ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
(РОСАВИАЦИЯ)

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

Кафедра основ радиотехники и защиты информации

А.А. Антонов

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебно-методическое пособие
по проведению практических занятий

для студентов
специальности 10.02.05
очной формы обучения

Москва
ИД Академии Жуковского
2021

УДК 004.056+003.26
ББК 001.8
А72

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

Антонов А.А.
А72 Криптографические методы защиты информации [Текст] : учебно-методическое пособие по проведению практических занятий / А.А. Антонов. – М.: ИД Академии Жуковского, 2021. – 24 с.

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

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

УДК 004.056+003.26
ББК 001.8

В авторской редакции

Подписано в печать 28.05.2021 г.
Формат 60x84/16 Печ. л. 1,5 Усл. печ. л. 1,395
Заказ № 779/0519-УМП47 Тираж 40 экз.

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

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

ОБЩИЕ МЕТОДИЧЕСКИЕ УКАЗАНИЯ

При подготовке к практическому занятию студенты должны:

уяснить цель и порядок проведения занятия;

изучить материалы, изложенные на лекциях и в рекомендуемой литературе.

На занятии студент должен иметь конспект лекций и данное пособие.

Практическое занятие начинается с опроса студентов по знанию теоретических положений изучаемого практического занятия, проверяются знания по представленным контрольным вопросам.

Далее студенты решают приведенные в пособии задания с последующим обсуждением полученных результатов. В случае дистанционного обучения оформляется отчет.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2010.

2. Бабаш А.В., Баранова Е.К. Криптографические методы защиты информации. Учебник. – М.: Кнорус, 2020.

3. Жданов О.Н., Ушаков Ю.Ю. Задачник-практикум по криптографическим методам защиты информации. – М.: Национальный открытый университет «ИНТУИТ», 2016.

4. Болелов Э.А. Криптографические методы защиты информации. Часть 1. Симметричные криптосистемы. – М.: МГТУ ГА, 2011.

5. Болелов Э.А. Криптографические методы защиты информации. Часть 2. Асимметричные криптосистемы. – М.: МГТУ ГА, 2013.

Практическое занятие № 1

Свойства простейших шифров. Освоение процессов зашифрования и расшифрования для простейших шифров

1. Цель занятия - закрепление теоретических знаний и практическое освоение процессов зашифрования и расшифрования для простейших шифров.

2. Контрольные вопросы

1. Понятие криптосистемы. Классификация криптосистем. Основные требования к криптосистеме.

2. Алгебраическая и вероятностная модели шифра.

3. Шифры замены: определение, разновидности шифров замены.

4. Шифры перестановки: определение, разновидности шифров перестановки.

3. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Имеется открытый текст X=БЛОЧНЫЙ ШИФР. Получить криптограмму, если матрица шифрования имеет вид:

$F = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix}$, а блок состоит из двух букв.

Для решения задачи использовать шифр Хилла, основанный на линейной алгебре.

Задача № 2

Криптограмма, имеющая вид Y=TEEEPJWQDPGY, получена линейным шифрующим преобразованием биграмм 26 буквенного латинского алфавита с числовыми эквивалентами от 0 до 25. Расшифровать сообщение при ключе равным $K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$.

Для нахождения обратного элемента по модулю необходимо использовать расширенный алгоритм Евклида.

Задача № 3

Имеется открытый текст X =АЛГЕБРАИЧЕСКАЯ АТАКА. Получить криптограмму, если матрица шифрования имеет вид:

$F = \begin{bmatrix} 5 & 4 & 4 \\ 4 & 5 & 6 \\ 3 & 2 & 5 \end{bmatrix}$, а блок состоит из трех букв.

Задача № 4

Расшифровать криптограмму Y=_впфнубжкйцбфёйебххшгжхсу. Открытый текст был записан в таблицу, после чего его столбцы были переставлены в соответствии с ключом К=(5,1,3,2,4). На втором этапе буквы первого столбца сдвинули на 1 позицию в алфавите (а=б, б=в, ..), второго - на две позиции, третьего - на 3, четвертого - на 4, пятого - на 5 позиций.

Задача № 5

Используется русский алфавит, буквы ё и е не различаются. Буквы алфавита кодируются следующим образом: каждой букве ставиться в соответствие двоичная запись ее номера, начиная с нуля. Таким образом, А =00000, Б=00001, В=00010 ...

Для передачи сообщения используется пять проводов, по каждому передается один разряд двоичного числа. При монтаже провода перепутали. Известно, что исходный текст был осмысленным. Восстановите его по сообщению: ЫАДАФЭС.

4. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 2

Освоение процессов зашифрования и расшифрования блочных криптосистем

1. Цель занятия - закрепление теоретических знаний и практическое освоение процессов зашифрования и расшифрования сообщений блочными симметричными криптосистемами

2. Контрольные вопросы

1. Симметричная криптосистема. Типы симметричных криптосистем.
2. Блочная криптосистема: понятие, принципы построения блочных криптосистем, достоинства и недостатки.
3. Режимы применения блочных криптосистем.
4. Криптосистема DES.

3. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Блочная криптосистема представлена схемой на рисунке 1.

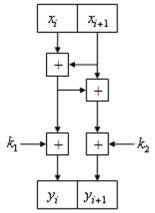

Рисунок 1 – Блочная криптосистема

Исходный текст разбивается на блоки по два символа, причем x_i нечетный символ, а x_{i+1} - четный. Все операции сложения вычисляются по модулю $m = |A|$.

Требуется зашифровать сообщение: $X =$АВСТРАЛИЯ. Ключ шифра - $K = \{k_1 = 3; k_2 = 7\}$.

Задача № 2

Блочная криптосистема имеет в своем составе S-блоки (блоки замены). Один из таких блоков осуществляет замену входного 4-х битового сообщения на выходное 3-х битовое сообщение в соответствии с таблицей:

a2a3a4 / a1	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**
0	4	6	1	3	5	7	2	5
1	5	7	2	4	6	1	3	6

Для следующих входных сообщений: 1101, 0010, 1010, 0101 найти сообщения на выходе S-блока.

Задача № 3

Блочная криптосистема имеет в своем составе S-блоки (блоки замены). Один из таких блоков осуществляет замену входного 4-х битового сообщения на выходное 2-х битовое сообщение в соответствии с таблицей:

a2a3 / a1a4	**00**	**01**	**10**	**11**
00	3	3	1	1
01	2	1	3	3
10	3	2	1	3
11	1	3	2	1

Для следующих входных сообщений: 1001, 0011, 1110, 0101 найти сообщения на выходе S-блока.

Задача № 4

Блочная криптосистема имеет в своем составе PE-блок, осуществляющий перестановку с расширением в соответствии с таблицей:

3	4	2	1	6	7	5	8	3	8	2	1

Для следующих входных сообщений: 11111001, 11000011, 00011110, 00000101 найти сообщения на выходе PE-блока.

4. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 3

Комбинирование криптосистем

1. Цель занятия - закрепление теоретических знаний по комбинированию криптосистем и практическое освоение процессов шифрования и расшифрования для комбинированных криптосистем

2. Контрольные вопросы

1. Криптосистема DES.
2. Криптосистема ГОСТ 28147-89.
3. Криптосистема AES.
4. Методы усложнения блочных симметричных криптосистем.

3. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Криптосистема является произведением шифра Виженера и шифра вертикальной перестановки. Зашифровать текст:

X =НЕВОЗМОЖНО ОБЪЯТЬ НЕОБЪЯТНОЕ

на ключе $K = \{$АМУР;3,5,2,1,4$\}$.

Сначала шифруется исходный текст шифром Виженера на ключе k_1=АМУР. Для второго криптографического преобразования строиться таблица 5×6 и в дальнейшем вписывается в нее полученная криптограмма.

Задача № 2

Зашифровать сообщение X =ВРАГИ - ЭТО БЫВШИЕ ДРУЗЬЯ, используя двукратное применение шифра «магический квадрат».

Магический квадрат:

2	7	6
9	5	1
4	3	8

Задача № 3

Зашифровать сообщение X = ИМПЕРАТОР ЦЕЗАРЬ.

1. Использую аффинный шифр Цезаря с ключами: K1=2, K2=3;
2. Получить криптограмму, если матрица шифрования имеет вид: $F = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix}$, а блок состоит из двух букв.

Задача № 4

Расшифровать сообщение $Y =$ РУЩХЧРЧРУЩВЁЧАК, полученное двукратным применением шифра Цезаря с ключом $K = \{3;12\}$.

Задача № 5

Вам предстоит подобрать пароль для входа в систему методом перебора. Известно, что пароль назначается компьютером и регулярно меняется, предыдущие пароли выглядят так:

abStwdRd
pVtrKRLp
iryzhToz
URbhhbEH
OJEXHZmJ
pzTDXJrZ

Какие выводы, можно сделать из условий задачи для ускорения процесса подбора пароля?

4. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 4

Криптоанализ простейших шифров замены

1. Цель занятия - закрепление теоретических знаний и выработка практических умений по применению методов криптоанализа простейших шифров

2. Контрольные вопросы

1. Метод полного перебора
2. Частотный метод криптоанализа
3. Методы линейного и дифференциального криптоанализа

3. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Имеется криптограмма: $Y =$СХТХУФЖ, полученная шифром Цезаря. Требуется методом полного перебора определить ключ шифра и прочесть сообщение.

Задача № 2

Определить ключ шифра Цезаря, если известна пара «открытый текст-криптограмма»: $X =$КРИПТОЛОГИЯ – $Y =$ПХНФЧУРУЗНД.

Задача № 3

Определить ключ шифра Цезаря, если даны пары «открытый текст-криптограмма»:

1) $X =$АПЕЛЬСИН – $Y =$САЦЬНВЩЮ;

2) $X =$АБРИКОС – $Y =$ЫЬЛГЕЙМ.

Задача № 4

Даны две криптограммы:

$Y =$ВЖТЕЛД;

$Y' =$ВЕЖСИЛБ.

Известно, что при шифровании текстов использовалась одна и та же γ-последовательность, причем вторая криптограмма Y' есть результат шифрования текста, полученного за счет видоизменения первого текста, а именно, за счет вставки после первой буквы произвольной буквы Г. Требуется определить γ-последовательность и прочитать текст.

Задача № 5

Перевести в двоичный вид S-блок криптосистемы S-DES.

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

Провести анализ переведенных в двоичный код таблицы S_1. На основе таблицы составить наиболее эффективные линейные уравнения.

4. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 5

Криптоанализ простейших шифров перестановки

1. Цель занятия - закрепление теоретических знаний и выработка практических умений по применению методов криптоанализа простейших шифров.

2. Контрольные вопросы

1. Метод чтения в колонках
2. Бесключевые методы криптоанализа простейших шифров
3. Метод «протяжки» вероятного слова

3. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Задана криптограмма: $Y =$СШЫУЙА, если известно, что при шифровании использована не равновероятная гамма, у которой все символы, кроме А, Б, И имеют нулевую вероятность. Априорно известно, что криптограмма представляет собой зашифрованное название одной из стран мира. Необходимо расшифровать криптограмму.

Задача № 2

Первая криптограмма получена из исходного текста перестановкой букв. Вторая получена из исходного текста заменой каждой буквы на другую букву так, что разные буквы заменены разными, а одинаковые - одинаковыми. Восстановите исходное сообщение.

Первый текст:

ИТШИЬОКТСОГМАОФОКЕТАПССЕОНССЫАВМЬЮЗТЫТАФОЬВВБ АСОЖЕЗТСИНЙАЯРРРОСНМЯПННОАТШАОВО

Второй текст:

ФЯРФРУЧРФЦЫСАБОВЯОРЦАГРФЦРЭЦЫГФИГРХНРШЧДНВЦВТВ НЧВЧИЖРЧВХДГВИЦФЭФЦРЛТРФЦЫМСАБОВ

Задача № 3

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

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

l	*f(l)*		*l*	*f(l)*		*l*	*f(l)*		*l*	*f(l)*
-	0,175		О	0,09		Е,Ё	0,72		А	0,062
И	0,062		Т	0,053		Н	0,053		С	0,045
Р	0,040		В	0,038		Л	0,035		К	0,028
М	0,026		Д	0,025		П	0,023		У	0,021
Я	0,018		Ы	0,016		З	0,016		Ь, Ъ	0,014
Б	0,014		Г	0,013		Ч	0,012		Й	0,010
Х	0,009		Ж	0,007		Ю	0,006		Ш	0,006
Ц	0,004		Щ	0,003		Э	0,003		Ф	0,002

Необходимо расшифровать сообщение:

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

Задача № 4

Задана криптограмма Y=ЫОЕЧТТОУ_СНСОРЧТРНАИДЬН_Е. Известно, что шифрование производилось сначала по столбцам, а затем по строкам. Необходимо расшифровать криптограмму.

4. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 6

Изучение идеально стойких криптосистем

1. Цель занятия - закрепление теоретических знаний по вопросам стойкости криптосистем и выработка практических умений по оценке расстояния единственности шифра.

2. Контрольные вопросы

1. Понятие совершенно стойкой криптосистемы.
2. Теорема Шеннона.
3. Теорема о совершенной стойкости шифра Вернама.

3. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Источник открытых сообщений без памяти характеризуется следующими параметрами: алфавит $A = \{a, b, c\}$ вероятности символов алфавита - $P(a) = 0{,}8,\ P(b) = 0{,}15,\ P(c) = 0{,}05.$

Используется шифр простой перестановки, причем все ключи равновероятные и имеют вид:

$k = 1: (a, b, c);$

$k = 2: (a, c, b);$

$k = 3: (b, a, c);$

$k = 4: (b, c, a);$

$k = 5: (c, a, b);$

$k = 6: (c, b, a).$

Перехвачена криптограмма: $Y = cccbc$. Требуется определить ключ.

Задача № 2

По имеющейся криптограмме найти апостериорные вероятности использованных ключей и соответствующие им сообщения, если известно, что используется шифр замены, а сообщения порождаются Марковским источником с матрицей вероятностей переходов:

$$\Pi = \begin{array}{c|ccc} & a & b & c \\ a & 0 & 0{,}9 & 0{,}1 \\ b & 0 & 0{,}1 & 0{,}9 \\ c & 0{,}4 & 0{,}3 & 0{,}3 \end{array}$$

и начальными вероятностями $P(a) = 0{,}19, P(b) = 0{,}34,\ P(c) = 0{,}47$:

1) $Y = bcacbcacc;$

2) $Y = caaabaaba;$

3) $Y = aaacaaaca.$

Используется шифр простой перестановки, причем все ключи равновероятные и имеют вид:

$k = 1: (a, b, c);$

$k = 2: (a, c, b);$

$k = 3: (b, a, c);$

$k = 4: (b, c, a);$

$k = 5: (c, a, b);$

$k = 6: (c, b, a).$

Задача № 3

Оценить расстояние единственности шифра Виженера со случайным ключевым словом длиной 4 символа для сообщений на английском языке. При средней длине сообщений равной h=1,5.

Задача № 4

Оценить расстояние единственности криптосистемы. Криптосистема представляет собой шифр простой перестановки. алфавит $A = \{a, b, c\}$ вероятности символов алфавита - $P(a) = 0{,}8,\ P(b) = 0{,}15,\ P(c) = 0{,}05.$

Используется шифр простой перестановки, причем все ключи равновероятные и имеют вид:

$k = 1: (a, b, c);$

$k = 2: (a, c, b);$

$k = 3: (b, a, c);$

$k = 4: (b, c, a);$

$k = 5: (c, a, b);$

$k = 6: (c, b, a).$

Перехвачена криптограмма: $Y = cccbc.$

4. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 7

Криптосистемы с открытым ключом

1. Цель занятия - закрепление теоретических знаний и практическое освоение процессов шифрования и расшифрования сообщений криптосистемами с открытым ключом.

2. Контрольные вопросы

1. Односторонняя функция.
2. Типы используемых односторонних функций.
3. Криптосистема с открытым ключом: понятие криптосистемы с открытым ключом, принципы построения, достоинства и недостатки.
4. Криптосистема Эль-Гамаля.
5. Криптосистема RSA.

3. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Передаваемое сообщение $x = 15$. Параметры криптосистемы Эль-Гамаля: $p = 23$, $g = 5$, $c_B = 13$. Сформировать криптограмму и восстановить открытый текст.

Задача № 2

Для криптосистемы Эль-Гамаля с заданными параметрами p, g, c_B и k найти недостающие параметры и описать процесс передачи сообщения x:

а) $p = 19$, $g = 2$, $c_B = 5$, $k = 7$, $x = 5$;

б) $p = 23$, $g = 5$, $c_B = 8$, $k = 10$, $x = 10$;

в) $p = 17$, $g = 3$, $c_B = 10$, $k = 5$, $x = 10$.

Задача № 3

Сформировать криптограмму и восстановить открытое сообщение, если криптосистема RSA имеет следующие параметры: $p_B = 3$, $q_B = 11$, $n_B = 33$ и открытый ключ - $d_B = 3$. Исходное сообщение необходимо взять из условия задачи 1.

Задача № 4

В криптосистеме RSA с заданными параметрами p_B, q_B, d_B найти недостающие параметры и описать процесс передачи сообщения x:

а) $p_B = 5$, $q_B = 11$, $d_B = 3$, $x = 12$;

б) $p_B = 7$, $q_B = 13$, $d_B = 5$, $x = 30$;

в) $p_B = 3$, $q_B = 11$, $d_B = 3$, $x = 15$.

4. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 8

Изучение алгоритма Шенкса, алгоритма исчисления порядка Адлемана и алгоритма Сильвера-Полига-Хеллмана

1. Цель занятия - закрепление теоретических знаний и выработка практических умений по применению методов криптоанализа криптосистем с открытым ключом.

2. Контрольные вопросы

1. Методы криптоанализа криптосистем с открытым ключом.
2. Метод криптоанализа «шаг младенца, шаг великана».
3. Метод исчисления порядка.

3. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Используя метод «шаг младенца, шаг великана» найти решение уравнений:

а) $2^x \bmod 23 = 9$;

б) $2^x \bmod 29 = 21$;

в) $3^x \bmod 31 = 25$;

г) $6^x \bmod 41 = 21$,

Задача № 2

Используя алгоритм исчисления порядка найти решение уравнений:

а) $10^x \bmod 47 = 37$;

б) $2^x \bmod 53 = 24$;

в) $7^x \bmod 71 = 41$;

г) $2^x \bmod 61 = 45$.

4. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 9

Изучение алгоритма Ферма и алгоритмов Полларда

1. Цель занятия - закрепление теоретических знаний и выработка практических умений по применению методов криптоанализа криптосистем с открытым ключом.

2. Контрольные вопросы

1. Алгоритм Ферма
2. Алгоритм Лемана модифицированный
3. Алгоритмы Полларда

3. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Разложить на множители число n=1387 используя алгоритм факторизации Ферма.

Задача № 2

Разложить на множители число n=517 используя метод факторизации Лемана.

Задача № 3

Разложить на множители число n=1387 используя $(p-1)$-метод Полларда.

4. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 10

Изучение алгоритмов, основанных на свойствах открытого ключа

1. Цель занятия - закрепление теоретических знаний и выработка практических умений по применению методов криптоанализа криптосистем с открытым ключом.

2. Контрольные вопросы

1. Криптоанализ на основе решения сравнения
2. Атака на основе Китайской теоремы об остатках
3. Алгоритм бесключевого чтения

3. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Пусть в наличии имеется открытый ключ (N=31459, e=5) и набор открытых пар соответствующих друг другу исходных и зашифрованных сообщений: (23, 18707), (755, 26871), (631, 6384).

Требуется расшифровать сообщение y=11638 используя криптоанализ на основе решения сравнения.

Задача № 2

Три пользователя сети имеют попарно взаимно простые модули N1=115, N2=187, N3=1363 и общий ключ шифрования e=3. Всем пользователям было послано сообщение X, Причем пользователи получили сообщения y1=95, y2=52, y3=622.

Необходимо найти x, используя атаку на основе Китайской теоремы об остатках.

Задача № 3

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

Начальные условия заданы таблицей:

	1	*2*
N	2419	4183
e1	7	7
e2	3	5
Y1	2412	51
Y2	13	3358

4. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 11

Изучение алгоритмов, основанных на свойствах закрытого ключа

1. Цель занятия - закрепление теоретических знаний и выработка практических умений по применению методов криптоанализа криптосистем с открытым ключом

2. Контрольные вопросы

1. Атака методом цепных дробей.
2. Атака повторным шифрованием.
3. Криптосистемы, основанные на задаче «об укладке рюкзака»

3. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Пусть задан открытый ключ (n,e)=(4617790059809965777, 2693216516134636609). Необходимо найти d (значение закрытого ключа) методом цепных дробей?

Задача № 2

Заданы значения: модуля шифрования **N**, отрытого ключа **e** и шифротекста **Y.** Необходимо используя метод перешифрования найти значение открытого текста **X,** не находя значения секретного ключа. Значения заданы таблицей:

	1	*2*
N	209	133
e	7	7
Y	107	117

Задача № 3

Сообщение зашифровано с помощью шифра на основе проблемы рюкзака. Расшифровать его Y=295 с помощью закрытого ключа – (2, 5, 8,16, 31, 63, 125), m=251 и n=56.

4. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 12

Электронная подпись

1. Цель занятия - закрепление теоретических знаний и практическое освоение алгоритмов формирования электронной цифровой подписи.

2. Контрольные вопросы

1. Электронная подпись на основе криптосистемы RSA.
2. Электронная подпись на базе криптосистемы Эль-Гамаля.

3. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Построить электронную подпись RSA для заданного сообщения x и известного значения его хэш-функции при следующих параметрах пользователя:

а) $p=5,\ q=11,\ c=27,\ h_X=13;$

б) $p=5,\ q=11,\ c=27,\ h_X=7;$

в) $p=5,\ q=13,\ c=29,\ h_X=10;$

г) $p=7,\ q=13,\ c=29,\ h_X=15.$

При формировании подписи считать, что $x=h_X$.

Задача № 2

Для указанных параметров пользователей RSA проверить подлинность подписанных сообщений:

а) $n=55,\ d=3;\ \langle 7,28\rangle,\ \langle 22,15\rangle,\ \langle 16,36\rangle;$

б) $n=65,\ d=5;\ \langle 6,42\rangle,\ \langle 10,30\rangle,\ \langle 6,41\rangle;$

в) $n=91,\ d=5\ \langle 15,71\rangle,\ \langle 11,46\rangle,\ \langle 16,74\rangle.$

Задача № 3

Для сети, абоненты которой применяют подпись Эль-Гамаля с общими параметрами $p=23,\ g=5$, построить подпись:

а) $c=7,\ k=5,\ h_X=3;$

б) $c=11,\ k=3,\ h_X=15;$

в) $c=10,\ k=15,\ h_X=5;$

с) $c=3,\ k=13,\ h_X=8.$

При формировании подписи считать, что $x=h_X$.

Задача № 4

Для указанных открытых ключей d пользователей системы Эль-Гамаля с общими параметрами $p=23,\ g=5$ проверить подлинность подписанных сообщений:

а) $d=22$: $\langle 15,20,3\rangle$, $\langle 15,10,5\rangle$, $\langle 15,19,3\rangle$;

б) $d=9$: $\langle 5,19,17\rangle$, $\langle 7,17,8\rangle$, $\langle 6,17,8\rangle$;

в) $d=11$: $\langle 15,7,1\rangle$, $\langle 10,15,3\rangle$, $\langle 15,7,16\rangle$.

4. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 13

Криптографические генераторы

1. Цель занятия - закрепление теоретических знаний и выработка практических умений по применению алгоритмов генерации псевдослучайных последовательностей

2. Контрольные вопросы

1. Конгруэнтные криптографические генераторы.
2. LFSR – генераторы.

3. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Линейный конгруэнтный генератор с параметрами $a=5,\ c=10,\ n=23$ порождает псевдослучайную последовательность x_i, $i=\overline{1,N}$. Определить значение двадцатого члена псевдослучайной последовательности.

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

состоит в минимальных отличиях по статистическим характеристикам последовательности $\{x_i\}$ от РРСП.

Конгруэнтные криптографические генераторы. Конгруэнтные криптографические генераторы бываю линейными, нелинейными и мультипликативные.

Линейным конгруэнтным генератором называется генератор, порождающий псевдослучайную последовательность $\{x_i\} \in A$, $A = \{0,1,...,N-1\}$ с помощью рекуррентного соотношения

$$x_{i+1} = (ax_i + c) \bmod N,\ i = \overline{0,\infty}.$$

Задача № 2

Для условий задачи 1 определить значение двадцатого члена псевдослучайной последовательности. Для общего члена последовательности $\{x_i\} \in A$ справедлива формула: $x_i = \left(a^i x_0 + \frac{a^i - 1}{a-1} c \right) \bmod N,\ i \geq 1.$

Задача № 3

Дан квадратичный конгруэнтный генератор с параметрами $a = 3,\ c = 11,$ $d = 6,\ n = 16$ и начальным состоянием $x_0 = 10$. Определить значения первых шести членов псевдослучайной последовательности и найти значение наибольшего периода этой последовательности $T_{\max}$.

Задача № 4

Построить блок-схему конгруэнтного генератора с переносом с параметрами $a = 7,\ n = 19$ и начальным состоянием $x_0 = 1,\ c_0 = 5.$ Сформировать первых пятнадцать значений псевдослучайной последовательности и определить период псевдослучайной последовательности.

Конгруэнтный генератор, использующий умножение с переносом определяется рекуррентным соотношением

$$x_i = (ax_i + c_i) \bmod N,\ i = \overline{0,\infty},$$

где приращение $c_i \in A$ изменяется во времени и нелинейно зависит от параметров генератора на предыдущем шаге: $c_i = \left\lfloor \frac{ax_{i-1} + c_{i-1}}{N} \right\rfloor$. Параметры x_0, c_0 являются стартовыми параметрами генератора.

4. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 14

Изучение алгоритмов Кнута и NIS. Криптографические генераторы

1. Цель занятия - закрепление теоретических знаний и выработка практических умений по применению алгоритмов генерации псевдослучайных последовательностей

2. Контрольные вопросы

1. Криптографические генераторы Фибоначчи.
2. Комбинированные криптографические генераторы.

3. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Генератор LFSR состоит из $N=5$ ячеек памяти. Начальные состояния ячеек памяти определяются вектором $S_0=(11011)$, а вектор коэффициентов передачи имеет вид $a=(11100)$.

Построить структурную схему генератора LFSR и определить первых десять членов псевдослучайной последовательности.

Генератор LFSR состоит из n ячеек памяти, двоичные состояния которых в дискретные моменты времени $t=0,1,2,...$ характеризуются $S_0(t),S_1(t),S_2(t),\ldots,S_{n-1}(t)\in A=\{0,1\}$.

Выходы ячеек памяти связаны не только последовательно друг с другом, но и с сумматорами $\oplus$ в соответствии с коэффициентами передачи $a_0,a_1,a_2,...,a_{n-1}\in A$. Если $a_i=1$, то значение $S_i(t)$ i-й ячейки передается на один из входов i-го сумматора, ели же $a_i=0$, то такая связь отсутствует. Полагается, что $a_1=1$.

Содержание ячеек памяти генератора LFSR с течением времени изменяется следующим образом, определяя тем самым динамику состояний

$$S_i(t+1)=\begin{cases} S_{i+1}(t), & \text{если} \quad i\in\{0,1,...,n-2\},\\ \sum_{j=0}^{n-1} a_j S_j(t), & \text{если} \quad i=n-1, \end{cases}$$

Задача № 2

Определить десять первых значений псевдослучайных последовательностей, порождаемые генератором Фибоначчи для $\Diamond\in\{+,\times\}$ и $k=3$. Параметры генератора: $r=3$, $s=2$, начальные значения $x_0=(1,7)$.

Общий вид рекуррентного соотношения, определяющего генератор Фибоначчи, задается уравнением:

$$x_t = x_{t-r} \Diamond x_{t-s},\ t = r, r+1, r+2, \ldots$$

где $r, s \ \ (r > s)$ - параметры генератора; $\Diamond$ - символ бинарного отношения: $\Diamond \in \{+, -, \times, \oplus\}$.

В случае $\Diamond \in \{+, -\}$ псевдослучайная последовательность $\{x_i\}$ представляет собой целые числа $\left(\bmod 2^k\right)$ для некоторого заданного k; в случае $\Diamond \in \{\times\}$ - нечетные числа $\left(\bmod 2^k\right)$; в случае $\Diamond \in \{\oplus\}$ - элемент x_i представляет собой двоичный вектор

Определить значение периода каждой псевдослучайной последовательности.

Задача № 3

Составить блок-схему и выполнить программную реализацию комбинированного LFSR генератора, включающего в себя $i = 3$ однотипных генератора. Параметры i-го LFSR генератора взять из условий задачи 6 за исключением вектора начального состояния, который требуется задать самостоятельно. Выходная функцию комбинированного LFSR генератора имеет вид:

$$F(x) = (x_1 + x_2 + x_3 + x_1 \oplus x_2 + x_1 \oplus x_3) \bmod 2.$$

Наиболее часто на практике комбинируют LFSR генераторы, которые так и называются *комбинированными LFSR генераторами*. Функция F имеет полиномиальный вид

$$\gamma = F(x) = \left(a_0 + \sum_{1 \le i \le M} a_i x_i + \sum_{1 \le i < j \le M} a_{ij} x_i x_j + \ldots + a_{12\ldots M} x_1 \cdots x_M \right) \bmod 2.$$

Так как каждая из последовательностей, порождаемая LFSR генераторами периодична, то и выходная последовательность $\{\gamma_i\}$ также периодична.

Комбинирование LFSR генераторов с помощью псевдослучайного прореживания. Это еще один из широко используемых способов комбинирования. Пусть LFSR генератор G_1 порождает элементарную последовательность $\{\xi_i\}$, а LFSR генератор G_2 - селектирующую последовательность $\{\eta_i\}$. С помощью двух последовательностей $\{\xi_i\}$ и $\{\eta_i\}$ строится выходная последовательность $\{x_j\}$, включающая те биты последовательности $\{\xi_i\}$, для который соответствующие биты селектирующей последовательности $\{\eta_i\}$ равны 1, т.е $\eta_i = 1$, в случае когда $\eta_i = 0$ - соответствующее значение последовательности $\{\xi_i\}$ отбрасывается. Такие генераторы носят название SG-генераторов (Shrinking Generator).

Еще один способ комбинирования генераторов. Пусть имеются два генератора G_1 и G_2. Комбинирование заключается в том, что параметры

генератора G_1 изменяются генератором G_2 с течением времени. Проиллюстрируем этот случай, когда G_1 - линейный конгруэнтный генератор

$$x_i = (a_i x_{i-1} + b_i) \bmod N,\ i = \overline{1,\infty}.$$

Параметры генератора G_1 $\mathbf{B}_i = \begin{bmatrix} a_i \\ b_i \end{bmatrix}$ есть некоторая псевдослучайная последовательность векторов, порождаемых генератором G_2.

4. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод