторого ключа *SK*, то *fk(10111101) = (01011101)*, так как *(1011)+ (1110) = (0101)*.

Теперь опишем отображение *F*. На входе этого отображения имеем 4-битовое значение (*n1 n2 n3 n4)* . Первой операцией является операция расширения/перестановки.

E/P							
4	1	2	3	2	3	4	1

Для дальнейшего рассмотрения удобнее представить результат в следующей форме:

$$\begin{matrix} n_4 & n_1 & n_2 & n_3 \\ n_2 & n_3 & n_4 & n_1 \end{matrix}$$

К этому значению с помощью операции XOR добавляется 8-битовый подключ $K_1 = (k_{11}\ ,\ k_{12}\ \ k_{13}\ \ k_{14}\ \ k_{15}\ \ k_{16}\ \ k_{17}\ \ k_{18}\ )$:

$$\begin{matrix} n_4 + k_{11} & n_1 + k_{12} & n_2 + k_{13} & n_3 + k_{14} \\ n_2 + k_{15} & n_3 + k_{16} & n_4 + k_{17} & n_1 + k_{18} \end{matrix}$$

Переименуем полученные в результате 8 битов, как показано ниже:

$$\begin{matrix} p_{00} & p_{01} & p_{02} & p_{03} \\ p_{10} & p_{11} & p_{12} & p_{13} \end{matrix}$$

Первые четыре бита (первая строка приведенной выше матрицы) поступают на вход модуля *S0*, на выходе которого получается 2-битовая последовательность, а оставшиеся четыре бита (вторая строка матрицы) – на вход модуля *S1*, на выходе которого получается другая 2-битовая последовательность. Эти S-модули (матрицы кодирования) работают следующим образом. Первый и четвертый биты входной последовательности рассматриваются как 2-битовые числа, определяющие строку, а второй и третий – как числа, определяющие столбец *S*-матрицы. Модули *S0* и *S1* можно определить следующим образом:

$$S0 = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 1 \end{bmatrix} \qquad S1 = \begin{bmatrix} 1 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix}$$

Элементы, находящиеся на пересечении соответствующей строки и столбца, задают двух битовые выходные значения. Например, если *(P0,0 P0,3) = (00)* и *(p0,1 p02) = (10)*, то выходные 2 бита задаются значением, которое нахо-дится на пересечении строки 0 и столбца 2 матрицы *S0* (оно равно *3* или *(11)* в двоичном представлении). Точно так же *(P1,0 P1,3)* и *(p1,1 p12)* служат для опреде-ления строки и столбца матрицы *S1*, на пересечении которых стоит значение, задающее вторые 2 бита.

Теперь 4 бита, полученные на выходе модулей *S0* и *S1*, преобразуются с помощью перестановки следующим образом:

P4			
2	4	3	1

Результат применения перестановки P4 и является результатом функции F.

Методика и порядок выполнения работы

1. Изучить теоретический материал работы.
2. Провести исследование процесса шифрования .

Каждый студент получает индивидуальное задание по осуществлению процесса шифрования. Открытый текст приведен в таблице 1. В качестве ключа для алгоритма S-DES использовать результаты предыдущего занятия.

Таблица 1 – Задание на разработку ключей для S-DES

№ п/п	Исходные данные	№ п/п	Исходные данные
1.	1111110101	15.	1100110101
2.	1100100101	16.	1010100101
3.	0111010101	17.	0001010101
4.	1110111101	18.	1010111101
5.	1001101011	19.	1011101011
6.	1100100001	20.	1100111101
7.	0100010101	21.	0011010101
8.	1101101111	22.	1100001111
9.	0111110101	23.	0100110101

№ п/п	Исходные данные	№ п/п	Исходные данные
10.	1011100101	24.	1011010101
11.	1111101100	25.	0100001100
12.	1111001010	26.	0011001010
13.	0100101001	27.	1110101000
14.	0001100110	28.	1100011111

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследования систем по своему варианту и ответы на контрольные вопросы.

Вопросы для защиты работы

1. Поясните особенности процесса шифрования в S-DES.
2. Сколько раундов используется в S-DES.
3. Основные операции шифрования с помощью алгоритма S-DES**.**

Лабораторная работа 5

ИССЛЕДОВАНИЕ ПРОЦЕССА РАСШИФРОВАНИЕ СООБЩЕНИЙ С ПОМОЩЬЮ УПРОЩЕННОГО S-DES

Цель и содержание:

1. Углубить знания, по основам построения алгоритма шифрования.
2. Исследовать вопросы расшифрования принятого сообщения.

Формируемые компетенции

1. Способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2).
2. Способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5).
3. Способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9).

Теоретическое обоснование

Алгоритм дешифрования S-DES в качестве исходных данных использует 8-битовый блок шифрованного текста и тот же 10-битовый ключ, который применялся для шифрования, а в результате работы алгоритм дешифрования должен генерировать 8-битовый блок открытого текста.

Алгоритм дешифрования включает последовательное выполнение пяти операций; начальной перестановки IP, сложной функции, являющейся композицией операций перестановки и подстановки и зависящей от полученного ключа, перестановки *SW*, при которой две половинки последовательности данных просто меняются местами, еще раз функции *f* и, наконец, перестановки, обратной начальной (IP^{-1}). Подробная схема дешифрования с использованием S-DES приведена на рисунке 1.

На вход алгоритма поступает 8-битовый блок закрытого текста, к которому применяется начальная перестановка, заданная функцией IP.

IP							
2	6	3	1	4	8	5	7

Все 8 битов закрытого текста сохраняют свои значения, но меняется порядок их следования. На завершающей стадии алгоритма выполняется обратная перестановка.

IP^{-1}							
4	1	3	5	7	2	8	6

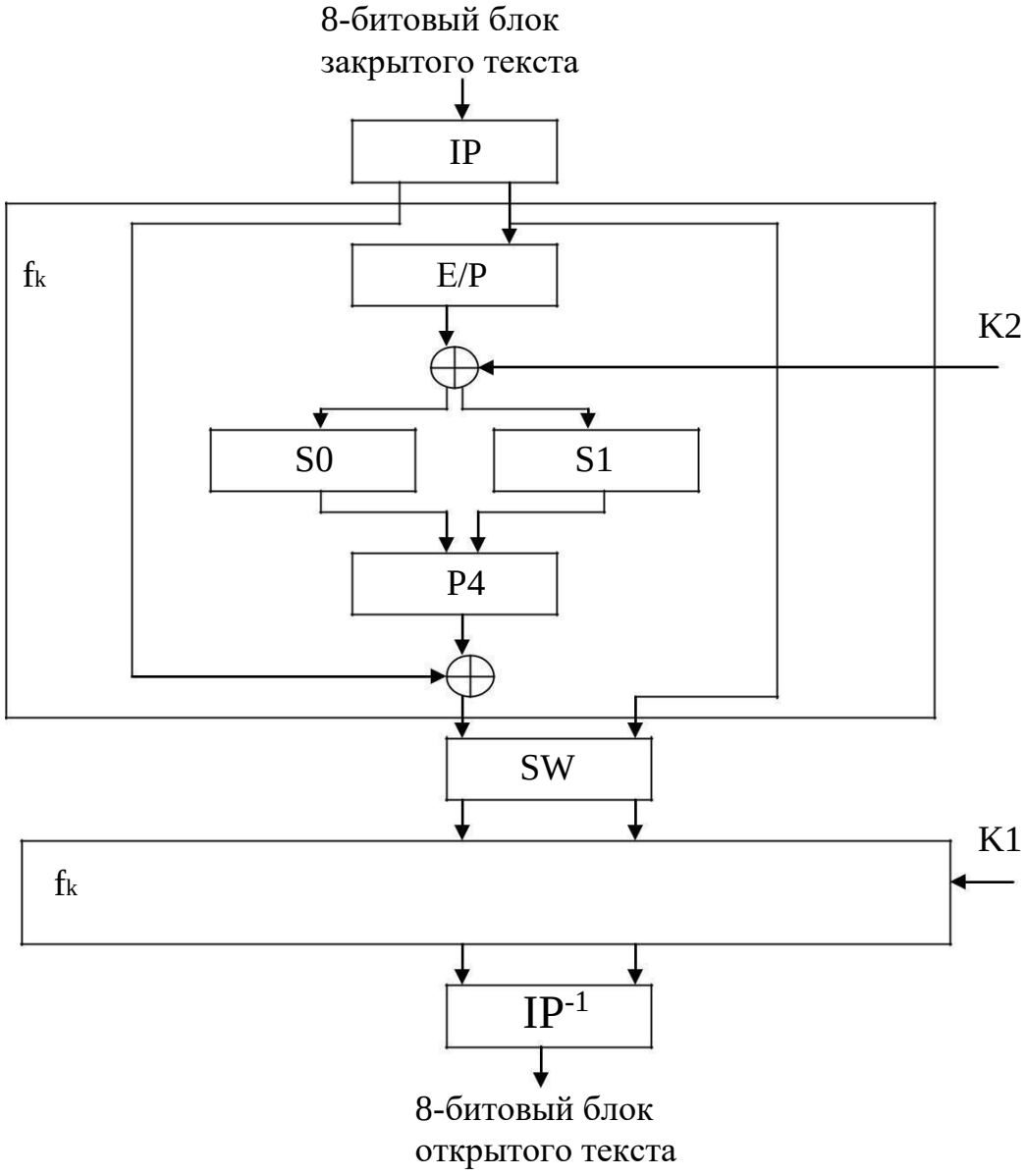


Рисунок 1 – Подробная схема расшифрования S-DES

Как легко убедиться с помощью простой проверки, вторая из приведенных выше перестановок действительно является обратной по отношению к первой, т.е. $IP^{-1}(IP(X)) = X$.

Функция f_k

Самым сложным компонентом S-DES является функция f_k, представляющая собой комбинацию перестановки и подстановки. Пусть *L* и *R* означают соответственно первые 4 бита и последние 4 бита 8-битовой последовательности, подаваемой на вход 4, и пусть *F* – некоторое отображение пространства 4-битовых строк в себя, не обязательно являющееся взаимно однозначным. Тогда

$$fk(L,B)=(L+F(E, SK), R),$$

где *SK* обозначает подключ, а + – операцию XOR (побитовое исключающее ИЛИ). Например, если в результате применения функции IP (рисунок 3) получено значение *(1011 1101)* и *F(1101, SK) = (1110)* для некоторого ключа *SK*, то *fk(10111101) = (01011101)*, так как *(1011)+ (1110) = (0101)*.

Теперь опишем отображение *F*. На входе этого отображения имеем 4-битовое значение $(n1\ n2\ n3\ n4)$. Первой операцией является операция расширения/перестановки.

E/P							
4	1	2	3	2	3	4	1

Для дальнейшего рассмотрения удобнее представить результат в следующей форме:

$$n4 \quad n1 \quad n2 \quad n3$$

$$n2 \quad n3 \quad n4 \quad n1$$

К этому значению с помощью операции XOR добавляется 8-битовый подключ $K1 = (k11, k12, k13, k14, k15, k16, k17, k18)$:

$$n4 + k11 \quad n1 + k12 \quad n2 + k13 \quad n3 + k14$$

$n2 + k15$ $n3 + k16$ $n4 + k17$ $n1 + k18$

Переименуем полученные в результате 8 битов, как показано ниже:

$$\begin{matrix} p_{00} & p_{01} & p_{02} & p_{03} \\ p_{10} & p_{11} & p_{12} & p_{13} \end{matrix}$$

Первые четыре бита (первая строка приведенной выше матрицы) поступают на вход модуля *S0*, на выходе которого получается 2-битовая последовательность, а оставшиеся четыре бита (вторая строка матрицы) – на вход модуля *S1*, на выходе которого получается другая 2-битовая последовательность. Эти S-модули (матрицы кодирования) работают следующим образом. Первый и четвертый биты входной последовательности рассматриваются как 2-битовые числа, определяющие строку, а второй и третий – как числа, определяющие столбец *S*-матрицы. Модули *S0* и *S1* можно определить следующим образом:

S0=

1	0	3	2
3	2	1	0
0	2	1	3
3	1	3	1

S1=

1	1	2	3
2	0	1	3
3	0	1	0
2	1	0	3

Элементы, находящиеся на пересечении соответствующей строки и столбца, задают двух битовые выходные значения. Например, если *(P0,0 P0,3) = (00)* и *(p0,1 p02) = (10)*, то выходные 2 бита задаются значением, которое находится на пересечении строки 0 и столбца 2 матрицы *S0* (оно равно *3* или *(11)* в двоичном представлении). Точно так же *(P1,0 P1,3)* и *(p1,1 p12)* служат для определения строки и столбца матрицы *S1*, на пересечении которых стоит значение, задающее вторые 2 бита.

Теперь 4 бита, полученные на выходе модулей *S0* и *S1*, преобразуются с помощью перестановки следующим образом:

P4			
2	4	3	1

Результат применения перестановки P4 и является результатом сложной функции F.

Методика и порядок выполнения работы

1. Изучить теоретический материал работы.
2. Провести исследование процесса расшифрования.

Каждый студент получает индивидуальное задание по осуществлению дешифрования. В качестве зашифрованного текста, а так же в качестве ключа для упрощенного S-DES использовать результаты предыдущих занятий

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследования системы по своему варианту и ответы на контрольные вопросы.

Вопросы для защиты работы

1. Поясните особенности процесса дешифрования в S-DES.
2. Сколько раундов в S-DES для осуществления дешифрования.
3. Проведите сравнение алгоритма DES и S-DES по этапу расширования передаваемого сообщения.

Лабораторная работа 6

ИССЛЕДОВАНИЕ ПОТОЧНОГО ШИФРОВАНИЯ СООБЩЕНИЙ В СИНХРОННЫХ СИСТЕМАХ, ПОСТРОЕННЫХ НА ОСНОВЕ МНОГОТАКТОВЫХ КОДОВЫХ ФИЛЬТРОВ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ РЕАЛИЗАЦИИ

Цель и содержание:

1. Углубить знания, по основам поточного шифрования .
2. Исследовать вопросы получения синхронного ПСП.

Формируемые компетенции

1. Способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9).
2. Способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).

Теоретическое обоснование

Построить эффективный криптоалгоритм можно, лишь отказавшись от абсолютной стойкости. Возникает задача разработки такого теоретически нестойкого шифра, для вскрытия которого противнику потребовалось бы выполнить такое число операций, которое неосуществимо на современных и ожидаемых в ближайшей перспективе вычислительных средствах за разумное время. В первую очередь представляет интерес схема, использующая ключ небольшой разрядности, который в дальнейшем выполняет функцию "зародыша", порождающего значительно более длинную ключевую последовательность.

Данный результат может быть достигнут при использовании *гаммировании*, схема которого показана на рисунке 1. Гаммированием называют процедуру наложения на входную информационную последовательность *гаммы* шифра, т. е. последовательности с выходов *генератора псевдослучайных кодов*. После-

довательность называется *псевдослучайной*, если она по своим статистическим свойствам она неотличима от истинно *случайной* последовательности, но в отличие от последней является детерминированной, т. е. знание алгоритма ее формирования дает возможность ее повторения необходимое число раз. Если символы входной информационной последовательности и гаммы представлены в двоичном виде, наложение чаще всего реализуется с помощью операции поразрядного сложения по модулю 2. Надежность шифрования методом гаммирования определяется качеством генератора гаммы Простейшие устройства синхронного и самосинхронизирующегося шифрования с использованием ГПК, реализованного на основе *N*-разрядного *регистра сдвига с линейной обратной связью* - *LFSR* (Linear Feedback Shift Register), называются *скремблерами*, а сам процесс преобразования – скремблированием.

Используя приложение выбираем производящий полином $P(x)$ такой, чтобы его степень была равна трем, а вес полинома – 3. В качестве образующего полинома используем $P(x) = x^4 + x + 1$.

Количество ячеек памяти должно равняться степени порождающего полинома (т.е. четырем), количество сумматоров по модулю два определяется числом ненулевых коэффициентов перед степенью *«x»* (т.е. один). Тогда схема кодирующего устройства примет следующий вид:

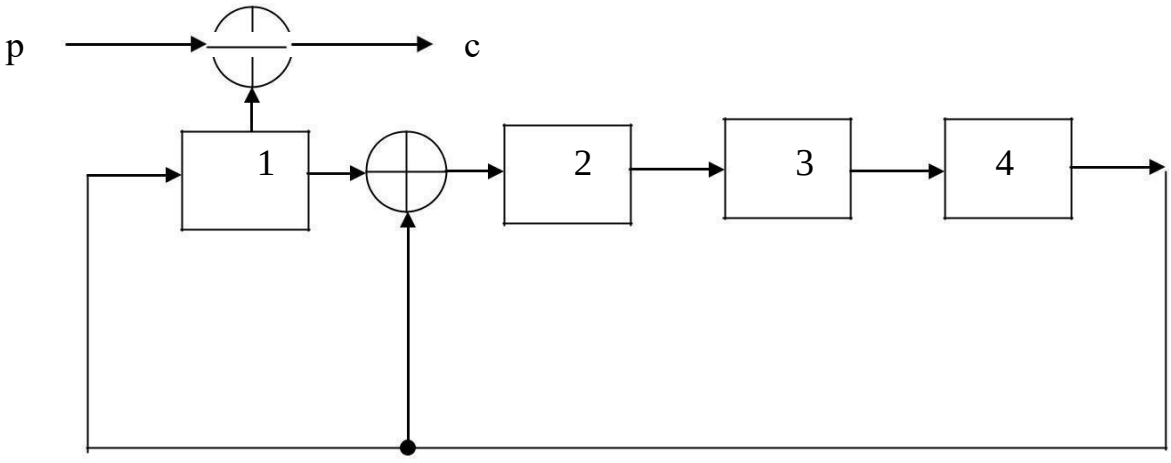


Рисунок 1 - Шифрующее устройство поточного кода.

Для иллюстрации работы кодирующего устройства воспользуемся соотношениями, показывающими процесс образования символов в ячейках:

Символ в 1 яч. = яч. 4^*

Символ в 2 яч. = яч. 4^* + яч.1^*

Символ в 3 яч. = яч. 2^*

Символ в 4 яч. = яч. 3^* В таблице 1 приведены результаты шифрования открытого кода в течение

первых 7 тактов.

Таблица 1.

Номер такта	Откры-тый текст	ЯЧЕЙКА № 1	ЯЧЕЙКА № 2	ЯЧЕЙКА № 3	ЯЧЕЙКА № 3	Закрытый текст
1	1	1	1	0	0	1
2	1	1	0	1	1	1
3	0	1	0	0	1	0
4	1	1	1	0	0	0
5	0	0	0	1	0	0
6	1	0	0	0	1	1
7	1	1	0	0	0	0

В синхронных поточных шифрах гамма формируется независимо от входной последовательности, каждый элемент (бит, символ, байт и т. п.) которой таким образом шифруется независимо от других элементов. В синхронных поточных шифрах отсутствует эффект размножения ошибок, т. е. число искаженных элементов в расшифрованной последовательности равно числу искаженных элементов зашифрованной последовательности, пришедшей из канала связи.

Вставка или выпадение элемента зашифрованной последовательности недопустимы, так как из-за нарушения синхронизации это приведет к неправильному расшифрованию всех последующих элементов.

В таблице 2 показан пример поточного шифрования и расшифрования двоичной последовательности *11100101010110* с использованием гаммы формируемой 4-разрядным *LFSR* при начальном состоянии **1001**. Зашифрованная

последовательность имеет вид ***01001010010010.***

Таблица 2 – Пример поточного шифрования и расшифрования двоичной последовательности, когда отсутствуют ошибки в принятой комбинации

Процедура поточного шифрования двоичной последовательности							Процедура поточного расшифрования, когда отсутствуют ошибки в принятой комбинации						
Передающая сторона							Приемная сторона						
c	*p*	Генератор ПСП					*c*	*p*	Генератор ПСП				
0	*1*	1	1	0	0		***0***	*1*	1	1	0	0	
1	*1*	0	1	1	0		***1***	*1*	0	1	1	0	
0	*1*	1	0	1	1		***0***	*1*	1	0	1	1	
0	*0*	0	1	0	1		***0***	*0*	0	1	0	1	
1	*0*	1	0	1	0		***1***	*0*	1	0	1	0	
0	*1*	1	1	0	1		***0***	*1*	1	1	0	1	
1	*0*	1	1	1	0		***1***	*0*	1	1	1	0	
0	*1*	1	1	1	1		***0***	*1*	1	1	1	1	
0	*0*	0	1	1	1		***0***	*0*	0	1	1	1	
1	*1*	0	0	1	1		***1***	*1*	0	0	1	1	
0	*0*	0	0	0	1		***0***	*0*	0	0	0	1	
0	*1*	1	0	0	0		***0***	*1*	1	0	0	0	
1	*1*	0	1	0	0		***1***	*1*	0	1	0	0	
0	*0*	0	0	1	0		***0***	*0*	0	0	1	0	

При отсутствии искажений в канале связи после расшифрования с использованием той же гаммы получается исходная последовательность.

На рисунке 2 приведена структура дешифратора поточного шифра, использующего ПСП, реализованного на основе многотактового кодового фильтра. Количество ячеек памяти должно равняться степени порождающего полинома (т.е. четырем), количество сумматоров по модулю два определяется числом ненулевых коэффициентов перед степенью *«x»* (т.е. один). Тогда схема кодирующего устройства примет следующий вид:

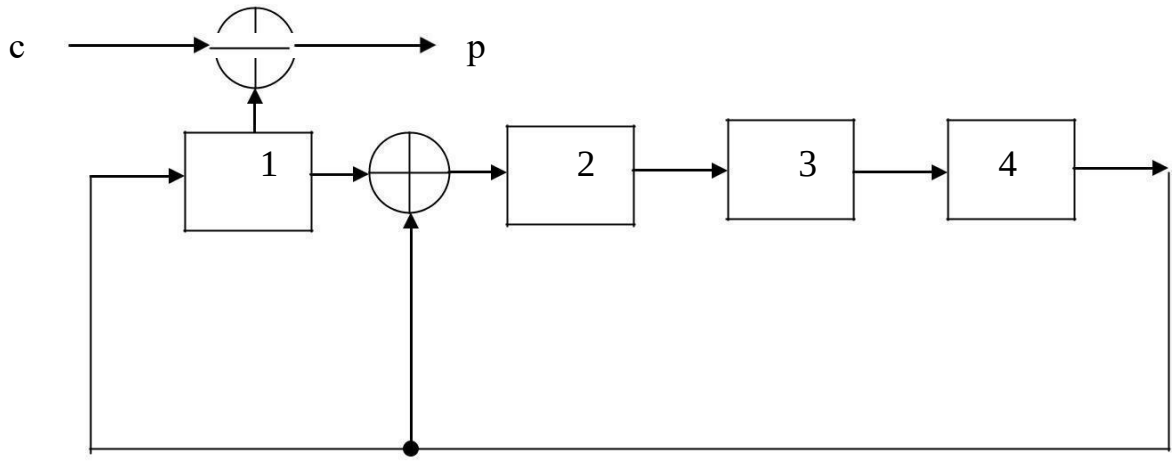


Рисунок 2 - Дешифратор поточного кода

В таблице 3 рассмотрена ситуация, когда при передаче зашифрованной последовательности был потерян четвертый бит, и вместо правильной последовательности к получателю пришла последовательность **0101010010010.**

Таблица 3 – Пример поточного шифрования и расшифрования двоичной последовательности, когда при передаче был потерян четвертый бит

Процедура поточного шифрования двоичной последовательности							Процедура поточного расшифрования, когда при передаче был потерян четвертый бит						
Передающая сторона							Приемная сторона						
c	*p*	Генератор ПСП					*c*	*p*	Генератор ПСП				
0	*1*	1	1	0	0		***0***	*1*	1	1	0	0	
1	*1*	0	1	1	0		***1***	*1*	0	1	1	0	
0	*1*	1	0	1	1		***0***	*1*	1	0	1	1	
0	*0*	0	1	0	1		***1***	*1*	0	1	0	1	
1	*0*	1	0	1	0		***0***	*1*	1	0	1	0	
0	*1*	1	1	0	1		***1***	*0*	1	1	0	1	
1	*0*	1	1	1	0		***0***	*1*	1	1	1	0	
0	*1*	1	1	1	1		***0***	*1*	1	1	1	1	
0	*0*	0	1	1	1		***1***	*1*	0	1	1	1	
1	*1*	0	0	1	1		***0***	*0*	0	0	1	1	
0	*0*	0	0	0	1		***0***	*0*	0	0	0	1	
0	*1*	1	0	0	0		***1***	*0*	1	0	0	0	
1	*1*	0	1	0	0		***0***	*0*	0	1	0	0	
0	*0*	0	0	1	0								

Видно, что после расшифрования всех битов, следующих после выпавшего, происходят искажения информации. В результате вместо битовой строки **0101010110** будет получена строка **1101110000.**

В таблице 4 рассмотрена ситуация, когда при передаче зашифрованной последовательности произошло искажение пятого (1 - 0) и восьмого (0 - 1) битов и вместо правильной последовательности к получателю пришла последовательность **01000011010010.** Видно, что после расшифрования вместо правильной строки будет получена строка **11101100010110** с искаженным пятым (0—1) и восьмым (1—0) битами.

Таблица 4 – Пример поточного шифрования и расшифрования двоичной последовательности, когда при передаче произошло искажение битов

Процедура поточного шифрования двоичной последовательности							Процедура поточного расшифрования, когда при передаче произошло искажение битов						
Передающая сторона							Приемная сторона						
c	*p*	Генератор ПСП					*c*	*p*	Генератор ПСП				
0	*1*	1	1	0	0		***0***	*1*	1	1	0	0	
1	*1*	0	1	1	0		***1***	*1*	0	1	1	0	
0	*1*	1	0	1	1		***0***	*1*	1	0	1	1	
0	*0*	0	1	0	1		***0***	*0*	0	1	0	1	
0	*0*	1	0	1	0		***0***	*1*	1	0	1	0	
0	*1*	1	1	0	1		***0***	*1*	1	1	0	1	
1	*0*	1	1	1	0		***1***	*0*	1	1	1	0	
1	*1*	1	1	1	1		***1***	*0*	1	1	1	1	
0	*0*	0	1	1	1		***0***	*0*	0	1	1	1	
1	*1*	0	0	1	1		***1***	*1*	0	0	1	1	
0	*0*	0	0	0	1		***0***	*0*	0	0	0	1	
0	*1*	1	0	0	0		***0***	*1*	1	0	0	0	
1	*1*	0	1	0	0		***1***	*1*	0	1	0	0	
0	*0*	0	0	1	0		***0***	*0*	0	0	1	0	

Методика и порядок выполнения работы

1. Изучить теоретический материал работы.
2. Провести исследование системы поточного шифрования.

Используя данные представленные в таблице 7 произвести разработку генератора ПСП и осуществить процедуры зашифрования и расшифрования.

Таблица 7 – Исходные данные

M	A0	A1	A2	A3	A4	A5	A6
4	1	0	0	1	1		
4	1	1	0	0	1		

M	A0	A1	A2	A3	A4	A5	A6
5	1	0	0	1	0	1	
5	1	0	1	0	0	1	
5	1	1	1	1	0	1	
5	1	1	0	1	1	1	
5	1	1	1	0	1	1	
6	1	0	0	0	0	1	1

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследования системы по своему варианту и ответы на контрольные вопросы.

Вопросы для защиты работы

1. Определение синхронного поточного шифрования.
2. Свойства синхронного поточного шифрования.
3. Основные способы построения М-последовательностей.

Лабораторная работа 7

ИССЛЕДОВАНИЕ ПОТОЧНОГО ШИФРОВАНИЯ СООБЩЕНИЙ В САМОСИНХРОНИЗУЮЩИХСЯ СИСТЕМАХ НА ОСНОВЕ МНОГОТАКТОВЫХ КОДОВЫХ ФИЛЬТРОВ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ РЕАЛИЗАЦИИ

Цель и содержание:

1. Углубить знания, по основам поточного шифрования .
2. Исследовать вопросы получения самосинхронизирующейся ПСП.

Формируемые компетенции

1. Способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5).
2. Способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9).
3. Способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).

Теоретическое обоснование

Различают гаммирование с *конечной* и *бесконечной* гаммами. В первом случае источником гаммы является аппаратный или программный ГПК. Примером бесконечной гаммы может служить последовательность цифр в десятичной записи числа 3,1415926...

В том случае, если множеством используемых для шифрования знаков является алфавит, отличный от бинарного ($Z_2 = \{0,1\}$), например алфавит Z_{33} - русские буквы и пробел, его символы и символы гаммы заменяются цифровыми эквивалентами, которые затем суммируются по модулю N:

$$c_i = (p_i + \tilde{\gamma}_i) \bmod N,\ i = 1,2,...m$$

где c_i , p_i ,γ_i - очередной i-й знак соответственно исходного сообщения, гаммы и шифротекста; N - число символов в алфавите; m - число знаков открытого текста.

В самосинхронизирующихся поточных шифрах элементы входной последовательности зашифровываются с учетом N предшествующих элементов (рисунок 1), которые принимают участие в формировании ключевой последовательности. В самосинхронизирующихся шифрах имеет место эффект размножения ошибок, в то же время в отличие от синхронных, восстановление синхронизации происходит автоматически через N элементов зашифрованной последовательности.

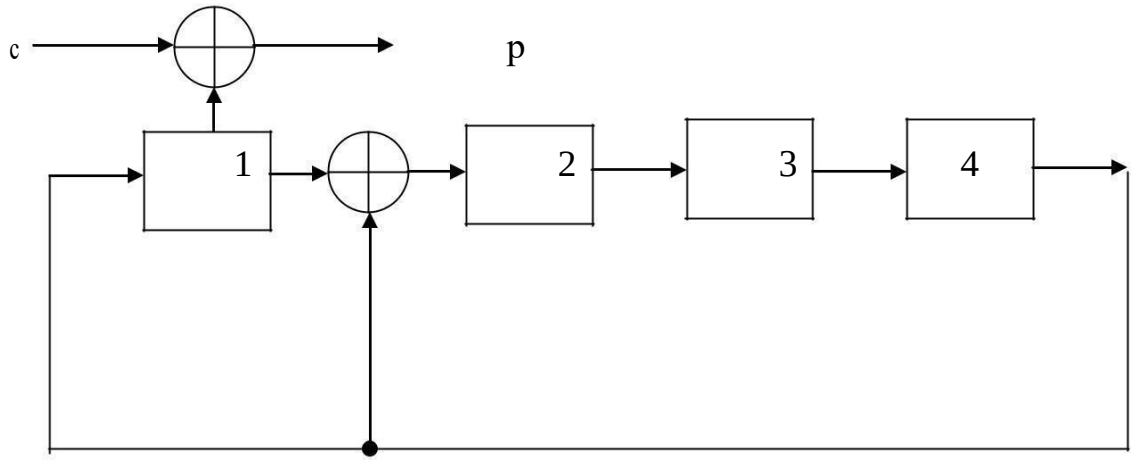


Рисунок 1 – Схема устройства зашифрования с ПСП Таблица

1 – Пример поточного шифрования и расшифрования двоичной последовательности, когда отсутствуют ошибки в принятой комбинации

Процедура поточного шифрования двоичной последовательности							Процедура поточного расшифрования, когда отсутствуют ошибки в принятой комбинации						
Передающая сторона							Приемная сторона						
c	*p*	Генератор ПСП					*c*	*p*	Генератор ПСП				
0	*1*	0	1	0	0		***0***	*1*	0	1	0	0	
1	*1*	1	0	1	0		***1***	*1*	1	0	1	0	
0	*1*	0	1	0	1		***0***	*1*	0	1	0	1	
1	*0*	1	0	1	0		***1***	*0*	1	0	1	0	
1	*0*	1	1	0	1		***1***	*0*	1	1	0	1	
0	*1*	0	1	1	0		***0***	*1*	0	1	1	0	
0	*1*	0	0	1	1		***0***	*1*	0	0	1	1	

1	*1*	1	0	0	1
1	*0*	1	1	0	0
1	*1*	1	1	1	0
1	*0*	1	1	1	1
1	*1*	1	1	1	1
0	*0*	0	1	1	1
0	*0*	0	0	1	1

1	*1*	1	0	0	1
1	*0*	1	1	0	0
1	*1*	1	1	1	0
1	*0*	1	1	1	1
1	*1*	1	1	1	1
0	*0*	0	1	1	1
0	*0*	0	0	1	1

В таблице 1 показан пример шифрования и расшифрования двоичной последовательности **11100111010100** с использованием 4-разрядного *LFSR* при начальном состоянии, равном 1001 Зашифрованная последовательность имеет вид **01011001111100.** При отсутствии искажений в канале после расшифрования получается исходная последовательность. В таблице 2 рассмотрена ситуация, когда при передаче зашифрованной последовательности был потерян третий, равный нулю бит и вместо правильной последовательности к получателю пришла последовательность **01111001111100.**

Видно, что после расшифрования может произойти искажение не более 4 бит (в общем случае не более *N),* следующих после выпавшего символа. В рассмотренном примере вместо 4-битовой строки 0011 будет получена строка 0010. Все остальные биты будут приняты без искажений

Таблица 2 – Пример поточного шифрования и расшифрования двоичной последовательности, когда при передаче был потерян третий бит

Процедура поточного шифрования двоичной последовательности							Процедура поточного расшифрования, когда при передаче был потерян третий бит						
Передающая сторона							Приемная сторона						
c	*p*	Генератор ПСП					*c*	*p*	Генератор ПСП				
0	*1*	0	1	0	0		***0***	*1*	0	1	0	0	
1	*1*	1	0	1	0		***1***	*1*	1	0	1	0	
0	*1*	0	1	0	1		***1***	*0*	0	1	0	1	
1	*0*	1	0	1	0		***1***	*0*	1	0	1	0	
1	*0*	1	1	0	1		***0***	*1*	1	1	0	1	
0	*1*	0	1	1	0		***0***	*0*	0	1	1	0	
0	*1*	0	0	1	1		***1***	*1*	0	0	1	1	
1	*1*	1	0	0	1		***1***	*0*	1	0	0	1	
1	*0*	1	1	0	0		***1***	*1*	1	1	0	0	
1	*1*	1	1	1	0		***1***	*0*	1	1	1	0	
1	*0*	1	1	1	1		***1***	*1*	1	1	1	1	
1	*1*	1	1	1	1		***0***	*0*	1	1	1	1	

Процедура поточного шифрования двоичной последовательности							Процедура поточного расшифрования, когда при передаче был потерян третий бит						
Передающая сторона							Приемная сторона						
c	*p*	Генератор ПСП					*c*	*p*	Генератор ПСП				
0	*0*	0	1	1	1		***0***	*0*	0	1	1	1	
0	*0*	0	0	1	1								

В таблице 3 рассмотрена ситуация, когда при передаче зашифрованной последовательности произошло искажение первого (0 - 1) бита и вместо правильной последовательности пришла последовательность 11011001111100. Видно, что после расшифрования помимо неправильно принятого бита, могут исказиться еще не более 4 последующих. В примере будет неправильно принят первый бит и вместо правильной 4-битовой строки 1100 будет получено - 1111.

Таблица 3 – Пример поточного шифрования и расшифрования, двоичной последовательности, когда при передаче произошло искажение битов

Процедура поточного шифрования двоичной последовательности							Процедура поточного расшифрования, когда при передаче произошло искажение битов						
Передающая сторона							Приемная сторона						
c	*p*	Генератор ПСП					*c*	*p*	Генератор ПСП				
1	*1*	0	1	0	0		***1***	*0*	0	1	0	0	
1	*1*	1	0	1	0		***1***	*1*	1	0	1	0	
0	*1*	0	1	0	1		***0***	*1*	0	1	0	1	
1	*0*	1	0	1	0		***1***	*1*	1	0	1	0	
1	*0*	1	1	0	1		***1***	*1*	1	1	0	1	
0	*1*	0	1	1	0		***0***	*1*	0	1	1	0	
0	*1*	0	0	1	1		***0***	*1*	0	0	1	1	
1	*1*	1	0	0	1		***1***	*1*	1	0	0	1	
1	*0*	1	1	0	0		***1***	*0*	1	1	0	0	
1	*1*	1	1	1	0		***1***	*1*	1	1	1	0	
1	*0*	1	1	1	1		***1***	*0*	1	1	1	1	
1	*1*	1	1	1	1		***1***	*1*	1	1	1	1	
0	*0*	0	1	1	1		***0***	*0*	0	1	1	1	
0	*0*	0	0	1	1		***0***	*0*	0	0	1	1	

Методика и порядок выполнения работы

1. Изучить теоретический материал работы.
2. Провести исследование системы с самосинхронизирующейся ПСП.

Используя данные представленные в таблице 7 произвести разработку генератора ПСП и осуществить процедуры зашифрования и расшифрования (ис-

ходное заполнение генератора произвольное).

Таблица 7 – Исходные данные для шифрования и расшифрования сообщений в самосинхронизующихся системах

M	A0	A1	A2	A3	A4	A5	A6
4	1	0	0	1	1		
4	1	1	0	0	1		
5	1	0	0	1	0	1	
5	1	0	1	0	0	1	
5	1	1	1	1	0	1	
5	1	1	0	1	1	1	
5	1	1	1	0	1	1	
6	1	0	0	0	0	1	1

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследования систем по своему варианту и ответы на контрольные вопросы.

Вопросы для защиты работы

1. Определение самосинхронизирующихся поточных шифров.
2. Свойства самосинхронизирующихся поточных шифров.

Лабораторная работа 8

ИССЛЕДОВАНИЕ ПОТОЧНОГО ШИФРОВАНИЯ СООБЩЕНИЙ В СИНХРОНИЗУЮЩИХСЯ СИСТЕМАХ, ПОСТРОЕННЫХ НА ОСНОВЕ ГЕНЕРАТОРОВ ФИББОНАЧИ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ РЕАЛИЗАЦИИ

Цель и содержание:

1. Углубить знания, по основам поточного шифрования .
2. Исследовать вопросы получения синхронного ПСП.

Формируемые компетенции

1. Способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2).

2. Способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5).

Теоретическое обоснование

Шифр Вернама можно считать исторически первым поточным шифром. Так как поточные шифры, в отличие от блочных, осуществляют поэлементное шифрование потока данных без задержки в криптосистеме, их важнейшим достоинством является высокая скорость преобразования, соизмеримая со скоростью поступления входной информации. Таким образом, обеспечивается шифрование практически в реальном масштабе времени вне зависимости от объема и разрядности потока преобразуемых данных.

Простейшие устройства синхронного и самосинхронизирующегося шифрования с использованием ГПК, реализованного на основе *N*-разрядного *регистра сдвига с линейной обратной связью* - *LFSR* (Linear Feedback Shift Register), называются *скремблерами*, а сам процесс преобразования – скремблированием.

В синхронных поточных шифрах гамма формируется независимо от

входной последовательности, каждый элемент (бит, символ, байт и т. п.) которой таким образом шифруется независимо от других элементов. В синхронных поточных шифрах отсутствует эффект размножения ошибок, т. е. число искаженных элементов в расшифрованной последовательности равно числу искаженных элементов зашифрованной последовательности, пришедшей из канала связи.

Вставка или выпадение элемента зашифрованной последовательности недопустимы, так как из-за нарушения синхронизации это приведет к неправильному расшифрованию всех последующих элементов. Синхронное поточное шифрование с использованием LFSR показано на рисунке 1.

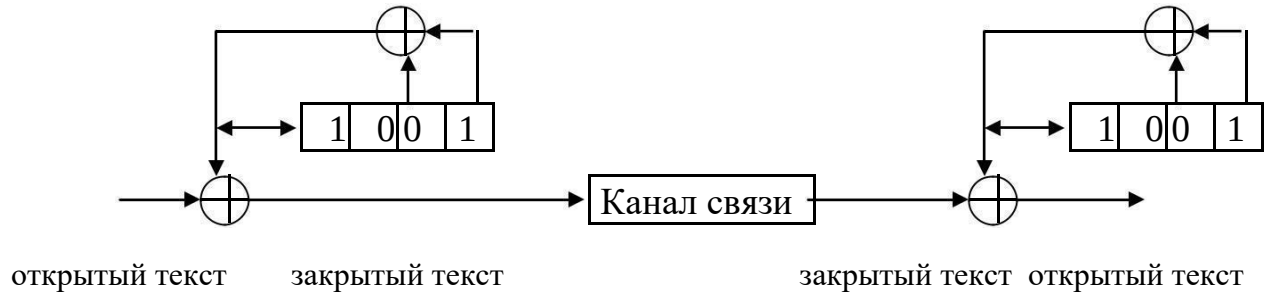


Рисунок 1 – Синхронное поточное шифрование

В таблице 1 показан пример поточного шифрования и расшифрования двоичной последовательности *11100101010110* с использованием гаммы формируемой 4-разрядным *LFSR* при начальном состоянии **1001**. Зашифрованная последовательность имеет вид ***01001010010010.***

При отсутствии искажений в канале связи после расшифрования с использованием той же гаммы получается исходная последовательность

Таблица 1 – Пример поточного шифрования и расшифрования двоичной последовательности, когда отсутствуют ошибки в принятой комбинации

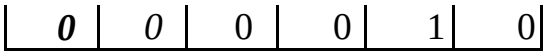
Процедура поточного шифрования двоичной последовательности							Процедура поточного расшифрования, когда отсутствуют ошибки в принятой комбинации						
Передающая сторона							Приемная сторона						
c	*p*	Генератор ПСП					*c*	*p*	Генератор ПСП				
0	*1*	1	1	0	0		***0***	*1*	1	1	0	0	

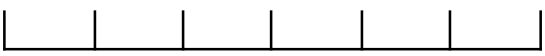
Процедура поточного шифрования двоичной последовательности							Процедура поточного расшифрования, когда отсутствуют ошибки в принятой комбинации						
Передающая сторона							Приемная сторона						
c	*p*	Генератор ПСП					*c*	*p*	Генератор ПСП				
1	*1*	0	1	1	0		***1***	*1*	0	1	1	0	
0	*1*	1	0	1	1		***0***	*1*	1	0	1	1	
0	*0*	0	1	0	1		***0***	*0*	0	1	0	1	
1	*0*	1	0	1	0		***1***	*0*	1	0	1	0	
0	*1*	1	1	0	1		***0***	*1*	1	1	0	1	
1	*0*	1	1	1	0		***1***	*0*	1	1	1	0	
0	*1*	1	1	1	1		***0***	*1*	1	1	1	1	
0	*0*	0	1	1	1		***0***	*0*	0	1	1	1	
1	*1*	0	0	1	1		***1***	*1*	0	0	1	1	
0	*0*	0	0	0	1		***0***	*0*	0	0	0	1	
0	*1*	1	0	0	0		***0***	*1*	1	0	0	0	
1	*1*	0	1	0	0		***1***	*1*	0	1	0	0	
0	*0*	0	0	1	0		***0***	*0*	0	0	1	0	

В таблице 2 рассмотрена ситуация, когда при передаче зашифрованной последовательности был потерян четвертый бит, и вместо правильной последовательности к получателю пришла последовательность **0101010010010.**

Таблица 2 – Пример поточного шифрования и расшифрования двоичной последовательности, когда при передаче был потерян четвертый бит

Процедура поточного шифрования двоичной последовательности							Процедура поточного расшифрования, когда при передаче был потерян четвертый бит						
Передающая сторона							Приемная сторона						
c	*p*	Генератор ПСП					*c*	*p*	Генератор ПСП				
0	*1*	1	1	0	0		***0***	*1*	1	1	0	0	
1	*1*	0	1	1	0		***1***	*1*	0	1	1	0	
0	*1*	1	0	1	1		***0***	*1*	1	0	1	1	
0	*0*	0	1	0	1		***1***	*1*	0	1	0	1	
1	*0*	1	0	1	0		***0***	*1*	1	0	1	0	
0	*1*	1	1	0	1		***1***	*0*	1	1	0	1	
1	*0*	1	1	1	0		***0***	*1*	1	1	1	0	
0	*1*	1	1	1	1		***0***	*1*	1	1	1	1	
0	*0*	0	1	1	1		***1***	*1*	0	1	1	1	
1	*1*	0	0	1	1		***0***	*0*	0	0	1	1	
0	*0*	0	0	0	1		***0***	*0*	0	0	0	1	
0	*1*	1	0	0	0		***1***	*0*	1	0	0	0	
1	*1*	0	1	0	0		***0***	*0*	0	1	0	0	


0 0 0 0 1 0



Видно, что после расшифрования всех битов, следующих после выпавшего, происходят искажения информации. В результате вместо битовой строки **0101010110** будет получена строка **1101110000.**

В таблице 3 рассмотрена ситуация, когда при передаче зашифрованной последовательности произошло искажение пятого (1 - 0) и восьмого (0 - 1) битов и вместо правильной последовательности к получателю пришла последовательность **01000011010010.** Видно, что после расшифрования вместо правильной строки будет получена строка **11101100010110** с искаженным пятым (0—1) и восьмым (1—0) битами.

Таблица 3 – Пример поточного шифрования и расшифрования двоичной последовательности, когда при передаче произошло искажение битов

Процедура поточного шифрования двоичной последовательности							Процедура поточного расшифрования, когда при передаче произошло искажение битов						
Передающая сторона							Приемная сторона						
c	*p*	Генератор ПСП					*c*	*p*	Генератор ПСП				
0	*1*	1	1	0	0		***0***	*1*	1	1	0	0	
1	*1*	0	1	1	0		***1***	*1*	0	1	1	0	
0	*1*	1	0	1	1		***0***	*1*	1	0	1	1	
0	*0*	0	1	0	1		***0***	*0*	0	1	0	1	
0	*0*	1	0	1	0		***0***	*1*	1	0	1	0	
0	*1*	1	1	0	1		***0***	*1*	1	1	0	1	
1	*0*	1	1	1	0		***1***	*0*	1	1	1	0	
1	*1*	1	1	1	1		***1***	*0*	1	1	1	1	
0	*0*	0	1	1	1		***0***	*0*	0	1	1	1	
1	*1*	0	0	1	1		***1***	*1*	0	0	1	1	
0	*0*	0	0	0	1		***0***	*0*	0	0	0	1	
0	*1*	1	0	0	0		***0***	*1*	1	0	0	0	
1	*1*	0	1	0	0		***1***	*1*	0	1	0	0	
0	*0*	0	0	1	0		***0***	*0*	0	0	1	0	

Методика и порядок выполнения работы

3. Изучить теоретический материал работы.
4. Провести исследование системы поточного шифрования.

Используя данные представленные в таблице 7 произвести разработку генератора ПСП и осуществить процедуры зашифрования и расшифрования.

Таблица 7 – Исходные данные

M	A0	A1	A2	A3	A4	A5	A6
4	1	0	0	1	1		
4	1	1	0	0	1		
5	1	0	0	1	0	1	
5	1	0	1	0	0	1	
5	1	1	1	1	0	1	
5	1	1	0	1	1	1	
5	1	1	1	0	1	1	
6	1	0	0	0	0	1	1

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследования системы по своему варианту и ответы на контрольные вопросы.

Вопросы для защиты работы

1. Определение синхронного поточного шифрования.
2. Свойства синхронного поточного шифрования.
3. Основные способы построения М-последовательностей.

Лабораторная работа 9

ИССЛЕДОВАНИЕ ПОТОЧНОГО ШИФРОВАНИЯ СООБЩЕНИЙ В САМОСИНХРОНИЗУЮЩИХСЯ СИСТЕМАХ НА ОСНОВЕ ГЕНЕРАТОРОВ ТИПА ФИБОНАЧЧИ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ РЕАЛИЗАЦИИ Цель и содержание:

1. Углубить знания, по основам поточного шифрования .
2. Исследовать вопросы получения самосинхронизирующейся ПСП.

Формируемые компетенции

1. Способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2).

2. Способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5).

3. Способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9).

4. Способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).

Теоретическое обоснование

В самосинхронизирующихся поточных шифрах элементы входной последовательности зашифровываются с учетом N предшествующих элементов (рисунок 1), которые принимают участие в формировании ключевой последовательности. В самосинхронизирующихся шифрах имеет место эффект размножения ошибок, в то же время в отличие от синхронных, восстановление синхронизации происходит автоматически через N элементов зашифрованной последовательности.

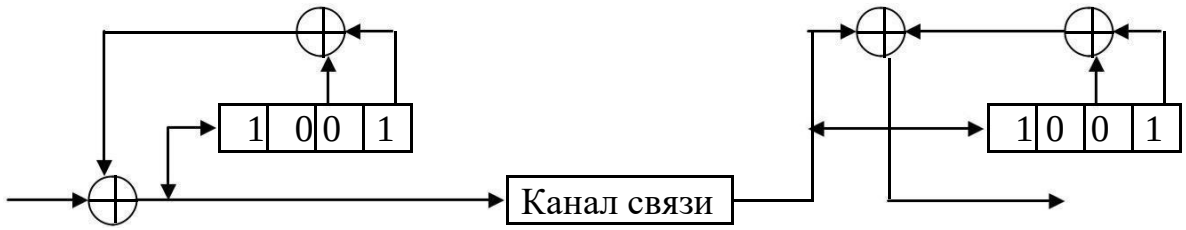


Рисунок 1 – Схема устройства зашифрования с ПСП Таблица 1 – Пример поточного шифрования и расшифрования двоичной последовательности, когда отсутствуют ошибки в принятой комбинации

Процедура поточного шифрования двоичной последовательности							Процедура поточного расшифрования, когда отсутствуют ошибки в принятой комбинации						
Передающая сторона							Приемная сторона						
c	*p*	Генератор ПСП					*c*	*p*	Генератор ПСП				
0	*1*	0	1	0	0		***0***	*1*	0	1	0	0	
1	*1*	1	0	1	0		***1***	*1*	1	0	1	0	
0	*1*	0	1	0	1		***0***	*1*	0	1	0	1	
1	*0*	1	0	1	0		***1***	*0*	1	0	1	0	
1	*0*	1	1	0	1		***1***	*0*	1	1	0	1	
0	*1*	0	1	1	0		***0***	*1*	0	1	1	0	
0	*1*	0	0	1	1		***0***	*1*	0	0	1	1	
1	*1*	1	0	0	1		***1***	*1*	1	0	0	1	
1	*0*	1	1	0	0		***1***	*0*	1	1	0	0	
1	*1*	1	1	1	0		***1***	*1*	1	1	1	0	
1	*0*	1	1	1	1		***1***	*0*	1	1	1	1	
1	*1*	1	1	1	1		***1***	*1*	1	1	1	1	
0	*0*	0	1	1	1		***0***	*0*	0	1	1	1	
0	*0*	0	0	1	1		***0***	*0*	0	0	1	1	

В таблице 1 показан пример шифрования и расшифрования двоичной последовательности **11100111010100** с использованием 4-разрядного *LFSR* при начальном состоянии, равном 1001 Зашифрованная последовательность имеет вид **01011001111100.** При отсутствии искажений в канале после расшифрования получается исходная последовательность. В таблице 2 рассмотрена ситуация, когда при передаче зашифрованной последовательности был потерян третий, равный нулю бит и вместо правильной последовательности к получателю пришла последовательность **01111001111100.**

Видно, что после расшифрования может произойти искажение не более 4 бит (в общем случае не более *N)*, следующих после выпавшего символа. В рассмотренном примере вместо 4-битовой строки 0011 будет получена строка 0010. Все остальные биты будут приняты без искажений

Таблица 2 – Пример поточного шифрования и расшифрования двоичной последовательности, когда при передаче был потерян третий бит

Процедура поточного шифрования двоичной последовательности							Процедура поточного расшифрования, когда при передаче был потерян третий бит						
Передающая сторона							Приемная сторона						
c	*p*	Генератор ПСП					*c*	*p*	Генератор ПСП				
0	*1*	0	1	0	0		***0***	*1*	0	1	0	0	
1	*1*	1	0	1	0		***1***	*1*	1	0	1	0	
0	*1*	0	1	0	1		***1***	*0*	0	1	0	1	
1	*0*	1	0	1	0		***1***	*0*	1	0	1	0	
1	*0*	1	1	0	1		***0***	*1*	1	1	0	1	
0	*1*	0	1	1	0		***0***	*0*	0	1	1	0	
0	*1*	0	0	1	1		***1***	*1*	0	0	1	1	
1	*1*	1	0	0	1		***1***	*0*	1	0	0	1	
1	*0*	1	1	0	0		***1***	*1*	1	1	0	0	
1	*1*	1	1	1	0		***1***	*0*	1	1	1	0	
1	*0*	1	1	1	1		***1***	*1*	1	1	1	1	
1	*1*	1	1	1	1		***0***	*0*	1	1	1	1	
0	*0*	0	1	1	1		***0***	*0*	0	1	1	1	
0	*0*	0	0	1	1								

В таблице 3 рассмотрена ситуация, когда при передаче зашифрованной последовательности произошло искажение первого (0 - 1) бита и вместо правильной последовательности пришла последовательность 11011001111100. Видно, что после расшифрования помимо неправильно принятого бита, могут исказиться еще не более 4 последующих. В примере будет неправильно принят первый бит и вместо правильной 4-битовой строки 1100 будет получено - 1111.

Таблица 3 – Пример поточного шифрования и расшифрования, двоичной последовательности, когда при передаче произошло искажение битов

Процедура поточного шифрования двоичной последовательности							Процедура поточного расшифрования, когда при передаче произошло искажение битов						
Передающая сторона							Приемная сторона						
c	*p*	Генератор ПСП					*c*	*p*	Генератор ПСП				
1	*1*	0	1	0	0		***1***	*0*	0	1	0	0	

Процедура поточного шифрования двоичной последовательности							Процедура поточного расшифрования, когда при передаче произошло искажение битов						
Передающая сторона							Приемная сторона						
c	*p*	Генератор ПСП					*c*	*p*	Генератор ПСП				
1	*1*	1	0	1	0		***1***	*1*	1	0	1	0	
0	*1*	0	1	0	1		***0***	*1*	0	1	0	1	
1	*0*	1	0	1	0		***1***	*1*	1	0	1	0	
1	*0*	1	1	0	1		***1***	*1*	1	1	0	1	
0	*1*	0	1	1	0		***0***	*1*	0	1	1	0	
0	*1*	0	0	1	1		***0***	*1*	0	0	1	1	
1	*1*	1	0	0	1		***1***	*1*	1	0	0	1	
1	*0*	1	1	0	0		***1***	*0*	1	1	0	0	
1	*1*	1	1	1	0		***1***	*1*	1	1	1	0	
1	*0*	1	1	1	1		***1***	*0*	1	1	1	1	
1	*1*	1	1	1	1		***1***	*1*	1	1	1	1	
0	*0*	0	1	1	1		***0***	*0*	0	1	1	1	
0	*0*	0	0	1	1		***0***	*0*	0	0	1	1	

Методика и порядок выполнения работы

3. Изучить теоретический материал работы.
4. Провести исследование системы с самосинхронизирующейся ПСП.

Используя данные представленные в таблице 7 произвести разработку генератора ПСП и осуществить процедуры зашифрования и расшифрования (исходное заполнение генератора произвольное).

Таблица 7 – Исходные данные для шифрования и расшифрования сообщений в самосинхронизующихся системах

M	A0	A1	A2	A3	A4	A5	A6
4	1	0	0	1	1		
4	1	1	0	0	1		
5	1	0	0	1	0	1	
5	1	0	1	0	0	1	
5	1	1	1	1	0	1	
5	1	1	0	1	1	1	
5	1	1	1	0	1	1	
6	1	0	0	0	0	1	1

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследования систем по своему варианту и ответы на контрольные вопросы.

Вопросы для защиты работы

3. Определение самосинхронизирующихся поточных шифров.
4. Свойства самосинхронизирующихся поточных шифров.

Семестр 6

Лабораторная работа 1

ИССЛЕДОВАНИЕ ПРОЦЕССА АССИМЕТРИЧНОГО ШИФРОВАНИЯ БЕЗ ПЕРЕДАЧИ КЛЮЧА

Цель и содержание:

1. Углубить знания, по основам шифрования без передачи ключа.
2. Исследовать основные характеристики алгоритма шифрования.

Формируемые компетенции

1. Способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9).

2. Способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).

Теоретическое обоснование

Пусть стороны *A* и *B* решили организовать секретную передачу информации между собой. Для этого выбирается большое число *p*, такое, что *p-1* хорошо разлагается на простые множители.

Далее абоненты независимо друг от друга осуществляют выбор ключей *a* и *b,* которые являются первыми секретными, согласно следующих правил:

$$1 < a < p - 2;\ 1 < b < p - 2\ .$$

Затем стороны производят вычисления вторых ключей, которые также являются секретными, согласно условия:

$$A : a \to \alpha \quad \alpha \cdot a \equiv 1 mod\ \varphi(p)$$

$$B : b \to \beta \quad \beta \cdot b \equiv 1 mod\ \varphi(p)\ ,$$

где $\varphi(p)$ – функция Эйлера.

1. Пусть абонент *A* решает передать сообщение *n*. Тогда сторона *A* зашифровывает это сообщение своим первым закрытым ключом:

$$n = n^{a} \bmod p$$
$$1$$

Полученное сообщение отправляется на сторону В.

2. Тогда сторона *B* зашифровывает принятое сообщение своим первым закрытым ключом:

$$n = n^{b} \bmod p$$
$$2 \quad 1$$

Полученное сообщение отправляется на сторону *B*.

3. Тогда сторона *A* зашифровывает принятое сообщение своим вторым закрытым ключом:

$$n_3 = n_2^{\alpha} \bmod p$$

Полученное сообщение отправляется на сторону *B*.

4. Тогда сторона *B* зашифровывает принятое сообщение своим первым закрытым ключом:

$$n = n^{\beta} \bmod p$$
$$3$$

Полученное сообщение отправлялось на сторону *B* от абонента *A*.

Основным недостатком рассмотренной системы криптозащиты является неоднократная передача информации от одного пользователя к другому, что в конечном итоге приводит к низкой скорости передачи информации. Кроме того, довольно сложно подобрать число *p*, чтобы обеспечить необходимую надёжность защиты.

Аппаратура и материалы

1. Компьютерный класс общего назначения с конфигурацией ПК не хуже рекомендованной для ОС Windows 2000\XP.
2. Операционная система Windows 2000\XP.

Методика и порядок выполнения работы

1. Изучить теоретический материал работы.
2. Провести исследование системы шифрования без передачи ключей.

Передаваемое сообщение m и кодирующее число p представлены в таблице 1.

Таблица 1 – Задание для исследования системы шифрования

Вариант	Кодирующее число p	Сообщение m
1	23	17

Вариант	Кодирующее число p	Сообщение m
2	29	18
3	31	19
4	37	20
5	41	21
6	43	22
7	47	23
8	53	24
9	23	16
10	29	15
11	31	14
12	37	13
13	41	28
14	43	29
15	47	30
16	53	31

Студенты самостоятельно выбирают значение ключей для обеих сторон (A и B) и исследуют процесс зашифрования и расшифрования сообщения.

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать исследование процесса зашифрования и расшифрования сообщения без передачи ключей по своему варианту и ответы на вопросы.

Вопросы для защиты работы

1. Принципы построения алгоритма шифрования без передачи ключей.
2. Основные характеристики алгоритма шифрования .
3. Достоинства и недостатки шифрования без передачи ключа.

Лабораторная работа 2

ИССЛЕДОВАНИЕ ПРОЦЕССА ШИФРОВАНИЯ RSA С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ РЕАЛИЗАЦИИ

Цель и содержание:

1. Углубить знания, по основам шифрования с использованием RSA.
2. Исследовать основные характеристики алгоритма шифрования.

Формируемые компетенции

1. Способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2).

2. Способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5).

3. Способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).

Теоретическое обоснование

Алгоритм асимметричного шифрования RSA является одним из первых полноценных алгоритмов с открытым ключом. Он был разработан Роном Риверсом, Ади Шамиром и Леонардо Адлеманом в 1976 году.

Суть данного алгоритма шифрования состоит в следующем. Пусть абоненты A и B решили наладить между собой секретную переписку с открытым ключом. Тогда каждый из них, независимо от другого, выбирает 2 больших простых числа, находит их произведению, функцию Эйлера $\varphi(P)$ от произведения, этих чисел, а затем выбирает случайное число согласно алгоритма:

$$A :\Rightarrow p_1 , p_2 ; P_1 = p_1 \cdot p_2 ;\Rightarrow \varphi(P_1) = (p_1 - 1)(p_2 - 1);\Rightarrow 0 < a < \varphi(P_1),(a,\varphi(P_1)) = 1;$$

$$B :\Rightarrow q_1 ,q_2 ; Q_1 = q_1 \cdot q_2 ;\Rightarrow \varphi(Q_1) = (q_1 - 1)(q_2 - 1);\Rightarrow 0 < b < \varphi(Q_1),(b,\varphi(Q_1)) = 1.$$

Затем открытые ключи a и $P1$, а так же b и $Q1$ печатаются в телефонной книге.

Каждый из абонентов независимо от другого выбирает свой секретный ключ согласно условия

$$A: \alpha \Rightarrow a \cdot \alpha \equiv 1 \bmod \varphi(P_1);$$

$$B: \beta \Rightarrow b \cdot \beta \equiv 1 \bmod \varphi(Q_1).$$

Пусть абонент *A* решает послать сообщение *m* абоненту *B* и пусть $0 < m < P_1$, иначе текст делят на блоки.

1. Абонент *A* шифрует сообщение m открытым ключом абонента *B*, который есть телефонной книге, и находит:

$$m_1 \equiv m^b \pmod{Q_1}$$

2. Абонент *B* расшифровывает сообщение своим секретным ключом β:

$$m \equiv m_1^{\beta} \pmod{Q_1}$$

Пусть абонент *B* решает послать сообщение *n* абоненту *A* и пусть $0 < n < Q_1$, иначе текст делят на блоки.

1. Абонент *B* шифрует сообщение *m* открытым ключом абонента *A*, который есть телефонной книге, и находит:

$$n_1 \equiv a_n \pmod{P_1}$$

2. Абонент *A* расшифровывает сообщение секретным ключом α:

$$n \equiv n_1^{\alpha} \pmod{P_1}$$

Аппаратура и материалы

1. Компьютерный класс общего назначения с конфигурацией ПК не хуже рекомендованной для ОС Windows 2000\XP.
2. Операционная система Windows 2000\XP.

Методика и порядок выполнения работы

3. Изучить теоретический материал работы.
4. Провести исследование системы RSA.

Передаваемое сообщение *m* и кодирующее число *p* представлены в таблице 1

Таблица 1 – Задание для исследования системы RSA

Вариант	Кодирующее число	Кодирующее число	Сообщение *m*
1	23	7	17

Вариант	Кодирующее число	Кодирующее число	Сообщение *m*
2	29	13	18
3	31	11	19
4	37	17	20
5	41	19	21
6	43	5	22
7	47	7	23
8	53	11	24
9	23	13	16
10	29	17	15
11	31	23	14
12	37	29	13
13	41	11	28
14	43	13	29
15	47	17	30
16	53	5	31

Студенты самостоятельно выбирают значение ключей для обеих сторон (*A* и *B*) и исследуют процесс зашифрования и расшифрования сообщения.

Содержание отчета и его форма

Отчет по лабораторной работе, тетради, должен содержать процесс исследования системы RSA по своему варианту и ответы на вопросы.

Вопросы для защиты работы

1. Основные принципы построения алгоритма RSA.
2. Основные характеристики алгоритма RSA.
3. Достоинства и недостатки симметричного и RSA шифрования.

Лабораторная работа 3

ИССЛЕДОВАНИЕ ПРОЦЕССА ШИФРОВАНИЯ ЭЛЬ-ГАМАЛЯ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ РЕАЛИЗАЦИИ

Цель и содержание:

1. Углубить знания, по основам асимметричного шифрования.
2. Исследовать основы алгоритма шифрования Эль-Гамаля.

Формируемые компетенции

1. Способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2).

2. Способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5).

3. Способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9).

4. Способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).

Теоретическое обоснование

Криптосистема Эль-Гамаля была преложена в 1985 году. Она используется для получения, как для цифровой подписи, так и для шифрования. Криптостойкость ассиметричного алгоритма шифрования определяется трудоемкостью вычисления дискретного логарифма в конечном поле Галуа. Для генерации пары ключей выбирается простое число p и два случайных числа g и x, причем $g<p$, $x<p$. Затем вычисляется значение:

$$y = g^{x} \bmod p$$

Открытым ключом являются:

1. p - простое число (может быть общим для группы абонентов).

2. $g < p$ (может быть общим для группы абонентов).

3. $y=g^X \bmod p$.

Секретным ключом является значение: $x < p$.

Процесс шифрования осуществляется следующим образом. Для шифрования сообщения M выбирается случайное число k, такое, что

$$НОД\ (k,(p-1))=1.$$

Затем вычисляется первая часть шифрования:

$$a=g^k \bmod p,$$

и вторая часть шифрования:

$$b = y^k \cdot M \bmod p$$

Пара (a, b) называется шифротекстом. Следует отметить, шифротекст имеет длину в два раза больше длины исходного текста. Полученная пара передается на противоположную сторону.

Процесс расшифрования осуществляется следующим образом:

$$M = \overline{a}^{b}_{x} \bmod p$$

Рассмотрим процесс зашифрования текста с использованием ассиметричного алгоритма Эль-Гамаля. Пусть в качестве ключей выбрали $p=11$ и $g=2$, $(2<11)$. Определяем секретный ключ $x=8$, $(8<11)$. Тогда вычислением значения,

$$y = 2^8 \bmod 11 = 3$$

В справочнике печатается: *пользователь A* $y=2, p=11, y=3$.

Пусть необходимо передать тест $M=5$.

Выбираем число $k=9$, так как $НОД\ (9,10)=1$, $k(p-1)=11-1=10$.

Определяем значение первой части шифра:

$$a = g^k \bmod 11 = 2^9 \bmod 11 = 6$$

Определяем вторую часть шифра:

$$b = y^k M \bmod p = 3^9 \cdot 5 \bmod 11 = 27 \bmod 11 = 5$$

Зашифрованное сообщение в виде пары (6,9) передается на другую сторону к пользователю B. Затем проводится процесс дешифрования. Тогда:

$$M = 6^{9}{}_{8} \bmod 11 = 9^{1} \bmod 11 = 5$$

Аппаратура и материалы

1. Компьютерный класс общего назначения с конфигурацией ПК не хуже рекомендованной для ОС Windows 2000\XP.

2. Операционная система Windows 2000\XP.

Методика и порядок выполнения работы

1. Изучить теоретический материал работы.

2. Провести исследование криптосистемы Эль-Гамаля.

Передаваемое сообщение *m* открытые ключи *p*, *g*, и секретный ключ представлены в таблице 1.

Таблица 1 – Задание для исследования криптосистемы Эль-Гамаля

Вариант	Открытый ключ		Закрытый ключ, *x*	Сообщение *m*
	p	*g*		
1	23	10	11	17
2	29	11	12	23
3	23	12	13	19
4	31	13	14	20
5	17	14	15	15
6	19	15	16	18
7	37	7	10	30
8	41	6	11	24
9	23	12	13	21
10	29	14	15	23
11	23	15	14	17
12	31	10	10	14
13	17	12	11	13
14	19	17	12	15
15	37	18	13	21
16	41	9	20	11

Студенты самостоятельно выбирают значение *k* согласно условию и исследуют процедуру зашифрования и расшифрования согласно варианту.

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследования криптосистемы Эль-Гамаля по

своему варианту и ответы на контрольные вопросы.

Вопросы для защиты работы

1. Основные принципы построения алгоритма Эль-Гамаля.
2. Основные характеристики алгоритма Эль-Гамаля.
3. Достоинства и недостатки алгоритма шифрования Эль-Гамаля.

Лабораторная работа 4

ИССЛЕДОВАНИЕ ПРОЦЕССА ПОСТРОЕНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ НА ОСНОВЕ АЛГОРИТМА RSA С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ РЕАЛИЗАЦИИ

Цель и содержание:

1. Углубить знания, по основам использования цифровой подписи асимметричных системах шифрования.

2. Исследовать основные характеристики алгоритма построения электронной подписи на основе RSA.

Формируемые компетенции:

1. Способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2).

2. Способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5).

3. Способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9).

4. Способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).

Теоретическое обоснование

Идея использования систем шифрования с открытыми ключами для построения систем цифровой подписи как бы заложена в постановке задачи. Действительно, пусть имеется пара преобразований *(E, D)*, первое из которых зависит от открытого ключа, а второе – от секретного. Для того чтобы вычислить цифровую подпись *S* для сообщения, владелец секретного ключа может приме-

нить к сообщению *M* второе преобразование *D: S = D(M).* В таком случае вычислить подпись может только владелец секретного ключа, в то время как проверить равенство *E(S) = M* может каждый. Основными требованиями к преобразованиям *E* и *D* являются:

– выполнение равенства *M = E(D(M))* для всех сообщений *M;*

– невозможность вычисления значения *D(M)* для заданного сообщения

M без знания секретного ключа.

Отличительной особенностью предложенного способа построения цифровой подписи является возможность отказаться от передачи самого подписываемого сообщения *M,* так как его можно восстановить по значению подписи. В связи с этим подобные системы называют *схемами цифровой подписи с восстановлением текста.*

Заметим, что если при передаче сообщение дополнительно шифруется с помощью асимметричного шифра, то пара преобразований *(E, D)*, используемая в схеме цифровой подписи, должна отличаться от той, которая используется для шифрования сообщений. В противном случае появляется возможность передачи в качестве шифрованных ранее подписанных сообщений. При этом более целесообразно шифровать подписанные данные, чем делать наоборот, то есть подписывать шифрованные данные, поскольку в первом случае противник получит только шифротекст, а во втором - и открытый, и шифрованный тексты.

Очевидно, что рассмотренная схема цифровой подписи на основе пары преобразований *(E, D)* удовлетворяет требованию невозможности подделки, в то время как требование невозможности создания подписанного сообщения не выполнено: для любого значения *S* каждый может вычислить значение *M = E(S)* и тем самым получить подписанное сообщение. Требование невозможности подмены сообщения заведомо выполняется, так как преобразование *E* взаимно однозначно.

Для защиты от создания злоумышленником подписанного сообщения можно применить некоторое взаимно однозначное отображение $R: M \rightarrow M^*$, вносящее избыточность в представление исходного сообщения, например, пу-

тем увеличения его длины, а затем уже вычислять подпись $S = D(M^*)$. *В* этом случае злоумышленник, подбирая *S* и вычисляя значения $M^* = E(S)$, будет сталкиваться с проблемой отыскания таких значений M^*, для которых существует прообраз *M*. Если отображение *R* выбрано таким, что число возможных образов M^* значительно меньше числа всех возможных последовательностей той же длины, то задача создания подписанного сообщения будет сложной.

Другой подход к построению схем цифровых подписей на основе систем шифрования с открытым ключом состоит в использовании бесключевых хэш-функций. Для заданного сообщения *M* сначала вычисляется значение хэш-функций $h(M)$, а затем уже значение подписи $S = D(h(M))$. Ясно, что в таком случае по значению подписи уже нельзя восстановить сообщение. Поэтому подписи необходимо передавать вместе с сообщениями. Такие подписи получили название *цифровых подписей с дополнением*. Заметим, что системы подписи, построенные с использованием бесключевых хэш-функций, заведомо удовлетворяют всем требованиям, предъявляемым к цифровым подписям.

В качестве системы шифрования с открытыми ключами можно использовать, например, систему RSA.

Аппаратура и материалы

1. Компьютерный класс общего назначения с конфигурацией ПК не хуже рекомендованной для ОС Windows 2000\XP.
2. Операционная система Windows 2000\XP.

Методика и порядок выполнения работы

1. Изучить теоретический материал работы.
2. Провести исследование процедуры построения подписи RSA.

Передаваемое сообщение *m* и кодирующее число *p* представлены в таблице 1

Таблица 1 – Задание для исследования

Вариант	Кодирующее число	Кодирующее число	Сообщение *m*
1	53	7	17
2	47	13	18
3	43	11	19
4	41	17	20

Вариант	Кодирующее число	Кодирующее число	Сообщение *m*
5	37	19	21
6	29	5	22
7	41	7	23
8	37	11	24
9	23	13	16
10	29	17	15
11	17	23	14
12	19	29	13
13	41	11	28
14	17	13	29
15	19	17	30
16	17	5	31

Студенты самостоятельно выбирают значение ключей для обеих сторон (*A* и *B*) и исследуют процесс зашифрования и расшифрования сообщения.

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследование процедуры построения цифровой подписи на основе RSA по своему варианту и ответы на вопросы.

Вопросы для защиты работы

1. Основные принципы построения цифровых подписей.

2. Основные характеристики построения цифровых подписей на основе алгоритма RSA.

3. Достоинства и недостатки построения цифровой подписи на основе алгоритма RSA.

Лабораторная работа 5

ИССЛЕДОВАНИЕ ПРОЦЕССА ПОСТРОЕНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ ЭЛЬ-ГАМАЛЯ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ РЕАЛИЗАЦИИ

Цель и содержание:

1. Углубить знания, по основам использования цифровой подписи.
2. Исследовать основные характеристики алгоритма построения электронной подписи Эль-Гамаля.

Формируемые компетенции

1. Способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2).
2. Способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9).
3. Способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).

Теоретическое обоснование

Одним из основных методов обеспечения безопасности информационных систем является цифровые шифрования. В современных шифровочных устройствах имеют дело с большим объёмом информации, записанной в q-ной системе счисления ($q = 2^4 - 10^4$). В процессе переработки данной информации осуществляются различные арифметические операции или преобразования. При этом возникает задача выбора эффективного метода выполнения этих действий или преобразований.

Криптосистема «открытый ключ» неудобна в том смысле, что получатель сообщения не знает, кто является отправителем сообщения. Этого недоставка лишена система «электронная подпись».

Для получения цифровой подписи выбирается простое число p и два случайных числа g и x, причем $g<p$, $x<p$. Затем вычисляется значение

$$y = g^{x} \bmod p$$

Открытым ключом являются:

1. p - простое число (может быть общим для группы абонентов).
2. $g < p$ (может быть общим для группы абонентов).
3. $y=g^{X} \bmod p$.

Секретным ключом является значение: $x < p$.

Чтобы подписать сообщение M, сначала выбирается число k, взаимно-простое с $p-1$. Затем вычисляется:

$$a = g^{k} \bmod p$$

Затем находится b из условия

$$M = (xa + kb) \bmod (p - 1)$$

Подписью является пара чисел a и b. Случайное значение k хранится в секрете. Для проверки подписи надо убедиться, что

$$y^{a} a^{b} \bmod p = g^{M} \bmod p$$

Каждая подпись требует нового значения k, следовательно, k выбирается случайным образом.

Рассмотрим процесс построения электронной подписи Эль-Гамаля. Пусть $p = 11$ и случайно выбираем $g = 2$. Пусть секретный ключ $x = 8$, тогда

$$y = g^{x} \bmod p$$

$$y = 2^{8} \bmod 11 = 3$$

Открытым ключом являются $y = 3$, $g = 2$ и $p = 11$. Необходимо подписать $M = 5$. Выбираем случайное число $k = 9$, оно взаимно простое с $p-1$, которое равно 10. Далее вычисляем

$$a = g^{k} \bmod 11 = 2^{9} \bmod 11 = 6$$

Затем с помощью расширенного алгоритма Евклида найдем b из уравнения

$$M = (ax + kb)mod\ p -$$
$$1\ 5 = (6 \cdot 8 + 9b)mod$$
$$10\ 8 + 9 \cdot 1mod\ 10 = 7$$
$$8 + 9 \cdot 2\ mod\ 10 = 6$$
$$8 + 9 \cdot 3\ mod\ 10 = 5$$

следовательно, $b = 3$.

Таким образом, подпись представляет собой пару чисел $a = 6$ и $b = 3$.

Проверяем правильность подписи согласно

$$y^{a}\ a^{b}\ \ mod\ p = g^{m}\ mod\ p$$

(пересылаем M и совместно с ним a, b, следовательно, на приемной стороне при истинном значении последнего выражения принимается решение о достоверности переданного).

Аппаратура и материалы

1. Компьютерный класс общего назначения с конфигурацией ПК не хуже рекомендованной для ОС Windows 2000\XP.
2. Операционная система Windows 2000\XP.

Методика и порядок выполнения работы

1. Изучить теоретический материал работы.
2. Провести исследование системы цифровой подписи.

Передаваемое сообщение m открытые ключи p, g, и секретный ключ представлены в таблице 1.

Таблица 1 – Задание для исследования системы

Вариант	Открытый ключ		Закрытый ключ, x	Сообщение m
	p	g		
1	23	12	13	21
2	29	14	15	23
3	23	15	14	17
4	31	10	10	14
5	17	12	11	13
6	19	17	12	15
7	37	18	13	21
8	41	9	20	11

Вариант	Открытый ключ		Закрытый ключ,	Сообщение *m*
9	23	10	11	17
10	29	11	12	23
11	23	12	13	19
12	31	13	14	20
13	17	14	15	15
14	19	15	16	18
15	37	7	10	30
16	41	6	11	24

Студенты самостоятельно выбирают значение *k* согласно условию и исследуют процедуру получения цифровой подписи согласно варианту.

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследование системы цифровой подписи на основе алгоритма Эль-Гамаля по своему варианту и ответы на вопросы.

Вопросы для защиты работы

1. Основные принципы построения цифровой подписи Эль-Гамаля.
2. Основные характеристики алгоритма Эль-Гамаля, используемого для получения цифровой подписи.
3. Сравнительная характеристика алгоритмов получения цифровой подписи RSA и Эль-Гамаля.

Лабораторная работа 6

ИССЛЕДОВАНИЕ МЕТОДА ЭКСПОНЕНЦИАЛЬНОГО КЛЮЧЕВОГО ОБМЕНА НА ОСНОВЕ АЛГОРИТМА ДИФФИ-ХЕЛМАНА

Цель и содержание:

1. Углубить знания, полученные на лекциях, по основам ключевого экспоненциального ключевого обмена.

2. Исследовать основные характеристики метода экспоненциального ключевого обмена на основе алгоритма Диффи-Хелмана.

Формируемые компетенции

1. Способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5).

2. Способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9).

3. Способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).

Теоретическое обоснование

Различают следующие типы протоколов распределения ключей:

– протоколы передачи (уже сгенерированных) ключей;

– протоколы (совместной) выработки общего ключа (открытое распределение ключей);

– схемы предварительного распределения ключей.

Различают также протоколы распределения ключей между отдельными участниками и между группами участников информационного взаимодействия.

Метод экспоненциального ключевого обмена Диффи-Хелмана основан на открытом ключе. Криптостойкость определяется трудностью вычисления дискретного логарифма.

Описание алгоритма Диффи-Хелмана

Выбираются:

– простое число q;

– число α, являющееся первообразным конем q.

Сторона A выбирает случайное число $X_A < q$ и вычисляет значение:

$$Y_A = \alpha^{X_A} \bmod q$$

Пользователь B случайно выбирает $X_B < q$ и вычисляет:

$$Y_B = \alpha^{X_B} \bmod q$$

Стороны обмениваются полученными значениями Y_A и Y_B, сохраняя в тайне значения X_A и X_B.

Тогда сторона A вычисляет ключ по формуле:

$$K_A = (Y_B)^{X_A} \bmod q$$

При этом сторона B определяет ключ согласно:

$$K_B = (Y_A)^{X_B} \bmod q = (\alpha^{X_A \cdot X_B}) \bmod q$$

Следует отметить, что данный алгоритм можно использовать при односторонней генерации ключей

Односторонняя генерация ключа.

1. Сторона A выбирает целое число X_A и генерирует

$$k = \alpha^{X_A} \bmod q$$

2. Сторона B выбирает случайное целое X_B и передаёт на сторону A значение

$$Y_B = \alpha^{X_B} \bmod q$$

3. Сторона A посылает стороне стороне B значение

$$Y_A = (Y_B)^{X_A} \bmod q = \alpha^{X_B \cdot X_A} \bmod q$$

4. Сторона B вычисляет сначала значение

$$Z = X_B^{-1} \bmod q$$

А затем осуществляет вычисление значения ключа

$$k^* = \left(Y_A^{Z} \bmod q\right) = \left(\alpha^{X_B \cdot X_A} \bmod q\right)^{\left(X_B \cdot X_A \cdot \frac{1}{X_B} \bmod q = \alpha\right)} \bmod q$$

Имеем ключ $k = k^*$.

Описанный протокол ключевого обмена можно расширить и для многих участников.

Первый этап. Сторона *A* выбирает значение X_A вычисляет и посылает на сторону B вычисленное значение:

$$Y_A = \alpha^{X_A} \bmod q$$

При этом сторона *A* получила Y_C от стороны *C*.

Сторона *B* выбирает значение X_B и вычисляет:

$$Y_B = \alpha^{X_B} \bmod q$$

Полученное значение посылается на сторону C, получив при этом Y_A.

Сторона *C* выбирает значение X_C и вычисляет:

$$Y_C = \alpha^{X_C} \bmod q$$

Полученное значение было послано на сторону *A*. При этом сторона *C* получила значение Y_B.

Второй этап. Станция *A* пересылает станции *B* значения

$$Z_A = (Y_C)^{X_A} \bmod q = (\alpha^{X_C \cdot X_A}) \bmod q$$

Станция *B* пересылает станции *C* значения

$$Z_B = (Y_A)^{X_B} \bmod q = (\alpha^{X_A \cdot X_B}) \bmod q$$

Станция *C* пересылает на станцию *A* значения

$$Z_C = (Y_B)^{X_C} \bmod q = (\alpha^{X_B \cdot X_C}) \bmod q$$

Третий этап. Станция *A* вычисляет ключ

$$K_A = (Z_C)^{X_A} \bmod q = (\alpha^{X_B \cdot X_C}) \bmod q = \alpha^{X_A X_B X_C} \bmod q$$

Станция *B* вычисляет ключ

$$K_B = (Z_A)^{X_B} \bmod q = (\alpha^{X_A \cdot X_C})^{X_B} \bmod q$$

Станция *C* вычисляет ключ

$$K_C = (Z_B)^{X_C} \bmod q = (\alpha^{X_A \cdot X_B})^{X_C} \bmod q$$

Аппаратура и материалы

1. Компьютерный класс общего назначения с конфигурацией ПК не хуже рекомендованной для ОС Windows 2000\XP.

2. Операционная система Windows 2000\XP.

Методика и порядок выполнения работы

1. Изучить теоретический материал работы.

2. Провести исследование метода экспоненциального ключевого обмена на основе алгоритма Диффи-Хелмана для двух сторон.

Кодирующее число g числа X_A и X_B представлены в таблице 1.

Таблица 1 – Задание для исследования метода экспоненциального ключевого обмена на основе алгоритма Диффи-Хелмана для двух сторон.

Вариант	Кодирующее число q	Число X_A	Число X_B
1	23	7	17
2	29	13	18
3	31	11	19
4	37	17	20
5	41	19	21
6	43	5	22
7	47	7	23
8	53	11	24
9	23	13	16
10	29	17	15
11	31	23	14
12	37	29	13
13	41	11	28
14	43	13	29
15	47	17	30
16	53	5	31

Студенты самостоятельно выбирают значение первообразный порождающий элемент и исследуют процесс двухстороннего обмена.

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследования метода экспоненциального ключевого обмена на основе алгоритма Диффи-Хелмана для двух сторон по

своему варианту и ответы на контрольные вопросы.

Вопросы для защиты работы

1. Основные принципы построения экспоненциального ключевого обмена на основе алгоритма Диффи-Хелмана.

2. Основные характеристики экспоненциального ключевого обмена на основе алгоритма Диффи-Хелмана.

3. Односторонняя генерация ключей с использованием алгоритма Диффи-Хелмана.

Лабораторная работа 7

ИССЛЕДОВАНИЕ МОДИФИКАЦИИ МЕТОДА ЭКСПОНЕНЦИАЛЬНОГО КЛЮЧЕВОГО ОБМЕНА НА ОСНОВЕ АЛГОРИТМА ДИФФИ-ХЕЛМАНА

Цель и содержание:

1. Углубить знания, полученные на лекциях, по основам экспоненциального ключевого обмена.

2. Исследовать основные характеристики модификации метода экспоненциального ключевого обмена Диффи-Хелмана.

Формируемые компетенции

1. Способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2).

2. Способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5).

3. Способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9).

4. Способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).

Теоретическое обоснование

Протокол МТИ (MTI) – (авторы Мацумото, Такашима, Иман) предназначен для реализации метода экспоненциального ключевого обмена на основе алгоритма Диффи-Хелмана и предлагает вместо цифровой подписи использовать модифицированную процедуру выработки общего ключа.

Пусть пользователи имеют секретные ключи, которые выбираются из условия:

$$A \rightarrow a,\ 1<a<p-2$$

$$B \rightarrow b,\ 1<b<p-2$$

Затем обе стороны публикуют открытые ключи:

$$A \rightarrow Z_A,\ Z_A = \alpha^a \bmod p$$

$$B \rightarrow Z_B,\ Z_B = \alpha^b \bmod p$$

Для выработки секретного ключа K обе стороны генерируют случайные числа вида:

$$1 < X_A < p-2$$

$$1 < X_B < p-2$$

Затем вычисляются соответствующие значения, которыми обе стороны обмениваются:

$$Y_A = \alpha^{X_A} \bmod p$$

$$Y_B = \alpha^{X_B} \bmod p.$$

После этого стороны вычисляют значения ключа согласно выражений:

$$B:\ K = (Y_A)^{X_B} \cdot Z_A^b \bmod p = (\alpha^{X_A \cdot X_B} \cdot \alpha)^{ab} \bmod p = \alpha^{X_A \cdot X_B + ab} \bmod p$$

$$A:\ K = (Y_B)^{X_A} \cdot Z_B^a \bmod p = (\alpha^{X_A \cdot X_B} \cdot \alpha^{ab} \bmod p = \alpha^{X_A \cdot X_B + ab} \bmod p$$

Рассмотрим процесс исследования метода экспоненциального ключевого обмена на основе алгоритма Диффи-Хелмана, предлагающего вместо цифровой подписи использовать модифицированную процедуру выработки общего ключа МТИ.

1. Выбираем в качестве значений $p=7,\ \alpha=3$.
2. Выбираем секретные ключи $A:\ a=2;\ B:\ b=6$.
3. Вычисляем открытые ключи

$$A \rightarrow Z_A = 3^2 \bmod 7 = 2;$$

$$B \rightarrow Z_B = 3^6 \bmod 7 = 1.$$

Полученные открытые ключи печатаются.

4. Выбираем случайные числа для шифрования и осуществляем процесс вычисления ключей, которыми будут обмениваться две стороны.

$$A \to X_A = 5;\ Y_A = \alpha_5 \bmod p = 3_5 \bmod 7 = 5;$$
$$B \to X_B = 4;\ Y_B = \alpha_4 \bmod p = 3_4 \bmod 7 = 4.$$

5. Осуществляем вычисление ключа для шифрования

$$A \to K = (Y_B)_{X_A} Z_a \bmod 7 = 4_5 \cdot 1_2 \bmod 7 = 2;$$
$$B \to K = (Y_A)_{X_B} Z_b \bmod 7 = 5_4 \cdot 2_6 \bmod 7 = 2.$$

Полученные значения ключей на стороне *A* и *B* совпадают.

Аппаратура и материалы

1. Компьютерный класс общего назначения с конфигурацией ПК не хуже рекомендованной для ОС Windows 2000\XP.

2. Операционная система Windows 2000\XP.

Методика и порядок выполнения работы

1. Изучить теоретический материал работы.

2. Провести исследование модификации метода экспоненциального ключевого обмена Диффи-Хелмана МТИ.

3. Показать его преимущества по сравнению с классическим методом ключевого обмена.

Кодирующее число *g* числа *XA* и *XB* представлены в таблице 1.

Таблица 1 – Задание для исследования модификации метода экспоненциального ключевого обмена Диффи-Хелмана МТИ.

Вариант	Кодирующее число *q*	Число *XA*	Число *XB*
1	23	7	16
2	29	13	15
3	31	11	14
4	37	17	13
5	41	19	28
6	43	5	29
7	47	7	30
8	53	11	31
9	23	13	17
10	29	17	18
11	31	23	19
12	37	29	20
13	41	11	21
14	43	13	22

15	47	17	23
16	53	5	24

Студенты самостоятельно выбирают значение первообразного порождающего элемента и исследуют модификацию процесса ключевого обмена для двухстороннего обмена.

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследования модификации метода экспоненциального ключевого обмена Диффи-Хелмана МТИ по своему варианту и ответы на контрольные вопросы.

Вопросы для защиты работы

1. Основные причины модификации метода экспоненциального ключевого обмена Диффи-Хелмана.

2. Основные характеристики модификации метода экспоненциального ключевого обмена Диффи-Хелмана.

3. Применение цифровой подписи при использовании алгоритма Диффи-Хелмана.

Лабораторная работа 8

ИССЛЕДОВАНИЕ ПРОЦЕССА ВЫЧИСЛЕНИЯ СЕКРЕТНОГО КЛЮЧА НА ОСНОВЕ СХЕМЫ ШАМИРА С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ РЕАЛИЗАЦИИ

Цель и содержание:

1. Углубить знания, полученные на лекциях, по основам вычисления секретного ключа.

2. Исследовать основные принципы получения распределенного секретного ключа на основе схемы Шамира.

Формируемые компетенции

1. Способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2).

2. Способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5).

3. Способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).

Теоретическое обоснование

Идея состоит в разделении секретного ключа на компоненты с последующим их распределением среди легальных пользователей. Восстановление ключа возможно только в том случае, если коалиция легальных пользователей будет содержать определенное число участников, при этом по одной похищенной части нельзя восстановить весь ключ.

Схема Шамира использует полиномиальное уравнение в ключевом поле. Выбирается большое простое число p, которое больше числа долей и больше самого большого секрета. Чтобы сделать секрет общим, генерируется полином степени $m-1$.Чтобы сделать $(3,n)$ пороговую схему для восстановления сообщения M требуется три доли, при этом генерируется квадратичный полином

$$(ax^2 + bx + M) mod\ p$$

Коэффициенты *a* и *b* выбираются случайным образом и хранятся в тайне, *M*-сообщение. Простое число *p* - открыто публикуется. Доли получаются с помощью вычисления многочлена в n различных точках $k_i = F(x_i)$

Первой долей, может быть значение многочлена при *x=1*, второй долей – значение многочлена при *x=2*, и.т.д.

Поскольку в квадратичных многочленах имеется три неизвестных коэффициента *a, b, M*, для создания трех уравнений используют любые три доли.

Рассмотрим исследование процесса вычисления секретного ключа на основе схемы Шамира. Определить секрет М. Пусть необходимо создать схему (3,5)-пороговую схему в которой три человека из пяти могут восстановить секрет – значение *M*. Для этого получим квадратное уравнение с числами *a=7* и *b =8*. Положим, что *M=11*. В качестве *p* выбираем число 13. Тогда имеем:

$$F(x) = (7 x^2 + 8x + 11) mod\ 13$$

Пятью долями являются:

$$k_1 = F(1) = 7 + 8 + 11 \equiv 0\ mod\ 13$$
$$k_2 = F(2) = 28 + 16 + 11 \equiv 3\ mod$$
$$13\ k_3 = F(3) \equiv 7\ mod\ 13$$
$$k_4 = F(4) \equiv 12 mod\ 13$$
$$k_5 = F(5) \equiv 5\ mod\ 13$$

Чтобы восстановить секрет М воспользуемся тремя долями k2, k3, k5.

$$(a \cdot 2^2 + b \cdot 2 + M) \equiv 3 mod\ 13$$

$$(a \cdot 3^2 + b \cdot 3 + M) \equiv 7\ mod\ 13$$
$$(a \cdot 5^2 + b \cdot 5 + M) \equiv 5\ mod\ 13$$

Для определения секрета, а он представляет собой точку пересечения с осью *Y* воспользуемся интерполяционными полиномами Лагранжа.

Коэффициенты интерполяционных полиномов Лагранжа применяется для интерполяции функции $y(x)$, заданной рядом ординатой $y_0 - y_n$ при абсциссах $x_0 - x_n$. В качестве нулевого узла можно использовать любой узел,

например, при 3 узлах и нулевом центральном узле значения функций обозначаются $y_{-1} = y(x_{-1}), y_0 = y(x_0), y_1 = y(x_1)$. Полином Лагранжа может быть записан в виде:

$$y(x) = A_0(x)y_0 + A_1(x)y_1 + \ldots + A_n(x)y_n \sum_{m=0}^{n} = A_m(x)y_m$$

где коэффициенты определяются из формулы:

$$A_m(x) = \frac{(x - x_0)(x - x_1)\ldots(x - x_{m-1})(x - x_{m+1})\ldots(x - x_n)}{(x_m - x_0)(x_m - x_1)\ldots(x_m - x_{m-1})(x_m - x_{m+1})\ldots(x - x_n)}$$

Ввиду сложности последней формулы коэффициенты сложно вычислить при $n + 1$ ординатах. При нормировке

$$x = x_0 + ph$$

где h - разность абсцисс соседних узлов

$$p = (x - x_0) / h$$

и будет вычисляться значение нормированных коэффициентов Лагранжа:

$X_0=1$	$Y_0=0$
$X_1=2$	$Y_1=3$
$X_2=3$	$Y_2=7$
$X_3=4$	$Y_3=12$
$X_4=5$	$Y_4=5$

Следовательно, имеем:

$X_1=2$, тогда $A_0=3$
$X_2=3$, тогда $A_1=7$
$X_4=5$, тогда $A_2=5$

$$y(x) = A_0(x)y_0 + A_1(x)y_1 + A_2(x)y_2$$

$$y(x) = A_0(x) \cdot 3 + A_1(x) \cdot 7 + A_2(x) \cdot 5$$

$$A_0(x) = \frac{(x - x_2) \cdot (x - x_4)}{(x_1 - x_2) \cdot (x_1 - x_4)} = \frac{x^2 - x \cdot (x_2 + x_4) + x_2 \cdot x_4}{(2-3) \cdot (2-5)} =$$

$$= \frac{x^2 - x \cdot (3+5) + 15}{(-1) \cdot (-3)} = \frac{x^2 - 8x + 15}{3}$$

$$A_1(x) = \frac{(x - x_1) \cdot (x - x_4)}{(3-2) \cdot (3-5)} = \frac{x^2 - x(x_1 + x_4) + x_1 \cdot x_4}{-2} = -\frac{x^2 - 7x + 10}{2}$$

$$A_2(x) = \frac{(x - x_1) \cdot (x - x_2)}{(5-2) \cdot (5-3)} = \frac{x^2 - x(x_1 + x_2) + x_1 \cdot x_2}{3 \cdot 2} = \frac{x^2 - 5x + 6}{6}$$

$$y(x) = \frac{x^2 - 8x + 15}{3} \cdot y_0 - \frac{x^2 - 7x + 10}{2} \cdot y_1 + \frac{x^2 - 5x + 6}{6} \cdot y_2$$

Найдём значение в точке $x = 0$. Это и есть секрет значения функции в нулевой точке $F(0)=11$. Тогда

$$y(0) = \frac{15 \cdot 3}{3} - \frac{10 \cdot 7 + 6}{2} \cdot 5 \bmod 13 = 15 - 35 + 5 \bmod 13 = 11 \bmod 13$$

Исходный полином

$$F(x) = 7x^2 + 8x + 11 \bmod 13$$

Полученное значение секрета $M=11$.

Аппаратура и материалы

1. Компьютерный класс общего назначения с конфигурацией ПК не хуже рекомендованной для ОС Windows 2000\XP.

2. Операционная система Windows 2000\XP.

Методика и порядок выполнения работы

1. Изучить теоретический материал работы.

2. Провести исследование вычисления секретного ключа на основе использования схемы Шамира, используя (3,5)-пороговую схему в которой три человека из пяти могут восстановить секрет – значение M системы RSA. Кодирующее число p числа a , b и секрет M представлены в таблице 1.

Таблица 1 – Задание для исследования.

Вариант	Кодирующее число p	Число a	Число b	Секрет M
1	23	7	12	17

2	29	13	14	18
3	31	11	21	19
4	37	17	23	20
5	41	19	11	21
6	43	5	12	22
7	47	7	13	23
8	29	11	14	24
9	23	13	15	16
10	29	17	16	15
11	31	23	17	14
12	37	29	18	13
13	41	11	17	28
14	43	13	16	29
15	29	17	15	14
16	23	5	14	21

Студенты самостоятельно выбирают значение 3 пользователей для определения секретного ключа на основе интерполяционных полиномов Лагранжа.

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследования вычисления секретного ключа на основе использования схемы Шамира по своему варианту и ответы на контрольные вопросы.

Вопросы для защиты работы

1. Назначение и особенности методов вычисления секретного ключа.
2. Основные характеристики метода Шамира.
3. Применение полиномов Лагранжа при вычислении секретного ключа.

Лабораторная работа 9

ИССЛЕДОВАНИЕ ПРОЦЕССА ШИФРОВАНИЯ РАБИНЕРА С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ РЕАЛИЗАЦИИ

Цель и содержание:

1. Углубить знания, по основам шифрования алгоритмом Рабина.
2. Исследовать основные характеристики алгоритма шифровании

Формируемые компетенции

1. Способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9).

2. Способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).

Теоретическое обоснование

Криптосистема Рабина (M. Rabin) является вариантом криптосистемы RSA. RSA базируется на возведении в степень сравнений. Криптосистема Рабина базируется на квадратичных сравнениях, и ее можно представить как криптографическую систему RSA, в которой значениям e и d присвоены значения e = 2 и d = 1/2. Другими словами, шифрование — $C \equiv p^2 \pmod{n}$ и дешифрование - $P = C^{1/2} \pmod{n}$.

Открытый ключ доступа в криптосистеме Рабина — n, секретный ключ является кортежем (p, q). Каждый может зашифровать сообщение, используя n, но только Боб может расшифровать сообщение, используя p и q. Дешифрование сообщения неосуществимо для Евы, потому что она не знает значения p и q. Рисунок .1 показывает шифрование и дешифрование.

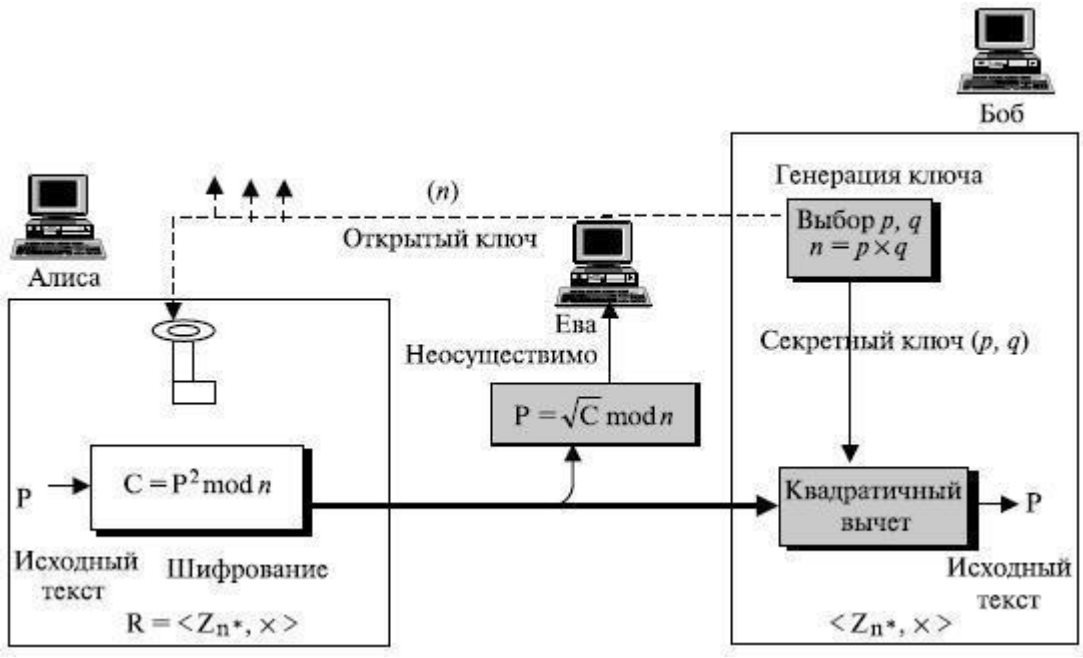


Рисунок 1 - Шифрование, дешифрование и генерация ключей в криптосистеме Рабина

Если Боб использует RSA, он может сохранить d и n и отказаться после генерации ключей от p, q и $\varphi(n)$. Если Боб использует криптосистему Рабина, он должен сохранить p и q.

Генерация ключей

Боб использует шаги, показанные в алгоритме 1, чтобы создать свой открытый ключ доступа и секретный ключ.

Rabin_Key_Generation

{

Выберите два больших простых числа p и q в форме 4k +3 и p ≠ q.

n ← p × q

Открытый_ключ ← n // Может быть объявлен публично

Секретный_ключ ← (q,n) // Должен сохраняться в секрете

return Открытый_ключ и Секретный_ключ

}

Пример Генерации ключей для криптосистемы Рабина (html)

Хотя два простых числа, p и q, могут быть в форме 4k + 1 или 4k + 3, процесс дешифрования становится более трудным, если используется первая

форма. Рекомендуют применять вторую форму, 4k + 3, для того чтобы сделать дешифрование для Алисы намного проще.

Шифрование

Любой может передать сообщение Бобу, используя его открытый ключ доступа. Процесс шифрования показан алгоритмом 2.

Rabin_Encryption (n, P) // n — открытый ключ доступа;

P — зашифрованный текст Z^*_n

{

C ← P^2 mod n // C — зашифрованный

текст return C

}

Пример 2. Шифрование в криптографической системе Рабина

Хотя исходный текст P может быть выбран из множества Z_n, но чтобы сделать дешифрование более простым, определяется множество Z_n*.

Шифрование в криптосистеме Рабина очень простое. Операция нуждается только в одном умножении, что может быть сделано быстро. Это выгодно, когда ресурсы ограничены: например, при использовании карт с интегральной схемой, содержащей микропроцессор с ограниченной памятью, и при необходимости задействовать центральный процессор на короткое время.

Дешифрование

Боб может использовать алгоритм 3, чтобы расшифровать полученный зашифрованный текст.

Rabin_Decryption (p, q, C) // C — зашифрованный текст; p и q — секретные ключи

a1 ← + $(C^{(p+1)/4})$ mod p

a2 ← - $(C^{(p+1)/4})$ mod p

b1 ← + $(C^{(q+1)/4})$ mod q

b2 ← - $(C^{(q+1)/4})$ mod q

// Алгоритм китайской теоремы об остатках вызывается четыре раза.

P1 ← Китайский_остаток (a1, b1, p, q)

P2 ← Китайский_остаток (a1, b2, p,

q) P3 ← Китайский_остаток (a2, b1,

p, q) P4 ← Китайский_остаток (a2,

b2, p, q) return P1, P2, P3 и P4

Пример 3. Дешифрование в криптосистеме Рабина Дешифрация базируется на решении квадратичного сравнения. Поскольку полученный зашифрованный текст — квадрат исходного текста, это гарантирует, что C имеет корни (квадратичные вычеты) в Z_n^*. Алгоритм китайской теоремы об остатке используется, чтобы найти четыре квадратных корня.

Самый важный пункт в криптосистеме Рабина — это то, что она недетерминирована. Дешифрование имеет четыре ответа. Задача получателя сообщения - точно выбрать один из четырех ответов как конечный ответ. Однако во многих ситуациях получатель может легко выбрать правильный ответ.

Криптосистема Рабина не детерминирована — дешифрование создает четыре одинаково вероятных исходных текста.

Пример 1

Вот очень тривиальный пример, чтобы проиллюстрировать идею.

1. Боб выбирает p = 23 и q = 7. Обратите внимание, что оба являются сравнениями 3 mod 4.

2. Боб вычисляет $n = p \times q = 161$.

3. Боб объявляет n открытым и сохраняет p и q в секрете.

4. Алиса хочет передать исходный текст P = 24. Обратите внимание, что 161 и 24 являются взаимно простыми; 24 находится в Z_{161}^*. Она вычисляет C = от $24^2 = 93 \bmod 161$ и передает зашифрованный текст 93 Бобу.

5. Боб получает 93 и вычисляет четыре значения:

a. $a1 = + (93^{(23+1)/4}) \bmod 23 = 1 \bmod 23$

b. $a2 = – (93^{(23+1)/4}) \bmod 23 = 22 \bmod 23$

c. $b1 = + (93^{(7+1)/4}) \bmod 7 = 4 \bmod 7$

d. $b2 = – (93^{(7+1)/4}) \bmod 7 = 3 \bmod 7$

1. Боб имеет четыре возможных ответа — (a1, b 1), (a1, b2),

2. (a_2, b_1), (a_2, b_2) и использует китайскую теорему об остатках, чтобы найти четыре возможных исходных текста: 116, 24, 137 и 45 (все из них взаимно простые к 161). Обратите внимание, что только второй ответ — исходный текст Алисы. Боб должен принять решение исходя из ситуации. Обратите внимание также, что все четыре ответа при возведении во вторую степень по модулю n дают зашифрованный текст 93, переданный Алисой.

$116^2 = 93 \bmod 161 \quad 24^2 = 93 \bmod 161 \quad 137^2 = 93 \bmod 161 \quad 45^2 = 93 \bmod 161$

Методика и порядок выполнения работы

1. Изучить теоретический материал работы.

2. Провести исследование системы Рабина

Студенты самостоятельно выбирают значение трех пользователей для определения секретного ключа на основе системы Рабина.

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследования вычисления секретного ключа на основе системы Рабина по своему варианту и ответы на вопросы.

Вопросы для защиты работы

1. Назначение и особенности методов вычисления секретного ключа.
2. Основные характеристики метода Рабина.

Лабораторная работа 10

ИССЛЕДОВАНИЕ ПРОЦЕССА ПОСТРОЕНИЯ СКРЫТОГО КАНАЛА НА ОСНОВЕ СХЕМЫ ЭЛЬ-ГАМАЛЯ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ РЕАЛИЗАЦИИ

Цель и содержание:

1. Углубить знания, полученные на лекциях, по основам вычисления секретного ключа.

2. Исследовать основные принципы построения скрытый канал на основе схемы Эль-Гамаля.

Формируемые компетенции

1. Способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2).

2. Способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5).

3. Способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9).

4. Способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).

Теоретическое обоснование

Идея состоит в разделении секретного ключа на компоненты с последующим их распределением среди легальных пользователей. Восстановление ключа возможно только в том случае, если коалиция легальных пользователей будет содержать определенное число участников, при этом по одной похищенной части нельзя восстановить весь ключ.

В вычислительных сетях возможно создание скрытого канала передачи данных при использовании алгоритмов электронной цифровой подписи (ЭЦП). Скрытый канал — непредусмотренный разработчиком коммуникационный канал, по которому могут быть переданы сообщения. Впервые концепцию создания скрытого канала предложил Г. Симмонс, на основе криптограмм, внедряя в них дополнительную информацию. Описанные им алгоритмы, опираются на свойства операций в кольце, и подмену генерируемого случайного числа. Был приведен «типичный» протокол скрытого канала: отправитель, используя секретный ключ, общий с получателем, подписывает невинное сообщение, пряча в подписи скрытое сообщение, создавая скрытый канал с помощью обычных алгоритмов цифровой подписи. Рассмотрим алгоритм построения скрытый канал на основе схемы Эль-Гамаля.

Генерация ключа выполняется так же, как и в основной схеме подписи Эль-Гамаля.

1) Выбирайте простое большое число p и два случайных числа r и g, меньшие p .

Затем вычисляется

$$K = g^{r} \bmod p \qquad (1)$$

открытыми ключами служат K,g,p. Секретным ключом является число r. Данный секретный ключ r известен на передающей и принимающей стороне. Это число используется не только для подписи сообщения -контейнера, но и в качестве ключа для отправки и чтения скрытого сообщения.

Для обработки скрытого сообщения в M в сообщении-контейнере M' необходимо, чтобы M и pбыли взаимно простыми, кроме того, взаимно простыми должны быть значения M и p-1.

2) Абонент A вычисляет

$$X = g^{M} \ mod \ p \qquad (2)$$

и решает следующие уравнения для Y

$$M' = rX + MY \ mod(\ p - 1 \ ) \qquad (3)$$

Подписью сообщения M' является (X,Y). Противник может проверить подпись Эль-Гамаля, он вычисляет1-скрытый ключ

$$K^X X^Y = g^{M'} \bmod p \qquad (4)$$

Пользователь В также должен проверить подлинность сообщения M', используя сравнение

$$(g^r)^X \cdot X^Y = g^{M'} \bmod p \qquad (5)$$

Если сообщение является подлинным, то абонент B производит восстановление секретного сообщения M.

Для этого он вычисляет

$$M = \frac{M' - rX}{Y} \bmod (p-1) \qquad (6)$$

Пример. Пусть $p=11$, $g=2$. Выбираем секретный ключ $r=8$.

Тогда открытый ключ

$$K = g^r \bmod p = 2^8 \bmod 11 = 3$$

Этим ключом противник может проверить подпись сообщения M'.

Пусть скрытое сообщение $M = 9$. Это сообщение удовлетворяет условию

$$НОД(M,p)=НОД(9,11)=1,\ НОД(M,p-1)=1.$$

Для проверки воспользуется контейнером $M'=5$. При этом проверяется условие, что

$$НОД(M',p)=(5,11)=1.$$

Затем отправитель M вычисляет подпись

$$X = g^M \bmod p = 2^9 \bmod 11 = 6$$

После этого решается уравнение (надо получить Y):

$$5 = 8 \cdot 6 + 9 \cdot Y \bmod 10$$

Получили $Y=3$. Тогда подпись имеет вид $(X=6, Y=3)$. Получатель проводить проверку подлинности сообщения M'.

$$(g^r)^X X^Y \bmod p = (2^8)^6 \cdot 6^3 \bmod 11 \equiv 2^5$$

Следовательно, принято сообщение $M' = 5$ является правильным. Так как неравенство справедливо, то получатель извлекает скрытое сообщение M, согласно (6)

$$M = (Y^{-1} (M' - rX))mod(p - 1) = (3^{-1} \cdot (5 - 8 \cdot 6))mod\ 10 = =$$

$$(7 \cdot (5 - 48))mod\ 10 = (7 \cdot (-3))nod10 = |7 \cdot 7|^{+}_{10} = 49|^{+}_{10} = 9$$

Аппаратура и материалы

1. Компьютерный класс общего назначения с конфигурацией ПК не хуже рекомендованной для ОС Windows 2000\XP.
2. Операционная система Windows 2000\XP.

Методика и порядок выполнения работы

1. Изучить теоретический материал работы.
2. Провести исследование вычисления построения скрытый канал на основе схемы Эль-Гамаля. Кодирующее число p числа a , b и секрет M представлены в таблице 1.

Таблица 1 – Задание для исследования.

Вариант	Кодирующее число p	Число a	Число b	Секрет M
1	23	7	12	17
2	29	13	14	18
3	31	11	21	19
4	37	17	23	20
5	41	19	11	21
6	43	5	12	22
7	47	7	13	23
8	29	11	14	24
9	23	13	15	16
10	29	17	16	15
11	31	23	17	14
12	37	29	18	13
13	41	11	17	28
14	43	13	16	29
15	29	17	15	14
16	23	5	14	21

Студенты самостоятельно выбирают значение 3 пользователей для определения секретного ключа на основе интерполяционных полиномов Лагранжа.

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследования вычисления построения скрытый канал на основе схемы Эль-Гамаля по своему варианту и ответы на контрольные вопросы.

Вопросы для защиты работы

1. Назначение и особенности методов вычисления секретного ключа.
2. Основные характеристики метода Шамира.
3. Применение полиномов Лагранжа при вычислении секретного ключа.

Лабораторная работа 11

ИССЛЕДОВАНИЕ ПРОЦЕССА ПОСТРОЕНИЯ СКРЫТОГО КАНАЛА НА ОСНОВЕ СХЕМЫ ГУСТАВА-СИММОНСОНА С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ РЕАЛИЗАЦИИ Цель и содержание:

1. Углубить знания, полученные на лекциях, по основам построения скрытого канала.

2. Исследовать основные принципы получения протокола обмена для скрытого канала на основе схемы Густава-Симмонсона.

Формируемые компетенции

1. Способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2).

2. Способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9).

3. Способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).

Теоретическое обоснование

Рассмотрим реализацию скрытого канала, которая была разработана Густавом и Симмонсоном.

Абонент *A* выбирает общедоступный модуль *p* – простое число, а затем определяет закрытый ключ, так чтобы *p* и *k* были взаимно простыми.

При этом этот ключ *k* знает и получатель *B*.

Открытый ключ вычисляется из условия

$$h = -k^2 \bmod p \,. \qquad (1)$$

Если абоненту *A* необходимо отправить скрытое сообщение *M* в сообщении M' необходимо:

1) проверить условие, что *M* и *p*, а также M' и *p* – взаимно простые числа
2) вычислить

$$S_1 = \frac{1}{2} \cdot \left(\frac{M'}{M} + M\right) \bmod p \qquad (2)$$

$$S_2 = \frac{1}{2} \cdot \left(\frac{M'}{M} - M\right) \bmod p \qquad (3)$$

Получается пара чисел S_1 и S_2 с одной стороны является подписью в схеме, а с другой стороны – содержит скрыто сообщение *M*.

Получатель *B* должен проверить истинность принятого сообщения с вложением согласно

$$S_1^2 - S_2^2 / k^2 \bmod p \qquad (4)$$

Если результат совпадает с M', т.е.

$$S_1^2 - S_2^2 / k^2 \equiv M' \bmod p\,, \qquad (5)$$

то это сообщение не навязано противником.

После доказательства подлинности сообщения абонент *B* может извлечь скрытое сообщение, используя следующую форму

$$M = \frac{M'}{(S_1 + S_2 k^{-1})} \bmod p \qquad (6)$$

Пример. Пусть в качестве модуля выбрали простое число *p=11*. В качестве секретного ключа *k* выбираем *k=10*. Затем вычисляем открытый ключ

$$h = -k^2 \bmod p = -10^2 \bmod 11 = -1 \bmod 11 = 10$$

Пусть абонент *A* хочет передать сообщение *M=4* по скрытому каналу. Он проверяет условие взаимной простоты *M=4* и *p=11*.

Для передачи воспользуемся сообщением $M'=3$, которое должно удовлетворять условию $НОД(M', p) = НОД(3,11) = 1$.

Вычислим значения S_1 и S_2.

$$S_1 = \frac{1}{2}(M' + M) \bmod p = \left|\frac{1}{2}\cdot(4+4)\right|_{11}^{+} = 6\cdot(3\cdot 3+4)_{11}^{+} =$$

$$= 6\cdot 13_{11}^{+} = 6\cdot 2_{11}^{+} = 12_{11}^{+} = 1$$

Затем определяем S_2

$$S_2 = \frac{k}{2}\left(\frac{M'}{2} - M\right) \bmod p = \left|\frac{10}{2}\cdot\left(\frac{3}{4} - 4\right)\right|_{11}^{+} = 5\cdot(3\cdot 3-4)_{11}^{+} = 5\cdot 5_{11}^{+} = 25_{11}^{+} = 3$$

Получим пару значений (1,3), которую передали абоненту *B* совместимо с сообщением M'.

Абонент *B* проверяет сообщение M' и на подлинность, используя формулу (4). Получаем

$$S_1 - \frac{S_2^2}{k^2} \bmod p = 1\left|^2 - \frac{3^2}{10}\right|_{11}^{+} = 1 - 9_{11}^{+} = -8_{11}^{+} = 3$$

В результате получили сообщение $M'=3$. Это означает, что принятое сообщение подлинное.

Произведем извлечение скрытого сообщения, используя формулу (6)

$$\frac{M'}{(S_1 + S_2\cdot k^{-1})} \bmod p = \frac{3}{(1+3\cdot 10^{-1})} \bmod 11 = \left|\frac{3}{(1+3\cdot 10)}\right|_{11}^{+} =$$

$$= \left|\frac{3}{1+30}\right|_{11}^{+} = \left|\frac{3}{9}\right|_{11}^{+} = \left|\frac{1}{3}\right|_{11}^{+} = 4$$

В результате секретное сообщение равно *M=4*.

Аппаратура и материалы

3. Компьютерный класс общего назначения с конфигурацией ПК не хуже рекомендованной для ОС Windows 2000\XP.

4. Операционная система Windows 2000\XP.

Методика и порядок выполнения работы

3. Изучить теоретический материал работы.

4. Провести исследование вычисления секретного ключа на основе использования схемы Шамира, используя (3,5)-пороговую схему в которой три человека из пяти могут восстановить секрет – значение *M* системы RSA.

Кодирующее число p числа a , b и секрет M представлены в таблице 1.

Таблица 1 – Задание для исследования.

Вариант	Кодирующее число p	Число a	Число b	Секрет M
1	31	23	17	14
2	37	29	18	13
3	41	11	17	28
4	43	13	16	29
5	29	17	15	14
6	23	5	14	21
7	23	7	12	17
8	29	13	14	18
9	31	11	21	19
10	37	17	23	20
11	41	19	11	21
12	43	5	12	22
13	47	7	13	23
14	29	11	14	24
15	23	13	15	16
16	29	17	16	15

Студенты самостоятельно выбирают значение 3 пользователей для определения секретного ключа на основе интерполяционных полиномов Лагранжа.

Содержание отчета и его форма

Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследования вычисления секретного ключа на основе использования схемы Шамира по своему варианту и ответы на контрольные вопросы.

Вопросы для защиты работы

4. Назначение и особенности методов вычисления секретного ключа.
5. Основные характеристики скрытого канала на основе схемы Густава-Симмонсона.
6. Применение полиномов Лагранжа при вычислении секретного ключа.

Указания по технике безопасности

1. Перед началом работы пользователь ПК обязан проверить, чтобы все кабели питания находились как можно дальше в компактном положении с тыльной стороны рабочего места.

2. Компьютер рекомендуется подключать к отдельной розетке. Розетка, используемая для подключения компьютер должна быть трехполюсной.

3. Запрещается приступать к работе при: а) обнаружении неисправности оборудования; б) отсутствии защитного заземления устройств.

4. Пользователю ПК во время работы запрещается:

а) касаться одновременно экрана монитора и клавиатуры (возможен разряд повышенного электростатического потенциала);

б) прикасаться к задней панели системного блока;

в) производить переключения интерфейсных кабелей периферийных устройств при включенном питании;

г) производить отключение питания во время выполнения задачи.

5. Категорически запрещается работать с ПК при снятом корпусе; оставлять включенный ПК без присмотра; самостоятельно вскрывать корпус ПК.

ЛИТЕРАТУРА

1. Основная литература:

- Рябко Б.Я. Фионов А.Н. Криптографические методы защиты информации. – М.: "Горячая линия-Телеком", 2012. - 229 с.
- Музыкантский А.И., Фурин В.В. Лекции по криптографии. – М.: МЦНМО, 2011. - 68 с.
- Глухов М. М. Круглов И. А., Пичкур А. Б., Черемушкин А. В. Введение в теоретико-числовые методы криптографии. – СПб.:"Лань", 2011. - 400 стр.
- Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДиК, 2008. – 448 с.
- Основы криптографии: Учебное пособие/Под ред. Алферова П.П. – М.:Гелиос, 2008. – 480 с.

2. Дополнительная литература:

- Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. – М.: "Бином. Лаборатория знаний", 2013. – 480 с.
- Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: "ДМК Пресс", 2008. – 448 с.
- Алферов А.П., Зубов А.Ю. и др. Основы криптографии: Учебное пособие, 2-е – М.: Гелиос АРВ, 2006 – 480 с.
- Баричев С.Г. Основы современной криптографии. Учебный курс. – М .: Телеком, 2007. – 129 с.
- Молдовян А.А. и др. Криптография. – СПб.: Лань, 2007. – 224 с.
- Введение в криптографию/Под ред В.В.Ященко. – М.: МЦНМО, 2006. – 288 с.

Практикум к выполнению
лабораторных работ по дисциплине
«Криптографические методы защиты информации»
для студентов специальностей 10.05.03
«Информационная безопасность автоматизированных систем »

Составители: д.т.н., профессор Калмыков И.А.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания к лабораторным работам

Криптографические методы защиты информации

Ставрополь, 2017

СОДЕРЖАНИЕ

1. Цель и задачи освоения дисциплины …..…… 4
2. Место дисциплины в структуре ООП специалитета ……. 4
3. Связь с предшествующими дисциплинами ….…… 4
4. Связь с последующими дисциплинами …. ……. 4
5. Компетенции обучающегося, формируемые в результате освоения дисциплины ……...……... 4
6. План график выполнения СРС по дисциплине ……... 6
7. Методические рекомендации к СРС ……..... 6
8. Рекомендуемая литература и Интернет-ресурсы ……...…. 8

1. Цель и задачи освоения дисциплины

Цель дисциплины состоит в формировании фундаментальных знаний основных положений теории криптографической защиты информации, оценки криптостойкости, имитостойкости и помехоустойчивости шифров, особенностей использования вычислительной техники в криптографии, привитие умений и навыков использования данных знаний при работе с системами криптографической защиты информации

Задачи дисциплины

- изучить математические основы криптографических методов защиты информации;
- изучить основные алгоритмы симметричного и асимметричного шиф-рования данных;

изучить основы организации структуры криптосистем

2. Место дисциплины в структуре ООП специалитета

Дисциплина относится к профессиональному циклу (базовой части). Ее освоение происходит в 5 и 6 семестрах.

3. Связь с предшествующими дисциплинами

Дисциплина «Криптографические методы защиты информации» базируется на знаниях, полученных студентами в ходе изучения дисциплин: «Информатика», «Дискретная математика», «Теория вероятности и математическая статистка».

4. Связь с последующими дисциплинами

Дисциплина «Криптографические методы защиты информации» обеспечивает изучение следующих дисциплин: «Техническая защита информации», «Управление информационной безопасности», «Программно-аппаратные средства обеспечения информационной безопасности». Знания и практические

навыки, полученные из дисциплины «Криптографические методы защиты информации», используются студентами при разработке курсовых и дипломных работ.

5. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих общекультурных, и профессиональных компетенций

№ п/п	Содержание компетенции	Шифр
Общекультурные компетенции		***ОК-(№)***
Профессиональные компетенции		***ПК-(№)***
1.	Способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач	ПК-2
2	способностью применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	ПК-9
3	способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности	ПК-9
4	способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	ПК-23

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ	–основные задачи и понятия криптографии; – требования к шифрам и основные характеристики шифров; –типовые поточные и блочные шифры; – частотные характеристики открытых тексов и способы их применения к анализу простейших шифров замены и перестановки; –типовые шифры с открытыми ключами; –модели шифров и математические методы их взаимодействия.
УМЕТЬ	- эффективно использовать криптографические методы средства защиты информации в автоматизированных системах; - применять математические методы исследования моделей шифров.
ВЛАДЕТЬ	– криптографической терминологией; – навыками использования типовых криптографических алгоритмов; – навыками использования ЭВМ в анализе простейших шифров; – навыками математического моделирования в криптографии

План график выполнения СРС по дисциплине

1. Виды и содержание самостоятельной работы студента; формы контроля

№	Наименование разделов и тем дисциплины, их краткое содержание; вид самостоятельной работы	Форма контроля	Зачетные единицы (часы)
	6 семестр		
1	Подготовка к лекциям	Устный опрос	6
2	Подготовка к лабораторным работам	Устный опрос	8
3	Самостоятельное изучение темы «Основные методы прямого и обратного преобразования непозиционных кодов» (сроки выполнения: 16 неделя, форма контроля - опрос)	Устный опрос	4
	Итого за 6семестр		**18**
	Подготовка к лекциям	Устный опрос	12
	Подготовка к лабораторным работам	Устный опрос	16
	Самостоятельное изучение «Криптографические хеш-функции» (сроки выполнения: 14 неделя, форма контроля - опрос)	Устный опрос	8
	Итого за 6семестр		**36**
	Всего		**54**

7. Рейтинговая оценка знаний студента

1. Рейтинговая оценка знаний студента

№	Тип занятия (контрольной точки)	Кол-во

		баллов
5 семестр		
1.	Лабораторная работа аудиторная Исследование процесса Шифрования сообщений с помощью упрощенного S-DES с использованием программной реализации	18
2.	Лабораторная работа аудиторная Исследование поточного шифрования сообщений в синхронных системах, построенных на основе многотактовых кодовых фильтров с использованием программной реализации	18
3.	Лабораторная работа аудиторная Исследование поточного шифрования сообщений в самосинхронизующихся системах на основе генераторов типа Фибоначчи с использованием программной реализации	19
	Итого за 5 семестр	**55.00**
6 семестр		
4.	Лабораторная работа аудиторная Исследование процесса шифрования без передачи ключа с использованием программной реализации	18
5.	Лабораторная работа аудиторная Исследование метода экспоненциального ключевого обмена на основе алгоритма Диффи-Хеллмана с использованием программной реализации	18
6.	**Лабораторная работа аудиторная Исследование процесса построения скрытого канала на основе схемы Эль-Гамаля с использованием программной реализации**	19
7.	**Итого за 6 семестр**	**55.00**

6. Методические рекомендации к СРС

При самостоятельном изучении тем лекционных и лабораторных работ дисциплины, студентам рекомендуется:

- в день проведения занятий проработать изученный на занятии учебный материал по конспекту лекций. При этом, необходимо выделить вопросы, на которые следует обратить большее внимание при дальнейшем изучении текущей темы. После изучения учебного материала необходимо ответить на рекомендуемые контрольные вопросы по конкретному занятию; - с целью качественного закрепления изученного материала следует более детально проработать учебный материал с использованием рекомендованной литературы. Рекомендованную литературу для каждого занятия необходимо уточнять у преподавателя.

Методика выполнения задания при конспектировании источников

Конспектирование источников проводится при детальном изучении темы с использованием рекомендованной литературы. При этом студентам рекомендуется:

- дополнять конспект лекционного занятия, лабораторной работы путем его расширения по наиболее важным вопросам, рассмотренным на занятии.

Конспектирование источников имеет цель дополнить конспект следующими положениями:

- основными определениями и описанием физического смысла;

- физическими принципами построения технических средств цифровой передачи информации и обработки сигналов в них с графическими иллюстрациями;

- основными характеристиками цифровой передачи информации и их практическим применением в телекоммуникационных системах;

- основными математическими соотношениями с раскрытием их физического смысла;

- выводами по учебным вопросам, изучаемой темы занятий.

Контроль этого вида самостоятельной работы осуществляется на учебных занятиях путем проверки преподавателем конспекта лекций и подготовки к лабораторным занятиям.

При конспектировании источников студенты должны исходить из рационального объема, конспектируемого материала. Конспект должен быть кратким и понятным при его использовании после изучения текущей темы.

При конспектировании источников рекомендуется отдельные рисунки, наиболее важные их фрагменты, наиболее важные формулы выделять цветом. При ведении конспекта на занятии рекомендуется заполнять две трети страницы листа тетради по вертикали, а свободную часть использовать при дополнении конспекта, по изучаемому вопросу.

Методика выполнения задания при подготовке к лабораторным работам:

Подготовка к лабораторным работам предусматривает изучение и закрепление учебного материала, рассмотренного на предыдущих лекциях и лабораторных работах, а так же при подготовке отчета по предыдущей лабораторной работе. Отчет по лабораторной работе должен включать:

- тему и цель лабораторной работы;
- задание на лабораторную работу;
- последовательное изложение каждого задания (положения теоретического обоснования, расчеты, выработанные предложения, пояснения, выводы по каждому заданию лабораторной работы).

При подготовке к лабораторной работе студенты должны подготовить ответы на контрольные вопросы, защищаемого задания. Контроль этого вида самостоятельной работы осуществляется при защите лабораторной работы.

Зачет проводится в 5 семестре и является накопительной формой отчетности, и проставляется по результатам выполнения и защиты лабораторных занятий в форме устного опроса.

Экзамен проводится в 6 семестре в форме устного опроса.

Вопросы к экзамену
(устная форма)

1. История криптографии
2. Характер криптографической деятельности
3. Простейшие шифры и их свойства. Шифр простой замены. Таблица Виженера
4. Композиции шифров
5. Блочные шифры и их свойства
6. Поточные шифры и их свойства
7. Различия между программными и аппаратными реализациями
8. Криптографические параметры узлов и блоков шифраторов
9. Методы получения случайных и псевдослучайных последовательностей
10. Линейные регистры сдвига
11. Блочные системы шифрования
12. Американский стандарт DES
13. Принцип построения ключей в алгоритме DES
14. Особенность алгоритма шифрования упрощенного DES.
15. Построение алгоритма получения ключей в S-DES
16. Стандарт шифрования данных ГОСТ 28147-89
17. Поточные системы шифрования
18. Принципы построения поточных шифрсистем
19. Синхронизация поточных шифров, принципы построения
20. Примеры поточных шифров
21. Методы реализации шифров
22. Программные реализации шифров
23. Особенности использования вычислительной техники в криптографии
24. Алгебраические модели шифров
25. Основные требования к шифрам
26. Системы шифрования с открытым ключом Шифрсистема RSA

27. Шифрсистема Эль-Гамаля
28. Шифр система без передачи ключа
29. Шифрсистема Мак-Элиса
30. Надежность шифров
31. Криптографическая стойкость шифров
32. Криптоатаки на шифры, оценки эффективности криптоатак
33. Теоретико-информационный подход к оценке криптостойкости шифров.
34. Совершенные шифры.
35. Теоретическая стойкость шифра. Стойкость шифров
36. Вопросы практической стойкости шифров
37. Рабочие характеристики шифров. Средний объем работы.
38. Имитостойкость и помехоустойчивость шифров
39. Оценка параметров имитостойкости шифров.
40. Помехоустойчивость шифра.
41. Цифровые подписи
42. Цифровые подписи на основе шифрсистем с открытыми ключами
43. Общие положения, алгоритмы цифровых подписей
44. Цифровая подпись Эль-Гамаля
45. Цифровая подпись Фиата-Шамира
46. Ключевые системы
47. Передача ключа с использованием симметричного шифрования
48. Ключевые системы. Двусторонние протоколы распределения ключей. Трехсторонние протоколы.
49. Передача ключа с использованием асимметричного шифрования
50. Протоколы без использования цифровой подписи.
51. Открытое распределение ключей.
52. Криптографические хеш-функции
53. Функция хеширования и целостность данных
54. Определение и назначение хеш-функций. Задачи хеш-функций.

55. Ключевые функции хеширования

56. Основные требования к хеш-функциям.

57. Бесконечные функции хеширования.

58. Вопросы организации сетей засекреченной связи.

59. Основные принципы организации сетей засекреченной связи

60. Сети засекреченной связи, назначение, состав , принцип функционирования

61. Протоколы сетей

62. Схемы разделения секретов.

63. Идентификация

64. Фиксированные пароли

65. Атаки на фиксированные пароли

8. Рекомендуемая литература и Интернет-ресурсы

8.1. Основная литература:

- Рябко Б.Я. Фионов А.Н. Криптографические методы защиты информации. – М.: "Горячая линия-Телеком", 2012. - 229 с.
- Музыкантский А.И., Фурин В.В. Лекции по криптографии. – М.: МЦНМО, 2011. - 68 с.
- Глухов М. М. Круглов И. А., Пичкур А. Б., Черемушкин А. В. Введение в теоретико-числовые методы криптографии. – СПб.:"Лань", 2011. - 400 стр.
- Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДиК, 2008. – 448 с.
- Основы криптографии: Учебное пособие/Под ред. Алферова П.П. – М.:Гелиос, 2008. – 480 с.

8.2. Дополнительная литература:

- Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. – М.: "Бином. Лаборатория знаний", 2013. – 480 с.

- Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: "ДМК Пресс", 2008. – 448 с.
- Алферов А.П., Зубов А.Ю. и др. Основы криптографии: Учебное пособие, 2-е – М.: Гелиос АРВ, 2006 – 480 с.
- Баричев С.Г. Основы современной криптографии. Учебный курс. – М .: Телеком, 2007. – 129 с.
- Молдовян А.А. и др. Криптография. – СПб.: Лань, 2007. – 224 с.
- Введение в криптографию/Под ред В.В.Ященко. – М.: МЦНМО, 2006. – 288 с.

8.1.3. Методическая литература

- Калмыков И.А. Криптографические методы защиты информации. Учебное пособие (курс лекций), 2012. – 298 с.
- Калмыков И.А. Криптографические методы защиты информации. Учебное пособие (лабораторный практикум), 2012. –91с.

8.1.4. Интернет-ресурсы:

- http://msdn.microsoft.com/ru-ru/library/default.aspx
- http://msdn.microsoft.com/library/4w3ex9c2.aspx

8.1.5. Программное обеспечение:

Специализированные программные продукты Microsot Visual Studio версии не ниже 2010, MS SQL Server 2008.

8.2. Материально-техническое обеспечение дисциплины (модуля) Специализированные классы ПЭВМ