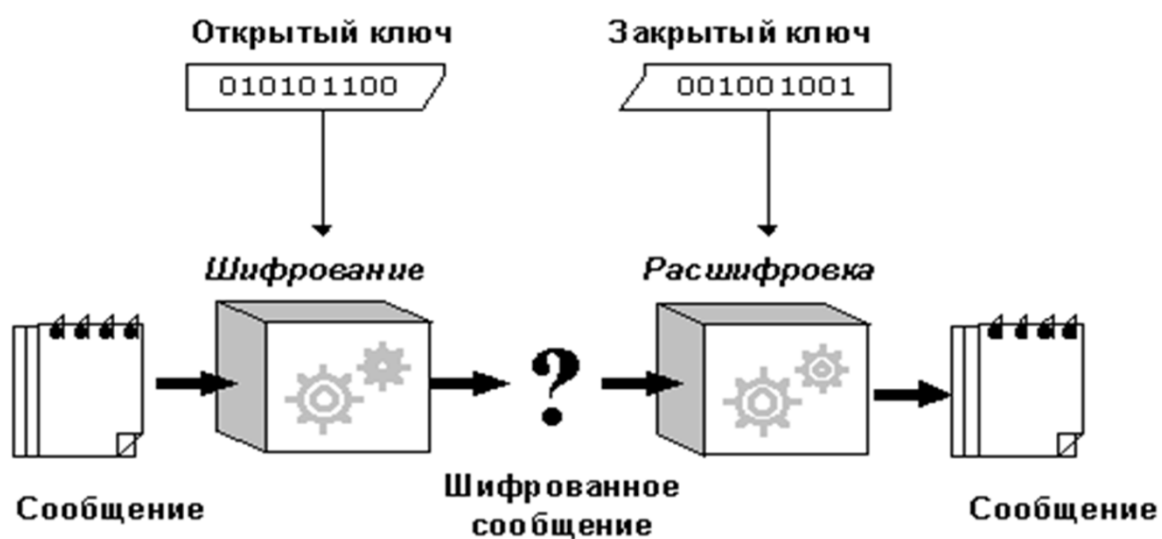


А.А. Ожиганов

КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ С СЕКРЕТНЫМ И ОТКРЫТЫМ КЛЮЧОМ



Санкт-Петербург
2015

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
УНИВЕРСИТЕТ ИТМО

А.А. Ожиганов

**КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ
С СЕКРЕТНЫМ И ОТКРЫТЫМ КЛЮЧОМ**

Учебное пособие

 **УНИВЕРСИТЕТ ИТМО**

Санкт-Петербург

2015

Ожиганов А.А. Криптографические системы с секретным и открытым ключом: учебное пособие. – СПб: Университет ИТМО, 2015. – 64 с.

Целью данного учебного пособия является ознакомление студентов с основами криптологии. Материал пособия разбит на два раздела. Первый раздел посвящен изучению криптографических систем с секретным ключом. Он включает в себя лабораторные работы по изучению основ шифрования данных, блочному и поточному симметричному шифрованию, а также - демонстрационную версию криптостойкого блочного алгоритма Rijndael. Второй раздел посвящен изучению криптографических систем с открытым ключом. Первые четыре лабораторных работы этого раздела позволяют изучить свойства RSA-криптосистем на числах небольшой разрядности, что позволяет обеспечить наглядность и понять принципиальные моменты. Последние шесть лабораторных работ второго раздела посвящены изучению криптографических систем на основе эллиптических кривых. В каждом разделе приведены краткие теоретические сведения и даны методические указания к выполнению соответствующей лабораторной работы.

Пособие предназначено для студентов, специализирующихся в области информационных технологий и может быть использовано при подготовке магистров по учебной программе «Безопасность вычислительных систем и сетей».

Рекомендовано Советом факультета Компьютерных технологий и управления 10 марта 2015 г., протокол № 3



Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

© Университет ИТМО, 2015

©А.А.Ожиганов, 2015

Содержание

	Стр.
Криптографические системы с секретным ключом	4
Лабораторная работа № 1. <i>Основы шифрования данных</i>	4
Лабораторная работа № 2. <i>Блочное симметричное шифрование</i> .	5
Лабораторная работа № 3. <i>Поточное симметричное шифрование</i>	6
Лабораторная работа № 4. <i>Демонстрационная версия криптостойкого блочного алгоритма Rijndael</i>	10
Криптографические системы с открытым ключом	11
Лабораторная работа № 1. <i>Атака на алгоритм шифрования RSA посредством метода Ферма</i>	11
Лабораторная работа № 2. <i>Атака на алгоритм шифрования RSA методом повторного шифрования</i>	21
Лабораторная работа № 3. <i>Атака на алгоритм шифрования RSA методом бесключевого чтения</i>	29
Лабораторная работа № 4. <i>Атака на алгоритм шифрования RSA, основанный на Китайской теореме об остатках</i>	38
Лабораторная работа № 5. <i>Шифрование открытого текста на основе эллиптических кривых</i>	46
Лабораторная работа № 6. <i>Расшифрование криптограммы на основе эллиптических кривых</i>	49
Лабораторная работа № 7. <i>Расчет точки $2P + 3Q - R$ на эллиптической кривой</i>	55
Лабораторная работа № 8. <i>Расчет точки nP на эллиптической кривой</i>	56
Лабораторная работа № 9. <i>Получение ЭЦП на основе эллиптических кривых</i>	57
Лабораторная работа № 10. <i>Проверка ЭЦП на основе эллиптических кривых</i>	59
Использованная литература	60

Криптографические системы с секретным ключом

Лабораторная работа № 1

Основы шифрования данных

Цель работы: изучение основных принципов шифрования информации, знакомство с широко известными алгоритмами шифрования, приобретение навыков их программной реализации.

Порядок выполнения работы

1. Ознакомьтесь с теоретическими основами шифрования данных, которые приведены в [1] и [2].
2. Получите вариант задания у преподавателя. 8
3. Напишите программу согласно варианту задания.
4. Отладьте разработанную программу и покажите результаты работы программы преподавателю.
5. Составьте отчет по лабораторной работе.

Содержание отчета

Отчет по лабораторной работе должен содержать следующие сведения:

- название и цель работы;
- вариант задания;
- листинг разработанной программы с комментариями;
- результаты работы программы.

Варианты заданий

1. Реализовать в программе шифрование и дешифрацию содержимого файла по методу Цезаря с ключевым словом.
2. Реализовать шифрование и дешифрацию файла по методу Виженера. Ключевая фраза вводится. Реализовать в программе частотный криптоанализ зашифрованного текста.
3. Реализовать шифрование и дешифрацию файла с использованием метода биграмм. Ключевое слово вводится.
4. Реализовать в программе шифрование и дешифрацию файла с использованием квадрата Полибия, обеспечив его случайное заполнение.
5. Реализовать в программе шифрование и дешифрацию файла с использованием квадрата Кардано размером 4x4.
6. Реализовать в программе шифрование и дешифрацию файла методом биграмм с двойным квадратом. Квадраты генерировать динамически для каждого шифрования.
7. Реализовать в программе шифрование и дешифрацию файла с использованием перестановочного шифра с ключевым словом. Ключевое слово вводится.
8. Реализовать в программе шифрование и дешифрацию файла с использованием аффинной криптосистемы. Провести частотный анализ

зашифрованного файла, осуществляя проверку по файлу с набором ключевых слов.

9. Реализовать шифрование и дешифрацию файла по методу Виженера с составным ключом. Набор ключей вводится.

10. Реализовать в программе шифрование и дешифрацию содержимого файла по методу Цезаря. Провести частотный анализ зашифрованного файла, осуществляя проверку по файлу с набором ключевых слов.

Контрольные вопросы

1. Дайте определение следующим понятиям: шифр, криптография, криптоанализ, ключ.

2. Классифицируйте алгоритм, полученный в качестве задания к лабораторной работе.

3. Чем отличаются одно- и многоалфавитные методы шифрования?

4. В чем заключается основной принцип частотного криптоанализа?

5. Какой метод криптоанализа применим для вскрытия алгоритма, полученного вами в качестве задания к лабораторной работе?

6. Оцените мощность ключевого пространства вашего алгоритма.

Лабораторная работа № 2

Блочное симметричное шифрование

Цель работы: изучение структуры и основных принципов работы современных алгоритмов блочного симметричного шифрования, приобретение навыков программной реализации блочных симметричных шифров.

Порядок выполнения работы

1. Ознакомьтесь с теоретическими основами шифрования данных, которые приведены в [1] и [2].

2. Получите вариант задания у преподавателя. 5Б

3. Напишите программу согласно варианту задания.

4. Отладьте разработанную программу и покажите результаты работы программы преподавателю.

5. Составьте отчет по лабораторной работе.

Содержание отчета

Отчет по лабораторной работе должен содержать следующие сведения:

- название и цель работы;
- вариант задания;
- листинг разработанной программы с комментариями;
- результаты работы программы.

Варианты заданий

Реализовать систему симметричного блочного шифрования, позволяющую шифровать и дешифровать файл на диске с использованием заданного блочного шифра в заданном режиме шифрования. Перечень блочных шифров и режимов шифрования приведен в таблице. Номер шифра и режима для реализации получить у преподавателя.

Таблица. Варианты заданий к лабораторной работе

Алгоритм		Режим шифрования	
Номер	Название	Номер	Режим
1	TEA	а	ECB
2	IDEA	б	CBC
3	RC6	в	PCBC
4	ГОСТ 28147-89	г	CFB
5	Rijndael	д	OFB
6	DES		

Контрольные вопросы

1. Перечислите основные обратимые операции, используемые в образующих функциях блочных шифров.
2. Что такое сеть Фейштеля? В чем ее основные достоинства?
3. Какие параметры блочных шифров влияют на его криптостойкость?
4. Какие блочные шифры, построенные по принципу сети Фейштеля, вам известны?
5. Проведите сравнительный анализ алгоритмов ГОСТ 28147-89 и Rijndael.
6. Проведите сравнительный анализ режимов шифрования CBC и ECB.
7. Проведите сравнительный анализ режимов шифрования CBC и CFB

Лабораторная работа № 3

Поточное симметричное шифрование

Цель работы: изучение структуры и основных принципов работы современных алгоритмов поточного симметричного шифрования, приобретение навыков программной реализации поточных симметричных шифров.

Порядок выполнения работы

1. Ознакомьтесь с теоретическими основами шифрования данных, которые приведены в [1] и [2].
2. Получите вариант задания у преподавателя.

3. Напишите программу согласно варианту задания.
4. Отладьте разработанную программу и покажите результаты работы программы преподавателю.
5. Составьте отчет по лабораторной работе

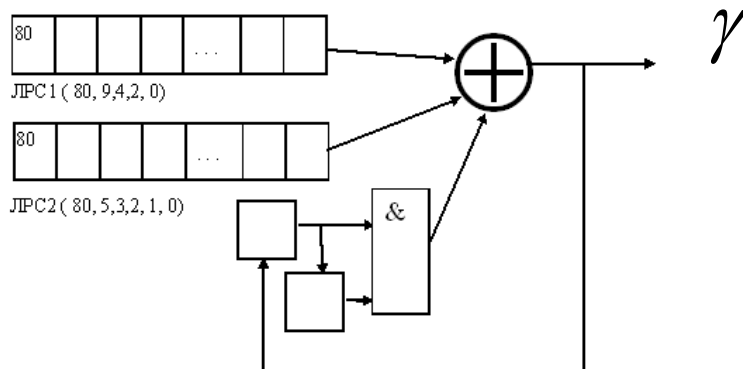
Содержание отчета

Отчет по лабораторной работе должен содержать следующие сведения:

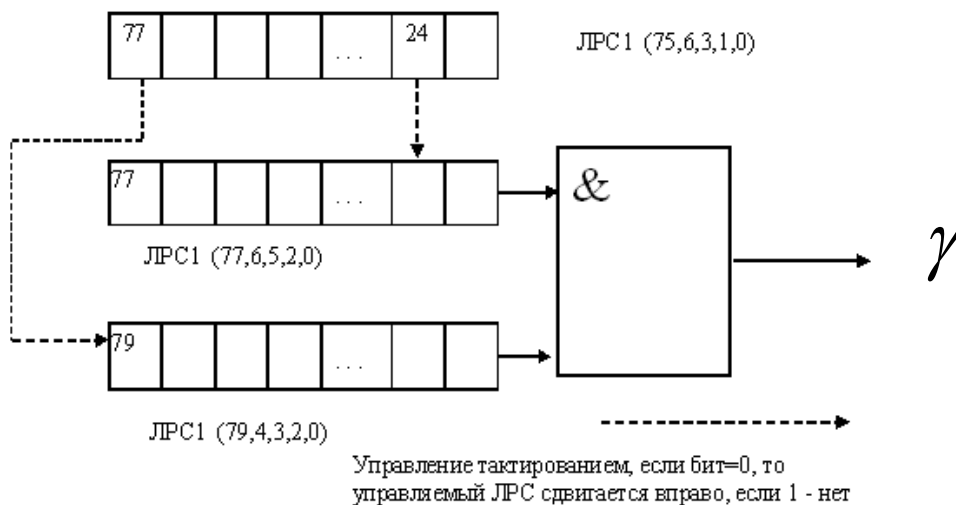
- название и цель работы;
- вариант задания;
- листинг разработанной программы с комментариями;
- результаты работы программы.

Варианты заданий

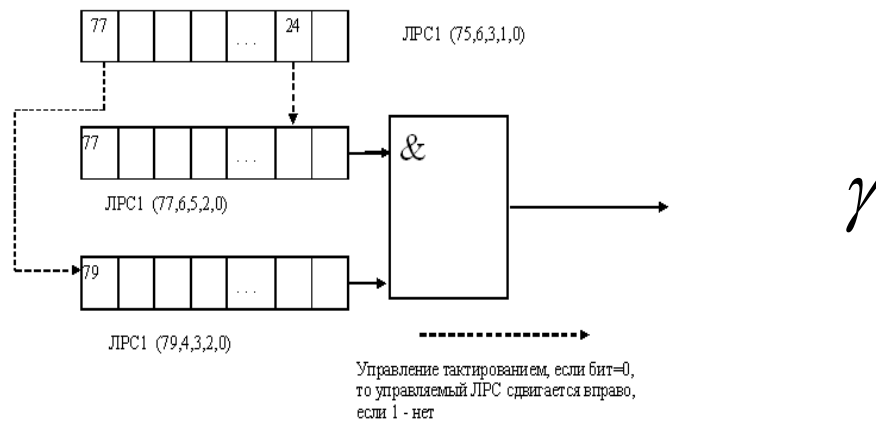
1. Реализовать в программе поточное кодирование текста, вводимого с клавиатуры, с помощью заданной нелинейной схемы, использующей дополнительные ячейки памяти РС.



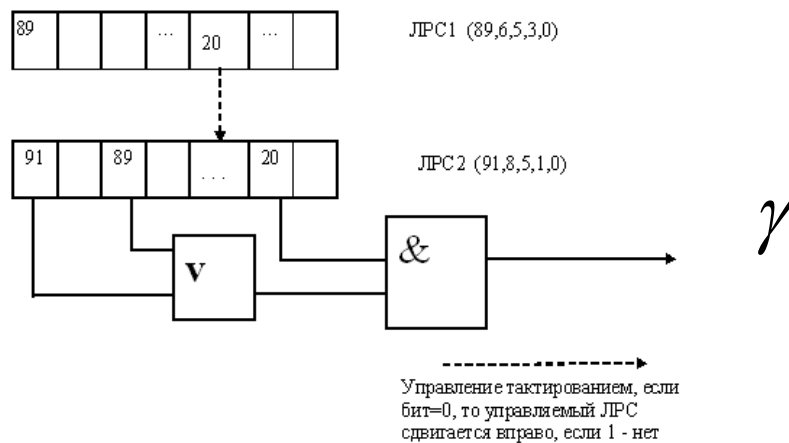
2. Реализовать в программе поточное кодирование текста, вводимого с клавиатуры, с помощью заданной нелинейной схемы РС с управляемым тактированием.



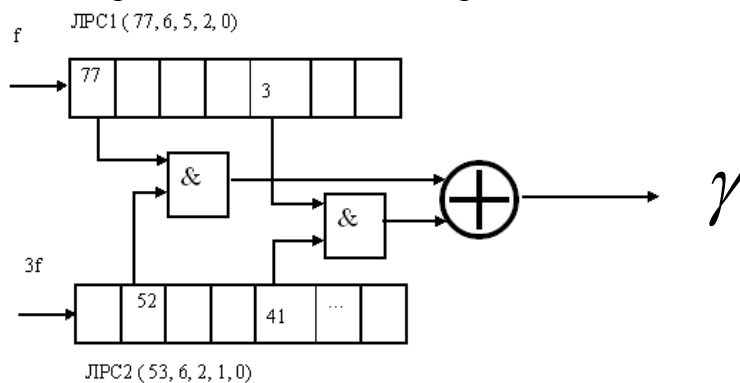
3. Реализовать в программе поточное кодирование текста, вводимого с клавиатуры, с помощью заданной нелинейной схемы РС.



4. Реализовать в программе поточное кодирование текста, вводимого с клавиатуры, с помощью заданной нелинейной схемы РС.

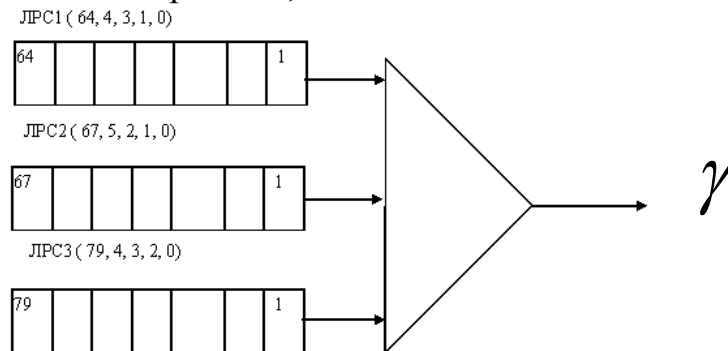


5. Реализовать в программе поточное кодирование текста, вводимого с клавиатуры, с помощью заданной нелинейной схемы, использующей разные частоты тактирования ЛРС.

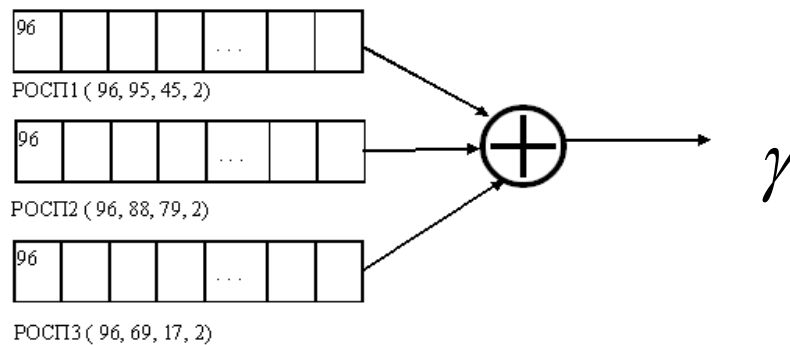


6. Реализовать в программе поточное кодирование текста, вводимого с клавиатуры, с помощью заданной нелинейной схемы,

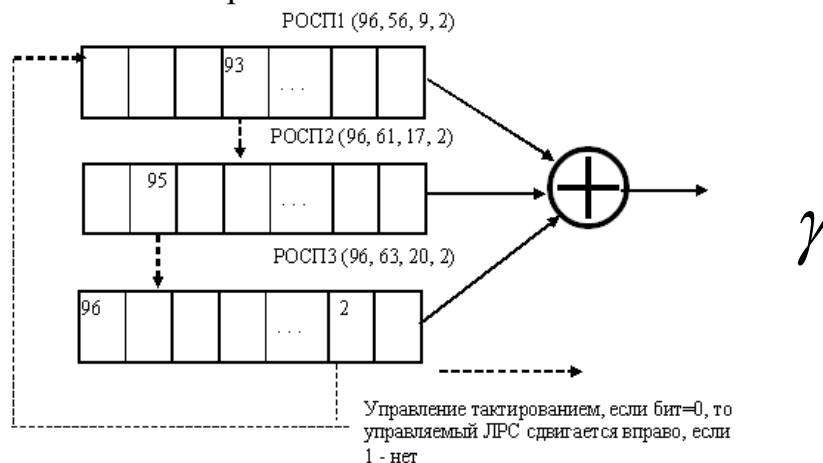
использующей пороговую функцию – если выход двух и более ЛРС 1, то выход гаммы равен 1, иначе – 0.



7. Реализовать в программе поточное кодирование текста, вводимого с клавиатуры, с помощью заданной схемы, объединяющей три регистра с обратной связью по переносу.



8. Реализовать в программе поточное кодирование текста, вводимого с клавиатуры, с помощью заданной схемы с управляемым тактированием на основе 3 РОСП.



9. Реализовать в программе поточное кодирование текста, вводимого с клавиатуры, с помощью алгоритма RC4 с размером блока n=16 бит.

10. Реализовать в программе поточное кодирование текста, вводимого с клавиатуры, с помощью алгоритма WAKE.

Контрольные вопросы

1. Какие методы формирования потока ключей для поточных шифров вам известны?
2. Что такое регистр сдвига с линейной обратной связью?
3. Каков критерий оптимальности структуры регистра сдвига с линейной обратной связью?
4. Для чего регистры сдвига с линейной обратной связью объединяют в нелинейные схемы подключения?
5. Что такое проблемы линейной сложности и корреляционной связи схем, использующих сдвиговые регистры с линейной обратной связью?
6. Объясните принцип работы сдвигового регистра с обратной связью по переносу.
7. Каков критерий оптимальности структуры регистра сдвига с обратной связью по переносу?

Лабораторная работа № 4

Демонстрационная версия криптостойкого блочного алгоритма

Rijndael

Цель работы: ознакомление с принципами шифрования, используемыми в алгоритме симметричного шифрования **AES RIJNDAEL**.

Порядок выполнения работы

1. Ознакомьтесь с теоретическими основами шифрования данных, которые приведены в [1] и [2].
2. Ознакомьтесь со сведениями о программе RijndaelDemo. Запустить программу RijndaelDemo.
3. Изучите на примере обычных текстовых файлов способы шифрования и дешифрования с помощью алгоритма Rijndael. Подробно рассмотреть действие всех цикловых преобразований (ByteSub, ShiftRow, MixColumn, AddRoundKey), как при шифровании, так и дешифровании. Исходный текст для шифрования может быть подготовлен заранее и сохранен в файле *.txt.
4. Сохраните в отчете экранные формы, демонстрирующие процесс шифрования и дешифрования информации.
5. Включите в отчет о лабораторной работе ответы на контрольные вопросы, выбранные в соответствии с номером варианта.
6. Примечание. Для ответов на контрольные вопросы можно воспользоваться п. 1 описания лабораторной работы и сведениями из прилагаемой статьи gost_aes.

Содержание отчета

Отчет по лабораторной работе должен содержать следующие сведения:

- название и цель работы;
- вариант задания;
- листинг программы с комментариями;
- результаты работы программы.

Варианты заданий и контрольные вопросы

24

Номер варианта	Контрольные вопросы
1	2
1,5,7,26	Сравните основные характеристики алгоритмов <i>Rijndael</i> и ГОСТ 28147-89.
2,4,6	Сравните основные характеристики алгоритмов <i>Rijndael</i> и <i>DES</i> .
11,13	Опишите структуру сети Фейстеля.
12,14,16	Приведите обобщенные схемы шифрования данных с помощью алгоритма <i>Rijndael</i> и ГОСТ 28147-89. Дайте их сравнительный анализ.
3,9,18,29	Сравните один раунд шифрования данных с помощью алгоритма <i>Rijndael</i> и ГОСТ 28147-89.
20,22,24	Сравните эквивалентность прямого и обратного преобразований в алгоритмах <i>Rijndael</i> и ГОСТ 28147-89.
10,17,19	Сравните выработку ключевой информации в алгоритмах <i>Rijndael</i> и ГОСТ 28147-89.
21,23,25	Сравните алгоритмы <i>Rijndael</i> и ГОСТ 28147-89 по показателям диффузии.
8, 28,27	Сравните алгоритмы <i>Rijndael</i> и ГОСТ 28147-89 по показателям стойкости.
12,15,30	Сравните алгоритмы <i>Rijndael</i> и ГОСТ 28147-89 по показателям производительности и удобству реализации.

Криптографические системы с открытым ключом

Лабораторная работа № 1

Атака на алгоритм шифрования RSA посредством метода Ферма

Цель работы: изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

Порядок выполнения работы:

- ознакомьтесь с теорией, изложенной в [3]. («Взлом алгоритма RSA при неудачном выборе параметров криптосистемы»);
- получите вариант задания у преподавателя;

- используя разложение модуля на простые числа методом Ферма и полученные исходные данные, определите следующие показатели:
- множители модуля (p и q);
- значение функции Эйлера для данного модуля $\varphi(N)$;
- обратное значение экспоненты по модулю $\varphi(N)$;
- дешифруйте зашифрованный текст, исходный текст должен быть фразой на русском языке;
- результаты и промежуточные вычисления оформите в виде отчета.

Примечание. Для выполнения практического задания рекомендуется использовать программу BCalc.exe.

Пример выполнения лабораторной работы с помощью программы BCalc

Исходные данные: $N = 65815671868057$; $e = 7423489$; $C = 38932868535359$. Найти

1. Вычисляем $n = [\sqrt{N}] + 1$. В поле A помещаем N , в поле $B - 2$; нажимаем кнопку « $D = A^{(1/B)}$ ». В поле D заносится число 8112686, в первую строку таблицы – сообщение «[error]». Это свидетельствует, о том, что N не является квадратом целого числа.

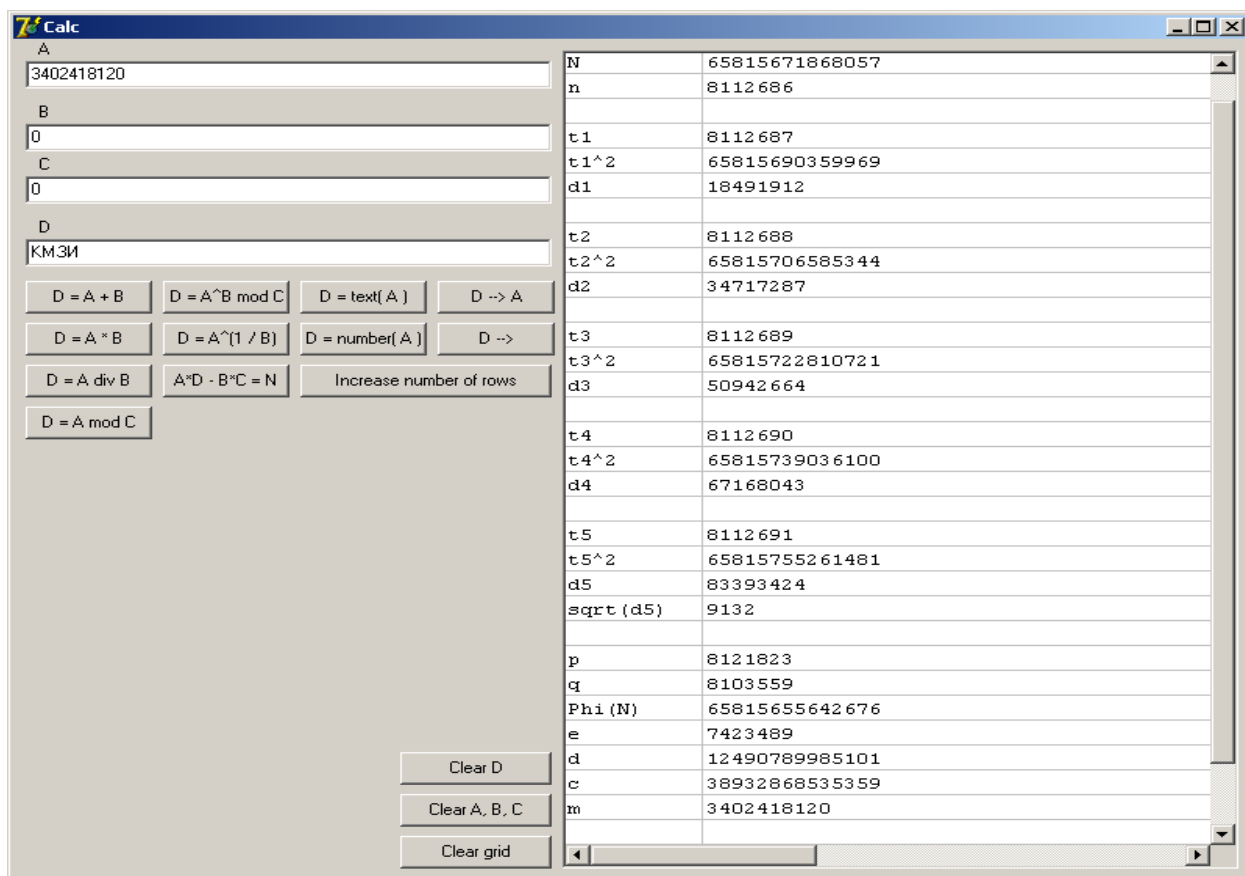
2. $t_1 = n + 1$. Возводим число t_1 в квадрат: $A := 8112687$, $B := 2$, $C := 0$ (возведение в квадрат будет производиться не по правилам модульной арифметики), нажимаем « $D = A^B \bmod C$ » $\Rightarrow D = t_1^2 = 65815690359969$. Вычисляем $w_1 = t_1^2 - N$. Для этого $A := t_1^2$, $B := -N$, затем нажимаем « $D = A + B$ » $\Rightarrow D = w_1 = 18491912$. Проверяем, является ли w_1 квадратом целого числа: $A := w_1$, $B := 2$, нажимаем « $D = A^{(1/B)}$ » \Rightarrow в первой строке таблицы появляется сообщение «[error]», следовательно проделываем п. 2 заново с $t_2 = n + 2$ и так далее, пока не найдем, что некое w_i является квадратом целого числа.

3. При вычислении квадратного корня w_5 первая строка таблицы остается пустой, а $D = \sqrt{w_5} = 9132$, что свидетельствует об успехе факторизации. $t_5 = 8112691$.

4. Вычисляем $p = t_5 + \sqrt{w_5}$; $A := t_5$, $B := \sqrt{w_5}$, нажимаем « $D = A + B$ » $\Rightarrow D = p = 8121823$; $q = t_5 - \sqrt{w_5} = 8103559$. Вычисляем $\Phi(N) = (p - 1)(q - 1)$, $A := 8121822$, $B := 8103558$, нажимаем « $D = A \cdot B$ » $\Rightarrow D = \Phi(N) = 65815655642676$. Вычисляем d , как обратный к e : $A := e$, $B := -1$, $C := \Phi(N)$, нажимаем « $D = A^B \bmod C$ » $\Rightarrow D = d = 12490789985101$.

5. Производим дешифрацию шифрблока C : $A := C$; $B := d$; $C := N$. Нажимаем « $D = A^B \bmod C$ ». В поле D находится исходное сообщение $M = 3402418120$. Переводим M в текстовый вид. Для этого $A := M$, нажимаем « $D = \text{text}(A)$ » $\Rightarrow D = \text{«КМЗИ»}$.

Снимок экрана с окном программы «BCalc» приведен ниже.



Варианты заданий

Вариант	Модуль, N	Экспонента, e	Блок зашифрованного текста, C
1	99595193774911	1908299	75790643190143 36869061035180 38422576553598 68899435645717 16193161920958 98487458352335 34167725433806 96613844267045 26583768908805 73052827576371 94695336463618 69092596694070
2	95841214023781	2005229	49190327214217 84609592142386 90112415897890 58321768145112 18048020096041 46703140105758 5914356051570 1805696039350 28838003818624

			70062757763886 13846553049563 90432970156505
3	93767386321457	2091619	62984326732858 22123186696272 24425203655789 45995309006047 8176196426076 12816278693250 27474201663022 86909026690842 20469575723850 29205116646939 21002901408912 79168478687790
4	89318473363897	2227661	3403106899606 26746900101177 67769260919924 77873792354218 15782947730235 15100267747684 28877721728826 62898555111378 4989704651236 55293402838380 4108112294245 8492269964172
5	87046121832829	2342047	38288567928461 32933111631628 3796990272007 14526017018271 6637183116942 46455894660145 17024410119252 49991104309343 20967672129390 3377231740209 37201047739579 56818318686813
6	85609460573249	2448539	523815866990 26788001211021 34569932939126 85581094055910 23256663175806 62527703621248 7622521689363 32655715523491 81242663069415

			60438288306445 73937478628138 7793112362388
7	84032429242009	2581907	54879925681459 72167008182929 17828219756166 17814399744948 37136636080011 77223434260215 4272415279426 73759271926435 74021335775875 16903113250201 77520052156956 41247980943013
8	81177745546021	2711039	61553353723258 11339642237403 55951185642146 38561524032018 34517298669793 33641624424571 78428225355946 50176820404544 68017840453091 5507834749606 26675763943141 47457759065088
9	78908333904637	2821057	66488995800290 61829195949215 75187156530365 66944513684556 15641889286263 25273508344802 33011686981708 63079735408371 71989137480846 15936556748887 35940951317181 65389528900590
10	77027476849549	2936957	18937689886043 6667195679130 53238895771820 6189192838687 48623327840257 47264919314001 42510070950746 16878504505970 22744978157662 23644842894223

			71614018816334 24651499733229
11	7533841359567	3063167	20373576587572 48282448633797 2859826820449 30302044163645 30736783387104 5008734894376 23296448238734 41172678840173 58656690066465 44574048719827 21962937148701 38826220113907
12	74701165267919	3145553	32035658541536 35242897170964 6268303368709 6877322610982 16329207109754 35007623593376 26715311593240 36220800128563 25019660581036 61639733671958 21186453949445 72477207535811
13	72903890242273	3261683	37429454018574 65632293727338 71955235122455 71474662312159 18537435780920 58372142077460 68330829196451 60882917270796 24142764117328 31238010810556 66143215653810 30769266886306
14	70109121369029	3401467	65044661056628 62698810905915 6384243931214 64581496145197 34821902367398 47317941132118 31834994240307 32916261351098 27399527764660 20797651714466 56226270748693

			51223181240405
15	67510894259489	3543923	1834956116931 7762509478845 22384877417897 36443182878894 61287041306052 17680469174617 14632055288035 23212409940234 45782556562975 7533626343287 14537172455552 60777304839141
16	64806601923671	3676721	20691828453967 58551582619533 52687210920168 20981648665029 19111617348524 54100651527277 13292121860367 56392703591321 14438767538210 42480181826283 48812319440355 15451410455351
17	62781628076903	3804071	25330591599065 45107236866391 8515908980750 18360023777159 60224747641795 24722319023840 4621794604408 11003643584575 42083518378885 62245525096402 41697616662831 32054453631323
18	60902079700513	3914857	31747356280388 54631087879066 42721453914357 12859490321362 47949527200923 39725118829906 37400171509625 34240435626806 20191794760289 16358289451487 35717279691675 60689890535412

19	59046883376179	4044583	32279109612093 17838629182964 4165776716262 13093284635895 20048651313008 54626454832531 12801053743903 54675332003643 4544911979279 31928373564570 798945495513 19569174668782
20	55925060669503	4156793	53145801111837 24757475715890 19729078348176 49091835965654 29986321429979 35162644705488 45317135042859 49645513101014 1804825908594 35789821714579 3713734911002 23648998987066
21	54296750879837	4282063	32264505547820 29767871186846 53860104221061 41263256335998 13036826201487 1768770254540 9330533044207 38163092407394 9296514119883 7805642363730 46249084085075 13177891469510
22	50824793010569	4440901	14852129687156 2828083503727 40199165363197 50374743756265 38804027318759 48809751439118 17692593759762 11950610647201 31150513650241 18538876359272 30210358214233 23631880532900
23	48992988576733	4545733	12530303611339

			47274247086952 20068556933394 41300245344157 27564916776233 45997492729411 11416336760074 17516700753417 10586755223028 5642378694993 17949047899806 13276902592875
24	47050437355283	4674517	30307619697810 38075405389785 37116384337234 20795372941054 22354675528431 20104615399105 403582911849 16733578384925 37765786204941 16059974394842 10942482418438 39745386116422
25	42982346145803	4777621	19787649423728 18211753517576 29287420774392 15153812654780 18356070190939 42856511463744 9446489409913 31515169706630 40480861340273 5995498078936 1615344586866 6467700235586
26	40874866482797	4890013	30098470920348 10084491526640 23441958595352 33281521148728 37973385618526 9343475069587 2406343345685 7678583166238 37712932671543 31339429556436 26029018118292 35429221689605
27	37853809989851	5000881	810492251513 3192611214542

			10318029344126 2220994223088 7937732363223 7917915062052 5784071798565 12491569110482 8519113859496 34533923334624 8671493920268 9656068990180
28	36382368990571	5138117	34729094860720 993016310794 32382972793694 11451559981371 27603779105556 2722565595283 27187050268006 14126480994141 30653849585538 29540033120497 20304283070750 5290885426574
29	33644210466973	5285461	2887763929737 14268468183889 17106478222082 11308338337725 22932870001788 22780920502986 3159009422412 22191880208231 24883589317156 20042326937734 21464252061935 6743660373779
30	30515981241589	5365813	6462676848037 11940196919771 26211958940622 16634847261054 8103271691885 2435085233132 6122398937225 12097045969811 16751413858962 23878019243430 23189713210013 13681118402740

Лабораторная работа № 2

Атака на алгоритм шифрования RSA методом повторного шифрования

Цель работы: изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

Порядок выполнения работы:

- ознакомьтесь с теорией в [3], рассмотренной в подразделе («Атака повторным шифрованием»);
- получите вариант задания у преподавателя;
- по полученным исходным данным, используя метод перешифрования, определите порядок числа e в конечном поле $Z_{\varphi(N)}$;
- используя значение порядка экспоненты, получите исходный текст методом перешифрования;
- результаты и промежуточные вычисления оформите в виде отчета.

Примечание. Для выполнения практического задания рекомендуется использовать программу PS.exe.

Пример выполнения лабораторной работы с помощью программы PS

Исходные данные: $N = 453819149023$; $e = 1011817$; $C = 442511634532$.

1. Определить порядок экспоненты. Для этого необходимо ввести значение модуля в поле N , экспоненты в поле e , в поле Y записывается произвольное число, меньше чем N . После этого нужно нажать кнопку **Запуск повторного шифрования** и дождаться, пока в поле X появится значение, равное корню e степени от числа Y по модулю N , а в поле i – порядок e в конечном поле $Z_{\varphi(N)}$. В данном примере он составляет 435.

2. Дешифровать зашифрованный текст. Для этого нужно в область редактирования поля C поместить блоки зашифрованного текста, разделенные символом конца строки, значение модуля в поле N , экспоненты в поле e и порядка экспоненты в поле i . Затем нажать на кнопку **Дешифрация** и дождаться появления исходного текста в области редактирования M . Ответ – открытый текст – «null».

Варианты заданий

Вариант	Модуль, N	Экспонента, e	Блок зашифрованного текста, C
1	307080138389	358703	150223836156 41077612181 164221721708 163231492773 84606189584 211632968571

			76644428054 67904620890 263054305449 31191567018 224545225463 30878012295 216396046580
2	707096259383	928253	6952874554 579478452421 88828702123 225263521086 340528371521 583666721140 254303812163 584762191247 620918717873 52726307774 172435791721 293646690249 323995569099
3	385181864647	938573	331245775481 282425324609 65377570000 89972965825 264803627317 320989226085 324723654667 294634302620 142237555971 221994269576 209958712589 221718426295 163788492835
4	489740760623	892627	237434928568 89382477865 257542914775 153947910848 219678068406 166466311168 49516725114 55375254449 370796045103 322927050068 196366079994 39243100230 299525662956
5	152206953707	959689	106157029398 26037756325 64970468176

			111381095515 102219112033 10446585653 125818085975 140293474360 118182182667 102323948722 81537011095 534009223 79513867811
6	299547350633	854929	273814931280 42731365375 226290712100 144895466043 54022172482 256403869247 20427366939 109560373874 17926624122 276548101136 138551457160 178721641850 153958773591
7	255886599799	1042193	75872140695 243623122014 66870731769 142602808011 42354989089 119395329034 242619634774 180213272917 166447493863 167768838568 120544075858 77559779546 136453339801
8	290716329017	497729	1135414239 169213008965 175441050863 109545918774 123669279758 149542889269 43068653151 32806195453 285151390718 137668394392 140567677417 176736386447 218957656245

9	144050016983	1163719	90401727778 50205386780 66796441575 1200754589 25390276538 64927766600 89595489304 12806265575 95100428023 7746226795 126261029912 66580024238 118827632497
10	517284804989	1016137	393966099521 489691449904 125845553926 278237347671 101391774540 70812690734 166080101475 356969244744 59015316810 480894389103 454155667817 124365264763 412526965953
11	301916099393	301319	300229084086 103375119523 47856681522 299308768883 259681434827 155394796250 203569645393 81385593446 153370193599 11291771251 297354725266 71677781247 298448677628
12	680953235477	920197	391097155052 640128264104 655783446185 380882921502 243151555158 525608289811 439378081915 674406455075 295448137012 494853048412

			566308391875 623790961908 222667625162
13	915012974539	1001953	763770087861 432343847598 764682728575 206635140312 627210520886 794063631890 309297959146 68118108284 116045398315 912085643674 257483784869 167814127445 55188158350
14	112546779899	280297	70526810403 14149862236 45856385641 70576010398 55035023176 13450029743 87602027501 5373321283 106271591904 105497609146 58279045288 104373761049 16432846070
15	674752561177	395173	419211463126 212906356161 631644741157 73228488037 302781784962 348369666049 269324039584 666490555214 580635922832 30319178550 304297088216 461362299290 408519568281
16	381864434327	1195459	163872954111 20331233144 247841893982 24077680684 186232454225 170708316287 287353419177

			53300545679 235380537126 229388042972 213972178887 351137706462 71827041797
17	509394020393	466357	240117673168 198646030609 299632505275 245910981124 103645806141 129428103430 20356709898 492178278680 233595118807 334625983625 176223275722 244450104851 63497900496
18	1123918263359	1296973	337170174448 110065284116 225074454552 978078749787 1113908641985 396219512028 932134251667 1046744729838 458139532624 319141259386 1098244186318 139438193945 197233306845
19	762930465497	369197	272601390768 146191862405 56417639739 25010208392 569176485965 292815488501 152909580675 634319609453 578700740159 648142948177 39319966771 517127377434 490584971826
20	544136348213	358793	91846629660 119935413056 171909861239 312597665654

			149569107987 217729521757 269500353046 510985189336 131214208695 241687081897 362099358567 467378483313 539916818577
21	836168881111	1031923	83092605748 825802235227 32508735922 407171918452 614975177493 774349835780 323601958615 82169286450 198807945618 594897575157 542729555491 812833939532 694084199661
22	914022837691	517823	133088999278 758078110965 705889026842 98403371042 768948684522 78137927374 383272719045 341665550116 407871370619 382219973835 653544166840 658599075370 825218892763
23	888532740131	508097	251133768996 359801014616 557356431645 75854873865 768478933532 624174758081 306027834198 586384787006 155294489444 358096762086 197284968232 498688500894 467532994504
24	175749265511	562439	148649649353

			106749700084 111279099426 123808752263 135559497150 641323741 146710462903 18875910866 10741502182 84181024769 83326297438 168979058954 74728979200
25	226206740959	931169	90602081758 155748167901 43664963557 119662283421 128548684055 224153458766 195788143843 18231611138 35594188617 74744847247 54882677589 38908769560 166766625254
26	300104708753	983363	143263029236 113515979624 198998498966 232259814103 36155668324 142429090416 112345291625 27921291938 269458157437 298799815265 162143730402 126750403087 51777038634
27	333333164557	953093	5481684542 14785211849 24230838324 156363450797 254864312357 282334378772 101468922110 330970823045 53322569148 330510315592 287013027083

			223374578887 26195032100
28	705703109311	795709	210618901858 461070758554 254341305329 432167203884 537128801619 307179448989 237267800094 276288788567 627186938797 7521018311 638757343218 263719789788 153146378944
29	414634315817	1039187	200343263939 13939901815 329718769183 169659670872 49667978685 11286581382 92461615100 173590557244 62542045222 310782145259 348390168011 308011216304 154928746700
30	81931393421117	1249841	53326375006739 60159105931963 20367806441444 77032482774732 38672218391631 6990304921236 44495129703609 76487744048201 58557027754174 1016517574381 49254811194021 674135756615 65887286918402

Лабораторная работа № 3

Атака на алгоритм шифрования RSA методом бесключевого чтения

Цель работы: изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.

Порядок выполнения работы:

- ознакомьтесь с теорией в [3], в подразделе («Бесключевое чтение»);
- получите вариант задания у преподавателя;
- по полученным данным определите значения r и s при условии, чтобы $e_1 \cdot r - e_2 \cdot s = 1$. Для этого необходимо использовать расширенный алгоритм Евклида;
- используя полученные выше значения r и s , запишите исходный текст;
- результаты и промежуточные вычисления значений для любых трех блоков шифрованного текста оформите в виде отчета.

Примечание. Для выполнения практического задания рекомендуется использовать программу BCalc.exe.

Пример выполнения лабораторной работы с помощью программы «BCalc»

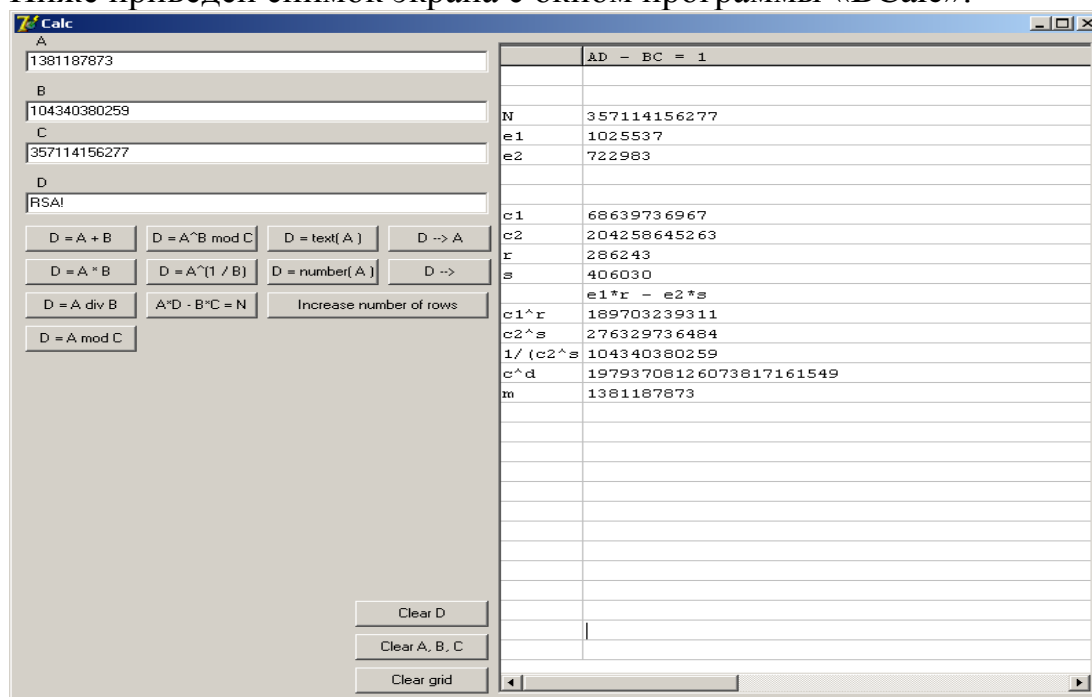
Исходные данные: $N = 357114156277$; $e_1 = 1025537$; $e_2 = 722983$; $C_1 = 68639736967$; $C_2 = 204258645263$.

1. Решаем уравнение $e_1 \cdot r - e_2 \cdot s = \pm 1$. Для этого в поле A помещаем значение e_1 , в поле B – значение e_2 . Нажимаем кнопку « $A \cdot D - B \cdot C = N$ », затем – кнопку $C = s = 406030$; $D = r = 286243$.

2. Производим дешифрацию: c_1 возводим в степень r , а c_2 – в степень $-s$ по модулю N , тогда $c_1^r = 189703239311$, $c_2^{-s} = 104340380259$.

После этого результаты перемножаем и получаем, что $m^{(e_1 \cdot r - e_2 \cdot s)} = 19793708126073817161549$. Далее берем модуль от полученного значения: $(m^{(e_1 \cdot r - e_2 \cdot s)} \bmod N) = 1381187873$ и преобразуем в текст «RSA!».

Ниже приведен снимок экрана с окном программы «BCalc».



Варианты заданий

Вариант	Модуль, N	Экспоненты		Блок зашифрованного текста	
		e_1	e_2	C_1	C_2
1	420882327013	1372369	961447	373413138774 142492164990 181970101695 71400620884 83588687662 111752930680 154836140461 191336073909 186412386345 303121580659 167437105893 279265271451	105783140624 384545054504 91022339898 266856044417 106548952403 160772152396 128969469496 242028887287 256618243529 47586486979 306022591934 419219258598
2	302296233419	1365787	763067	4735234112 222492941603 91642935786 258679721851 127352436654 270884254827 278389245811 229277148124 143477017416 56472903944 229332603068 60190953676	131720982156 50767819341 146687208678 65444189922 275196580101 21582029531 14338137631 4177778322 75624657756 274012339373 159018739186 49970035122
3	445632735571	1120289	559633	348555354398 351363944134 96907337112 141119651255 317600466893 84967944527 340088880266 311235549494 41838603784 333172824695 89494655477 3256803669	366337925832 29318249989 120058862823 428190500861 322426909958 286841513079 150392378882 441874945028 297137742269 304115257300 123106598046 110955623263
4	535598392051	455341	396971	444982997352 277831853272 133187882628 331361392426 273206302188 470299046774 168157171491 258737286129 312335302650	358696089912 360292494113 91390259562 534590606880 193203217609 166702058071 68207231399 487524624411 325841328769

				489235057221 427689116872 418723605534 135022585485	533726724224 369967614519 247201359991 478832067683
5	572953270159	337903	301933	342095517391 19455909955 221503536026 316042040322 311339725976 339044089754 359623172126 138544673544 148226083413 3486028632 23290754913 425720995382	32476529608 452342848743 506694128118 262070340689 206245109461 116518622136 147952236274 457665805346 27001690429 396682057113 239803556225 519526641494
6	622722921281	924383	648391	416413766755 461616049371 495579558550 119296856822 288338597320 189325419759 179661796706 26462194558 543527404419 511749608651 131463006437 116692606609	363561291438 349913226640 410678799422 49400187802 264465166065 617558055726 378919757053 550605507870 341759776368 125364611909 288965980272 434023259043
7	516439217617	1206433	1141277	400408320444 241545246801 282223079755 490328978748 350509811006 142356755075 109547314116 414823859933 330990395685 377471732609 44017319588 499241372980 171071879560	374984721363 438491303024 498951362977 218681974856 365827206348 175049781656 359111505460 297734746741 96963152197 362138584797 102758207364 37817394150 120430068125
8	392117053283	744721	1297633	188779427301 142624237358 222856552604 64779987640 184552630472 357891671735 159800573947 320365191568	330155414629 183843269790 113231290101 381735803560 115846890704 117837936469 188064551177 241636957582

				53704108470 29809614757 236651896578 5185872557 374026260505	253908524873 219235963059 333424804843 278400905892 254102728294
9	319418480417	602087	523639	52405618926 216147098445 216743861265 66972942908 191820297330 190353918873 110095200781 90183965366 296876615222 154988611456 166443759664 9906682687	82810335170 187684665216 48173641649 96024498047 247351492178 97241452868 255901558905 27364319220 227156630511 66990230889 183816391944 104719299259
10	308044228439	976013	667829	41142528888 168186504906 136093203364 242964689121 35088399935 235615713434 255931630761 243205294010 282148730043 167665545881 236133809262 248077895012	188066920245 300946560686 297065980706 52463722858 288700402082 74622590470 304422560213 89572425507 192865433148 279658192310 97431270440 276505744422
11	287726313019	632699	418997	214922055033 35721658373 111494982431 18199110430 42343010608 252248400710 63424999529 119923175349 154343666939 161871538168 66104514148 20594515433 120762948296	236363326198 60659772128 89634195001 159962549494 38784417281 280743496547 132419834073 260926903227 246447810193 110060458786 96973974426 175463381167 178887056429
12	385751370271	365797	1109663	58541562205 167003685579 381877628242 256218527098 164244249864 6588741823 180308234660	78032032470 13064174635 326727914830 364066420370 177576861402 65863828523 111437045566

				174572441677 259951955034 378589342820 319378579620 21405495597 226860843155	124743274954 119577259869 85769669875 4688914942 261002397567 341722428571
13	518587807081	293177	1209781	373852443734 447989059513 140756140384 207791711792 252160015422 151272799305 431450717984 252882800366 112417596471 301753741810 480461056512 334158277030 368394150653	22286870422 343015689591 281801228231 360270382562 264253306719 128520421967 399665129411 448878989738 70913527757 295285211952 247990966487 202711954425 201121363025
14	573308195401	973169	550351	327707922480 455697659443 469317095774 41173012855 95114431187 183548202066 114278917224 111319924653 302320646938 497834611165 207393954597 469317095774 184588110993	484439401392 92203619034 199299165882 100840467257 42877265767 537319004931 212469277565 335238563578 215934710265 248375790884 8143413999 199299165882 484325656679
15	634875396959	797611	375841	215938301159 156476855390 629025629999 390282732416 486255942680 301447617826 611079544000 9815582940 238155160282 89572033554 259610717355 561079697420 68884371224	592194596499 618920283747 481110939902 118468312259 152271753836 245706953152 357574573601 517943651115 449088004034 549269593969 274641120696 170397276793 150603791351
16	512453104601	1365347	972793	17680290297 359514971944 395933838767 135375405636	410084071984 150398051936 489149759410 11043062086

				424188955183 480774525813 176693333558 366722473439 257271491888 437238044102 280697746591 192092245943 180087210668	452072614483 94954712588 373871024394 194623183329 478231887994 452346492359 145030784098 310653569484 280971453825
17	549840164113	830309	1122659	421894113021 70151618285 256033134230 230572827320 345706195727 379296943648 131864337239 345346802879 460224575827 28746971542 176535748663 395695787161	460364462002 377869829708 315408321663 403500544217 90051720740 398226212020 357731842992 394252754984 318030259077 317217533534 42352806819 277427982170
18	521194405273	293767	492511	70696562 136043022917 65407415375 164404262967 445647345197 118953770797 512196733213 103009198361 317437263597 284559552852 490098245083 149823933745 224803955806	139896254161 268972783372 281244321042 190886094 183760973977 127631527830 29296947894 342466717237 76798964679 346421581772 345796314978 281195436813 359213893561
19	500984306287	470149	267797	274230487503 6821302647 172152295595 454539302130 462305524774 73589652382 274794725040 295185494003 159348742119 62021560582 311827395163 159638616315	176943898057 272954693703 141643708385 238296127866 270971764501 389314459147 476866404163 295344931481 288885538254 144738759088 52793710114 416204845784
20	502110569407	693661	366287	451590415251 110439571420 183752091528	489035727840 352254618578 112984103119

				274872936616 28541011195 450835617776 260759622383 342128341762 158761845107 190701543235 336633436793 107036107438 143086295492	324252397833 258279989467 309371933868 309370695834 275718202556 484547254614 319090281932 321505940571 499673648361 445389404030
21	635476116169	866707	1123211	164724618825 386399947495 569519600328 335674131307 591926181226 331711492017 222632530911 159285067102 529695664488 462703958023 508391137110 573759000564 48989336806	119849004283 156284059617 399964659582 411242163372 473998672968 449146422851 178846180173 431421957979 209987811333 627608476514 23204756436 43305372061 542459119849
22	606089625293	524123	1109309	496663520230 573686340098 317277380080 311062242263 87966670626 156120202050 517816376872 255107405391 70642465288 390229374493 333422604916 2671384922 509131255766	196561923290 102658895412 577585560553 44037449636 508496748333 278687486043 261550581766 487843663934 314450235982 345028986924 104569551730 486557652833 337080661180
23	303958823183	1173551	1366693	300865234944 280167078723 44778324729 15647443106 72500796041 127042219796 220297476381 159193146152 281783946206 83397684706 218587175059 32628200905 87293077359	158205869566 47430389231 235868270647 60933642983 230961885063 189840956692 155026770625 118061171422 64695094087 90093203015 140628953794 156685525752 96578125026

24	216044621671	493001	693169	204707607052 131209885175 74127570208 167559112602 114202832764 175086144102 173536223165 123432367535 82425793128 185507595143 95061918272 193636415087 162487637030	161085576818 166651266503 210362428729 29681376125 51404224010 85147589057 53004594773 4926673942 28134852744 16056810738 57750263032 146784016398 143689492474
25	193576240729	376133	633317	159391395691 157577675381 191080992560 149368918681 53984801508 4424043610 58203874858 76432058336 16217372577 149007313066 63447430442 64914562999 127848484896	187917061998 100356696331 115395060871 22072994636 10119558157 166188791942 81150163516 112715855314 19232790590 106250648527 21826060759 12414159731 192871647135
26	199463062753	419513	830477	177528135337 131197957980 181321285074 96738779356 127632416974 161779284378 148599198368 2033602084 141914496373 105405878640 120038779975 7139491789	63508097139 142467940607 131649552179 182684157712 22912524157 94825501208 189716623763 86236434624 94875774697 120252092430 26215384541 53782670605
27	588649943243	829883	1365563	280515585129 474432358443 550494122120 286014860208 177909397442 66300460308 528884282560 399515563309 304891197599 119078987025 209691758955	565691730736 150449148254 518339002836 225616510542 385610089653 374937066213 115466710052 142918798684 522983594973 48256241870 459229046518

				462036206743 586085056988	179338322451 224548199183
28	731873369393	492413	667421	47341507804 127997685870 257646548539 354472751726 587866819301 488667442604 462576579278 538441126972 558240817424 150554102888 253275371077 417636957585 568703073461	74847904635 278470286823 448348870301 607786930695 529369369754 75925175772 29907063957 10458852803 90276241841 730446811079 467685526579 583892394223 353477871749
29	1176879950087	550169	376237	236505725833 12096288569 1062670335800 541231133081 529745761698 79574674510 518908160088 195753762481 284194617926 861518052504 844805726716 575330762793 319168661888 377123370130	169179266140 617962027334 332483986069 1065692323879 420409290920 733896529297 201622748685 457529162746 1037225648947 732504268577 1172056967964 1002467039854 850197148213 279510203667
30	1254157128997	975427	1209269	1098122654723 224532500446 195052151737 340669256856 1019975678508 210896047315 749213378601 949523491515 154878238856 1101522983540 511950016486	435736453734 873855208934 68049065095 513397077403 1191564999894 524725711866 662476316059 229085787378 943515500203 942246429245 905815635635

Лабораторная работа № 4

Атака на алгоритм шифрования RSA,

основанная на Китайской теореме об остатках

Цель работы: изучить атаку на алгоритм шифрования RSA посредством Китайской теоремы об остатках.

Порядок выполнения работы:

– ознакомьтесь с теорией в [3], в подразделе («Атака на основе Китайской теоремы об остатках»);

- получите вариант задания у преподавателя. Экспонента для всех вариантов $e = 3$;
- используя Китайскую теорему об остатках, получите исходный текст;
- результаты и промежуточные вычисления значений для любых трех блоков шифрованного текста оформите в виде отчета.

Примечание. Для выполнения практического задания рекомендуется использовать программу BCalc.exe.

Пример выполнения лабораторной работы с помощью программы «BCalc»

Исходные данные: $N_1 = 363542076673$; $N_2 = 728740902979$; $N_3 = 522993716719$; $C_1 = 246562834516$; $C_2 = 291375746601$; $C_3 = 222724269731$.

Последовательно вычисляем следующие значения:

$$M_0 = N_1 \cdot N_2 \cdot N_3 = 138555669564008119302694433926047373;$$

$$m_1 = N_2 \cdot N_3 = 381126913374147389205901;$$

$$m_2 = N_1 \cdot N_3 = 190130221862955939995887;$$

$$m_3 = N_1 \cdot N_2 = 264927981225542872108867;$$

$$n_1 = m_1^{(-1)} \bmod N_1 = 287993142707;$$

$$n_2 = m_2^{(-1)} \bmod N_2 = 106614970676;$$

$$n_3 = m_3^{(-1)} \bmod N_3 = 32171022265;$$

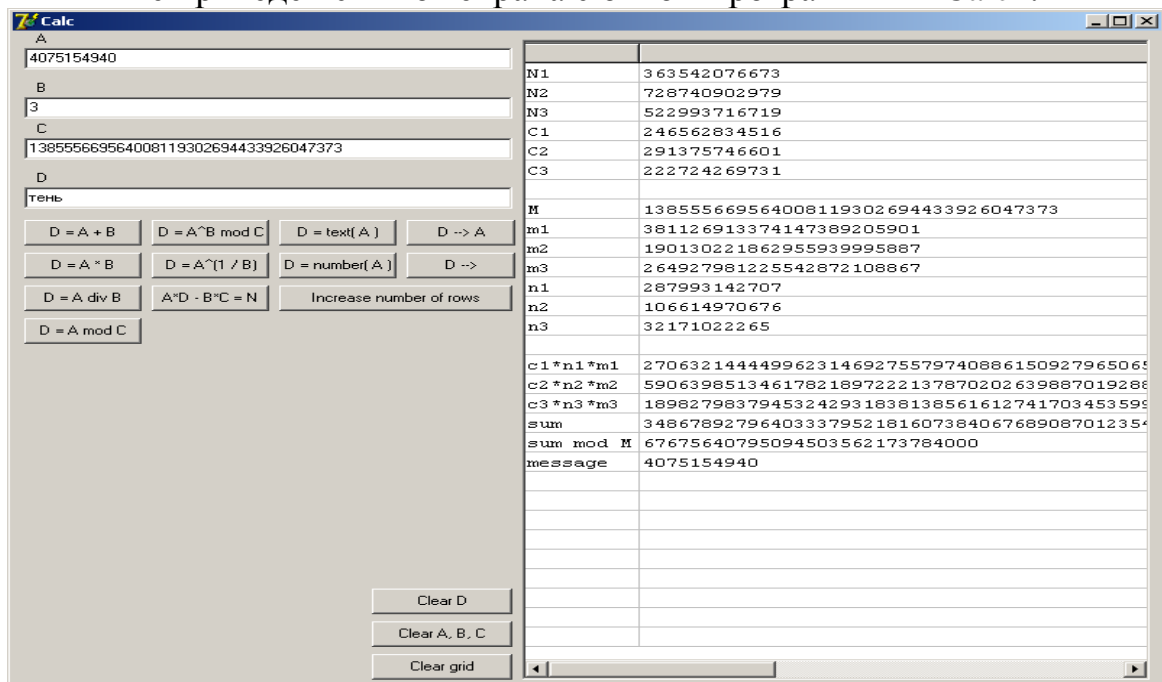
$$S = c_1 \cdot n_1 \cdot m_1 + c_2 \cdot n_2 \cdot m_2 + c_3 \cdot n_3 \cdot m_3 = 34867892796403337952181607384067689087012354329;$$

$$S \bmod M_0 = 67675640795094503562173784000;$$

$$M = (S \bmod M_0)^{(1/e)} = 4075154940;$$

$\text{text}(M) = \text{«тень»}.$

Ниже приведен снимок экрана с окном программы «BCalc».



Варианты заданий

Вариант	Модуль			Блок зашифрованного текста		
	N_1	N_2	N_3	C_1	C_2	C_3
1	359690807803	361062169537	363514381513	177412278620 8631904062 60910035474 297496979396 44306701511 223949114264 95163574676 126740768642 306466049596 82343556476 97754924718 242675823829	227891126441 175684889961 108275398403 50799922679 50861774819 120598551775 214220319631 193858968963 243446962166 168236630688 260389624172 86845867002	230974691188 345734293737 118726556071 220369632983 69236028918 121704957571 269179568504 201685371953 75708873566 101720600746 131962627319 44909629158
2	368166998833	368656533313	371205502531	100018221941 357476497416 360704892674 258968522463 363378787391 38938998120 165805097876 328038699497 297851010158 184316347833 202277180039 260169809092 136359418113	219670103959 299234661384 321665231322 303452309552 197707480483 271136973244 31151628083 195899793924 230643014304 323745610236 125326155250 4695289469 154882534227	258489005115 193486305912 317085850998 228076833982 118470145682 302313432794 214437258395 132123789026 96889642413 300010020637 249393170795 187672572758 93192923225
3	380077454101	380903460337	383306345689	120321295984 116941070964 156315192664 260149644765 357688967002 165841867143 349826484990 337993834720 117681826230 36279369135 124613350713 106958422772	261990433834 232071459327 305414687540 348455852917 206680974925 327578130329 5548686870 295985428633 157420509616 256913681356 271869775627 310864218021	322305651846 286065905390 188633713225 131649116365 253206684415 46677871611 65268441973 317133281785 52226297600 255637668770 201873507225 260192105953
4	389091381643	391569053221	393864798289	23283117034 199910300344 122379231308 129836433029 266167362913 322794903721 164367877138 317459368677 210705957227 38878534867 199295177267 116980227366	81950696329 310054893565 132301878314 52795246284 276197768422 265696804182 238369333190 66855113681 316766995365 321182915473 118193576787 190068391425	57844537762 368640254231 220965124671 260183659429 299904567942 286935730637 266053541214 146542714390 79442443012 28368938795 30970811879 72570776324
5	397066122499	397797027109	400288163101	257953403766 177168684125 98569851945 111013170885 126870693789	128730750274 391893911248 323200994518 152862355610 23614632228	382653707323 186385219382 394103230832 16445037923 382954747667

				356996906573 369112783220 118662185076 192227498736 13981739973 77574341290 98562917188 14769259640	96365786831 207779539976 70218040709 317562220506 111815966551 1949429944 8329351035 147453838103	387456992444 258166753697 375871570884 342932316985 104729956068 46092487953 69550838402 289762815713
6	408685041841	409542365311	411702675541	161938982030 93539768747 198680625546 324985467275 364301388858 121946924018 130171610724 264709094112 198127513690 98490234931 86416406414 347341863803 261057850418	227240021793 240397026641 319693734726 143364329762 267584092696 104392885896 60224870888 54379930123 281164821607 51747910478 152858842656 198634569843 304306303763	124238176183 56013695777 98169308648 320302328458 257566073714 180123701720 231998512656 220441010255 105926142958 104088206001 312601660772 358423325011 229574485891
7	420250053679	420998138947	422793377077	17599664694 221343847340 181796040962 210108814452 124320289825 323995715057 260285700707 72474978285 226746757036 369084323018 133261286623 336107911000 303767221006	388099839383 141363764478 253757042128 162556515860 289849639847 126598663712 171600933709 80576580207 347679322161 408725538627 244886980553 171682264557 366784660912	84003082499 245906362572 398398702796 157559004814 157418944324 411242039391 270378838199 182942084181 33847193530 149137845569 382620866773 120769412025 272019119100
8	431972773933	432558060211	434276528083	43268974598 302331913599 47134049761 126642563008 165827503054 232086597542 31465887151 30373336865 284998624093 89084365158 322533676789 383736009455 108545189851	330701159000 104807592171 45038416117 81063981859 427734601871 27505991527 81910363197 190166502949 116404011104 249933949107 90486698466 206265723002 276536042468	269237460393 165034165638 207280715083 151936477226 7495879547 141105308724 316939568874 360819196331 46940627813 137301580237 168518778628 113124777920 282998095133
9	441716293693	442258294987	444399387571	324500796659 324547036186 367901833181 38558700097 401956144715 260421328704 356041474179 113539876955 304515179769 302662240842 282367185538 432213853716	364411844182 137247785047 389030356498 293766643714 259139396276 429702138150 17968702271 84037113464 91988591941 425057692992 391906969363 244207991747	57065247639 130359065508 391859459727 128196485994 412050631244 367300386309 83703862830 218100297714 10243576841 232358719915 412546535924 398872645339

10	449094675559	449774960461	451557288811	445451352210 249439394113 387029823615 132042218903 73614801093 101481466259 448458747498 443385035969 75012412264 19096037043 259197438248 220559106494	424531890296 430487757843 273579896124 163172411830 299409036513 34387871280 190507227268 108323290415 332577990284 213248626661 78257808298 238075298353	118710004991 307218752883 366564784860 182819846943 86662518238 405369976705 111221455773 368248616971 227865580737 38736323891 137144185691 231896396336
11	457829717113	461639371789	4638114511073	118519640042 325725597818 449577094588 225738390357 390837010969 417997930307 186946730799 307353836168 331923022405 439103095463 415559987555 407104561771	68925059719 320794723471 106708759661 267503416207 176633626568 370938941185 256010935139 375173961262 50942041502 13373860798 369523972407 268680126161	360911630335 49077546247 367587011852 205773073385 166430526462 166130351420 240614091730 1307748376 289507057580 309981198851 123903944003 113555743553
12	473302960111	476210148031	478258728547	384927940677 473049749478 98141220439 47772742554 85402795076 49762300554 243238759870 132174590679 394107604075 292566652796 394413369679 176379334217 425745574767 279970734890	47337377053 15502694428 81559584886 360290532716 378412185459 471133458035 276394936545 2116712669 37111299200 387986386867 97786707059 256442600412 455327955288 119517607360	342954751710 440889851539 67503329756 462595462377 84092175909 57911552136 60433527302 25311956275 370327609107 296462225245 241699085506 465708091819 454345671530 210180151910
13	483603920323	484627023409	486046777033	45854580612 105237269523 169259415669 93616181002 111788215636 19646301574 344814513220 284120677804 135039654745 8393533606 277869220393 95747282494 31789892340	274960963762 445004609734 314321127441 121008447611 77289255193 185428067959 268033072619 483476916533 378663280169 145768361237 164058939780 427513468440 16789037076	245417628800 58500957429 337297880630 192371047425 368079140170 444426125103 485088147460 384977923665 52336096116 217360431271 261094805307 77329919173 280539607542
14	494980336813	495019868347	496510218943	405186643929 264588538265 58896941920 424470122024 445830333875 98276685134 210238595626 176058872641	298462743436 26894204289 266800308083 469634672912 423565503334 418775305332 112405305103 302129659337	372083067441 354383414943 31782553847 213067042090 22742161466 313919341914 71514328634 117790204322

				185715938214 418034348683 52552730024 481876348312 438600466605	323850375295 438598232992 10359943018 298111389169 277384894755	268549130622 409153352258 316714994539 270152277750 128472385009
15	503847739471	505210110529	506974617943	65555047695 224704827698 426614994776 482499765759 499927141525 251539329355 288065643935 500487899533 284158354428 179929130009 4059729507 337999368066	324422804544 374009722121 291369610887 103658691090 355087189555 403634830552 45811542091 342405362400 397470779417 143094497045 16866311017 162845742211	435445028187 207888333371 344446367064 372373145295 26158114757 389306763320 15362084660 342395172034 275443080668 219501574324 343966567526 291026935191
16	519445678909	522088422619	523328119219	302279248041 398777422648 382393465830 109346520792 393648988334 83456507369 503695835656 409770589873 483819180150 358939341533 402486907104 347176414967 1633679742	48522238217 116578598684 98210011370 452947538650 113090002659 130683028799 170075383039 19947030841 458406287083 178964953872 500143943025 189689940709 218613469572	129856570412 82270781294 140695444887 510689827054 42634086860 516267119547 5616396143 8388941434 73724586316 290433741122 102266925300 75736288391 406132000561
17	530262062431	533023659991	534655902139	281386842307 121824522874 245939933284 25488678869 245966715725 346164781438 240458184136 477792982000 50321051371 249631869316 346825618977 352450998028	5670875437 330566529390 465969872193 104239877954 421060036048 26548660136 226283588677 232398586638 141813896655 455313322872 64540250896 175680952596	380269517653 366125418676 400608227248 119236616785 40916016109 6459310768 111454112735 191143773891 428929030217 441962444995 334966880931 380319156170
18	542029523461	545442955261	543651655507	252761993375 439317043104 524563666624 200316247013 168730893537 276462662401 95027181355 153947838824 517609475112 21916921129 186570691221 188654245468	175866403284 297457023908 352677317646 525837137252 500452725795 255875720416 484409681814 36312121014 208360918386 288089579742 492797454334 91193680807	432443719708 291474822430 142735272242 317684793012 216551100123 30474056356 501398385288 405101779653 371861659744 467319917841 209273129747 270602387237
19	553399203289	555525439597	556783358239	532587529932 466776013367 194393214430 551419753294 235808018295	453172264962 295084884945 184687156359 110229199835 452343899082	283795978048 548212520352 50623875598 45628043554 374654069771

				521345765147 62408122881 238014267850 282320724474 421626850723 477001857725 59354292288	61700963597 371846842 184524760412 349901424433 66575580602 38470059268 27434041612	454067424044 140771995786 230698987467 416727167751 87650410693 75414175302 305387967882
20	564051718543	567177464083	568582697167	178430347017 275798270566 150441557212 35319995468 214899391564 454509168990 241622156972 47081057682 532012996953 114671548487 272811533565	464060851187 466784394057 113750938542 50225874889 135816601540 383147938913 445379546704 20609631777 530473256199 291868875010 327407870868	112360892551 48950009370 204834012880 472985274437 150470587109 437368878774 348445464666 120707881073 424353814205 495774818876 460590967231
21	570206339323	572010531679	573673162471	400967861722 402921963995 345366187498 170749944344 398474550143 14128843304 525338681306 553357177665 554714202377 378737847392 241207247252 330231009566	400511331925 359110439723 156672928720 81237697207 446268495117 567101402400 380678770261 405322363448 250349383856 480141604318 201068876886 160562856485	365230039044 503139848290 452112473725 98832137945 16750539498 496867432761 98372266130 349596187748 172522293935 161623878001 405142270947 404286756199
22	582980801989	585089367091	586408807447	428799001102 417746620458 233652090970 425829696584 132807280253 540064099057 191642450251 364237792802 294540030550 287338190886 8030576378 562848664519	330278110381 413803169370 399528613141 431344022162 133251402314 579394141601 339286468279 235332969532 1036448642 400656499573 47204841232 249621210713	426468615928 348743875265 261688856582 29957256669 108448874326 23970225383 410917339855 179638698652 282723305676 115801357719 575898855271 528022904569
23	588465234361	586195041433	587299922977	179564892807 489396036392 176575769058 269255594799 422117999595 257369618664 539258064402 177014956905 234449256532 387357205774 183843097094 189558056464	376452630248 569864359142 124688754894 562457224201 22357940168 151586582904 533949898858 116088884375 221471039114 16723092454 343577678223 313846942324	369376837096 167105576017 449990310238 417101045217 404468253839 1603305513 478144160973 212789604411 559954258624 55850508600 85339397069 409000193866
24	590059443367	586035939793	582032534407	534935192069 586334468916 575821575470 158445010924 168022188272	70956316615 196061328294 472946437612 167175113770 213280914294	547351293988 558349441596 209735294323 257527905634 328543700761

				419451618702 403150327598 462915818163 156960926738 423280293357 308065052008	97582680057 87487791156 319786583031 526032348303 561873181810 93452497746	241383661927 318686253990 391540759391 124252499803 400043751247 36326931192
25	593974289329	590987500549	585323335717	461743067035 16510154740 541409292183 147537040251 121241807149 383535805471 420328432686 360735839890 426786420629 268507362618 381406130147 369378326912	429395271160 404839447718 431790388728 84465928224 179431496912 250884484533 367066937735 493669050691 588637988770 235309880383 79134719899 469747448675	293399822655 408678947374 461462830734 469093286418 229214387811 405621273396 566681986508 381039554115 30236954381 124256080362 424813292522 425803797156
26	589912731103	586562277157	585692399101	480322890668 244470713436 462556788069 362053532314 129240753531 544548971962 471246885335 471262437778 271836962090 394188269580 178451939299	197569306719 256707875408 318007508695 214091275189 161567294188 87540207148 401376536208 21963401602 283235880013 180909701662 310291949010	62477508978 13427830322 123762397027 398319090007 260268164234 400914805152 112841539554 295019543024 63931832229 41567356849 260659808675
27	588420697063	587923144219	588187913011	549837201524 41062678977 558361700271 340524813262 380989701140 72777555501 148516910596 239893043138 550275162587 504639682332 286887201361 109402692159	549767170235 417891652669 18105731747 561561302352 24647793868 459446623668 97023224221 315504133409 175823987146 98357398109 554098076849 2182860074	431364287035 324545189457 251931822912 72129334869 312886718193 268813577112 455339743965 91344488466 67230102308 491296963100 514352457528 80958415820
28	588740645851	584129775637	585272485753	471258791682 512980753348 322484372265 538756637439 317805186675 366951662937 587477142741 68752542454 430997342376 161403026083 50500565847 79917839116	239747618261 468272716420 275958595006 87603018262 331796452131 345512142914 565661549787 319582444655 403978789269 303825337329 452342997389 267966157661	309319918217 185898586915 308249502751 44445413863 449569591513 11827383253 481618003611 226750819584 92751686853 138208291614 78550840689 423076706001
29	582270860077	583571056801	588041120767	301957293366 422372499160 367264077803 200553983048 552090919991 511311819647	380571398658 274564613819 427604843641 201608075041 170827048149 38704990415	458070084011 321585917344 535492729100 366740626240 479766734947 114744478843

				198014108536 60996803849 51278851473 142223911954 7655292102 163043538613	111915962261 397434320138 372982884858 373432544252 318605249871 276204030043	580651081116 352640075141 121134933335 16649676893 327976264894 99216599320
30	588858863227	593022249661	586952985613	83775950282 499684444618 249072759951 493679699487 441751231546 223784905416 105330855230 208113933189 541948134894 23436365527 494488176283 316805307951	71012941259 123921632644 529814173563 561882221400 217161522052 214335556154 513051401804 330790125104 409144828637 182758754527 197544530536 14524587796	262947010943 51615754782 240863300083 377803962605 331127107982 27311727587 402318079295 41197363802 564624489377 349281398612 569063475434 300796590703

Лабораторная работа № 5

Шифрование открытого текста на основе эллиптических кривых

Цель работы: зашифровать открытый текст, используя алфавит, приведенный в [4], в подразделе «Задачи к лабораторным работам по криптографии на эллиптических кривых (используется кривая $E_{751}(-1,1)$ – и генерирующая точка $G = (0, 1)$)».

Порядок выполнения работы:

– ознакомьтесь с теорией в учебном пособии «Криптография», а также в учебно-методическом пособии к выполнению лабораторного практикума по дисциплине «Криптография»;

– получите вариант задания у преподавателя;

– зашифруйте открытый текст;

– результаты и промежуточные вычисления оформить в виде отчета.

Алфавит представляет собой множество символов языка открытых текстов и соответствующих им текстов эллиптической кривой над конечным полем.

Для заданий лабораторной работы выбрана кривая $E_{751}(-1,1)$, т.е. $y^2 = x^3 - x + 1 \pmod{751}$. Предлагается следующий (один из возможных) алфавит, приведенный в таблице.

Таблица. Алфавит точек эллиптической кривой для выполнения лабораторных работ

№	символ	точка	35	В	(67, 84)	70	е	(99, 456)	105	Й	(198, 527)
1	пробел	(33, 355)	36	С	(67, 667)	71	f	(100, 364)	106	К	(200, 30)
2	!	(33, 396)	37	D	(69, 241)	72	g	(100, 387)	107	Л	(200, 721)
3	"	(34, 74)	38	E	(69, 510)	73	h	(102, 267)	108	М	(203, 324)
4	#	(34, 677)	39	F	(70, 195)	74	i	(102, 484)	109	Н	(203, 427)
5	\$	(36, 87)	40	G	(70, 556)	75	j	(105, 369)	110	О	(205, 372)

6	%	(36, 664)	41	H	(72, 254)	76	k	(105,382)	111	Π	(205, 379)
7	&	(39, 171)	42	I	(72, 497)	77	l	(106, 24)	112	P	(206, 106)
8	'	(39, 580)	43	J	(73, 72)	78	m	(106, 727)	113	C	(206, 645)
9	((43, 224)	44	K	(73, 679)	79	n	(108, 247)	114	T	(209, 82)
10)	(43, 527)	45	L	(74, 170)	80	o	(108, 504)	115	Y	(209, 669)
11	*	(44, 366)	46	M	(74, 581)	81	p	(109, 200)	116	Φ	(210, 31)
12	+	(44, 385)	47	N	(75, 318)	82	q	(109, 551)	117	X	(210, 720)
13	,	(45, 31)	48	O	(75, 433)	83	r	(110, 129)	118	Ц	(215, 247)
14	-	(45, 720)	49	P	(78, 271)	84	s	(110, 622)	119	Ч	(215, 504)
15	.	(47, 349)	50	Q	(78, 480)	85	t	(114, 144)	120	Ш	(218, 150)
16	/	(47, 402)	51	R	(79, 111)	86	u	(114, 607)	121	Щ	(218, 601)
17	0	(48, 49)	52	S	(79, 640)	87	v	(115, 242)	122	Ъ	(221, 138)
18	1	(48, 702)	53	T	(80, 318)	88	w	(115, 509)	123	Ы	(221, 613)
19	2	(49, 183)	54	U	(80, 433)	89	x	(116, 92)	124	Ь	(226, 9)
20	3	(49, 568)	55	V	(82, 270)	90	y	(116, 659)	125	Э	(226, 742)
21	4	(53, 277)	56	W	(82, 481)	91	z	(120, 147)	126	Ю	(227, 299)
22	5	(53, 474)	57	X	(83, 373)	92	{	(120, 604)	127	Я	(227, 452)
23	6	(56, 332)	58	Y	(83, 378)	93		(125, 292)	128	a	(228, 271)
24	7	(56, 419)	59	Z	(85, 35)	94	}	(125, 459)	129	б	(228, 480)
25	8	(58, 139)	60	[(85, 716)	95	~	(126, 33)	130	в	(229, 151)
26	9	(58, 612)	61	\	(86, 25)	96	A	(189, 297)	131	г	(229, 600)
27	:	(59, 365)	62]	(86, 726)	97	Б	(189, 454)	132	д	(234, 164)
28	;	(59, 386)	63	^	(90, 21)	98	B	(192, 32)	133	е	(234, 587)
29	<	(61, 129)	64	_	(90, 730)	99	Г	(192, 719)	134	ж	(235, 19)
30	=	(61, 622)	65	`	(93, 267)	100	Д	(194, 205)	135	з	(235, 732)
31	>	(62, 372)	66	a	(93, 484)	101	Е	(194, 546)	136	и	(236, 39)
32	?	(62, 379)	67	b	(98, 338)	102	Ж	(197, 145)	137	й	(236, 712)
33	@	(66, 199)	68	c	(98, 413)	103	З	(197, 606)	138	к	(237, 297)
34	A	(66, 552)	69	d	(99, 295)	104	И	(198, 224)	139	л	(237, 454)

140	м	(238, 175)	145	с	(243, 664)	150	ц	(250, 14)	155	ы	(253, 540)
141	н	(238, 576)	146	т	(247, 266)	151	ч	(250, 737)	156	ь	(256, 121)
142	о	(240, 309)	147	у	(247, 485)	152	ш	(251, 245)	157	э	(256, 630)
143	п	(240, 442)	148	ф	(249, 183)	153	щ	(251, 506)	158	ю	(257, 293)
144	р	(243, 87)	149	х	(249, 568)	154	ъ	(253, 211)	159	я	(257, 458)

Заметим, что мощность множества точек на этой кривой $N = 727$, поэтому при необходимости можно точками закодировать и некоторые специальные знаки (например, знак интеграла и т.п.), а также целые слова.

Пример шифрования

Пусть выбрана генерирующая точка $G = (0,1)$. Предположим, пользователь А решил отправить пользователю В сообщение: строчную латинскую букву «А». В нашем алфавите эта буква кодируется точкой $P_m = (66, 522)$. Пусть пользователь А выбрал случайное значение $k = 3$, а открытым ключом В является точка $P_B = (406, 397)$, при этом секретным ключом В является число $n_b = 45$.

Шифрованный текст имеет вид $C_m = \{kG, P_m + kP_B\}$.

Находим $kG = 3 \times (0,1)$.

Для нахождения $3G$ используем правила сложения точек эллиптической кривой. Напомним их:

$$\begin{aligned}x_3 &= \lambda^2 - x_1 - x_2 \pmod{p} \\y_3 &= \lambda(x_1 - x_3) - y_1 \pmod{p} \\ \lambda &= \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{если } P \neq Q; \\ \frac{3x_1^2 + a}{2y_1}, & \text{если } P = Q. \end{cases}\end{aligned}$$

Вычисляем $2G$:

$$\begin{aligned}\lambda &= \frac{3(0^2) - 1}{2 \times 1} = \frac{-1}{2} \equiv 375 \pmod{751} \left(\frac{-1 + 751}{2} = 375 \right) \\x_3 &= 375^2 - 0 - 0 = 140625 \equiv 188 \pmod{751} \\y_3 &= 375(0 - 188) - 1 = -70501 \equiv 93 \pmod{23}\end{aligned}$$

Итак, мы нашли $2G = (188, 93)$. Теперь находим $3G$.

$$\begin{aligned}\lambda &= \frac{188 - 0}{93 - 1} = \frac{188}{92} \equiv 368 \pmod{751} \\x_3 &= 368^2 - 0 - 188 = 135236 \equiv 56 \pmod{751} \\y_3 &= 368(0 - 56) - 1 = 20607 \equiv 419 \pmod{751}\end{aligned}$$

Таким образом, мы нашли точку $kG = 3 \cdot (0, 1) = (56, 419)$.

Вычисляем $P_m + kP_B = (66, 552) + 3 \cdot (406, 397) = (301, 734)$.

В результате: $C_m = \{(56, 419), (301, 734)\}$.

Пользователь В для расшифрования сообщения должен провести следующие вычисления:

$$P_m + kP_B - n_b(kG) = P_m + k(n_b G) - n_b(kG) = (301, 734) - 45 \cdot (56, 419) = (301, 734) + (175, 559) = (66, 552).$$

После этого пользователь В по алфавиту определяет открытый буквенный текст: точке $(66, 552)$ соответствует строчная латинская буква «А».

Варианты заданий

№ варианта	Открытый текст	Открытый ключ B	Значения случайных чисел k для букв открытого текста
1	передряга	(489, 468)	18, 15, 14, 18, 5, 10, 19, 14, 19
2	латышский	(179, 275)	15, 17, 12, 2, 2, 4, 8, 6, 17
3	регрессор	(425, 663)	6, 12, 16, 4, 9, 4, 19, 9, 18
4	симметрия	(179, 275)	11, 17, 18, 19, 16, 6, 12, 8, 2
5	уверовать	(425, 663)	6, 14, 5, 7, 12, 11, 4, 9, 19
6	терновник	(188, 93)	8, 14, 17, 17, 2, 10, 8, 2, 2
7	терпеливо	(725, 195)	17, 5, 4, 17, 13, 2, 17, 14, 19
8	ремонтный	(188, 93)	2, 2, 4, 18, 15, 19, 11, 2, 15
9	ренессанс	(725, 195)	2, 19, 4, 8, 2, 2, 16, 10, 2
10	репарация	(435, 663)	12, 11, 18, 7, 16, 18, 17, 2, 3
11	пролежень	(179, 275)	9, 5, 17, 2, 2, 2, 3, 17, 15
12	прокрутка	(618, 206)	10, 15, 16, 2, 3, 4, 2, 11, 16
13	прокопать	(489, 468)	3, 16, 17, 5, 16, 18, 3, 7, 15
14	отступить	(188, 93)	7, 9, 3, 8, 18, 18, 8, 11, 16
15	отставной	(286, 136)	5, 3, 3, 2, 4, 19, 2, 4, 10
16	отслужить	(16, 416)	2, 8, 4, 2, 6, 10, 3, 3, 18
17	отследить	(188, 93)	19, 2, 13, 5, 19, 5, 7, 8, 5
18	новенький	(425, 663)	19, 12, 13, 2, 12, 14, 19, 18, 12
19	нищенский	(489, 468)	2, 2, 7, 11, 19, 4, 2, 15, 6
20	никелевый	(568, 355)	9, 9, 2, 3, 8, 19, 6, 18, 9
21	низменный	(286, 136)	12, 5, 7, 17, 18, 2, 12, 10, 11
22	неэтичный	(489, 468)	14, 18, 11, 11, 6, 6, 17, 2, 5
23	мысленный	(346, 242)	6, 17, 18, 11, 18, 2, 4, 2, 12
24	муштровка	(618, 206)	5, 19, 8, 2, 5, 8, 15, 19, 6
25	латентный	(725, 195)	9, 10, 13, 2, 2, 12, 12, 5, 7
26	купальщик	(188, 93)	17, 17, 9, 12, 17, 7, 15, 7, 16
27	излечимый	(179, 275)	10, 14, 2, 2, 10, 10, 14, 3, 7
28	звездочка	(725, 195)	11, 17, 10, 10, 5, 2, 10, 19, 4
29	абберация	(56, 419)	16, 2, 17, 19, 8, 4, 3, 2, 8
30	белиберда	(286, 136)	2, 9, 18, 2, 19, 4, 5, 11, 9

Лабораторная работа № 6

Расшифрование криптограммы на основе эллиптических кривых

Цель работы: дан шифртекст, используя алфавит, приведенный в [4], в подразделе «Задачи к лабораторным работам по криптографии на эллиптических кривых (используется кривая $E_{751}(-1,1)$ – и генерирующая точка $G = (0,1)$)» и зная секретный ключ n_b , найти открытый текст.

Порядок выполнения работы:

– ознакомьтесь с теорией в учебном пособии «Криптография», а также в учебно-методическом пособии к выполнению лабораторного практикума по дисциплине «Криптография»;

- получите вариант задания у преподавателя;
- найдите открытый текст;
- результаты и промежуточные вычисления оформите в виде отчета.

Алфавит представляет собой множество символов языка открытых текстов и соответствующих им текстов эллиптической кривой над конечным полем.

Для заданий лабораторной работы выбрана кривая $E_{751}(-1,1)$, т.е. $y^2 = x^3 - x + 1 \pmod{751}$. Предлагается следующий (один из возможных) алфавит, приведенный в таблице.

Таблица. Алфавит точек эллиптической кривой для выполнения лабораторных работ

№	символ	точка	35	В	(67, 84)	70	е	(99, 456)	105	Й	(198, 527)
1	пробел	(33, 355)	36	С	(67, 667)	71	f	(100, 364)	106	К	(200, 30)
2	!	(33, 396)	37	D	(69, 241)	72	g	(100, 387)	107	Л	(200, 721)
3	"	(34, 74)	38	E	(69, 510)	73	h	(102, 267)	108	М	(203, 324)
4	#	(34, 677)	39	F	(70, 195)	74	i	(102, 484)	109	Н	(203, 427)
5	\$	(36, 87)	40	G	(70, 556)	75	j	(105, 369)	110	О	(205, 372)
6	%	(36, 664)	41	H	(72, 254)	76	k	(105, 382)	111	П	(205, 379)
7	&	(39, 171)	42	I	(72, 497)	77	l	(106, 24)	112	Р	(206, 106)
8	'	(39, 580)	43	J	(73, 72)	78	m	(106, 727)	113	С	(206, 645)
9	((43, 224)	44	K	(73, 679)	79	n	(108, 247)	114	Т	(209, 82)
10)	(43, 527)	45	L	(74, 170)	80	o	(108, 504)	115	У	(209, 669)
11	*	(44, 366)	46	M	(74, 581)	81	p	(109, 200)	116	Ф	(210, 31)
12	+	(44, 385)	47	N	(75, 318)	82	q	(109, 551)	117	Х	(210, 720)
13	,	(45, 31)	48	O	(75, 433)	83	r	(110, 129)	118	Ц	(215, 247)
14	-	(45, 720)	49	P	(78, 271)	84	s	(110, 622)	119	Ч	(215, 504)
15	.	(47, 349)	50	Q	(78, 480)	85	t	(114, 144)	120	Ш	(218, 150)
16	/	(47, 402)	51	R	(79, 111)	86	u	(114, 607)	121	Щ	(218, 601)
17	0	(48, 49)	52	S	(79, 640)	87	v	(115, 242)	122	Ъ	(221, 138)
18	1	(48, 702)	53	T	(80, 318)	88	w	(115, 509)	123	Ы	(221, 613)
19	2	(49, 183)	54	U	(80, 433)	89	x	(116, 92)	124	Ь	(226, 9)
20	3	(49, 568)	55	V	(82, 270)	90	y	(116, 659)	125	Э	(226, 742)
21	4	(53, 277)	56	W	(82, 481)	91	z	(120, 147)	126	Ю	(227, 299)
22	5	(53, 474)	57	X	(83, 373)	92	{	(120, 604)	127	Я	(227, 452)
23	6	(56, 332)	58	Y	(83, 378)	93		(125, 292)	128	а	(228, 271)
24	7	(56, 419)	59	Z	(85, 35)	94	}	(125, 459)	129	б	(228, 480)
25	8	(58, 139)	60	[(85, 716)	95	~	(126, 33)	130	в	(229, 151)
26	9	(58, 612)	61	\	(86, 25)	96	А	(189, 297)	131	г	(229, 600)
27	:	(59, 365)	62]	(86, 726)	97	Б	(189, 454)	132	д	(234, 164)
28	;	(59, 386)	63	^	(90, 21)	98	В	(192, 32)	133	е	(234, 587)

29	<	(61, 129)	64	_	(90, 730)	99	Г	(192, 719)	134	ж	(235, 19)
30	=	(61, 622)	65	`	(93, 267)	100	Д	(194, 205)	135	з	(235, 732)
31	>	(62, 372)	66	a	(93, 484)	101	Е	(194, 546)	136	и	(236, 39)
32	?	(62, 379)	67	b	(98, 338)	102	Ж	(197, 145)	137	й	(236, 712)
33	@	(66, 199)	68	c	(98, 413)	103	З	(197, 606)	138	к	(237, 297)
34	A	(66, 552)	69	d	(99, 295)	104	И	(198, 224)	139	л	(237, 454)

140	м	(238, 175)	145	с	(243, 664)	150	ц	(250, 14)	155	ы	(253, 540)
141	н	(238, 576)	146	т	(247, 266)	151	ч	(250, 737)	156	ь	(256, 121)
142	о	(240, 309)	147	у	(247, 485)	152	ш	(251, 245)	157	э	(256, 630)
143	п	(240, 442)	148	ф	(249, 183)	153	щ	(251, 506)	158	ю	(257, 293)
144	р	(243, 87)	149	х	(249, 568)	154	ъ	(253, 211)	159	я	(257, 458)

Заметим, что мощность множества точек на этой кривой $N = 727$, поэтому при необходимости можно точками закодировать и некоторые специальные знаки (например, знак интеграла и т.п.), а также целые слова.

Пример шифрования

Пусть выбрана генерирующая точка $G = (0,1)$. Предположим, пользователь А решил отправить пользователю В сообщение: строчную латинскую букву «А». В нашем алфавите эта буква кодируется точкой $P_m = (66, 522)$. Пусть пользователь А выбрал случайное значение $k = 3$, а открытым ключом В является точка $P_B = (406, 397)$, при этом секретным ключом В является число $n_b = 45$.

Шифрованный текст имеет вид $C_m = \{kG, P_m + kP_B\}$.

Находим $kG = 3 \times (0,1)$.

Для нахождения $3G$ используем правила сложения точек эллиптической кривой. Напомним их:

$$\begin{aligned}
 x_3 &= \lambda^2 - x_1 - x_2 \pmod{p} \\
 y_3 &= \lambda(x_1 - x_3) - y_1 \pmod{p} \\
 \lambda &= \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{если } P \neq Q; \\ \frac{3x_1^2 + a}{2y_1}, & \text{если } P = Q. \end{cases}
 \end{aligned}$$

Вычисляем $2G$:

$$\begin{aligned}
 \lambda &= \frac{3(0^2) - 1}{2 \times 1} = \frac{-1}{2} \equiv 375 \pmod{751} \left(\frac{-1 + 751}{2} = 375 \right) \\
 x_3 &= 375^2 - 0 - 0 = 140625 \equiv 188 \pmod{751} \\
 y_3 &= 375(0 - 188) - 1 = -70501 \equiv 93 \pmod{23}
 \end{aligned}$$

Итак, мы нашли $2G = (188, 93)$. Теперь находим $3G$.

$$\lambda = \frac{188 - 0}{93 - 1} = \frac{188}{92} \equiv 368 \pmod{751}$$

$$x_3 = 368^2 - 0 - 188 = 135236 \equiv 56 \pmod{751}$$

$$y_3 = 368(0 - 56) - 1 = 20607 \equiv 419 \pmod{751}$$

Таким образом, мы нашли точку $kG = 3 \cdot (0, 1) = (56, 419)$.

Вычисляем $P_m + kP_B = (66, 552) + 3 \cdot (406, 397) = (301, 734)$.

В результате: $C_m = \{(56, 419), (301, 734)\}$.

Пользователь В для расшифрования сообщения должен провести следующие вычисления:

$$P_m + kP_B - n_B(kG) = P_m + k(n_B G) - n_B(kG) = (301, 734) - 45 \cdot (56, 419) = (301, 734) + (175, 559) = (66, 552).$$

После этого пользователь В по алфавиту определяет открытый буквенный текст: точке (66, 552) соответствует строчная латинская буква «А».

Варианты заданий

№ варианта	Секретный ключ n_b	Шифртекст
1	29	$\{(440, 539), (128, 672)\}; \{(489, 468), (282, 341)\};$ $\{(489, 468), (45, 720)\}; \{(72, 254), (227, 299)\};$ $\{(188, 93), (251, 506)\}; \{(72, 254), (319, 518)\};$ $\{(745, 210), (129, 659)\}; \{(286, 136), (515, 684)\};$ $\{(568, 355), (395, 414)\}$
2	25	$\{(72, 254), (397, 184)\}; \{(188, 93), (526, 412)\};$ $\{(188, 93), (328, 290)\}; \{(135, 82), (433, 47)\};$ $\{(179, 275), (711, 341)\}; \{(568, 355), (546, 670)\};$ $\{(16, 416), (734, 170)\}; \{(568, 355), (371, 14)\};$ $\{(596, 433), (604, 610)\}; \{(16, 416), (734, 170)\}$
3	40	$\{(188, 93), (573, 583)\}; \{(188, 93), (128, 79)\};$ $\{(425, 663), (703, 125)\}; \{(489, 468), (109, 200)\};$ $\{(568, 355), (348, 27)\}; \{(377, 456), (323, 657)\};$ $\{(72, 254), (399, 65)\}; \{(16, 416), (660, 275)\};$ $\{(179, 275), (267, 670)\}; \{(568, 355), (642, 53)\}$
4	34	$\{(618, 206), (426, 662)\}; \{(72, 254), (67, 667)\};$ $\{(286, 136), (739, 574)\}; \{(16, 416), (143, 602)\};$ $\{(618, 206), (313, 203)\}; \{(618, 206), (114, 607)\};$ $\{(618, 206), (438, 711)\}; \{(188, 93), (573, 168)\}$
5	41	$\{(283, 493), (314, 127)\}; \{(425, 663), (561, 140)\};$ $\{(568, 355), (75, 433)\}; \{(440, 539), (602, 627)\};$ $\{(188, 93), (395, 414)\}; \{(179, 275), (25, 604)\};$ $\{(72, 254), (47, 349)\}; \{(72, 254), (417, 137)\};$ $\{(188, 93), (298, 225)\}; \{(56, 419), (79, 111)\}$
6	44	$\{(377, 456), (367, 360)\}; \{(425, 663), (715, 398)\};$ $\{(188, 93), (279, 353)\}; \{(179, 275), (128, 79)\};$ $\{(568, 355), (515, 67)\}; \{(568, 355), (482, 230)\};$

		{(377, 456), (206, 645)}; {(188, 93), (300, 455)}; {(489, 468), (362, 446)}; {(16, 416), (69, 510)}; {(425, 663), (218, 601)}
7	12	{(16, 416), (128, 672)}; {(56, 419), (59, 386)}; {(425, 663), (106, 24)}; {(568, 355), (145, 608)}; {(188, 93), (279, 398)}; {(425, 663), (99, 295)}; {(179, 275), (269, 187)}; {(188, 93), (395, 337)}; {(188, 93), (311, 68)}; {(135, 82), (556, 484)}; {(56, 419), (106, 727)}; {(16, 416), (307, 693)}
8	45	{(745, 210), (259, 401)}; {(568, 355), (606, 147)}; {(188, 93), (407, 82)}; {(56, 419), (739, 574)}; {(286, 136), (329, 447)}; {(425, 663), (520, 749)}; {(72, 254), (374, 315)}; {(188, 93), (149, 97)}; {(745, 210), (13, 134)}; {(440, 539), (235, 19)}; {(425, 663), (128, 79)}
9	32	{(188, 93), (623, 166)}; {(725, 195), (513, 414)}; {(346, 242), (461, 4)}; {(489, 468), (739, 574)}; {(725, 195), (663, 476)}; {(745, 210), (724, 522)}; {(725, 195), (663, 476)}; {(618, 206), (438, 40)}; {(286, 136), (546, 670)}; {(179, 275), (73, 72)}
10	18	{(179, 275), (269, 564)}; {(179, 275), (73, 72)}; {(440, 539), (189, 454)}; {(618, 206), (628, 458)}; {(568, 355), (660, 275)}; {(72, 254), (709, 595)}; {(745, 210), (12, 314)}; {(188, 93), (36, 664)}; {(618, 206), (530, 22)}; {(286, 136), (532, 50)}; {(425, 663), (660, 275)}; {(725, 195), (482, 230)}
11	27	{(745, 210), (185, 105)}; {(188, 93), (681, 385)}; {(377, 456), (576, 465)}; {(440, 539), (138, 298)}; {(745, 210), (520, 2)}; {(188, 93), (681, 385)}; {(286, 136), (282, 410)}; {(72, 254), (200, 721)}; {(72, 254), (643, 94)}; {(745, 210), (476, 315)}; {(440, 539), (724, 229)}
12	25	{(425, 663), (651, 191)}; {(188, 93), (177, 562)}; {(286, 136), (603, 562)}; {(440, 539), (588, 707)}; {(72, 254), (269, 187)}; {(56, 419), (49, 568)}; {(16, 416), (426, 662)}; {(425, 663), (557, 28)}; {(188, 93), (149, 97)}; {(179, 275), (711, 341)}
13	48	{(179, 275), (712, 186)}; {(725, 195), (395, 414)}; {(72, 254), (434, 136)}; {(425, 663), (251, 506)}; {(16, 416), (383, 340)}; {(745, 210), (102, 484)}; {(346, 242), (78, 271)}; {(179, 275), (712, 186)}; {(725, 195), (739, 574)}; {(346, 242), (78, 271)}
14	51	{(425, 663), (273, 481)}; {(188, 93), (85, 716)}; {(16, 416), (422, 162)}; {(283, 493), (36, 87)}; {(179, 275), (100, 364)}; {(188, 93), (298, 225)}; {(56, 419), (555, 303)}; {(745, 210), (100, 387)}; {(377, 456), (526, 412)}; {(286, 136), (316, 228)}; {(745, 210), (49, 183)}; {(179, 275), (428, 247)}
		{(618, 206), (99, 456)}; {(425, 663), (31, 136)}

15	27	{(377, 456), (688, 741)}; {(425, 663), (636, 747)}; {(16, 416), (298, 526)}; {(188, 93), (356, 175)}; {(489, 468), (147, 390)}; {(346, 242), (546, 670)}; {(72, 254), (114, 144)}; {(377, 456), (25, 147)}
16	48	{(16, 416), (724, 522)}; {(489, 468), (719, 538)}; {(56, 419), (205, 372)}; {(72, 254), (628, 293)}; {(188, 93), (594, 337)}; {(440, 539), (588, 707)}; {(568, 355), (707, 556)}; {(489, 468), (719, 538)}; {(16, 416), (590, 376)}; {(56, 419), (612, 329)}; {(188, 93), (594, 337)}
17	51	{(56, 419), (739, 177)}; {(16, 416), (282, 410)}; {(425, 663), (221, 138)}; {(188, 93), (329, 447)}; {(286, 136), (235, 19)}; {(725, 195), (496, 31)}; {(56, 419), (236, 712)}; {(440, 539), (514, 662)}; {(377, 456), (323, 94)}; {(179, 275), (203, 324)}; {(568, 355), (197, 606)}
18	16	{(745, 210), (268, 597)}; {(725, 195), (310, 582)}; {(618, 206), (59, 365)}; {(440, 539), (371, 14)}; {(188, 93), (348, 27)}; {(72, 254), (434, 136)}; {(16, 416), (623, 166)}; {(188, 93), (235, 19)}; {(440, 539), (660, 275)}; {(188, 93), (434, 615)}; {(725, 195), (73, 679)}; {(188, 93), (642, 53)}
19	34	{(725, 195), (538, 325)}; {(725, 195), (176, 413)}; {(425, 663), (689, 670)}; {(346, 242), (652, 315)}; {(283, 493), (463, 736)}; {(16, 416), (744, 133)}; {(179, 275), (542, 351)}; {(56, 419), (298, 225)}; {(286, 136), (719, 538)}; {(568, 355), (319, 518)}; {(16, 416), (704, 46)}
20	25	{(725, 195), (329, 304)}; {(440, 539), (59, 386)}; {(618, 206), (543, 357)}; {(188, 93), (520, 749)}; {(489, 468), (585, 211)}; {(179, 275), (707, 556)}; {(596, 433), (419, 38)}; {(377, 456), (643, 94)}; {(188, 93), (385, 749)}; {(725, 195), (150, 355)}; {(725, 195), (197, 606)}
21	58	{(16, 416), (93, 484)}; {(489, 468), (531, 397)}; {(188, 93), (654, 102)}; {(489, 468), (218, 150)}; {(16, 416), (530, 729)}; {(425, 663), (295, 219)}; {(725, 195), (742, 299)}; {(188, 93), (367, 360)}; {(188, 93), (235, 732)}; {(618, 206), (251, 245)}; {(425, 663), (688, 10)}
22	50	{(179, 275), (326, 675)}; {(725, 195), (83, 378)}; {(440, 539), (340, 78)}; {(425, 663), (67, 84)}; {(425, 663), (620, 71)}; {(72, 254), (251, 245)}; {(568, 355), (75, 318)}; {(725, 195), (228, 271)}; {(188, 93), (734, 170)}; {(188, 93), (704, 705)}; {(286, 136), (235, 732)}
23	19	{(618, 206), (294, 595)}; {(188, 93), (13, 617)}; {(188, 93), (206, 106)}; {(188, 93), (67, 667)}; {(56, 419), (350, 184)}; {(440, 539), (275, 456)};

		{(745, 210), (301, 17)}; {(346, 242), (588, 707)}; {(188, 93), (256, 121)}; {(425, 663), (209, 82)}; {(16, 416), (687, 660)}
24	54	{(188, 93), (295, 219)}; {(618, 206), (646, 706)}; {(440, 539), (573, 583)}; {(16, 416), (694, 581)}; {(179, 275), (585, 540)}; {(377, 456), (701, 570)}; {(618, 206), (67, 667)}; {(286, 136), (36, 664)}; {(72, 254), (727, 65)}; {(568, 355), (438, 40)}
25	55	{(725, 195), (9, 150)}; {(745, 210), (138, 453)}; {(56, 419), (36, 87)}; {(283, 493), (39, 580)}; {(377, 456), (515, 684)}; {(346, 242), (458, 261)}; {(283, 493), (105, 369)}; {(568, 355), (326, 675)}; {(425, 663), (529, 358)}; {(283, 493), (668, 409)}
26	24	{(16, 416), (150, 355)}; {(188, 93), (394, 20)}; {(725, 195), (13, 134)}; {(377, 456), (209, 669)}; {(56, 419), (514, 662)}; {(56, 419), (243, 87)}; {(618, 206), (719, 538)}; {(618, 206), (159, 13)}; {(618, 206), (326, 76)}; {(188, 93), (557, 28)}
27	43	{(440, 539), (279, 398)}; {(568, 355), (295, 219)}; {(16, 416), (724, 229)}; {(346, 242), (730, 240)}; {(72, 254), (334, 226)}; {(188, 93), (310, 169)}; {(72, 254), (36, 664)}; {(179, 275), (481, 369)}; {(188, 93), (236, 39)}; {(377, 456), (438, 711)}; {(377, 456), (307, 58)}
28	20	{(16, 416), (675, 505)}; {(72, 254), (611, 579)}; {(72, 254), (727, 686)}; {(489, 468), (39, 171)}; {(72, 254), (531, 354)}; {(568, 355), (36, 87)}; {(188, 93), (588, 44)}; {(618, 206), (70, 195)}; {(568, 355), (267, 81)}; {(56, 419), (525, 674)}
29	47	{(725, 195), (651, 560)}; {(425, 663), (147, 361)}; {(286, 136), (109, 551)}; {(440, 539), (90, 730)}; {(618, 206), (668, 342)}; {(745, 210), (109, 200)}; {(425, 663), (147, 361)}; {(72, 254), (228, 480)}; {(346, 242), (530, 22)}
30	50	{(16, 416), (726, 608)}; {(188, 93), (395, 337)}; {(440, 539), (163, 513)}; {(188, 93), (269, 187)}; {(725, 195), (177, 562)}; {(188, 93), (115, 509)}; {(188, 93), (734, 170)}; {(745, 210), (110, 622)}; {(179, 275), (576, 286)}; {(188, 93), (325, 297)}

Лабораторная работа № 7

Расчет точки $2P + 3Q - R$ на эллиптической кривой

Цель работы: Даны точки P , Q , R на эллиптической кривой E_{751} $(-1,1)$. Найти точку $2P + 3Q - R$.

Порядок выполнения работы:

- ознакомьтесь с теорией в [4];
- получите вариант задания у преподавателя;
- найдите точку $2P + 3Q - R$;

– результаты и промежуточные вычисления оформите в виде отчета.

Варианты заданий

№ варианта	Координаты точек		
	P	Q	R
1	(58, 139)	(67, 667)	(82, 481)
2	(61, 129)	(59, 365)	(105, 369)
3	(62, 372)	(70, 195)	(67, 84)
4	(56, 332)	(69, 241)	(83, 373)
5	(59, 386)	(70, 195)	(72, 254)
6	(72, 497)	(61, 622)	(70, 556)
7	(74, 170)	(53, 277)	(86, 25)
8	(48, 702)	(69, 241)	(98, 338)
9	(59, 386)	(61, 129)	(100, 364)
10	(72, 497)	(53, 474)	(90, 730)
11	(59, 365)	(59, 386)	(105, 382)
12	(61, 622)	(61, 622)	(90, 730)
13	(61, 129)	(69, 510)	(72, 497)
14	(70, 556)	(56, 419)	(86, 726)
15	(67, 84)	(69, 241)	(66, 199)
16	(73, 72)	(56, 332)	(85, 35)
17	(69, 241)	(53, 277)	(106, 24)
18	(74, 581)	(53, 277)	(85, 35)
19	(56, 419)	(69, 510)	(79, 640)
20	(58, 612)	(67, 84)	(83, 373)
21	(62, 379)	(53, 474)	(110, 622)
22	(53, 277)	(66, 552)	(99, 456)
23	(67, 667)	(53, 474)	(105, 382)
24	(69, 241)	(66, 552)	(69, 510)
25	(69, 510)	(53, 277)	(105, 369)
26	(72, 497)	(62, 372)	(69, 241)
27	(61, 129)	(59, 365)	(105, 369)
28	(61, 622)	(59, 365)	(102, 267)
29	(58, 139)	(67, 84)	(85, 35)
30	(69, 510)	(62, 372)	(74, 170)

Лабораторная работа № 8

Расчет точки nP на эллиптической кривой

Цель работы: дана точка P на эллиптической кривой $E_{751}(-1,1)$ и натуральное число n . Найти точку nP .

Порядок выполнения работы:

- ознакомьтесь с теорией в [4];
- получите вариант задания у преподавателя;
- найдите точку nP ;
- результаты и промежуточные вычисления оформите в виде отчета.

Варианты заданий

№ варианта	P	n
1	(62, 372)	128
2	(43, 527)	116
3	(39, 171)	110
4	(43, 527)	107
5	(36, 87)	111
6	(49, 568)	122
7	(39, 580)	109
8	(75, 318)	142
9	(45, 720)	111
10	(78, 480)	147
11	(53, 474)	120
12	(43, 527)	109
13	(49, 568)	124
14	(39, 171)	108
15	(49, 183)	126
16	(58, 139)	121
17	(33, 355)	111
18	(39, 580)	101
19	(44, 366)	113
20	(73, 72)	103
21	(85, 716)	159
22	(66, 199)	103
23	(44, 385)	113
24	(45, 720)	111
25	(39, 171)	107
26	(34, 677)	106
27	(34, 74)	107
28	(34, 677)	105
29	(79, 640)	149
30	(58, 139)	124

Лабораторная работа № 9

Получение ЭЦП на основе эллиптических кривых

Цель работы: сгенерировать ЭЦП для сообщения с известным значением хэш-свертки e , зная секретный ключ подписи d при данном значении выбираемого случайным образом числа k . Используется эллиптическая кривая $E_{751}(-1,1)$ и генерирующая точка $G = (416, 55)$ порядка $n=13$.

Порядок выполнения работы:

- ознакомьтесь с теорией в [4];
- получите вариант задания у преподавателя;
- сгенерируйте ЭЦП для сообщения;

– результаты и промежуточные вычисления оформите в виде отчета.

Пример генерации и проверки подписи

Пусть используется эллиптическая кривая $E_{751}(-1,1)$ – и генерирующая точка $G=(384, 475)$ порядка $n=13$ (13 – наибольший из делителей порядка кривой $N=728$). Предположим, абонент подписывает личным секретным ключом $d=12$ сообщение, хеш-свертка которого равна $e=12$.

Пусть абонент, подписывающий сообщение, выбрал случайное $k=3$. Тогда он вычисляет $kG=(x,y)=3 \cdot (384, 475)=(596, 318)$ и затем $r=x \bmod n=596 \bmod 13=11$. Используя расширенный алгоритм Евклида, определяем $z=k^{-1} \bmod n=3^{-1} \bmod 13=9$ (так как $3 \cdot 9=27 \equiv 1 \pmod{13}$). Наконец, $s=z(e+dr) \bmod n=9 \cdot (12+12 \cdot 11) \bmod 13=9$. Таким образом, $(r, s)=(11,9)$ – цифровая подпись данного абонента для сообщения.

Пусть теперь необходимо проверить подлинность данной подписи. Открытый ключ абонента, подписавшего сообщение, равен $Q=dG=12 \cdot (384, 475)=(384, 276)$. Проверка подписи начинается с проверки условий $1 \leq r \leq n-1, 1 \leq s \leq n-1$ – в данном случае они соблюдаются. Затем последовательно вычисляем $v=s^{-1} \bmod n=9^{-1} \bmod 13=3$, $u_1=ev \bmod 12 \cdot 3 \bmod 13=10$ и $u_2=r \cdot v \bmod 13=11 \cdot 3 \bmod 13=7$. Находим точку $X=u_1 \cdot G+u_2 \cdot Q=10 \cdot (384,475)+7 \cdot (384,276)=(596,318)$. Наконец, сравниваем значения $r=11$ и $x \bmod n=596 \bmod 13=11$ – они совпадают, следовательно, подпись действительная.

Варианты заданий

№ варианта	e	d	k
1	9	3	5
2	3	9	6
3	12	9	2
4	3	4	7
5	5	12	6
6	6	12	7
7	8	5	5
8	8	2	5
9	11	5	6
10	3	3	11
11	10	9	2
12	11	2	8
13	8	6	3
14	3	10	6
15	4	6	11
16	6	12	11

17	2	11	5
18	10	5	11
19	11	5	7
20	6	10	7
21	10	9	11
22	6	10	2
23	9	6	6
24	8	12	8
25	3	2	8
26	6	5	6
27	6	7	11
28	7	3	7
29	9	11	2
30	5	12	8

Лабораторная работа № 10

Проверка ЭЦП на основе эллиптических кривых

Цель работы: проверить подлинность ЭЦП (r,s) для сообщения с известным значением хэш-свертки e , зная открытый ключ проверки подписи Q . Используется эллиптическая кривая $E_{751}(-1,1)$ и генерирующая точка $G = (562, 89)$ порядка $n = 13$.

Порядок выполнения работы:

- ознакомьтесь с теорией в [4];
- получите вариант задания у преподавателя;
- проверьте подлинность ЭЦП для сообщения;
- результаты и промежуточные вычисления оформите в виде отчета.

Пример генерации и проверки подписи

Пусть используется эллиптическая кривая $E_{751}(-1,1)$ – и генерирующая точка $G = (384, 475)$ порядка $n = 13$ (13 – наибольший из делителей порядка кривой $N = 728$). Предположим, абонент подписывает личным секретным ключом $d = 12$ сообщение, хэш-свертка которого равна $e = 12$.

Пусть абонент, подписывающий сообщение, выбрал случайное $k = 3$. Тогда он вычисляет $kG = (x,y) = 3 \cdot (384, 475) = (596, 318)$ и затем $r = x \bmod n = 596 \bmod 13 = 11$. Используя расширенный алгоритм Евклида, определяем $z = k^{-1} \bmod n = 3^{-1} \bmod 13 = 9$ (так как $3 \cdot 9 = 27 \equiv 1 \pmod{13}$). Наконец, $s = z(e + dr) \bmod n = 9 \cdot (12 + 12 \cdot 11) \bmod 13 = 9$. Таким образом, $(r, s) = (11, 9)$ – цифровая подпись данного абонента для сообщения.

Пусть теперь необходимо проверить подлинность данной подписи. Открытый ключ абонента, подписавшего сообщение, равен $Q = dG = 12 \cdot (384, 475) = (384, 276)$. Проверка подписи начинается с проверки условий $1 \leq r \leq n-1, 1 \leq s \leq n-1$ – в данном случае они соблюдаются.

Затем последовательно вычисляем $v = s^{-1} \bmod n = 9^{-1} \bmod 13 = 3$, $u_1 = ev \bmod 12 \cdot 3 \bmod 13 = 10$ и $u_2 = -11 \cdot 3 \bmod 13 = 7$. Находим точку $X = u_1 \cdot G + u_2 \cdot Q = 10 \cdot (384, 475) + 7 \cdot (384, 276) = (596, 318)$. Наконец, сравниваем значения $r = 11$ и $x \bmod n = 596 \bmod 13 = 11$ – они совпадают, следовательно, подпись действительная.

Варианты заданий

№ варианта	e	Q	(r, s)
1	4	(596, 318)	(11, 4)
2	5	(455, 368)	(3, 7)
3	6	(135, 669)	(5, 7)
4	6	(562, 662)	(5, 7)
5	2	(135, 669)	(7, 6)
6	8	(135, 82)	(11, 10)
7	4	(384, 475)	(11, 9)
8	7	(596, 433)	(11, 1)
9	7	(455, 368)	(11, 11)
10	7	(384, 475)	(5, 5)
11	5	(384, 475)	(11, 1)
12	10	(455, 383)	(11, 10)
13	8	(384, 276)	(3, 1)
14	3	(135, 669)	(11, 10)
15	6	(455, 383)	(3, 1)
16	2	(596, 433)	(3, 10)
17	10	(455, 368)	(11, 6)
18	5	(596, 433)	(11, 12)
19	9	(135, 82)	(7, 7)
20	2	(596, 433)	(11, 4)
21	6	(596, 318)	(7, 5)
22	5	(596, 318)	(7, 4)
23	12	(135, 669)	(5, 11)
24	12	(562, 89)	(3, 2)
25	6	(562, 662)	(7, 10)
26	12	(135, 82)	(7, 8)
27	7	(384, 276)	(5, 2)
28	8	(596, 318)	(11, 6)
29	10	(384, 276)	(7, 6)
30	9	(416, 696)	(11, 11)

Использованная литература

1. Учебное пособие по дисциплине «Криптография». Электронный ресурс находится по адресу: <http://isu.ifmo.ru> (Вход через личный кабинет).
2. Учебно-методическое пособие к выполнению лабораторных работ по дисциплине «Криптография». Электронный ресурс находится по адресу: <http://isu.ifmo.ru> (Вход через личный кабинет).
3. Алгоритм RSA: метод. указания к выполнению лабораторных работ для студентов спец. 090105 «Комплексное обеспечение информационной безопасности автоматизированных систем» очной формы обучения/сост.: О. Н. Жданов, И. А. Лубкин ; Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2007. – 38 с. Электронный ресурс находится по адресу: <http://isu.ifmo.ru> (Вход через личный кабинет).
4. Эллиптические кривые и их применение в криптографии: учеб. пособие / О. Н. Жданов, В. А. Чалкин; Сиб. гос. аэрокосмич. ун-т.-Красноярск, 2011.- 106 с. Электронный ресурс находится по адресу: <http://isu.ifmo.ru> (Вход через личный кабинет).

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

На кафедре ВТ проводятся научные исследования в соответствии с программой развития научной школы кафедры «Организация вычислительных систем и сетей», включенной в реестр ведущих научных и научно-педагогических школ Санкт-Петербурга. Магистранты и аспиранты активно участвуют в научно-исследовательских работах по следующим основным направлениям.

Работы в области **вычислительных систем и сетей** направлены на разработку методов и средств системотехнического проектирования вычислительных систем и сетей на основе аналитических и имитационных моделей и измерений на реальных системах. Решаются задачи оценки эффективности и оптимизации отказоустойчивых высоконадежных систем, создания методологии комплексного обеспечения надежности, безопасности и устойчивости функционирования систем в условиях сбоев, отказов и внешних деструктивных воздействий. Разрабатываются методы и средства реализации информационной безопасности и защиты информации от несанкционированного доступа в вычислительных системах.

Исследования в области **параллельных и распределенных вычислений** связаны с решением задач анализа технологий параллельного программирования в системах с общей памятью и модификацией последовательных алгоритмов для выполнения в параллельном режиме. Исследования включают в себя анализ и разработку lock-free структур данных, оценку их эффективности при различных нагрузках. Исследуется эффективность организации параллельных вычислений на графических процессорах с использованием технологии CUDA. Значительное внимание уделяется инструментам и методам динамического анализа выполнения параллельных программ.

Исследования в области **обработки и распознавания цифровых изображений и аудио сигналов** направлены на разработку новых методов, алгоритмов и программных средств для решения задач обработки

и анализа изображений с целью повышения их качества, анализа динамических изображений с целью формирования траектории движения объекта, распознавания изображений объектов независимо от их положения, ориентации и масштаба, спектральной обработки изображений. Проводятся исследования эффективности существующих и разработка новых методов маркирования изображений встраиваемыми в них цифровыми водяными знаками и методов повышения робастности (устойчивости) распознавания в мультимодальных биометрических системах.

Более 30 лет на кафедре ведутся работы в области **микропроцессорной техники и встроенных вычислительных систем**, связанные с разработкой и исследованием распределенных информационно-управляющих систем с высокой надежностью, контроллерных сетей промышленной и транспортной автоматики, средств автоматизации программирования и отладки распределенных систем реального времени. В рамках научного направления "Автоматизация высокоуровневых этапов проектирования информационно-управляющих систем" решаются задачи создания встраиваемых систем, систем реального времени, реконфигурируемых систем и систем-на-кристалле. Ведутся работы по развитию методологии проектирования киберфизических систем. Стремительно развивается направление работ по созданию IP-ядер для систем-на-кристалле.

Работы в области **интеллектуальных информационных систем** нацелены на создание быстрых алгоритмов поиска в базах знаний, организацию данных в базах знаний, обеспечивающую быстрый логический вывод, извлечение знаний из неформализованных источников, в том числе из социальных сетей. Кроме интеллектуальных информационных систем в сферу интересов кафедры входят также интеллектуальные методы управления в технических системах.

Кроме того, на кафедре проводятся научные исследования, связанные с проблемами **проектирования, разработки, сопровождения и реинжиниринга корпоративных информационных систем**, а также с разработкой **преобразователей перемещений на основе рекурсивных кодовых шкал** с улучшенными массогабаритными, технологическими и надежностными характеристиками.

Сотрудники кафедры участвуют в работе Международных научных лабораторий:

- «Архитектура и методы проектирования встраиваемых систем и систем на кристалле».
- «Лаборатория нелинейных и адаптивных систем управления».
- «Многомодальные биометрические и речевые системы».

Существующие международные программы

На кафедре реализуются совместные программы подготовки:

- бакалавров с Пекинским политехническим университетом;
- магистров по программе двойного диплома с Казахским национальным университетом им. аль-Фараби;
- магистров по программе двойного диплома с Восточно-Казахстанским государственным техническим университетом им. Серикбаева.

Компании, в которых осуществляется производственная и преддипломная практика, а также компании, трудоустраивающие выпускников

Производственная практика: ОКБ "Электроавтоматика", ОАО «НИИ Масштаб», ЛМТ, Elcom Ltd, а также в лабораториях кафедры. Наши выпускники работают в ЗАО "ПетерСтар", ЗАО "ПетербургТранзит Телеком", ОАО "МТТ", ОАО "СвязьТрансНефть", Управление Центробанка РФ по СПб и ЛО, ОАО "Радар-ММС", ОАО "Авионика, tBricks, EMC, Dr. Web, Intel, JetBrains, Microsoft, Intel Labs, Sun Microsystems, Motorola Solutions, Yota Lab, Siemems, Alcatel, Luxoft, Reksoft, Exigen Services, i-Free, Promt, T-Systems, Enkata Technologies, Digital Design, Arcadia, NetCracker, Grid Dynamics, Yandex, VIAcode, Devexperts, Actimind, Kentor, Oracle Development SPb, ЗАО "Пассат", МТС, БиЛайн, Центр речевых технологий, Пулково, Сбербанк, РЖД, Государственный архив, Пенсионный фонд, Ростелеком, ЛОМО, ЦНИИ «Гранит», Санкт-Петербургский информационно-аналитический центр, ЛОНИИС, ОАО "Авангард", Транзас, Российский Федеральный Ядерный Центр ВНИИТФ, ВСС ("Бизнес Компьютер Центр"), ООО "Газинформсервис", ФГУП ЦНИИ "Электроприбор", Tune IT, ЗАО "НПП "Информационные технологии в бизнесе", Kortec и др.

Ожиганов Александр Аркадьевич

**Криптографические системы с секретным и
открытым ключом**

Учебное пособие

В авторской редакции

Редакционно-издательский отдел Университета ИТМО

Зав. РИО

Н.Ф. Гусарова

Подписано к печати

Заказ №

Тираж

Отпечатано на ризографе

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверкский пр., 49