Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

И. В. Воробейкина

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

учебно-методическое пособие по выполнению лабораторных работ
для студентов специальности
10.05.03 «Информационная безопасность автоматизированных систем»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2022

Рецензент
доцент кафедры информационной безопасности ФГБОУ ВО
«Калининградский государственный технический университет
А. Г. Жестовский

Воробейкина, И. В.
Методы и средства криптографической защиты информации: учеб-методич. пособие по лабораторным работам для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» / И. В. Воробейкина. - Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 59 с.

Учебно-методическое пособие является руководством по проведению цикла лабораторных работ по дисциплине «Методы и средства криптографической защиты информации» студентами, обучающимися по специальности 10.05.03 «Информационная безопасность автоматизированных систем».

Лабораторные работы предназначены для закрепления теоретического материала.

Список лит. – 5 наименований

Учебно-методическое пособие рассмотрено и одобрено в качестве локального электронного методического материала кафедрой информационной безопасности 14 июня 2022 г., протокол № 09

Учебно-методическое пособие рекомендовано в качестве локального электронного методического материала к использованию в учебном процессе методической комиссией института цифровой технологии 28 июня 2022 г., протокол № 4

ОГЛАВЛЕНИЕ

Введение

Данное учебно-методическое пособие предназначено для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем, изучающих дисциплину «Методы и средства криптографической защиты информации».

Цель лабораторного практикума по дисциплине: изучение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Лабораторный практикум содержит 10 лабораторных работ.

Лабораторные работы проводятся в лабораториях кафедры.

В результате выполнения лабораторных работ ожидается, что студенты сформируют навыки применения математических методов, используемых в оценке стойкости криптосистем; получат необходимые практические навыки использования типовых криптографических алгоритмов.

Лабораторная работа № 1. Простой и расширенный алгоритм Евклида. Модульная арифметика. Операции в системе вычетов Z_n. Аддитивная и мультипликативная инверсии

ОБЩИЕ СВЕДЕНИЯ

Цель: познакомиться с модульной арифметикой, системой вычетов, усвоить понятие аддитивной и мультипликативной инверсий.

Материалы, оборудование, программное обеспечение: тетрадь, калькулятор.

Условия допуска к выполнению: показать конспект по теоретической подготовке.

Критерии положительной оценки: показать выполненную работу, четко ответить на вопросы, увязать последовательность изученных разделов дисциплины.

ТЕОРЕТИЧЕСКОЕ ВВЕДЕНИЕ

В криптографии применяются бинарных операции на множестве z целых чисел. У бинарных операций два входа и один выход. Для множества z определены три бинарных операции – умножение, сложение и вычитание. Эти операции имеют два входа (целые числа a и b) и выход (c). Для операции деления требуются два выхода. Уравнение деления: $a=q\times n+r$, где a – делимое, n – делитель, q – частное, r – остаток.

При использовании уравнения деления в криптографии существуют два ограничения:

1) делитель должен быть положительным целым числом ($n>0$);

2) остаток должен быть неотрицательным целым числом ($r\geq 0$).

Если числа a, r, q отрицательные, т. е. ограничение $r\geq 0$ не выполняется, можно уменьшить значение q на 1 и сложить значение n с r, чтобы r стало положительным.

Элементы теории делимости применяются в криптографии, поэтому рассмотрим следующие несколько свойств теории делимости.

1. Если $a|1$, то $a=\pm 1$,

2. Если $a|b$ и $b|a$, то $a=\pm b$,

3. Если $a|b$ и $b|c$, то $a|c$,

4. Если $a|b$ и $a|c$, то $a|(m\times b + n\times c)$, где m и n – произвольные целые числа.

Расширенный алгоритм Евклида.

Даны целые числа a и b. Найти два целых числа s и t такие, что $s \times a + t \times b = НОД(a,b)$.

В расширенном алгоритме Евклида выполняются те же самые шаги, что и в простом алгоритме Евклида. Но, в отличие от простого алгоритма, на каждом шаге применяются три группы вычислений. Переменным присваиваются начальные значения $r1=a$, $r2=b$, $s1=1$, $s2=0$, $t1=0$ и $t2=1$, r – остаток от деления $r1$ на $r2$.

Модульная арифметика

Уравнение деления ($a=q \times n+r$) имеет два входа (a и n) и два выхода (q и r). В модульной арифметике нас интересует только один выход – остаток r.

Операции по модулю.

Оператор *mod* называется оператором по модулю. Он определяет неотрицательный остаток r. Второй вход n называется модулем. Вывод r назван вычетом. То есть $a \bmod n = r$.

Система вычетов Z_n

Результат операции по модулю n – это целое число, удовлетворяющее условию: $0 \leq a \bmod n < n$. С помощью операция по модулю создается некоторое множество, которое в модульной арифметике понимается как система наименьших вычетов по модулю n, или Z_n. Существует много вычетов Z_n, но только одно для каждого значения n. Некоторые наборы Z_n:

$\boldsymbol{Z_n=\{0,1,2,3,\ldots,(n-1)\}}$, $Z_2=\{0,1\}$, $Z_6=\{0,1,2,3,4,5\}$, $Z_{11}=\{0,1,2,3,4,5,6,7,8,9,10\}$

Сравнения в модульной арифметике.

В криптографии часто используется понятие сравнения вместо равенства. Например, $3 \bmod 10 = 3$, $13 \bmod 10 = 3$, $33 \bmod 10 = 3$, и так далее. В модульной арифметике такие целые числа, как 3, *13*, и *33*, называются *сравнимыми по модулю 10 (mod 10)*. В общем случае они называются *сравнимыми по модулю n (mod n)*. Для указания, того, что числа сравнимы, используется оператор *(≡)*. Операция *mod n* добавляется к правой стороне сравнения. Например: $2 \equiv 12 \pmod{10}$, $13 \equiv 23 \pmod{10}$, $34 \equiv 24 \pmod{10}$, $-8 \equiv 12 \pmod{10}$, $3 \equiv 8 \pmod{5}$, $8 \equiv 13 \pmod{5}$, $23 \equiv 33 \pmod{5}$, $8 \equiv 2 \pmod{5}$.

Здесь обозначение (*mod n*) не имеет того же самого смысла, как в уравнении деления. То есть, оператор *mod* в выражении (*13 mod 10)* является оператором, а в сравнении $2 \equiv 12 \pmod{10}$ означает, что мы работаем на множестве целых чисел Z_{10}.

Аддитивная инверсия.

В Z_n два числа a и b аддитивно инверсны друг другу, если $b=n-a$. Значит, аддитивная инверсия *7* в Z_{10} равна $10 - 7 = 3$.

В системе вычетов любое число имеет только одну аддитивную инверсию. Справедливо утверждение: $a+b\equiv 0 \pmod n$.

Мультипликативная инверсия.

Если $a\times b\equiv 1 \pmod n$ в Z_n, то говорят, что два числа a и b мультипликативно инверсны друг другу. Например, если модуль равен *10*, то мультипликативной инверсией *3* будет *7* или $(3\times 7) \bmod 10\equiv 1$.

Не каждое число в модульной арифметике имеет мультипликативную инверсию. Число a имеет мультипликативную инверсию в Z_n, если $НОД(n, a) = 1$ (то есть когда a и n взаимно простые).

В криптографии часто приходится работать с инверсиями. Если отправитель **А** посылает секретный ключ (число), приемник **Б** берет инверсию этого числа, которое является ключом дешифрования. Если алгоритм шифрования/дешифрования является сложением, множество Z_n рассматривается как множество возможных ключей, ведь у каждого элемента Z_n есть аддитивная инверсия. Но если алгоритм шифрования/дешифрования – умножение, тогда Z_n не может рассматриваться как множество возможных ключей, так как известно, что не для всех элементов этого множества существует мультипликативная инверсия. Необходимо другое множество Z_{n*}, которое будет подмножеством Z_n и при этом включать в себя только целые числа, которые в Z_n имеют мультипликативную инверсию. Любой элемент из Z_n имеет аддитивную инверсию, но мультипликативная инверсия существует только для некоторых элементов; любой элемент из Z_{n*} имеет мультипликативную инверсию, но аддитивная инверсия существует только для некоторых элементов.

Литература:

Воробейкина, И. В. Методы и средства криптографической защиты информации: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения / И. В. Воробейкина; БГАРФ ФГБОУ ВО «КГТУ». – Калининград: Изд-во БГАРФ, 2022. - 114 с.

Глава I «Арифметика целых чисел. Модульная арифметика. Система вычетов Z_n**».**

ЗАДАНИЕ К ЛАБОРАТОРНОЙ РАБОТЕ

Освоить простой и расширенный алгоритмы Евклида для вычисления НОД, изучить построение системы вычетов, модульную арифметику

Вопросы, на которые необходимо дать ответ:

1. Что такое модульная арифметика?
2. Как строится система вычетов?
3. Могут ли в системе вычетов присутствовать дробные и отрицательные числа?

4. Верно ли утверждение: любой элемент системы вычетов имеет и аддитивную, и мультипликативную инверсии.

5. Вычисление наибольшего общего делителя.

6. Модульная арифметика. Операции по модулю.

7. Система вычетов z_n. Операции в системе вычетов z_n.

8. Аддитивная и мультипликативная инверсии.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Построить расширенный алгоритм Евклида.

Пример.

a = 161 и *b = 28*, найти *НОД (a, b)* и значения *s* и *t*.

Решение:

$r = r1 - q \times r2$ $s = s1 - q \times s2$ $t = t1 - q \times t2$.

Алгоритм отображен в следующей таблице:

q	r1	r2	r	s1	s2	s	t1	t2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0		-1	4		6	-23	

НОД *(161, 28) = 7, s = –1 и t = 6.* Проверка: *(–1)×161+6×28 = 7.*

Построить систему вычетов Z_{26}.

Пример построения Z_{10}:

Для *n = 10*, мы получаем множество из десяти элементов *[0], [1], [2], [3], [4], [5], [6], [7], [8], [9].*

для *n = 0: [0] = {…., –15, -10, –5, 0, 5, 10, 15, …},*

для *n = 1: [1] = {…., –14, –9, –4, 1, 6 , 11, 16,…},*

для *n = 2: [2] = {…., –13, –8, –3, 2, 7, 12, 17,…},*

для *n = 3: [3] = {…., –12, –7, –2, 3, 8, 13, 18,…},*

для *n = 4: [4] = {…., –11, –6, –1, 4, 9, 14, 19,…}* и так далее.

Найти все мультипликативно-инверсные пары в Z_{26} и построить соответствующую таблицу.

Пример.

27 mod 5=2,

36 mod 12=0,

-18 mod 14. Разделим *(-18)* на *14*, получим результат: *r=–4*. Чтобы сделать остаток неотрицательным, нужно прибавить модуль *(14)*. Получим: *r =-4 + 14 = 10*. Это означает, что *-18 mod 14 = 10.*

-7mod10. Разделим *(-7)* на *10*, получим результат: *r=–7*. После добавления модуля *(-7)* мы получаем *r=3*. Это означает, что *-7mod10=3.*

Пример.

Выполните следующие операции:

а. Сложить *7* и *14* в Z_{15}

б. Вычесть *11* из *7* в Z_{13}

в. Умножить *11* на *7* в Z_{20}

Решение:

(14+7) mod 15 → (21) mod 15 = 6

(7–11) mod 13 → (-4) mod 13 = 9

(7×11) mod 20 → (77) mod 20 = 17

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

Вариативность не предполагается.

1. Запишите свойства теории делимости.
2. Верно ли, что *5|25* и *25|50* то *5|50?* Почему?
3. Вычислите НОД(740,700) с помощью простого алгоритма Евклида.
4. С помощью расширенного алгоритма Евклида найти НОД(168,35) и значения *s* и *t*.
5. Запишите в фигурных скобках значения систем вычетов:

$Z_2=\{...\}$, $Z_{11}=\{...\}$, $Z_{26}=\{...\}$, $Z_{33}=\{...\}$

6. Запишите свойства оператора *mod:*

(a + b) mod n =

(a – b) mod n =

(a× b) mod n=

7. Выполните следующие операции:

а. сложить *117+ 20* в Z_{26}

б. вычесть *53– 112* в Z_{19}

в. умножить *120× (–8)* в Z_{33}

ТРЕБОВАНИЯ К ОТЧЕТУ И ЗАЩИТЕ

Показать выполненную в тетради работу. Знать ответы на сформулированные выше вопросы. Защита работы проводится во время занятий. После защиты работа помещается в ЭИОС.

Лабораторная работа № 2. Алгебраические структуры. Группа. Циклические подгруппы. Циклические группы. Кольцо. Поле. Поля $GF(p^n)$

ОБЩИЕ СВЕДЕНИЯ

Цель: научиться создавать циклические группы, уяснить место алгебраических структур в криптографии.

Материалы, оборудование, программное обеспечение:

Условия допуска к выполнению: показать конспект по теоретической подготовке.

Критерии положительной оценки: показать выполненную работу, четко ответить на вопросы.

ТЕОРЕТИЧЕСКОЕ ВВЕДЕНИЕ

Мы рассмотрели некоторые множества чисел, таких как Z, Z_n, Z_{n*}, Z_p и Z_{p*}. В криптографии требуется задание множества целых чисел и операций, определенных для них. В математике существуют **алгебраические структуры**, которые объединяют в себе некоторые множества и операции над этими множествами. Рассмотрим алгебраических структуры: группы, кольца и поля.

Группа.

Группа G – множество элементов произвольной природы с бинарной операцией "•", обладающее следующими свойствами:

1. Замкнутость. Если $a \in G$ и $b \in G$, то $c = a \bullet b \in G$.

2. Ассоциативность. Если $a \in G$, $b \in G$ и $c \in G$ – элементы G, то справедливо $(a \bullet b) \bullet c = a \bullet (b \bullet c)$.

3. Коммутативность. Для всех элементов $a \in G$ и $b \in G$ справедливо $a \bullet b = b \bullet a$. Группы, которые в дополнение к другим свойствам обладают свойством коммутативности, называются коммутативными или абелевыми группами.

4. Существование нейтрального элемента. Существует *нейтральный* элемент $e \in G$, такой, что $e \bullet a = a \bullet e = a$ для любого $a \in G$.

5. Существование инверсии. Для каждого $a \in G$ существует инверсия a', такая, что $a \bullet a' = a' \bullet a = e$.

В криптографии элементами группы будем считать вычеты.

Хотя группа включает единственный оператор, но позволительно использовать пары операций, если они инверсны друг другу: если в группе определен оператор сложение, то группа поддерживает и сложение, и вычитание, так как вычитание и сложение – аддитивно инверсные операции. Это утверждение справедливо для умножения и деления. Но группа может одновременно поддерживать только сложение/вычитание или умножение/деление, но не оба сочетания операторов одновременно.

Группа называется **конечной**, если ей принадлежит конечное число элементов; в противном случае – это бесконечная группа.

Количество элементов, принадлежащих группе, называется **порядком** группы. Порядок группы будет бесконечным, если группа бесконечна.

Пусть H – подмножество группы G. H называется **подгруппой** G, если H – группа относительно операции на G. То есть, если $G=<S,\bullet>$ – группа, $H=<T, \bullet>$ – группа для той же самой операции, и T – непустое подмножество S, то H – подгруппа G. Значит:

- если $a, b \in G$ и $a, b \in H$, то $c=a\bullet b \in G$ и $c=a\bullet b \in H$;
- нейтральный элемент e один и тот же для G и H;
- пусть $e \in G$ и $e \in H$, тогда инверсия $a' \in G$ и $a' \in H$;
- группа, единственным элементом которой является нейтральный элемент G, $H=<\{e\},\bullet>$, является подгруппой G;
- каждая группа является подгруппой для самой себя.

Циклические подгруппы.

Подгруппа H группы G называется **циклической**, если H можно создать при помощи возведения в степень некоторого элемента группы G. Возведение в степень здесь означает многократное применение к элементу операции группы:

$a^n \rightarrow a\bullet a\bullet a\bullet \ldots \bullet a$ (n раз).

Множество, полученное в результате этого процесса, обозначается $<a>$. Здесь также $a^0 = e$.

Циклические группы.

Циклической называется группа, которая является собственной циклической подгруппой. В примере 2.4 группа G имеет циклическую подгруппу $H_5 = G$. Значит, группа G – циклическая группа. В этом случае элемент, генерирующий циклическую подгруппу, может также генерировать саму группу. Этот элемент именуется **генератором**. Если g – генератор, элементы в конечной циклической группе записываются как $\{e, g, g^2, \ldots\ldots, g^{n-1}\}$, где $g^n = e$.

Циклическая группа может иметь много генераторов.

Кольцо.

Кольцо $R=\{\ldots\},\bullet,\perp$ – это алгебраическая структура с двумя операциями. Первая операция должна удовлетворять пяти свойствам абелевой группы, вторая – только первым двум свойствам абелевой группы (см. п. 2.1.1. Группа). Кроме того, вторая операция должна быть распределена с помощью первой. Дистрибутивность означает, что для всех элементов a, b и c, принадлежащих R, справедливо: $a\perp(b\bullet c)=(a\perp b)\bullet(a\perp c)$ и $(a\bullet b)\perp c=(a\perp c)\bullet(b\perp c)$.

Коммутативное кольцо – кольцо, в котором коммутативное свойство удовлетворено и для второй операции. Множество Z с двумя операциями –

сложением и умножением – является коммутативным кольцом, которое обозначается $R=Z,+,\times$. Сложение удовлетворяет пяти свойствам; умножение удовлетворяет только трем свойствам.

Поле.

Поле $F=\{...\},\bullet,\perp$ – коммутативное кольцо, в котором вторая операция удовлетворяет пяти свойствам (см. п. 2.1.1. Группа), определенным для первой операции, за исключением того, что нейтральный элемент первой операции (нулевой элемент) не имеет инверсии.

Поле – структура, которая поддерживает две пары операций, используемые в математике: сложение/вычитание и умножение/деление.

В криптографии используются только конечные поля. Галуа показал, что поля, чтобы быть конечными, должны иметь число элементов p^n, где p – простое, а n – положительное целое число. Конечные поля обычно называют **полями Галуа** и обозначают как $GF(p^n)$.

Поле Галуа $GF(p^n)$ – конечное поле с p^n элементами.

При $n=1$ получаем поле $GF(p)$. Это поле может быть множеством $Z_p=\{0, 1,...,p–1\}$ с двумя арифметическими операциями (сложением и умножением). Любой элемент в этом множестве имеет аддитивную инверсию, и элементы, отличные от нуля, имеют мультипликативную инверсию (мультипликативная инверсия для *0* отсутствует по причине невозможности деления на *0*).

В криптографии также используются поля $GF(p^n)$. Множества Z, Z_n, Z_{n*} и Z_p, которые мы рассматривали до сих пор с операциями сложения и умножения, не могут удовлетворить требованиям поля. Поэтому должны быть определены некоторые новые множества и некоторые новые операции на этих множествах. Таким множеством является поле GF(2n).

Литература:

Воробейкина, И. В. Методы и средства криптографической защиты информации: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения / И. В. Воробейкина; БГАРФ ФГБОУ ВО «КГТУ». – Калининград: Издательство БГАРФ, 2022. - 114 с.

Глава 2. Алгебраические структуры. Группы, кольца, поля

ЗАДАНИЕ К ЛАБОРАТОРНОЙ РАБОТЕ

Изучить свойства алгебраических структур и уяснить их применение в криптографии. Научиться генерировать циклические группы и подгруппы.

Вопросы, на которые необходимо дать ответ:

1. Перечислить изученные алгебраические структуры.
2. Что такое коммутативная группа?

3. Сколько операций определено на кольце?
4. Что такое генератор циклической группы?
5. Дайте определение поля Галуа.
6. Чем отличается кольцо от поля? От группы?

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Пример.

Вычет $G=<Z_n, +>$, является коммутативной группой. Результат операций сложения/вычитания на элементах множества Z_n также принадлежит этому множеству. Проверим свойства группы:

– результат сложения двух целых чисел в Z_n принадлежит Z_n, следовательно, замкнутость удовлетворяется;

– ассоциативность тоже удовлетворяется – например, $3+(2+1)=(3+2)+1$;

– коммутативность выполняется – например, $2 + 4 = 4 + 2$;

– нейтральный элемент – 0, например, $2 + 0 = 0 + 2 = 2$;

– также каждый элемент имеет аддитивную инверсию – например, инверсия 2 это $(–2)$ и инверсия $(–2)$ это 2; заметим, что инверсия позволяет выполнять вычитание на нашем множестве.

Пример.

Группа $G = <Z_n, *>$ является абелевой. Результат операции умножения/деления на элементах множества Z_n принадлежит этому множеству. Имеется нейтральный элемент, равный 1. И для каждого элемента существует инверсия.

Пример.

Дана группа $G=<Z_{10*}, \times>$, найдем для нее циклические подгруппы. Циклические подгруппы – $H_1=<\{1\}, \times>$, $H_2=<\{1,9\}, \times>$ и $H_3=G$, так как G имеет только четыре элемента: 1, 3, 7 и 9.

а. Циклическая подгруппа, сгенерированная на основе 1, – это H_1 и имеет только один элемент – нейтральный.

$1^0 \bmod 10 = 1$ (далее процесс повторяется).

б. Циклическая подгруппа, сгенерированная на основе 3, – это H_3, которая и есть сама группа G.

$3^0 \bmod 10 = 1$

$3^1 \bmod 10 = 3$

$3^2 \bmod 10 = 9$

$3^3 \bmod 10 = 7$ (дальнейшие вычисления прекращаем, так как результаты повторяются).

в. Циклическая подгруппа, сгенерированная на основе *7*, – это H_3, является группой *G*.

$7^0 \bmod 10 = 1$

$7^1 \bmod 10 = 7$

$7^2 \bmod 10 = 9$

$7^3 \bmod 10 = 3$ (дальнейшие вычисления прекращаем, так как результаты повторяются).

г. Циклическая подгруппа, сгенерированная на основе *9*, – это H_2. Подгруппа имеет только два элемента.

$9^0 \bmod 10 = 1$

$9^1 \bmod 10 = 9$ (дальнейшие вычисления прекращаем, так как результаты повторяются).

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

Вариативность не предполагается.

1. Докажите, что вычет $G=<Z_4, +>$, является коммутативной группой.
2. Дана группа $G=<Z_5,+>$, найти ее циклические подгруппы.
3. Что такое поле Галуа?

ТРЕБОВАНИЯ К ОТЧЕТУ И ЗАЩИТЕ

Показать выполненную в тетради работу. Знать ответы на сформулированные выше вопросы. Защита работы проводится во время занятий. После защиты работа помещается в ЭИОС.

Лабораторная работа № 3. Аффинный шифр. Шифр Плейфера. Шифр Виженера. Шифр Хилла

ОБЩИЕ СВЕДЕНИЯ

Цель: познакомиться с шифрованием. Изучить шифры подстановки и криптоанализ.

Материалы, оборудование, программное обеспечение:

Условия допуска к выполнению: показать конспект по теоретической подготовке.

Критерии положительной оценки: показать выполненную работу, четко ответить на вопросы.

ТЕОРЕТИЧЕСКОЕ ВВЕДЕНИЕ

Шифрование с симметричными ключами использует один и тот же ключ и для кодирования, и для дешифрования. Здесь алгоритмы шифрования и дешифрования инверсны друг другу. Пусть P – исходный текст, C – зашифрованный текст, а K – ключ. Алгоритм кодирования $E_k(x)$ создает зашифрованный текст из исходного текста, а алгоритм дешифрования $D_k(x)$ создает исходный текст из зашифрованного текста. То есть, $E_k(x)$ и $D_k(x)$ инверсны относительно друг друга.

Эти операции принято обозначать так: шифрование: $C = E_k(P)$, дешифрование: $P = D_k(C)$, где $D_k(E_k(x))=E_k(D_k(x))=x$.

Еще один элемент в шифровании симметричными ключами – количество ключей. В самом деле, для группы из m человек, в которой каждый должен иметь возможность связываться друг с другом, необходимо $(m\times(m–1))/2$ ключей (каждому человеку надо $(m–1)$ ключ), но ключ между двумя человеками может использоваться в обоих направлениях.

Аффинный шифр – комбинация аддитивного и мультипликативного шифров с парой ключей. Первый ключ используется мультипликативным шифром, второй – аддитивным шифром. Аффинный шифр – фактически два шифра, применяемые один за другим. При аффинном шифре отношение между исходным текстом P и шифрованным текстом C определяется, как это показано ниже.

$C = (P\times k_1 + k_2) \bmod 26$ $P = ((C – k_2)\times k_1^{-1}) \bmod 26$,

где k_1^{-1} мультипликативная инверсия k_1, а $(-k_2)$ – аддитивная инверсия k_2.

Аффинный шифр использует пару ключей, в которой первый ключ из Z_{26}*, а второй – из Z_{26}. $X=Y=Z_{26}$, $K= Z_{26*}\times Z_{26}$. $k=(\alpha,\beta)\in K$, $\alpha\neq 0$, $x=(x_1,\dots,x_m)$, $y=(y_1,\dots,y_m)$, полагаем

$y= E_k(x)=(\alpha\times x_1+\beta,\dots,\alpha\times x_m+\beta)$, $x=D_k(y)=((y_1+(26 – \beta))\times\alpha^{-1},\dots, (y_m+(26 – \beta))\times\alpha^{-1})$, где + и × являются операциями кольца Z_{26}, а α^{-1} элемент мультипликативной группы Z_{26*}, обратный α.

Шифр Плейфера.

Шифр Плейфера – многоалфавитный шифр. Ключ в этом шифре генерируется из *25* букв английского алфавита, которые размещаются в матрице *5×5* (буквы *I* и *J* рассматриваются при шифровании как одинаковые) или из 30 букв русского алфавита, размещенных в матрице *5×6* (буквы *Ё, Й* и *Ъ* исключаются при шифровании).

При шифровании исходный текст записывается в виде последовательности биграмм. Если текст имеет нечетную длину или содержит биграмму, состоящую из одинаковых букв, то в него добавляются «пустышки». «Пустышкой» или фиктивным символом является какая-нибудь редко встречающаяся в данном тексте буква (или знак), которая вставляется между одинаковыми буквами биграммы или добавляется в конец текста, для того, чтобы его длина стала четной.

Основой шифра Плейфера является прямоугольная матрица, в которую записан систематически перемешанный алфавит (одно из возможных соглашений). Систематически перемешанный алфавит – это буквы алфавита, записанные по порядку их следования в алфавите, исключая буквы, использованные в ключевом слове. В случае применения систематически перемешанного алфавита, если в ключевом слове используются несколько одинаковых букв, то из них остается только одна. Например: ключевое слово *«хорошо»* превращается в *«хорш».*

Правила для шифрования: буквы биграммы *(ij), i≠j* находятся в таблице. Биграмма *(i j)* заменяется биграммой *(kl),* где *k* и *l* определяются следующим образом:

1. Если *i* и *j* не лежат в одной строке или одном столбце, то их позиции образуют противоположные вершины прямоугольника. Тогда *k* и *l* – другая пара вершин, причем *k* – вершина, лежащая в той же строке, что и вершина *i.*

2. Если *i* и *j* лежат в одной строке, то *k* и *l* – буквы той же строки, расположенные непосредственно справа от *i* и *j.* При этом если одна из букв – последняя в строке, то ее правым соседом является первая буква той же строки.

3. Аналогично, если *i* и *j* лежат в одном столбце, то они заменяются их соседями снизу.

Шифр Виженера.

Это многоалфавитный шифр был создан Блезом де Виженером, французским математиком шестнадцатого столетия. Здесь используется различная стратегия создания потока ключей. Поток ключей – повторение начального потока секретного ключа длины *m, 1<m<26.*

(k_1, k_2, …., k_m) – первоначальный секретный ключ, согласованный между ***А*** и Б.

$P = P_1P_2P_3$…..

$C = C_1C_2C_3$…..

$k = [(k_1,k_2), (k_3,k_4),.....]$

Шифрование $C_i = k_i$

Дешифрование $P_i = k_i$

При шифровании и дешифровании обычно используется таблица Виженера. Первая строка показывает символы исходного текста, который будет зашифрован. Первая колонка содержит столбец символов, которые используются ключом. Остальная часть таблицы показывает символы зашифрованного текста. Чтобы найти зашифрованный текст для исходного текста *"she is listening"*, используя слово *"PASCAL"* как ключ, мы можем найти *s* в первой строке, *P* в первом столбце, на пересечении строки и столбца – символ из зашифрованного текста *H*. Находим *h* в первой строке и *A* во втором столбце, на пересечении строки и столбца – символ *H* из зашифрованного текста. И повторяем те же действия, пока все символы зашифрованного текста не будут найдены.

Шифр Хилла.

Здесь исходный текст разделен на блоки равного размера. Шифрвеличинами шифра Хилла являются n-граммы открытого текста ($n \geq 2$), представленного некоторым числовым кодом, так, что алфавитом открытого текста служит кольцо вычетов Z_l. Правило шифрования представляет собой линейное преобразование кольца Z_l: если $x=(x_1,\ldots,x_n)$ – n-грамма открытого текста, $k=k_{ij}$ – ключ – некоторая обратимая квадратная матрица над Z_l и $y=(y_1,\ldots,y_n)$ – n-грамма шифртекста, то $y^{\downarrow} = E_k(x)=k\times x^{\downarrow}$. Соответственно, $x^{\downarrow}=D_k(y)=k^{-1}\times y^{\downarrow}$, где k^{-1} – матрица, обратная матрице k. Не забываем, что матричные операции здесь производятся над кольцом Z_l. В шифре Хилла ключ – квадратная матрица размера $m\times m$, в котором m является размером блока. Ключ в шифре Хилла:

$$\begin{pmatrix} k_{11} & k_{12} & \ldots\ldots & k_{1m} \\ k_{21} & k_{22} & \ldots\ldots & k_{2m} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ k_{m1} & k_{m2} & \ldots\ldots & k_{mm} \end{pmatrix}$$

Если мы обозначим m символов блоков исходного текста $P_1, P_2 \ldots, P_m$, соответствующие символы в блоках зашифрованного текста будут $C_1, C_2, \ldots, C_m$. Тогда:

$C_1 = P_1k_{11}+P_2k_{21}+\ldots\ldots+P_mk_{m1}$

$C_2 = P_1k_{12}+P_2k_{22}+\ldots\ldots+P_mk_{m2}$

$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$

$C_m = P_1k_{1m}+ P_2k_{2m} +\ldots\ldots+ P_mk_{mm}$

Уравнения показывают, что каждый символ зашифрованного текста зависит от символов всего исходного текста в блоке (P_1, P_2,..., P_m). Ключевая матрица в шифре Хилла должна иметь мультипликативную инверсию.

Литература:

Воробейкина, И. В. Методы и средства криптографической защиты информации: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения / И. В. Воробейкина; БГАРФ ФГБОУ ВО «КГТУ». – Калининград: Изд-во БГАРФ, 2022. - 114 с.

Глава 3. Понятие шифрования. Шифры подстановки.

ЗАДАНИЕ К ЛАБОРАТОРНОЙ РАБОТЕ.

Изучить аффинный шифр, шифры Плейфера, Виженера и Хилла.

Вопросы, на которые необходимо дать ответ:

1. Назовите отличия аффинного шифра от аддитивного и мультипликативного шифров.

2. Можно ли в качестве ключа для шифра Хилла выбрать матрицу *mxn*, где $m<n$?

3. Расскажите правила шифрования Плейфера при условии нахождения букв блока в разных столбцах и строках.

4. Можно ли работать с шифром Виженера, не используя таблицу Виженера?

5. Назовите правило выбора мультипликативного ключа в аддитивном шифре.

6. От чего зависит размерность ключевой матрицы в шифре Хилла?

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Пример.

С помощью аффинного шифра зашифровать сообщение *"happy"* с ключевой парой *(3,2)* в Z_{26}.

Решение:

Мы используем *3* для мультипликативного ключа и *2* для аддитивного ключа. Получаем *"XCVVW"*.

h=07 шифруем *(07×03+2)mod26* зашифрованный текст *23=X*

a=00 шифруем *(00×03+2)mod26* зашифрованный текст *02=C*

p=15 шифруем *(15×03+2) mod 26* зашифрованный текст *21=V*

p=15 шифруем *(15×03+2) mod 26* зашифрованный текст *21=V*

y=24 шифруем *(24×03+2) mod 26* зашифрованный текст *22=W*

Пример.

С помощью аффинного шифра расшифровать сообщение *"XCVVW"* с ключевой парой $(\alpha=3, \beta=2)$ в Z_{26}.

Решение:

Для расшифрования сообщения прибавим аддитивную инверсию ключа β *(-2)* к зашифрованному тексту. Потом умножим результат на мультипликативную инверсию от $\alpha^{-1}=3^{-1}=9$.

23=X дешифруем *(23 –2)×9 mod 26* расшифрованный текст *07=h*
02=C дешифруем *(02 –2)×9 mod 26* расшифрованный текст *00=a*
21=V дешифруем *(21 –2)×9 mod 26* расшифрованный текст *15=p*
21=V дешифруем *(21 –2)×9 mod 26* расшифрованный текст *15=p*
22=W дешифруем *(22 –2)×9 mod 26* расшифрованный текст *24=y*

Пример.

Пусть шифр использует матрицу *5×6,* в которой записан систематически перемешанный русский 30-буквенный алфавит, основанный на ключевом слове *командир:*

к	***о***	***м***	***а***	***н***	***д***
и	***р***	*б*	*в*	*г*	*е*
ж	*з*	*л*	*п*	*с*	*т*
у	*ф*	*х*	*ц*	*ч*	*ш*
щ	*ы*	*ь*	*э*	*ю*	*я*

Зашифруем методом Плейфера фразу *автором метода является Уитстон.* В качестве «пустышки» будем использовать редкую букву *ф.* Представим фразу в виде последовательности биграмм (здесь придется дважды вставлять «пустышку»):

АВ ТО РО МФ МЕ ТО ДА ЯВ ЛЯ ЕТ СЯ УИ ТС ТО НФ

В соответствии с правилами получаем зашифрованный текст (без пробелов): *впздзрохдбздкнэетытштющжжтздоч*

Пример.

Зашифровать сообщение *"She is listening"*, используя ключевое слово из *6* символов *"PASCAL"* и таблицу Виженера.

Пример.

Пусть *n=4*, зашифруем методом Хилла фразу: *без труда не вынешь рыбку из пруда,* записанную в 30-буквенном русском алфавите. Условимся о числовом кодировании букв в соответствии с таблицей:

а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п
1	18	11	6	0	15	20	5	21	23	13	4	16	8	25
р	с	т	у	ф	х	ц	ч	ш	щ	ы	ь	э	ю	я
24	10	19	26	12	2	28	7	17	22	29	3	27	14	9

В качестве ключа выберем матрицу, являющуюся обратимой над кольцом Z_{30}:

$$k=\begin{pmatrix}1&2&3&4\\1&2&3&5\\1&3&3&5\\1&3&4&5\end{pmatrix},\qquad k^{-1}=\begin{pmatrix}5&28&1&27\\0&29&1&0\\0&0&29&1\\29&1&0&0\end{pmatrix}$$

Запишем открытый текст по столбцам матрицы *P:*

$$P=\begin{pmatrix}18&24&16&16&24&26&24\\15&26&15&15&29&21&26\\5&0&11&17&18&5&0\\19&1&29&3&23&25&1\end{pmatrix}$$

и получим шифртекст в виде столбцов матрицы *k×P:*

$$\begin{pmatrix}1&2&3&4\\1&2&3&5\\1&3&3&5\\1&3&4&5\end{pmatrix}\times\begin{pmatrix}18&24&16&16&24&26&24\\15&26&15&15&29&21&26\\5&0&11&17&18&5&0\\19&1&29&3&23&25&1\end{pmatrix}=\begin{pmatrix}19&20&15&19&18&3&20\\8&21&14&22&11&28&21\\23&17&29&7&10&19&17\\28&17&10&24&28&24&17\end{pmatrix}$$

Теперь выпишем шифртекст в буквенном виде: *токцжишшеюыстщчрбвсцьцтржишши*

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

1. С помощью аффинного шифра зашифровать сообщение *"cryptography"* в Z_{26}. Ключи выбрать самостоятельно.

2. Пусть шифр использует матрицу *6×5,* в которой записан систематически перемешанный русский 30-буквенный алфавит. Придумайте ключевое слово и текст и зашифруйте его с помощью шифра Плейфера.

3. Найдите ключевую матрицу для шифра Хилла и обоснуйте свой выбор.

4. Используя таблицу Виженера, ДЕШИФРОВАТЬ текст *XBTTKUZ*. Ключевое слово – *engl*.

ТРЕБОВАНИЯ К ОТЧЕТУ И ЗАЩИТЕ

Показать выполненную в тетради работу. Знать ответы на сформулированные выше вопросы. Защита работы проводится во время занятий. После защиты работа помещается в ЭИОС.

Лабораторная работа № 4. ШИФР ВЕРТИКАЛЬНОЙ ПЕРЕСТАНОВКИ

ОБЩИЕ СВЕДЕНИЯ

Цель: познакомиться с ключевыми и бесключевыми шифрами. Изучить шифр вертикальной перестановки.

Материалы, оборудование, программное обеспечение:

Условия допуска к выполнению: показать конспект по теоретической подготовке.

Критерии положительной оценки: показать выполненную работу, четко ответить на вопросы.

ТЕОРЕТИЧЕСКОЕ ВВЕДЕНИЕ

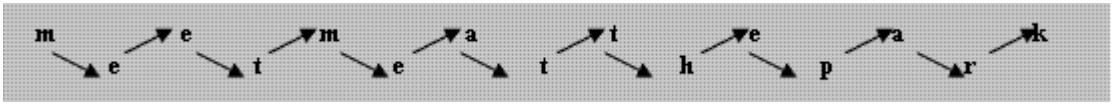
Шифр перестановки не заменяет одним символом другой, вместо этого он изменяет местоположение символов. Символ в первой позиции исходного текста может появиться в десятой позиции зашифрованного текста. Символ, который находится в восьмой позиции исходного текста, может появиться в первой позиции зашифрованного текста. Другими словами, шифр перестановки ставит в другом порядке (перемещает) символы. **Шифр перестановки меняет порядок следования символов.**

Бесключевые шифры перестановки.

Простые шифры перестановки, которые применялись в прошлом, не использовали ключ. Есть два метода для перестановки символов. В первом методе текст записывается в таблице столбец за столбцом и затем передается строка за строкой. Во втором методе текст написан в таблицы строка за строкой и затем передается столбец за столбцом.

Пример.

Пример шифра без использования ключа – шифр изгороди (rail fence cipher). В этом шифре исходный текст размещен на двух линиях как зигзагообразный шаблон (что может рассматриваться как столбец за столбцом таблицы, которая имеет две строки); зашифрованный текст составляется при чтении шаблона строка за строкой. Например, чтобы передать сообщение *"Meet me at the park"*, **А** пишет **Б**:



А создает зашифрованный текст *"MEMATEAKETETHPR"*, посылая первую строку, сопровождаемую второй строкой. ***Б*** получает зашифрованный текст и разделяет его пополам (в этом случае вторая половина имеет на один символ меньше). Первая половина формы – первая строка; вторая половина –

вторая строка. ***Б*** читает результат по зигзагу. Поскольку нет никакого ключа и номер строк установлен (2), криптоанализ зашифрованного текста был бы очень прост для злоумышленника ***Е***. Все, что ***Е*** должен знать, – это то, что используется шифр изгороди.

Ключевые шифры перестановки

Бесключевые шифры переставляют символы, используя запись исходного текста одним способом (например, строка за строкой) и передачу этого текста в другом порядке (например, столбец за столбцом). Перестановка делается во всём исходном тексте, чтобы создать весь зашифрованный текст. Другой метод состоит в том, чтобы разделить исходный текст на группы заранее определенного размера, называемые блоками, а затем использовать ключ, чтобы переставить символы в каждом блоке отдельно.

Широкое распространение получила так называемая **вертикальная перестановка**. Здесь используется прямоугольная таблица, в которую сообщение записывается слева направо, выписывается же сообщение по вертикалям (сверху вниз), при этом столбцы выбираются в порядке, определяемом числовым ключом.

Литература:

Воробейкина, И. В. Методы и средства криптографической защиты информации: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения / И. В. Воробейкина; БГАРФ ФГБОУ ВО «КГТУ». – Калининград: Изд-во БГАРФ, 2022. - 114 с.

Глава 4. Ключевые и бесключевые шифры перестановки.

ЗАДАНИЕ К ЛАБОРАТОРНОЙ РАБОТЕ

Изучить шифр вертикальной перестановки.

Вопросы, на которые необходимо дать ответ:

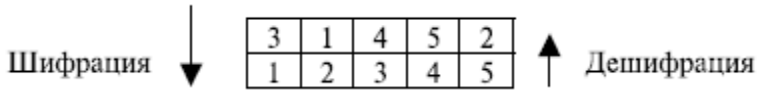
1. Расскажите принцип работы ключевых и бесключевых шифров.
2. Как строится ключ для шифра вертикальной перестановки?
3. Корректны ли указанные ключи для шифра вертикальной изгороди: (3, 2, 0, 1, 4)? (4, 6, 1, 2, 3,)? Почему?
4. Что из себя представляют элементы ключа в вертикальной перестановке?

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Пример.

А должен передать ***Б*** сообщение *"Enemy attacks tonight"*. ***А*** и ***Б*** согласились разделить текст на группы по пять символов и затем переставить символы

в каждой группе. Ниже показана группировка после добавления фиктивного символа в конце, чтобы сделать последнюю группу одинаковой по размеру с другими: *Enemy atttac kston ightz.* Ключ, используемый для шифрования и дешифрования, – ключ перестановки, который показывает, как переставлять символы. Для этого сообщения примем, что ***А*** и ***Б*** использовали следующий ключ:



Третий символ в блоке исходного текста становится первым символом в зашифрованном тексте в блоке, первый символ в блоке исходного текста становится вторым символом в блоке зашифрованного текста и так далее. Результат перестановки: *EEMYN TAACT TKONS HITZG.* ***А*** передает зашифрованный текст ***Б*****:** *EEMYNTAACTTKONSHITZG*. ***Б*** делит зашифрованный текст на группы по 5 символов и, используя ключ в обратном порядке, находит исходный текст.

Пример.

Зашифруем фразу *вот пример шифра вертикальной перестановки,* используя матрицу *6×7* и числовой ключ *(5,1,4,7,2,6,3)*

5	*1*	*4*	*7*	*2*	*6*	*3*
в	*о*	*т*	*п*	*р*	*и*	*м*
е	*р*	*ш*	*и*	*ф*	*р*	*а*
в	*е*	*р*	*т*	*и*	*к*	*а*
л	*ь*	*н*	*о*	*й*	*п*	*е*
р	*е*	*с*	*т*	*а*	*н*	*о*
в	*к*	*и*				

Отметим, что нецелесообразно заполнять последнюю строку матрицы «нерабочими» буквами, так ка это дало бы противнику, получившему в свое распоряжение данную криптограмму, сведения о длине числового ключа. Действительно, в этом случае длину ключа следовало бы искать среди делителей длины сообщения. Выписывая буквы по столбцам в порядке, указанном числовым ключом, получим криптограмму:

ореьекрфийамааеотшрнсивевлрвиркпнпитот

При расшифровании в первую очередь надо определить число длинных столбцов, то есть число букв в последней строке прямоугольника. Для этого делим число букв в сообщении на длину числового ключа. Остаток от деления и будет искомым числом. Когда это число определено, буквы криптограммы водворяются на их собственные места, и сообщение будет прочитано. В нашем примере *38=7×5+3,* поэтому в заполненной таблице имеются *3* длинных и *4* коротких столбца. Согласно числовому ключу начальные буквы криптограммы

берутся из второго (по счету слева) столбца, он длинный (так как первые три столбца длинные), поэтому первые шесть букв образуют второй столбец. Следующие пять букв образуют пятый столбец (он короткий). И так далее.

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

1. С помощью бесключевого шифра изгороди зашифруйте фразу *"Attack is today"*.

2. С помощью ключевого шифра перестановки зашифровать фразу *«все дороги ведут в деканат»,* используя матрицу 5×5 и числовой ключ *(5,1,4,3,2).*

ТРЕБОВАНИЯ К ОТЧЕТУ И ЗАЩИТЕ

Показать выполненную в тетради работу. Знать ответы на сформулированные выше вопросы. Защита работы проводится во время занятий. После защиты работа помещается в ЭИОС.

Лабораторная работа № 5. Шифрование с помощью симметричного алгоритма DES

ОБЩИЕ СВЕДЕНИЯ

Цель: получить представление о современных блочных шифрах. Изучить алгоритм шифрования DES.

Материалы, оборудование, программное обеспечение:

Условия допуска к выполнению: показать конспект по теоретической подготовке.

Критерии положительной оценки: показать выполненную работу, четко ответить на вопросы,

ТЕОРЕТИЧЕСКОЕ ВВЕДЕНИЕ

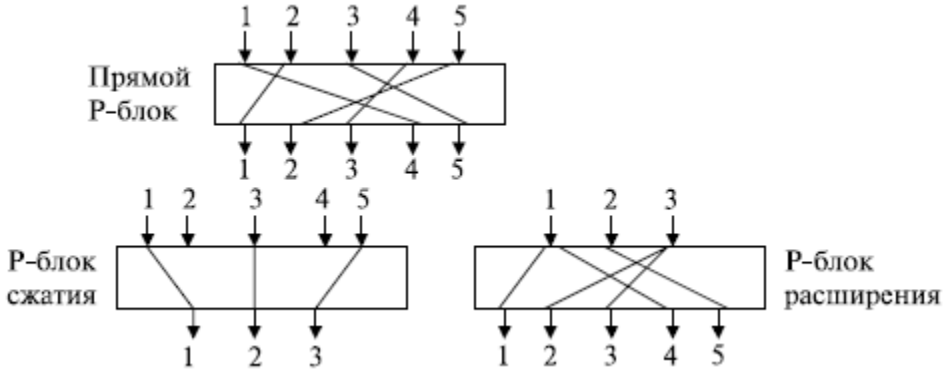
Современный блочный шифр с симметричными ключами шифрует *n*-битовый блок исходного текста или расшифровывает *n*-битовый блок зашифрованного текста. Алгоритм шифрования или дешифрования используют *k*-битовый ключ. Алгоритм дешифрования должен быть инверсией алгоритма шифрования, и оба в работе используют один и тот же ключ засекречивания так, чтобы **Б** мог восстановить сообщение, передаваемое **А**.

Если сообщение имеет размер меньше, чем *n* бит, нужно добавить заполнение, чтобы создать этот *n*-разрядный блок; если сообщение имеет больше, чем *n* бит, оно должно быть разделено на *n*-разрядные блоки, и в случае необходимости нужно добавить к последнему блоку соответствующее заполнение. Общие значения для *n* обычно *64, 128, 256* или *512* бит.

Блочный шифр и его компоненты.

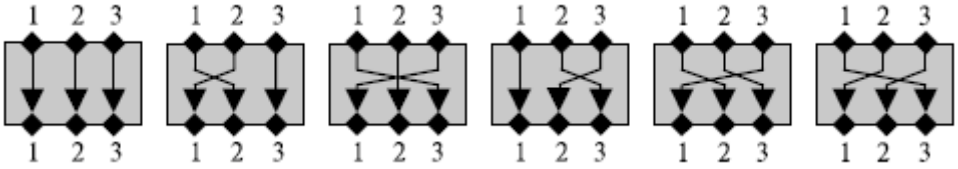
Современные блочные шифры обычно являются ключевыми шифрами подстановки, в которых ключ позволяет только частичные отображения возможных входов информации в возможные выходы. Чтобы обеспечивать требуемые свойства современного блочного шифра, такие как рассеяние и перемешивание информации, этот шифр формируется как комбинация модулей транспозиции (называемых *P*-блоками), модулей подстановки (называемых *S*-блоками) и некоторыми другими модулями.

P-блок (блок перестановки) подобен традиционному шифру транспозиции символов. Он перемещает биты. Существует три типа *P*-блоков: прямые *P*-блоки, *P*-блоки расширения и *P*-блоки сжатия. Рисунок показывает прямой *P*-блок *5×5, P*-блок сжатия *5×3* и *P*-блок расширения *3×5*:



Прямой *P*-блок с *n* входами и *n* выходами – это перестановка с *n!* возможными отображениями.

Возможные отображения *P*-блока 3×3:



P*-блок сжатия** – это ***P-блок с *n* входами и *m* выходами, где $m<n$. Некоторые из информационных входов блокированы и не связаны с выходом. *P*-блоки сжатия, используемые в современных блочных шифрах, обычно являются бесключевыми с таблицей перестановки, которая указывает правила перестановки бит.

***P*-блок расширения** – *P*-блок с *n* входами и *m* выходами, где $m>n$. Некоторые из входов связаны больше чем с одним выходом. *P*-блоки расширения, используемые в современных блочных шифрах, обычно без ключа. Правила перестановки бит указываются в таблице. Обратите внимание, что каждый из *1, 3, 9* и *12* соединен с двумя выходами.

S-блок – $m \times n$ модуль подстановки, где *m* и *n* не обязательно равны.

Другой компонент, применяемый в некоторых современных блочных шифрах, – операция циклического сдвига. Смещение может быть влево или вправо.

Литература:

Воробейкина, И. В. Методы и средства криптографической защиты информации: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения / И. В. Воробейкина; БГАРФ ФГБОУ ВО «КГТУ». – Калининград: Изд-во БГАРФ, 2022. - 114 с.

Глава 5. Блочный шифр DES.

ЗАДАНИЕ К ЛАБОРАТОРНОЙ РАБОТЕ

Изучить блочный шифр DES.

Вопросы, на которые необходимо дать ответ:

1. Какие *P*-блоки вы знаете? Дайте им характеристику.
2. Где хранятся *P*-блоки?
3. Объясните алгоритм Фейстеля. Сколько раундов в этом алгоритме?
4. Объясните алгоритм создания ключа следующего раунда.
5. Покажите, как работает циклический сдвиг каждого раунда.
6. Объясните принцип работы с таблицей *S*-блоков.
7. Запишите логическую таблицу *XOR*.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Зашифровать *64*-битовую последовательность *123456ABCD132536* ключом *AABB09182736CCDD*.

Решение.

1) Запишем исходную последовательность в двоичном коде и пронумеруем все элементы слева направо: в первой строке нумерация двоичного кода исходного текста, во второй строке – двоичный код, в третьей строке – исходный текст.

1 2 3 4	5 6 7 8	9 10 11 12	13 14 15 16	17 18 19 20	21 22 23 24	25 26 27 28	29 30 31 32	33 34 35 36	37 38 39 40	41 42 43 44	45 46 47 48	49 50 51 52	53 54 55 56	57 58 59 60	61 62 63 64
0 0 0 1	0 0 1 0	0 0 1 1	0 1 0 0	0 1 0 1	0 1 1 0	1 0 1 0	1 0 1 1	1 1 0 0	1 1 0 1	0 0 0 1	0 0 1 1	0 0 1 0	0 1 0 1	0 0 1 1	0 1 1 0
1	*2*	*3*	*4*	*5*	*6*	*A*	*B*	*C*	*D*	*1*	*3*	*2*	*5*	*3*	*6*

2) Первоначальная подстановка.

0001	0100	1010	0111	1101	0110	0111	1000	0001	1000	1100	1010	0001	1000	1010	11101
1	*4*	*A*	*7*	*D*	*6*	*7*	*8*	*1*	*8*	*C*	*A*	*1*	*8*	*A*	*D*
L_0								R_0							

После первоначальной подстановки L_0=*14A79678*, R_0=*18CA18AD*.

3) Далее – работаем с ключом; записываем ключ в двоичном коде и исключаем биты *8, 16, 24, 32, 40, 48, 56, 64*. Они являются битами четности и не несут текстовой информации.

1 2 3 4	5 6 7 8	9 10 11 12	13 14 15 16	17 18 19 20	21 22 23 24	25 26 27 28	29 30 31 32	33 34 35 36	37 38 39 40	41 42 43 44	45 46 47 48	49 50 51 52	53 54 55 56	57 58 59 60	61 62 63 64
1 0 1 0	1 0 1 **0**	1 0 1 1	1 0 1 **1**	0 0 0 0	1 0 0 **1**	0 0 0 1	1 0 0 **0**	0 0 1 0	0 1 1 **1**	0 0 1 1	0 1 1 **0**	1 1 0 0	1 1 0 **0**	1 1 0 1	1 1 0 **1**
A	*A*	*B*	*B*	*0*	*9*	*1*	*8*	*2*	*7*	*3*	*6*	*C*	*C*	*D*	*D*

На выходе получаем *56*-битовый ключ:

1 2 3 4	5 6 7 8	9 10 11 12	13 14 15 16	17 18 19 20	21 22 23 24	25 26 27 28	29 30 31 32	33 34 35 36	37 38 39 40	41 42 43 44	45 46 47 48	49 50 51 52	53 54 55 56
1 0 1 0	1 0 1 1	0 1 1 1	0 1 0 0	0 0 1 0	0 0 0 0	1 1 0 0	0 0 1 0	0 1 1 0	0 1 1 0	1 1 1 1	0 0 1 1	0 1 1 0	1 1 1 0

Полученный ключ преобразуем по таблице 5.2 Приложения 5 и делим на 2 части по 28 бит:

1 2 3 4	5 6 7 8	9 10 11 12	13 14 15 16	17 18 19 20	21 22 23 24	25 26 27 28	29 30 31 32	33 34 35 36	37 38 39 40	41 42 43 44	45 46 47 48	49 50 51 52	53 54 55 56
1 1 0 0	0 0 1 1	1 1 0 0	0 0 0 0	0 0 1 1	0 0 1 1	1 0 1 0	0 0 1 1	0 0 1 1	1 1 1 1	0 0 0 0	1 1 0 0	1 1 1 1	1 0 1 0
левая часть ключа 28 бит							правая часть ключа 28 бит						

Согласно таблице 5.6 Приложения 5 циклических сдвигов, сдвигаем влево на 1 бит левую и правую части ключа **по отдельности**. Получаем:

1 2 3 4	5 6 7 8	9 10 11 12	13 14 15 16	17 18 19 20	21 22 23 24	25 26 27 28	29 30 31 32	33 34 35 36	37 38 39 40	41 42 43 44	45 46 47 48	49 50 51 52	53 54 55 56
1 0 0 0	0 1 1 1	1 0 0 0	0 0 0 0	0 1 1 0	0 1 1 1	0 1 0 1	0 1 1 0	0 1 1 1	1 1 1 0	0 0 0 1	1 0 0 1	1 1 1 1	0 1 0 0
левая часть ключа после циклического сдвига влево на 1 бит							правая часть после циклического сдвига влево на 1 бит						

Далее, по таблице 5.3 сжатия Приложения 5 получаем *48*-битовый ключ 1-го раунда:

0 0 0 1	1 0 0 1	0 1 0 0	1 1 0 0	1 1 0 1	0 0 0 0	0 1 1 1	0 0 1 0	1 1 0 1	1 1 1 0	1 0 0 0	1 1 0 0
1	*9*	*4*	*C*	*D*	*0*	*7*	*2*	*D*	*E*	*8*	*C*

Итак, ключ 1-го раунда – *194CD072DE8C*.

4) После вычисления ключа по таблице 5.4 Приложения 5 расширяем правую часть исходного текста с *32* бит до *48* бит.

1 2 3 4	5 6 7 8	9 10 11 12	13 14 15 16	17 18 19 20	21 22 23 24	25 26 27 28	29 30 31 32
0 0 0 1	1 0 0 0	1 1 0 0	1 0 1 0	0 0 0 1	1 0 0 0	1 0 1 0	1 1 0 1
R_0 – правая часть исходного текста до расширения							

1 2 3 4	5 6 7 8	9 10 11 12	13 14 15 16	17 18 19 20	21 22 23 24	25 26 27 28	29 30 31 32	33 34 35 36	37 38 39 40	41 42 43 44	45 46 47 48
1 0 0 0	1 1 1 1	0 0 0 1	0 1 1 0	0 1 0 1	0 1 0 0	0 0 0 0	1 1 1 1	0 0 0 1	0 1 0 1	0 1 0 1	1 0 1 0
R_0 – правая часть исходного текста после расширения до 48 бит											

Теперь расширенную правую часть складываем с ключом по модулю 2 (*XOR*):

R_0=	1 0 0 0	1 1 1 1	0 0 0 1	0 1 1 0	0 1 0 1	0 1 0 0	0 0 0 0	1 1 1 1	0 0 0 1	0 1 0 1	0 1 0 1	1 0 1 0
K_1=	0 0 0 1	1 0 0 1	0 1 0 0	1 1 0 0	1 1 0 1	0 0 0 0	0 1 1 1	0 0 1 0	1 1 0 1	1 1 1 0	1 0 0 0	1 1 0 0
$R_0 \oplus K_1$=	1 0 0 1	0 1 1 0	0 1 0 1	1 0 1 0	1 0 0 0	0 1 0 0	0 1 1 1	1 1 0 1	1 1 0 0	1 0 1 1	1 1 0 1	0 1 1 0

Результат сгруппируем по *6* бит, получим *S*-блоки:

1 0 0 1 0 1	1 0 0 1 0 1	1 0 1 0 1 0	0 0 0 1 0 0	0 1 1 1 1 1	0 1 1 1 0 0	1 0 1 1 1 1	0 1 0 1 1 0
S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8

5) Работаем с таблицей *S*-блоков Приложения 5 (индекс d – десятичное число, индекс b – двоичное число):

S_1	№ строки $11_b=3_d$ № столбца $0010_b=2_d$	$=8_d=1000_b$
S_2	№ строки $11_b=3_d$ № столбца $0010_b=2_d$	$=10_d=1010_b$
S_3	№ строки $10_b=2_d$	$=15_d=1111_b$

	№ столбца $0101_b=5_d$	
S_4	№ строки $00_b=0_d$ № столбца $0010_b=2_d$	$=14_d=1110_b$
S_5	№ строки $01_b=1_d$ № столбца $1111_b=15_d$	$=6_d=0110_b$
S_6	№ строки $00_b=0_d$ № столбца $1110_b=14_d$	$=5_d=0101_b$
S_7	№ строки $11_b=3_d$ № столбца $0111_b=7_d$	$=7_d=0111_b$
S_8	№ строки $00_b=0_d$ № столбца $1011_b=14_d$	$=14_d=1110_b$

В результате получен 32-битовый блок,

1 2 3 4	5 6 7 8	9 10 11 12	13 14 15 16	17 18 19 20	21 22 23 24	25 26 27 28	29 30 31 32
1 0 0 0	1 0 1 0	1 1 1 1	1 1 1 0	0 1 1 0	0 1 0 1	0 1 1 1	1 1 1 0

который преобразуется с помощью таблицы 5.5 Приложения 5 перестановки битов *P*.

Получаем:

0 1 0 0	1 1 1 0	1 1 0 1	1 1 1 1	0 0 1 1	0 1 0 1	1 1 1 0	1 1 0 0
4	*E*	*D*	*F*	*3*	*5*	*E*	*C*

В результате получили функцию шифрования *f=4EDF35EC*, которую сложим по модулю 2 *(XOR)* с L_0:

$L_0=$	0 0 0 1	0 1 0 0	1 0 1 0	0 1 1 1	1 1 0 1	0 1 1 0	0 1 1 1	1 0 0 0
$f=$	0 1 0 0	1 1 1 0	1 1 0 1	1 1 1 1	0 0 1 1	0 1 0 1	1 1 1 0	1 1 0 0
$L_0 \oplus f=$	0 1 0 1	1 0 1 0	0 1 1 1	1 0 0 0	1 1 1 0	0 0 1 1	1 0 0 1	0 1 0 0

Значит, результат $L_0 \oplus f=5A78E394$.

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

С помощью алгоритма DES зашифровать свою фамилию. Ключ - ваше полное имя.

ТРЕБОВАНИЯ К ОТЧЕТУ И ЗАЩИТЕ

Показать выполненную в тетради работу. Знать ответы на сформулированные выше вопросы. Защита работы проводится во время занятий. После защиты работа помещается в ЭИОС.

Лабораторная работа № 6. Алгоритм рюкзака.

ОБЩИЕ СВЕДЕНИЯ

Цель: познакомиться с принципами работы алгоритмов с открытым ключом. Изучить алгоритм рюкзака.

Материалы, оборудование, программное обеспечение: калькулятор.

Условия допуска к выполнению: показать конспект по теоретической подготовке.

Критерии положительной оценки: показать выполненную работу, четко ответить на вопросы,

ТЕОРЕТИЧЕСКОЕ ВВЕДЕНИЕ

Проблема рюкзака: дано множество предметов различного веса, можно ли положить некоторые из этих предметов в рюкзак так, чтобы вес рюкзака стал равен определенному значению? Формально: дан набор значений M_1, M_2, …, M_n и сумма S, вычислить значения b_i, такие, что $S=b_1M_1+ b_2M_2+…+ b_nM_n$. b_i может быть либо нулем (предмет не кладут в рюкзак), либо единицей (предмет кладут в рюкзак).

Существуют две различные проблемы рюкзака, одна решается за линейное время, а другая – нет. Легкую проблему можно превратить в трудную. Открытый ключ представляет собой трудную проблему, которую легко использовать для шифрования, но невозможно для дешифрования.

Легкая проблема: если перечень весов предметов является **сверхвозрастающей последовательностью** (последовательность, в которой каждый элемент больше суммы всех предыдущих элементов), то проблему рюкзака легко решить: возьмите полный вес и сравните его с самым большим числом последовательности. Если полный вес меньше, чем это число, то соответствующий ему предмет не кладут в рюкзак. Если полный вес больше либо равен этому числу, то его кладут в рюкзак. Уменьшим массу рюкзака на это значение и перейдем к следующему по величине числу последовательности. Будем повторять, пока процесс не закончится. Если полный вес уменьшится до нуля, то решение найдено, в противном случае – нет.

Трудная проблема: нормальные (не сверхвозрастающие) рюкзаки, быстрого алгоритма для них не найдено. Единственный известный способ – методическая проверка возможных решений. Существует экспоненциальная зависимость от числа возможных предметов: добавьте к последовательности весов еще один элемент, и найти решение станет вдвое труднее, в то время как для сверхвозрастающего рюкзака, если добавить один предмет, поиск решения увеличится на одну операцию.

На этом свойстве основан алгоритм Меркла-Хеллмана. Закрытый ключ – последовательность весов сверхвозрастающего рюкзака, открытый ключ – по-

следовательность весов нормального рюкзака с тем же решением. Используя модульную арифметику, Меркл и Хеллман разработали способ преобразования проблемы сверхвозрастающего рюкзака в проблему нормального рюкзака.

Например, веса предметов могут быть *1, 5, 6, 11, 14* и *20*. Можно упаковать рюкзак так, чтобы его вес стал *22*, использовав веса *5, 6* и *11*. Невозможно упаковать рюкзак так, чтобы его вес стал *24*. В общем случае время, необходимое для решения этой проблемы, с ростом количества предметов растет экспоненциально.

Пример шифрования с помощью проблемы рюкзака:

Открытый текст	1 1 1 0 0 1	0 1 0 1 1 0	0 0 0 0 0 0	0 1 1 0 0 0
Рюкзак	1 5 6 11 14 20	1 5 6 11 14 20	1 5 6 11 14 20	1 5 6 11 14 20
Шифртекст	1+5+6+20=32	5+11+14=30	0=0	5+6=11

Литература:

Воробейкина, И. В. Методы и средства криптографической защиты информации: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения / И.В. Воробейкина; БГАРФ ФГБОУ ВО «КГТУ». – Калининград: Изд-во БГАРФ, 2022. - 114 с.

Глава 6. Алгоритмы с открытыми ключами. 6.9. Алгоритмы рюкзака.

ЗАДАНИЕ К ЛАБОРАТОРНОЙ РАБОТЕ

Изучить алгоритмы рюкзака.

Вопросы, на которые необходимо дать ответ.

1. Объясните понятие сверхвозрастающей и нормальной последовательностей в алгоритме рюкзака.

2. Что такое легкая и трудная проблема в алгоритме рюкзака?

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Создание открытого ключа из закрытого. Рассмотрим алгоритм: чтобы получить нормальную последовательность рюкзака, возьмем сверхвозрастающую последовательность рюкзака, например, *(2, 3, 6, 13, 27, 52)*, и умножим все значения на число *n* по модулю *m.* Значение модуля должно быть больше суммы всех чисел последовательности, например, *105*. Множитель должен быть взаимно простым с модулем, например, *31*. Нормальной последовательностью рюкзака будет:

$2 \times 31 \bmod 105 = 62$

3×31 mod 105=93
6×31 mod 105=81
13×31 mod 105=88
27×31 mod 105=102
52×31 mod 105=37
Итого – *(62, 93, 81, 88, 102, 37)*.

Пример.
Получение открытого ключа

Закрытый ключ k_i	*2*	*3*	*6*	*13*	*27*	*52*	*105*	*210*
Открытый ключ $(k_i*n) \bmod m=(k_i*31) \bmod 420$	*62*	*93*	*186*	*403*	*417*	*352*	*315*	*210*

Сверхвозрастающая последовательность рюкзака является закрытым ключом, а нормальная последовательность рюкзака – открытым ключом.

Шифрование. Для шифрования сообщение сначала разбивается на блоки, равные по длине числу элементов последовательности рюкзака. Затем, считая, что единица указывает на присутствие элемента последовательности, а ноль – на его отсутствие, вычисляем полные веса рюкзаков – по одному для каждого блока сообщения.

Например, если сообщение в бинарном виде: *011000110101101110*, шифруем (используя предыдущую последовательность рюкзака *(62, 93, 81, 88, 102, 37)*):

сообщение=*011000 110101 101110*
011000 соответствует *93+81=174*
110101 соответствует *62+93+88+37=280*
101110 соответствует *62+81+88+102=333*
Шифротекстом будет последовательность *174, 280, 333*.

Дешифрование. Получатель данного сообщения знает закрытый ключ: оригинальную сверхвозрастающую последовательность, а также значения *n* и *m*, использованные для превращения ее в нормальную последовательность рюкзака. Для дешифрования получатель должен сначала определить n^{-1}, такое, что $n(n^{-1}) \equiv 1 \pmod m$. Каждое значение шифротекста умножается на $(n^{-1} \bmod m)$, а затем разделяется с помощью закрытого ключа. В нашем примере сверхвозрастающая последовательность *(2, 3, 6, 13, 27, 52)*, *m=105*, *n=31*, шифротекст *(174, 280, 333)*. В этом случае $n^{-1}=61$, поэтому значения шифротекста умножаются на *61 mod 105:*

174×61 mod 105=9=3+6, что соответствует *011000*
280×61 mod 105=70=2+3+13+52, что соответствует *110101*

333×61 mod 105=48=2+6+13+27, что соответствует *101110*

Расшифрованным открытым текстом является *011000 110101 101110*.

Пример.

Рассмотрим открытое сообщение *АБРАМОВ*, символы которого представим в бинарном виде в соответствии с таблицей кодов символов *Windows 1251*. Сверхвозрастающая последовательность равна *{2, 3, 6, 13, 27, 52, 105, 210}*. Результат шифрования с помощью открытого ключа *{62, 93, 186, 403, 417, 352, 315, 210}*, вычисленном в примере 6.10, представлен в следующей таблице:

Открытое сообщение		Сумма весов	Шифрограмма (рюкзак), c_i
Символ	Bin-код		
А	*1100 0000*	*62+93*	*155*
Б	*1100 0001*	*62+93+210*	*365*
Р	*1101 0000*	*62+93+403*	*558*
А	*1100 0000*	*62+93*	*155*
М	*1100 1100*	*62+93+417+352*	*924*
О	*1100 1110*	*62+93+417+352+315*	*1239*
В	*1100 0010*	*62+93+315*	*470*

Для дешифрования сообщения получатель должен сначала определить обратное число n^{-1}, такое что $(n * n^{-1}) \bmod m = 1$. После определения обратного числа каждое значение шифрограммы умножается на n^{-1} по модулю m и с помощью закрытого ключа определяются биты открытого текста.

В нашем примере сверхвозрастающая последовательность равна *{2, 3, 6, 13, 27, 52, 105, 210}, m=420, n=31,* $n^{-1} = 271$ *(31*271 mod 420 = 1).*

Результат дешифрования с помощью закрытого ключа *{2, 3, 6, 13, 27, 52, 105, 210}* представлен в следующей таблице:

Шифрограмма (рюкзак), c_i	$(c_i * n^{-1}) \bmod m = (c_i * 271) \bmod 420$	Сумма весов	Открытое сообщение	
			Bin-код	Символ
155	*5*	*2+3*	*1100 0000*	*А*
365	*215*	*2+3+210*	*1100 0001*	*Б*
558	*18*	*2+3+13*	*1101 0000*	*Р*
155	*5*	*2+3*	*1100 0000*	*А*
924	*84*	*2+3+27+52*	*1100 1100*	*М*
1239	*189*	*2+3+27+52+105*	*1100 1110*	*О*
470	*110*	*2+3+105*	*1100 0010*	*В*

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

С помощью алгоритма рюкзака зашифровать и дешифровать свою фамилию. Ключ шифрования выбрать самостоятельно.

ТРЕБОВАНИЯ К ОТЧЕТУ И ЗАЩИТЕ

Показать выполненную в тетради работу. Знать ответы на сформулированные выше вопросы. Защита работы проводится во время занятий. После защиты работа помещается в ЭИОС.

Лабораторная работа № 7. Усовершенствованный шифр Цезаря

ОБЩИЕ СВЕДЕНИЯ

Цель: познакомиться с усовершенствованным шифром Цезаря.

Материалы, оборудование, программное обеспечение: калькулятор.

Условия допуска к выполнению: показать конспект по теоретической подготовке.

Критерии положительной оценки: показать выполненную работу, четко ответить на вопросы,

ТЕОРЕТИЧЕСКОЕ ВВЕДЕНИЕ

В шифре Цезаря каждая буква сообщения заменяется на другую, номер которой в алфавите на три больше. Например, А заменяется на Г, Б на Д и т.д. Три последние буквы русского алфавита – Э, Ю, Я – шифруются буквами А, Б, В соответственно. Например, слово ПЕРЕМЕНА после применения к нему шифра Цезаря превращается в ТИУИПИРГ (если исключить букву Ё и считать, что в алфавите 32 буквы).

Если пронумеровать буквы русского алфавита числами от 0 до 31 (исключив букву Ё), правило шифрования запишется следующим образом:

$$c = (m + k) \bmod 32$$

где m и c – номера букв соответственно сообщения и шифротекста, а k – ключ шифра

Чтобы расшифровать зашифрованный текст, нужно применить обратный алгоритм

$$m = (c - k) \bmod 32.$$

Например, слово ПЕРЕМЕНА после применения к нему шифра Цезаря с ключом k=3 превращается в ТИУИПИРГ.

Естественный способ увеличить количество возможных значений ключа для шифра Цезаря – использовать разные ключи для разных букв сообщения. Например, мы можем шифровать каждую нечетную букву ключом k_1, а четную ключом k_2. Тогда секретный ключ $k = (k_1, k_2)$ будет состоять из двух чисел, и количество возможных ключей будет $32^2 = 1024$.

Зашифруем слово ПЕРЕМЕНА ключом $k = (3, 5)$:

ПЕРЕМЕНА $\xrightarrow{(3,5)}$ ТКУКПКРЕ.

Литература:

Рябко Б. Я., Фионов А. Н. Криптография в информационном мире.- Москва: Горячая линия - Телеком, 2018. - 300 с.

ЗАДАНИЕ К ЛАБОРАТОРНОЙ РАБОТЕ

Изучить аддитивные шифры.

Вопросы, на которые необходимо ответить:

1. К какому типу шифров относится шифр Цезаря?
2. Чем простой шифр Цезаря отличается от усовершенствованного?
3. Может ли аддитивный ключ в системе вычетов Z_n быть больше n?
4. Может ли аддитивный ключ быть отрицательным?

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Нумерация букв:

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Один из вариантов шифра Цезаря может выглядеть так:

$\tilde{m}_i = m_i + m_{i+1}$,

$\tilde{m}_{i+1} = m_{i+1} + \tilde{m}_i$,

$c_i = \tilde{m}_i + k_1$,

$c_{i+1} = \tilde{m}_{i+1} + k_2 \pmod{32}$

Здесь m_i – нечетная буква исходного текста, m_{i+1} – четная буква, k_1 , k_2 – символы ключа, а c_i , c_{i+1} – получаемые символы шифротекста. Например, пара символов ПЕ шифруется ключом k = (3, 5) следующим образом:

$\tilde{m}_i$ = П + Е = Ф,

$\tilde{m}_{i+1}$ = Е + Ф = Щ,

c_i = Ф + 3 = Ч,

c_{i+1} = Щ + 5 = Ю,

т.е. ПЕ превращается в ЧЮ.

Алгоритм дешифрования выглядит следующим образом:

$\tilde{m}_{i+1} = c_{i+1} - k_2$,

$\tilde{m}_i = c_i - k_1$,

$m_{i+1} = \tilde{m}_{i+1} - \tilde{m}_i$,

$m_i = \tilde{m}_i - m_{i+1} \pmod{32}$.

Применяя к нашему сообщению шифр с ключом (3, 5), получаем

ПЕРЕМЕНА ⟶ ФЩХЪСЦН

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

Вариативность не предполагается.

Зашифровать усовершенствованным шифром Цезаря (2 раунда) слово ЛУНА. Ключ $k1 = 6$, $k2 = 11$.

ТРЕБОВАНИЯ К ОТЧЕТУ И ЗАЩИТЕ

Показать выполненную в тетради работу. Знать ответы на сформулированные выше вопросы. Защита работы проводится во время занятий. После защиты работа помещается в ЭИОС.

Лабораторная работа № 8. Криптосистемы с открытым ключом: RSA, Шамира, Эль-Гамаля

ОБЩИЕ СВЕДЕНИЯ

Цель: изучить криптосистемы с открытым ключом.

Материалы, оборудование, программное обеспечение: калькулятор.

Условия допуска к выполнению: показать конспект по теоретической подготовке.

Критерии положительной оценки: показать выполненную работу, четко ответить на вопросы,

ТЕОРЕТИЧЕСКОЕ ВВЕДЕНИЕ

Генерация ключей *RSA*. Генерация ключей (открытый и закрытый ключ) в *RSA* осуществляется следующим образом:

1. выбираются два простых числа p и q, $p \neq q$;
2. вычисляется модуль $n = p * q$;
3. вычисляется значение функции Эйлера от модуля n: $\phi(n) = (p-1)(q-1)$;
4. выбирается число e, называемое открытой экспонентой, такое что $1 < e < \phi(N)$, а также быть взаимно простым со значением функции $\phi(n)$.
5. вычисляется число d, называемое секретной экспонентой, такое, что $d * e = 1 (mod \phi(N))$, т. е. является мультипликативно обратное к числу e по модулю $\phi(N)$.

Другими словами, $d = e^{-1} mod((p-1)(q-1))$. Заметим, что d и n также взаимно простые числа. Числа p и q больше не нужны. Они должны быть отброшены, но не должны быть раскрыты. Итак, мы получили пару ключей: пара (e,n) – открытый ключ, пара (d,n) – закрытый ключ.

Пусть ***А*** и ***Б*** переписываются. ***А*** заранее генерирует закрытый и открытый ключ, а затем отправляет открытый ключ ***Б***. ***Б*** посылает зашифрованное сообщение ***А***.

Шифрование: ***Б*** шифрует сообщение M, используя открытый ключ ***А*** (e,n): $C = E(M) = M^e mod(n)$, и отправляет ***А***.

Расшифровывание: ***А*** принимает зашифрованное сообщение C. Используя закрытый ключ (d,n), расшифровывает сообщение $M = D(C) = C^d mod(n)$.

Шифр Шамира.

Пусть есть два абонента A и B, A выбирает случайное большое простое число p и открыто передает его B. Затем A выбирает два числа c_A и d_A, такие, что $c_A d_A \ mod(p-1) = 1$.

Эти числа A держит в секрете и передавать не будет. B тоже выбирает два числа c_B и d_B, такие, что $c_B d_B \ mod \ (p-1) = 1$, и держит их в секрете. После это-

го A передает свое сообщение m, используя трехступенчатый протокол. Если $m < p$ (m рассматривается как число), то сообщение m передается сразу , если же $m \geq p$, то сообщение представляется в виде $m_1, m_2, \ldots, m_t$, где все $m_i < p$, и затем передаются последовательно $m_1, m_2, \ldots, m_t$. При этом для кодирования каждого m_i лучше выбирать случайно новые пары (c_A, d_A) и (c_B, d_B) – в противном случае надежность системы понижается. В настоящее время такой шифр, как правило, используется для передачи чисел, например, секретных ключей, значения которых меньше p. Таким образом, мы будем рассматривать только случай $m<p$.

Описание алгоритма Шамира.

Шаг 1. A вычисляет число $x_1 = m_{cA} \, mod \, p$, где m — исходное сообщение, и пересылает x_1 к B.

Шаг 2. B, получив x_1, вычисляет число $x_2 = (x_1)^{c_B} \, mod \, p$ и передает x_2 к A.

Шаг 3. A вычисляет число $x_3 = (x_2)^{dA} \ mod \, p$ и передает его B.

Шаг 4. B, получив x_3, вычисляет число $x4 = (x_3)^{dB} \ mod \, p$.

Шифр Эль-Гамаля.

Фактически здесь используется схема Диффи-Хеллмана, чтобы сформировать общий секретный ключ для двух абонентов, и затем сообщение шифруется путем умножения его на этот ключ. Для каждого следующего сообщения секретный ключ вычисляется заново.

Для всей группы абонентов выбираются некоторое большое простое число p и число g, такие, что различные степени g – различные числа по модулю p. Числа p и g передаются абонентам в открытом виде. Затем каждый абонент группы выбирает свое секретное число ci, $1 < ci < p - 1$, и вычисляет соответствующее ему открытое число di , $di = gci \bmod p$.

Алгоритм Эль-Гамаля.

Будем предполагать, что сообщение представлено в виде числа $m < p$.

Шаг 1. A формирует случайное число k, $1 \leq k \leq p - 2$, вычисляет числа $r = gk \bmod p$, $e = m \cdot (d_B)^k \, mod \, p$ и передает пару чисел (r, e) абоненту B.

Шаг 2. B, получив (r, e), вычисляет $m' = e \cdot r^{p-1-cB} \, mod \, p$.

Литература:

Рябко Б. Я., Фионов А. Н. Криптография в информационном мире. - М.: Горячая линия - Телеком, 2018. - 300 с.

Глава 2. Криптосистемы с открытым ключом

ЗАДАНИЕ К ЛАБОРАТОРНОЙ РАБОТЕ

Изучить шифры RSA, Шамира, Эль-Гамаля.

Вопросы, на которые необходимо ответить:

1. Найти значения функции Эйлера $\varphi(14)$, $\varphi(20)$.
2. Используя свойства функции Эйлера, вычислить $\varphi(53)$, $\varphi(21)$, $\varphi(159)$.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Для выполнения заданий рекомендуется освоить какой-нибудь калькулятор модульной арифметики. Множество таких калькуляторов доступно в Интернете. Например, по поисковому запросу "*modular arithmetic online*" находим сайт https://planetcalc.com/8326/.

Пример. Зашифровать сообщение *RSA*, пусть цифровые значения букв для простоты соответствуют их номерам в алфавите: *R=18; S=19; A=1*. Расшифровать зашифрованное сообщение.

Решение:

Выбираем простые числа (небольшие, чтобы упростить вычисления): $p=3$ и $q=11$, вычисляем модуль $n=p\times q=3\times 1=33$. Вычисляем функцию Эйлера от модуля n: $\phi(n)=(p-1)\times(q-1)=2\times 10=20$. Выбираем открытую экспоненту $e=7$, определяем закрытую экспоненту d: $d\times e=1(\mathrm{mod}\,\phi(n)) \Rightarrow d=3$. Открытый ключ: $(e,n)=(7,33)$.

$C_1=(18^7)\mathrm{mod}33=6$

$C_2=(19^7)\mathrm{mod}33=13$

$C_3=(1^7)\mathrm{mod}33=1$

$C("RSA")=6131$

Расшифрование: используем закрытый ключ $(d,n)=(3,33)$.

$M_1=(6^3)\mathrm{mod}33=18$

$M_2=(13^3)\mathrm{mod}33=19$

$M_3=(1^3)\mathrm{mod}33=1$

$18=R;\ 19=S;\ 1=A;$ получаем исходное сообщение *RSA*.

Пример Шифр Шамира. Пусть *A* хочет передать *B* сообщение $m = 10$. *A* выбирает $p = 23$, $c_A = 7$ ($gcd(7, 22) = 1$) и вычисляет $d_A = 19$. Аналогично, *B* выбирает параметры $c_B = 5$ (взаимно простое с 22) и $d_B = 9$. По алгоритму Шамира:

Шаг 1. $x_1 = 10^7 \bmod 23 = 14$.

Шаг 2. $x_2 = 14^5 \bmod 23 = 15$.

Шаг 3. $x_3 = 15^{19} \bmod 23 = 19$.

Шаг 4. $x_4 = 19^9 \bmod 23 = 10$.

Таким образом, *B* получил передаваемое сообщение $m = 10$.

Пример Шифр Эль-Гамаля. Передадим сообщение $m = 15$ от A к B. Возьмем $p = 23$, $g = 5$.

Пусть абонент B выбрал для себя секретное число $cB = 13$ и вычислил $d_B = 5^{13} \bmod 23 = 21$.

Абонент A выбирает случайно число k, например $k = 7$, и вычисляет:

$r = 5^7 \bmod 23 = 17$, $e = 15 \cdot 21^7 \bmod 23 = 15 \cdot 10 \bmod 23 = 12$.

Теперь A посылает к B зашифрованное сообщение в виде пары чисел (*17, 12*). B вычисляет:

$m' = 12 \cdot 17^{23-1-13} \bmod 23 = 12 \cdot 179 \bmod 23 = 12 \cdot 7 \bmod 23 = 15$.

B смог расшифровать переданное сообщение.

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

Вариативность не предполагается.

1. Для шифра Шамира с параметрами $p = 30803$, $c_A = 501$, $c_B = 601$ и сообщения $m = 11111$ вычислить d_A, d_B, x_1, x_2, x_3, x_4.

2. Для шифра Эль-Гамаля с параметрами $p = 30803$, $g = 2$, $c = 500$, $k = 600$ и сообщения $m = 11111$ вычислить зашифрованное сообщение.

3. Для шифра *RSA* с параметрами пользователя $P = 131$, $Q = 227$, $d = 3$ и сообщения $m = 11111$ вычислить зашифрованное сообщение. Найти секретный ключ c и расшифровать сообщение.

ТРЕБОВАНИЯ К ОТЧЕТУ И ЗАЩИТЕ

Показать выполненную в тетради работу. Знать ответы на сформулированные выше вопросы. Защита работы проводится во время занятий. После защиты работа помещается в ЭИОС.

Лабораторная работа № 9. Электронная подпись

ОБЩИЕ СВЕДЕНИЯ

Цель: изучить электронную подпись.

Материалы, оборудование, программное обеспечение: калькулятор.

Условия допуска к выполнению: показать конспект по теоретической подготовке.

Критерии положительной оценки: показать выполненную работу, четко ответить на вопросы,

ТЕОРЕТИЧЕСКОЕ ВВЕДЕНИЕ

Рассмотрим электронную подпись, базирующуюся на схеме RSA.

Алиса для подписи документа выбирает параметры RSA – два больших простых числа P и Q, вычисляет $N = P\ Q$ и $\phi = (P - 1)(Q - 1)$. Затем она выбирает число d, взаимно простое с ϕ, и вычисляет $c = d{-}1\ mod\ \phi$. Далее она публикует числа N и d и хранит в секрете число c (остальные числа P, Q и ϕ можно забыть, они больше не потребуются). Теперь Алиса готова ставить свои подписи на документах или сообщениях.

Пусть Алиса хочет подписать сообщение $\bar{m} = m1,\ldots,mn$. Тогда вначале она вычисляет криптографическую хеш-функцию $y = h(m1, \ldots , mn)$, которая ставит в соответствие сообщению $\bar{m}$ число y. Предполагается, что алгоритм вычисления хеш-функции всем известен. Нам известно, что практически невозможно изменить основной текст $\bar{m}$, не изменив y. Поэтому на следующем шаге Алисе достаточно снабдить подписью только число y, и эта подпись будет относиться ко всему сообщению $\bar{m}$.

Алиса вычисляет число $s = y^c \bmod N$, т. е. она возводит число y в свою секретную степень. Число s это и есть цифровая подпись. Она просто добавляется к сообщению $\bar{m}$, и тем самым Алиса имеет сформированное подписанное сообщение $\langle \bar{m}, s \rangle$ (*).

Теперь каждый, кто знает открытые параметры Алисы, т. е. числа N и d, может проверить подлинность ее подписи. Для этого необходимо, взяв подписанное сообщение (*), вычислить значение хеш-функции $h(\bar{m})$, число $w = s^d \bmod N$ и проверить выполнение равенства $w = h(\bar{m})$.

Во многих странах сегодня существуют стандарты на электронную цифровую подпись. Для российского алгоритма ЭЦП ГОСТ Р34.10-94:

Вначале для пользователей выбираются общие открытые параметры. Необходимо найти два простых числа, q длиной *256* бит и p длиной *1024* бита, между которыми выполняется соотношение $p = bq + 1$ для некоторого целого b. Старшие биты в p и q должны быть равны единице. Затем выбирается число $a > 1$, такое, что $a^q \bmod p = 1$. В результате получаем три общих параметра — p, q и a.

Далее, каждый пользователь выбирает случайно число x, удовлетворяющее неравенству $1 < x < q$, и вычисляет $y = a^x \bmod p$.

Число x будет секретным ключом пользователя, а число y – открытым ключом. Предполагается, что открытые ключи всех пользователей указываются в некотором несекретном, но «сертифицированном» справочнике, который должен быть у всех, кто собирается проверять подписи. Отметим, что в настоящее время найти x по y практически невозможно при указанной выше длине модуля p. На этом этап выбора параметров заканчивается, и мы готовы к тому, чтобы формировать и проверять подписи.

Пусть имеется сообщение $\bar{m}$, которое необходимо подписать. Генерация подписи выполняется следующим образом:

1. Вычисляем значение хеш-функции $h = h(\bar{m})$, длина хеш-значения должна быть *256* бит (в российском варианте хеш-функция определяется ГОСТом Р34.11-94).

2. Формируем случайное число k, $0 < k < q$.

3. Вычисляем $r = (a^k \bmod p) \bmod q$. Если оказывается так, что $r = 0$, то возвращаемся к шагу 2.

4. Вычисляем $s = (kh + xr) \bmod q$. Если $s = 0$, то возвращаемся к шагу 2.

5. Получаем подписанное сообщение $\langle \bar{m}; r, s \rangle$.

Для проверки подписи делаем следующее.

1. Вычисляем хеш-функцию для сообщения $h = h(\bar{m})$.

2. Проверяем выполнение неравенств $0 < r < q$, $0 < s < q$.

3. Вычисляем $u1 = s \cdot h^{-1} \bmod q$, $u2 = -r \cdot h^{-1} \bmod q$.

4. Вычисляем $v = (a^{u1} y^{u2} \bmod p) \bmod q$.

5. Проверяем выполнение равенства $v = r$.

Если хотя бы одна из проверок на шагах 2 и 5 не дает нужного результата, то подпись считается недействительной. Если же все проверки удачны, то подпись считается подлинной.

Литература:

Рябко Б. Я., Фионов А. Н. Криптография в информационном мире. - М.: Горячая линия - Телеком, 2018. - 300 с.

Глава 3. Электронная цифровая подпись

ЗАДАНИЕ К ЛАБОРАТОРНОЙ РАБОТЕ

Изучить методы составления электронной подписи

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Для вычислений используем онлайн калькулятор *https://planetcalc.com/8326* или аналогичный. В качестве хеш-функции возьмем *sha256_3* – из значения хеш-функции *sha256* берутся три старшие подряд идущие десятичные цифры (включая *0*), буквы отбрасываются. Опять можно использовать онлайн калькулятор. Ищем "*hash calculator online"*, вводим сообщение и выбираем метод *sha256.*

Пример электронной подписи.

Пусть $P = 5, Q = 11$. Тогда $N = 5 \cdot 11 = 55, \phi = 4 \cdot 10 = 40$.

Пусть $d = 3$. Такой выбор d возможен, так как $gcd(40, 3) = 1$. Параметр $c = 3^{-1} \bmod 40$ вычисляем с помощью обобщенного алгоритма Евклида, $c = 27$.

Пусть, например, Алиса хочет подписать сообщение $\bar{m} = abbbaa$,

для которого значение хеш-функции равно, например, *13*:

$y = h(abbbaa) = 13$.

В этом случае Алиса вычисляет $s = 13^{27} \bmod 55 = 7$ и формирует подписанное сообщение $\langle abbbaa, 7\rangle$. Теперь тот, кто знает открытые ключи Алисы $N = 55$ и $d = 3$, может проверить подлинность подписи. Получив подписанное сообщение, он заново вычисляет значение хеш-функции $h(abbbaa) = 13$ (если содержание сообщения не изменено, то значение хеш-функции совпадет с тем, которое вычисляла Алиса) и вычисляет $w = 7^3 \bmod 55 = 13$.

Значения w и хеш-функции совпали, значит, подпись верна.

Для российского алгоритма ЭЦП ГОСТ Р34.10-94:

Пример. Выберем общие несекретные параметры $q = 11$, $p = 6q + 1 = 67$, возьмем $g = 10$ и вычислим $a = 10^6 \bmod 67 = 25$. Выберем секретный ключ $x = 6$ и вычислим открытый ключ $y = 25^6 \bmod 67 = 62$.

Сформируем подпись для сообщения $\bar{m} = baaaab$. Пусть для хеш-функции этого сообщения $h(\bar{m}) = 3$. Возьмем случайно число $k = 8$.

Вычислим

$r = (25^8 \bmod 67) \bmod 11 = 24 \bmod 11 = 2,$

$s = (8 \cdot 3 + 6 \cdot 2) \bmod 11 = 36 \bmod 11 = 3.$

Получаем подписанное сообщение

$\langle baaaab; 2, 3\rangle$.

Теперь проверим подпись. Если сообщение не изменено, то $h = 3$. Вычислим

$h^{-1} = 3^{-1} \bmod 11 = 4,$

$u1 = 3 \cdot 4 \bmod 11 = 1,$

$u2 = -2 \cdot 4 \bmod 11 = -8 \bmod 11 = 3,$

$v = (25^1 \cdot 62^3 \bmod 67) \bmod 11 =$

= (25 · 9 mod 67) mod 11 = 24 mod 11 = 2.

Мы видим, что $v = r$, значит, подпись верна.

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

Вариативность не предполагается.

1. Для системы *RSA* с параметрами пользователя *P = 131, Q = 227, d = 3* и секретного ключа *c*, найденного в первой лабораторной работе, вычислить подпись для сообщения *m* = "*Happy New Year"*. Осуществить проверку подписи.

2. В подписанный документ внести ошибку (искажение). Еще раз сделать проверку подписи.

3. Для алгоритма ЭЦП ГОСТ Р34.10-94 выбраны следующие общие параметры: *p = 22921, q = 191, a = 9281*. Секретный ключ пользователя – автора документа *x = 100*. Найти открытый ключ, вычислить и проверить подпись для того же сообщения при том же значении хеш-функции, что и в первом задании.

ТРЕБОВАНИЯ К ОТЧЕТУ И ЗАЩИТЕ

Показать выполненную в тетради работу. Знать ответы на сформулированные выше вопросы. Защита работы проводится во время занятий. После защиты работа помещается в ЭИОС.

Лабораторная работа № 10. Алгоритм Диффи-Хеллмана

ОБЩИЕ СВЕДЕНИЯ

Цель: изучить алгоритм Диффи-Хеллмана.

Материалы, оборудование, программное обеспечение: калькулятор.

Условия допуска к выполнению: показать конспект по теоретической подготовке.

Критерии положительной оценки: показать выполненную работу, четко ответить на вопросы,

ТЕОРЕТИЧЕСКОЕ ВВЕДЕНИЕ

При работе алгоритма Диффи-Хеллмана каждая сторона:

1. генерирует случайное число – закрытый ключ;

2. совместно с удаленной стороной устанавливает *открытые параметры* p и q (обычно значения p и q генерируются на одной стороне и передаются другой), где p является случайным простым числом, $(p-1)/2$ также должно быть случайным простым числом (для повышения безопасности), q – первообразный корень по модулю p (также является простым числом);

3. каждая сторона вычисляет *открытый ключ*, используя преобразование над *закрытым ключом;*

4. обменивается *открытыми ключами* с удаленной стороной;

5. каждая сторона вычисляет *общий секретный ключ* K, используя открытый ключ удаленной стороны и свой закрытый ключ.

K получается равным с обеих сторон, потому что:

$$B^a \bmod p = (q^b \bmod p)^a \bmod p = \boldsymbol{q^{ab} \bmod p} = (q^a \bmod p)^b \bmod p = A^b \bmod p$$

Пусть существует два абонента Алиса и Боб. Обоим абонентам известны некоторые два числа p и q, которые не являются секретными и могут быть известны также другим заинтересованным лицам. Для того, чтобы создать неизвестный более никому секретный ключ, оба абонента генерируют большие случайные числа: Алиса – число a, Боб – число b. Затем Алиса вычисляет:

$$A=q^a \bmod p \qquad (1)$$

и пересылает его Бобу, а Боб вычисляет:

$$B=q^b \bmod p \qquad (2)$$

и передает Алисе. Предполагается, что злоумышленник может получить оба этих значения, но не модифицировать их (то есть у него нет возможности вмешаться в процесс передачи). На втором этапе Алиса на основе имеющегося у нее a и полученного по сети B вычисляет значение:

$$B^a \bmod p=q^{ba} \bmod p \qquad (3)$$

Боб на основе имеющегося у него b и полученного по сети A вычисляет значение:

$$A^b mod\ p = q^{ab} mod\ p \quad (4)$$

У Алисы и Боба получилось одно и то же число:

$$K = q^{ab} mod\ p \quad (5)$$

Его они и могут использовать в качестве секретного ключа, поскольку здесь злоумышленник встретится с практически неразрешимой (за разумное время) проблемой вычисления (3) или (4) по перехваченным $q^a mod$ ри $q^b mod$ p, если числа p, a, b выбраны достаточно большими.

Алгоритм Диффи-Хеллмана на эллиптических кривых.

Эллиптической кривой *E* над полем *F* называется множество точек *(x,y),* координаты которых принадлежат полю и удовлетворяют кубическому уравнению

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in F. \ (6)$$

Вместо (1) используется и функция

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0. \quad (7)$$

Эллиптическую кривую *E* называют ***сингулярной***, если на кривой существует хотя бы одна особая точка *(x,y),* в которой одновременно выполняются условия

$$\frac{\partial f}{\partial x} = 0 \ \text{ и } \ \frac{\partial f}{\partial y} = 0. \ (8)$$

Нас будет интересовать ***форма Вейерштрасса***: если характеристика поля $p \neq 2$ и $p \neq 3$, то

$$y^2 = x^3 + ax + b. \ (9)$$

Суммой двух точек *P* и *Q* называется точка *R=P+Q,* обратная третьей точке пересечения эллиптической кривой и прямой, проходящей через точки *P* и *Q.*

Если суммируемые точки *P* и *Q* совпадают, то *P+Q=P+P=R*, что равносильно удвоению точки *2P=R.* При *P=Q* секущая *PQ* превращается в касательную к кривой, и геометрически удвоенная точка *2P* – это точка, обратная к точке пересечения этой касательной и эллиптической кривой.

Формулы сложения и удвоения точек эллиптической кривой справедливы для всех полей, кроме полей характеристик *2* и *3*.

Таблица формул для операций с точками эллиптической кривой:

Операция	*Поле характеристики p (p≠2 и p≠3)*
Сложение точек $P \neq \pm Q$ $P(x_1,y_1)+Q(x_2,y_2)=R(x_3,y_3)$	$\lambda = \frac{y_2 - y_1}{x_2 - x_1} (mod\ p)$ $x_3 = \lambda^2 - x_1 - x_2\ (mod\ p)$

	$y_3 = \lambda(x_1 - x_3) - y_1 (mod\ p)$
Удвоение точки $R(x_3,y_3)=2\ P(x_1,y_1)$	$\lambda = \frac{3{x_1}^2 + a}{2y_1} (mod\ p)$ $x_3 = \lambda^2 - 2x_1\ (mod\ p)$ $y_3 = \lambda(x_1 - x_3) - y_1 (mod\ p)$
$O+O=O$ $P(x,y)+O= P(x,y)$ $P(x,y)+ P(x,-y)=O$	

Точку *mP*, равную *m*-кратному сложению точки *P* в аддитивной группе точек эллиптической кривой, называют *скалярным произведением точки P на число m,* а сами точки *mP – скалярными кратными точками.* Таким образом, $mP=P+P+...+P$, при этом $O \cdot P=O$ и $-mP(x,y)= mP(x, -y)$.

Арифметика эллиптических кривых не содержит прямых формул для вычисления кратного *mP* для заданной точки *P(x,y).* Эту операцию выполняют с помощью операций сложения и удвоения точки. Для этого надо представить число *m* в двоичной форме $m=b_t b_{t-1}...b_0$, потом вычислить все точки *2P, 4P,...,*2^tP и вычислить сумму тех точек 2^iP, для которых $b_i=1$. Например, $13_{10}=1101_2=1\times2^0+0\times2^1+1\times2^2+1\times2^3$, значит, *13P=P+4P+8P.*

Порядок точки *P* – это наименьшее натуральное число *n*, при котором *nP=O.*

Криптоалгоритмы на эллиптических кривых строятся аналогично алгоритмам в простых конечных полях. Возведение в степень по большому модулю, определяющее стойкость шифра, заменяется на скалярное произведение точки эллиптической кривой. Таблица перевода обычного криптоалгоритма в эллиптический:

Термины и понятия	*Криптосистема над простым конечным полем*	*Криптосистема на эллиптической кривой над конечным полем*
Группа	Z_p^*	*E(GF(p))*
Элементы группы	Целые *{1,2,...,p-1}*	Точки *P(x,y)* на кривой и точка *O*
Групповая операция	Умножение по модулю *p*	Сложение точек
	Элементы *g* и *h*	Точки *P* и *Q*
	Обратный элемент g^{-1}	Обратная точка *-P*
	Деление $g \cdot h^{-1}$	Вычитание точек *P–Q*
	Возведение в степень g^a	Скалярное умножение

		mP
Проблема дискретного логарифмирования	$g \epsilon Z_p^*$; $h=g^a(mod\ p)$; найти a	$P \epsilon E(GF(p))$; $Q=mP$; найти m

Приведем эллиптический аналог открытого распределения ключей Диффи-Хеллмана (ECDH).

Пользователи ***A*** и ***B*** выбирают общие параметры:

– эллиптическую кривую над конечным полем;

– точку P на этой кривой, имеющую большой порядок n (она не обязательно должна быть порождающим элементом группы точек кривой, но порожденная ею подгруппа должна быть большой, предпочтительно того же порядка, что и сама группа). Точка P называется ***базовой.***

Общие параметры передаются открытым каналом связи.

1. Пользователь ***A*** случайно выбирает число K_A – свой секретный ключ, а пользователь ***B*** случайно выбирает число K_B – свой секретный ключ (числа близки по порядку к общему числу N_E точек кривой). Далее пользователи находят свои точки $Q= K_AP$ и $R= K_BP$ соответственно.

2. Пользователи обмениваются точками Q и R по открытому каналу.

3. Пользователь ***A***, получив точку R, вычисляет точку $S= K_AR$.

4. Пользователь ***B***, получив точку Q, вычисляет точку $S= K_BQ$.

Так как $K_AR= K_A(K_BP)= K_B(K_AP)= K_BQ$, то S – общий секретный ключ пользователей.

Литература:

Воробейкина, И. В. Методы и средства криптографической защиты информации: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения / И. В. Воробейкина; БГАРФ ФГБОУ ВО «КГТУ». – Калининград: Изд-во БГАРФ, 2022. - 114 с.

Глава 6. Алгоритмы с открытыми ключами. 6.5 Алгоритм Диффи-Хеллмана. 6.6 Реализация алгоритм Диффи-Хеллмана на эллиптических кривых.

ЗАДАНИЕ К ЛАБОРАТОРНОЙ РАБОТЕ

1. Разложить на простые множители числа *108, 77, 65, 30, 159.*

2. Определить, какие из пар чисел *(25, 12), (25, 15), (13, 39), (40, 27)* взаимно просты.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Для выполнения заданий рекомендуется освоить какой-нибудь калькулятор модульной арифметики. Множество таких калькуляторов доступно в Интернете. Например, по поисковому запросу "*modular arithmetic online*" находим сайт https://planetcalc.com/8326/.

Пример. Ева – криптоаналитик. Она читает пересылку Боба и Алисы, но не изменяет содержимого их сообщений. Исходные данные: $p = 23$ – открытое простое число, $g = 5$ – первообразный корень по модулю p (тоже открытое число), $a = 6$ – секретный ключ Алисы, $b = 15$ – секретный ключ Боба. $A = g^a \bmod p$ – открытый ключ Алисы, $B = g^b \bmod p$ – открытый ключ Боба.

Алиса		*Боб*		*Ева*	
Знает	Не знает	Знает	Не знает	Знает	Не знает
$p=23$	$b=?$	$p=23$	$a=?$	$p=23$	$a=?$
$g=5$		$g=5$		$g=5$	$b=?$
$a=6$		$b=15$			$K=?$
$A=5^6 mod\ 23=8$		$B=5^{15} mod 23=19$		$A=5^a mod\ 23 =8$	
$B=5^b mod\ 23=19$		$A=5^a mod\ 23 = 8$		$B=5^b mod\ 23=19$	
$K=19^6 mod\ 23=\mathbf{2}$		$K=8^{15} mod\ 23=\mathbf{2}$		$K=19^a mod\ 23?$	
				$\boldsymbol{K}=8^b mod\ 23?$	

$K = 2$ – секретный ключ.

Алгоритм Диффи-Хеллмана на эллиптических кривых.

Пример

Вычислить в группе $E_{11}(1,6)$: *а) (8,3)+(3,6); б) 2(1,8).*

Решение:

а) $(x_1,y_1)=(8,3)$; $(x_2,y_2)=(3,6)$.

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod\ p = \frac{6-3}{3-8} mod 11 = \frac{3}{-5} mod 11 = -3 \cdot 5^{-1} mod 11$$

$$= -3 \cdot 9 mod 11 = 6 mod 11 = 6$$

$$x_3 = \lambda^2 - x_1 - x_2 mod\ p = 36 - 8 - 3 mod 11 = 3$$

$$y_3 = \lambda(x_1 - x_3) - y_1 mod\ p = 6(8-3) - 3 mod 11 = 5$$

Ответ: (8,3)+(3,6)=(3,5).

б) $(x_1,y_1)=(1,8)$.

$$\lambda = \frac{3x_1^2 + a}{2y_1} mod\ p = \frac{3 \cdot 1^2 + 1}{2 \cdot 8} mod 11 = \frac{4}{16} mod 11 = 4^{-1} mod 11 = 3 mod 11 = 3$$

$$x_3 = \lambda^2 - 2x_1 mod\ p = 9 - 2 \cdot 1 mod 11 = 7$$

$$y_3 = \lambda(x_1 - x_3) - y_1 mod\ p = 3(1 - 7) - 8 mod 11 = 7$$

Ответ: 2(1,8)=(7,7).

Пример.

Найти порядок точки *P(9,4)* в группе эллиптической кривой $E_{11}(6,3)$.

Решение:

1) *2P=P+P=(9,4)+(9,4):*

$$\lambda = \frac{3 \cdot 9^2 + 6}{2 \cdot 4} mod 11 = 249 \cdot 8^{-1} mod 11 = 249 \cdot 7 mod 11 = 5$$

$$x_3 = 5^2 - 2 \cdot 9 mod 11 = 7,\ \ y_3 = 5(9 - 7) - 4 mod 11 = 6,$$

$$2P(9,4) = (7,6)$$

2) *3P=2P+P=(7,6)+(9,4):*

$$\lambda = \frac{4 - 6}{9 - 7} mod 11 = \frac{-2}{2} mod 11 = -1 mod 11 = 10$$

$$x_3 = 10^2 - 2 - 9 mod 11 = 7,\ \ y_3 = 10(7 - 7) - 6 mod 11 = 5,$$

$$3P(9,4) = (7,5)$$

3) *4P=3P+P=(7,5)+(9,4):*

$$\lambda = \frac{4 - 5}{9 - 7} mod 11 = \frac{-1}{2} mod 11 = -2^{-1} mod 11 - 6 mod 11 = 5$$

$$x_3 = 5^2 - 7 - 9 mod 11 = 9,\ \ y_3 = 5(7 - 9) - 5 mod 11 = 7,$$

$$4P(9,4) = (9,7)$$

4) *5P=4P+P=(9,7)+(9,4):*

$$\lambda = \frac{4 - 7}{9 - 9} mod 11 \to \infty$$

5P=O, значит, порядок точки *P(9,4)* равен *5*.

Пример.

Найти общий ключ для шифрования *K=(x,y)*, используя алгоритм Диффи-Хеллмана на основе эллиптических кривых, если кривая имеет вид $y^2 = x^3 + 2x + 2\ mod 17$ и задает циклическую группу порядка *#C=19*. Примитивный элемент равен *P=(5,1)*. Секретный ключ Алисы *c=3*, секретный ключ Боба *d=10*.

Решение:

Алиса шифрует точку P своим секретным ключом: $Q=c\times P$, результат Q пересылает Бобу. Боб шифрует точку P своим секретным ключом: $R=d\times P$, результат R пересылает Алисе. Передача осуществляется по открытому каналу. Далее, Алиса шифрует полученный результат: $S=c\times R=c\times d\times P$, Боб шифрует полученный результат: $S=d\times Q=d\times c\times P$. Получается общий секретный ключ S.

Шифрует Алиса:

$3P(5,1)=11_2(5,1)=1\times 2^0P(5,1)+1\times 2^1P(5,1)= P(5,1)+2P(5,1)=P(6,3)+P(5,1)= P(10,6)$ (вычисления см. ниже).

Вычисляем *$2P(5,1)$:*

$$\lambda=\frac{3\cdot 5^2+2}{2\cdot 1}mod17=\frac{77}{2}mod17=77\cdot 2^{-1}mod17=77\cdot 9mod17=13$$

$$x_3=13^2-2\cdot 5mod17=6,\ \ y_3=13\cdot(5-6)-1mod17=3$$

Следовательно, *$2P(5,1)=P(6,3)$*.

Вычисляем *$2P(5,1)+ P(5,1)=P(6,3)+P(5,1)$:*

$$\lambda=\frac{3-1}{6-5}mod17=2mod17=2$$

$$x_3=2^2-5-6mod17=10,\ \ y_3=2\cdot(5-10)-1mod17=6$$

Результат шифрования Алисы*: $3P(5,1)=P(10,6)$*.

Шифрует Боб:

$10P(5,1)=1010_2P(5,1)= 1\times 2^3P(5,1)+1\times 2^1P(5,1)=8\ P(5,1)+2P(5,1)=$

$2P(5,1)+2P(5,1)+2P(5,1)+2P(5,1)+2P(5,1)=P(6,3)+P(6,3)+P(6,3)+ P(6,3)+ P(6,3)=2P(6,3)+2P(6,3)+ P(6,3)= P(3,1)+P(3,1)+P(6,3)= =2P(3,1)+P(6,3)= P(13,7)+P(6,3)=P(7,11)$ (вычисления см. ниже).

Вычисляем *$2P(6,3)$:*

$$\lambda=\frac{3\cdot 6^2+2}{2\cdot 3}mod17=\frac{110mod17}{6mod17}=8\cdot 6^{-1}mod17=$$
$$=8\cdot 3mod17=7$$

$$x_3=7^2-2\cdot 6mod17=3,\ \ y_3=7\cdot(6-3)-3mod17=1$$

Следовательно, *$2P(6,3)=P(3,1)$*.

Вычисляем 2P(3,1):

$$\lambda=\frac{3\cdot 3^2+2}{2\cdot 1}mod17=\frac{29mod17}{2mod17}=\frac{12}{2}mod17=6$$

$$x_3=6^2-2\cdot 3mod17=13,\ \ y_3=6\cdot(3-13)-1mod17=7$$

Следовательно*, $2P(3,1)=P(13,7)$*.

Вычисляем *$P(13,7)+P(6,3)$:*

$$\lambda = \frac{3-7}{6-13} mod 17 = \frac{4}{7} mod 17 = 4 \cdot 7^{-1} mod 17 =$$
$$= 4 \cdot 5 mod 17 = 3$$
$$x_3 = 3^2 - 13 - 16 mod 17 = 7,$$
$$y_3 = 3 \cdot (13-7) - 7 mod 17 = 11$$

Следовательно, *P(13,7)+P(6,3)=P(7,11).*

Алиса передает Бобу результат *P(10,6),* Боб передает Алисе результат *P(7,11).*

Алиса шифрует:

3P(7,11)=11$_2$(7,11)=1×2^{0}P(7,11)+1×2^{1}P(7,11)=

*=P(7,11)+2P(7,11)=P(7,11)+P(5,1)=**P(13,10)*** (вычисления см. ниже).

Вычисляем *2P(7,11):*

$$\lambda = \frac{3 \cdot 7^2 + 2}{2 \cdot 11} mod 17 = \frac{149 mod 17}{22 mod 17} = 13 \cdot 5^{-1} mod 17 = 6$$
$$x_3 = 6^2 - 2 \cdot 7 mod 17 = 5, \;\; y_3 = 6 \cdot (7-5) - 11 mod 17 = 1$$

Следовательно, *2P(7,11)=P(5,1).*

Вычисляем *P(7,11)+P(5,1):*

$$\lambda = \frac{1-11}{5-7} mod 17 = \frac{10}{2} mod 17 = 10 \cdot 2^{-1} mod 17 = 5$$
$$x_3 = 5^2 - 7 - 5 mod 17 = 13,$$
$$y_3 = 5 \cdot (7-13) - 11 mod 17 = 10$$

Следовательно, *P(7,11)+P(5,1)=P(13,10) – **общий секретный ключ**.*

Боб шифрует:

10P(10,6)=1010$_2$P(10,6)=1×2^{3}P(10,6)+1×2^{1}P(10,6)=8P(10,6)+2P(10,6)=
2P(10,6)+2P(10,6)+2P(10,6)+2P(10,6)+2P(10,6)+2P(10,6)=P(16,13)+P(16,13)
+P(16,13)+P(16,13)+P(16,13)=2P(16,13)+2P(16,13)+P(16,13)=P(0,11)+P(0,11)+
*P(16,13)=2P(0,11)+P(16,13)=P(9,16)+P(16,13)=**P(13,10)*** (вычисления см. ниже).

Общий секретный ключ – ***P(13,10)*** – у Алисы и Боба совпадает.

Вычисляем 2P(10,6):

$$\lambda = \frac{3 \cdot 10^2 + 2}{2 \cdot 6} mod 17 = \frac{302 mod 17}{12 mod 17} = 13 \cdot 12^{-1} mod 17 = 11$$
$$x_3 = 11^2 - 2 \cdot 10 mod 17 = 16,$$
$$y_3 = 11 \cdot (10-16) - 6 mod 17 = 13$$

Следовательно, *2P(10,6)=P(16,13).*

Вычисляем *2P(16,13):*

$$\lambda = \frac{3 \cdot 16^2 + 2}{2 \cdot 13} mod 17 = \frac{770 mod 17}{26 mod 17} = 5 \cdot 9^{-1} mod 17 = 10$$

$$x_3 = 10^2 - 2 \cdot 16 mod 17 = 0,$$
$$y_3 = 10 \cdot (16 - 0) - 13 mod 17 = 11$$

Следовательно, *2P(16,13)=P(0,11).*

Вычисляем *2P(0,11):*

$$\lambda = \frac{3 \cdot 0^2 + 2}{2 \cdot 11} mod 17 = \frac{2}{22 mod 17} = 1 \cdot 11^{-1} mod 17 = 14$$
$$x_3 = 14^2 - 2 \cdot 0 mod 17 = 9,$$
$$y_3 = 14 \cdot (0 - 9) - 11 mod 17 = 16$$

Следовательно, *2P(0,11)=P(9,16).*

Вычисляем *P(9,16)+P(16,13):*

$$\lambda = \frac{13 - 16}{16 - 9} mod 17 = -\frac{3}{7} mod 17 = 14 \cdot 7^{-1} mod 17 = 2$$
$$x_3 = 2^2 - 9 - 16 mod 17 = 13,$$
$$y_3 = 2 \cdot (9 - 13) - 16 mod 17 = 10$$

Следовательно, *P(9,16)+P(16,13)=P(13,10)* – ***общий секретный ключ***.

В процессе вычислений можно проверять результаты, подставляя значения *x* и *y* в уравнение эллиптической кривой. Если окажется, что точка *P(x, y)* принадлежит кривой (т.е. значения левой и правой частей уравнения совпадают), то координаты точки вычислены верно.

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

Вариативность не предполагается.

1. Для системы Диффи-Хеллмана с параметрами *p = 30803*, *g = 2*, *XA = 1000*, *XB = 2000* вычислить открытые ключи и общий секретный ключ.

2. Сгенерировать общий секретный ключ для двух пользователей по схеме Диффи-Хеллмана, если выбрана эллиптическая кривая $E_{211}(0, -4)$ и точка *P(2,2).* Пусть секретный ключ пользователя *A* будет $K_A=121$, а пользователя *B* – $K_B=203$.

ТРЕБОВАНИЯ К ОТЧЕТУ И ЗАЩИТЕ

Показать выполненную в тетради работу. Знать ответы на сформулированные выше вопросы. Защита работы проводится во время занятий. После защиты работа помещается в ЭИОС.

Заключение

В данном пособии на примерах рассматриваются различные методы и приемы защиты информации. Каждое занятие состоит из теоретических положений, упражнений. Пособие рассчитано как для начинающих специалистов по защите информации, так и для тех, кто хочет усовершенствовать свои знания.

Предполагается, что студенты пользуются лекционным материалом и рекомендованной литературой, поэтому теоретический материал в полном объеме не приводится.

В основу пособия положены лабораторные занятия, проводимые автором по дисциплине «Криптографические методы защиты информации» для студентов специальности 10.05.03 «ИБАС».

Литература

1. Алферов, А. П. Основы криптографии: учебное пособие. - Москва: Гелиос АРВ, 2005. - 480 с.

2. Молдовян, Н. А. Криптография. От примитивов к синтезу алгоритмов: практическое пособие / Н. А. Молдовян, А. А. Молдовян, М. А. Еремеев. – Санкт_Петербург: БХВ-Петербург, 2004. - 448 с.

3. Рябко, Б. Я. Криптография в информационном мире / Б. Я. Рябко, А. Н. Фионов. - Москва: Горячая линия - Телеком, 2018. - 300 с.

4. Романьков, В. А. Введение в криптографию: курс лекций / В. А. Романьков. - Москва: Форум, 2012. - 240 с.

5. Воробейкина, И. В. Методы и средства криптографической защиты информации: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения / И. В. Воробейкина; БГАРФ ФГБОУ ВО «КГТУ». – Калининград: Изд-во БГАРФ, 2022. - 114 с.

Локальный электронный методический материал

Ирина Владимировна Воробейкина

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Редактор Г. А. Смирнова

Уч.-изд. л. 3,75. Печ. л. 3,75

Издательство федерального государственного бюджетного образовательного учреждения высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1