Презентация

КРИПТОСИСТЕМА ЭЛЬ-ГАМАЛЯ. ЛАБОРАТОРНАЯ РАБОТА

Ковун В. А., магистрант 2-го курса факультета ПММ

- ***Воронков Б. Н., к. т. н., доцент***
- ***факультета ПММ***
- *(Воронежский государственный университет, vrnkv@mail.ru)*

Постановка задачи

- Провести анализ криптографического алгоритма Эль-Гамаля.
- Разработать сценарий выполнения лабораторной работы по изучению алгоритма Эль-Гамаля.
- Ознакомиться с обучающими программами по криптографии: DES, ГОСТ 28147-89, Crypto-03, Elgamal, выявить их достоинства и недостатки.
- Разработать и реализовать обучающую компьютерную программу ***El-Gamal_Tutor***.

Постановка задачи
(в лабораторной работе)

- Ознакомиться с обучающей компьютерной программой ***El-Gamal_Tutor*.**
- Изучить и привести описание алгоритма Эль Гамаля (в соответствии с обозначениями из [4]) с доказательством корректности алгоритма, его достоинствами и недостатками.
- Зафиксировать (для отчета) последовательность этапов обучения в программе ***El-Gamal_Tutor.***
- Провести тестирование программы ***El-Gamal_Tutor*** с целью выявления ошибок и недочетов.

Постановка задачи
(в лабораторной работе)

- С помощью пакета прикладных программ Maple произвести шифрование и расшифрование сообщения, заданного в виде одного блока открытого текста.
- Сформулировать и обосновать принципы работы алгоритма Эль Гамаля.
- Одним из методов решения задачи дискретного логарифмирования осуществить криптоанализ заданного шифрованного текста на основе известных составляющих открытого ключа .
- Ответить на контрольные вопросы.
- Составить и защитить отчет о проделанной работе.

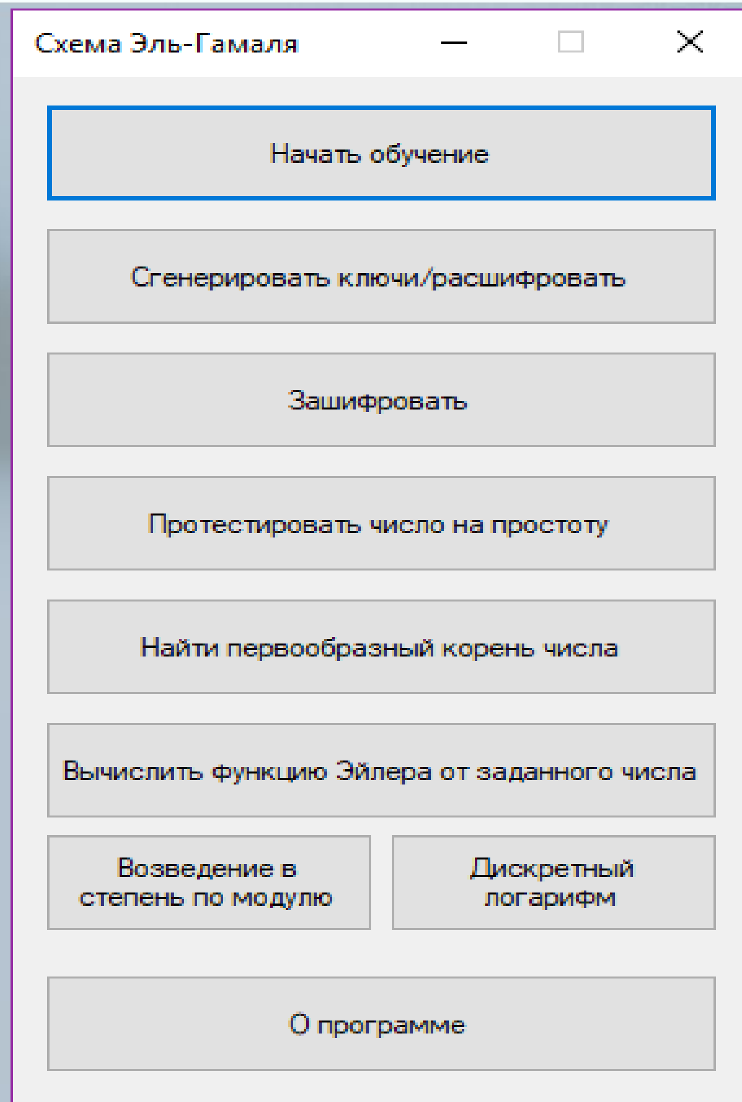
Содержание отчёта

- Постановка задачи
- Описание криптосистемы Эль Гамаля.
- Последовательность этапов и результаты обучения с использованием программы ***El-Gamal_Tutor***.
- Выявление ошибок и недочетов в обучающей программе ***El-Gamal_Tutor***.
- Результаты шифрования и расшифрования с использованием ППП.
- Принципы работы алгоритма Эль Гамаля.
- Последовательность этапов и результаты криптоанализа.
- Ответы на контрольные вопросы.
- Выводы
- Библиография

Принципы работы алгоритма Эль Гамаля

- 1. Криптосистема асимметричная (двухключевая).
- 2. Блочная, с длиной блока открытого текста, меньше или равной длине открытого (публичного) ключа.
- 3. Длина открытого и закрытого ключей, по современным представлениям, 2048 бит или более.
- 4. Используется лишь один метод шифрования – метод аналитических преобразований.
- 5. Базируется на вычислительно трудной задаче дискретного логарифмирования.
- 6. Предоставляет возможность реализации электронной подписи.

Основная форма



Режим обучения: 1-ый шаг

Возведение в степень по модулю

Возведение в степень по модулю – это вычисление остатка от деления натурального числа b (основание), возведенного в степень e (показатель степени), на натуральное число m (модуль).
Например, пусть нам даны b = 5, e = 3 и m = 13, тогда решение c = 8 - это остаток от деления 5^3 на 13.
Обозначение: c = b^e mod m.

Попробуйте возвести 3 в степень 3 по модулю 15

Ответ: 12

9^4 mod 19 =

Ответ: 6

6^4 mod 13 =

Ответ: 9

Далее

Режим обучения: 2-ой шаг

Функция Эйлера

Функция Эйлера fi(n)– мультипликативная арифметическая функция, равная количеству натуральных чисел, меньших n и взаимно простых с ним. При этом полагают, что число 1 взаимно просто со всеми натуральными числами, и fi(1)=1.

Например, для числа 24 существует 8 меньших него и взаимно простых с ним чисел (1, 5, 7, 11, 13, 17, 19, 23), поэтому fi(24)=8.

Для произвольного натурального числа n функция Эйлера может быть вычислена по следующей формуле, где p[1]...p[n] - простые числа, являющиеся делителями числа n согласно основной теореме арифметики:

$$\varphi\left(\prod_{i=1}^{n} p_i^{k_i}\right) = \prod_{i=1}^{n} (p_i^{k_i} - p_i^{k_i-1})$$

fi(24) = 8

fi(9) = 6

fi(8) = 4

Назад

Далее

Режим обучения: 3-ий шаг

Нахождение обратного по модулю

В обычной арифметике a^-1 = 1/a, a*(a^-1) = 1, a!= 0.
В модулярной арифметике x называется величиной, обратной a по модулю m, если выполняется сравнение a*x = 1 mod m, при этом (a, m) = 1 (т.е. a и m взаимно просты).
Основные способы нахождения обратных по модулю величин:
1. Подставляя поочередно вместо x значения 1, 2, ..., (m-1), найти решение уравнения (a*x) mod m = 1

x = 4^(-1) mod 9 = 7

2. Если известна функция Эйлера fi(m), то
(a^-1)mod m = a^(fi(m)-1)mod m.

x = 18^(-1) mod 29 = 21

Назад

Далее

Режим обучения: 4-ый шаг

Тахер Эль-Гамаль

Египетский криптограф Тахер Эль-Гамаль родился в 1955 году. Свои первые шаги в криптографии он сделал путем вывода алгоритма Дискретных Квадратичных Логарифмов, который используется для факторизации целых чисел. Стал известен всему миру благодаря разработке «цифровой подписи по схеме Эль-Гамаля» в 1984 году, после этого занимался в основном графикой и разработкой технологии сжатия данных в компании Hewlett-Packard. В 1985 году представил свои разработки по созданию систем асимметричного шифрования и цифровой подписи, эксплуатирующих сложность проблемы дискретного логарифмирования. Предложенная им схема ЭЦП стала основой для алгоритма DSA, принятого Национальным институтом стандартов и технологий США (NIST) в качестве стандарта цифровой подписи. В 1994 году стал активно развивать алгоритм SSL; результатом его работы было заключение договора с Microsoft, что сыграло одну из ключевых ролей в успехе SSL. Тахер Эль-Гамаль также участвовал в создании протокола оплаты по кредитной карте SET, а также ряда схем интернет-платежей.

Назад

Далее

Режим обучения: 5-ый шаг

Описание алгоритма

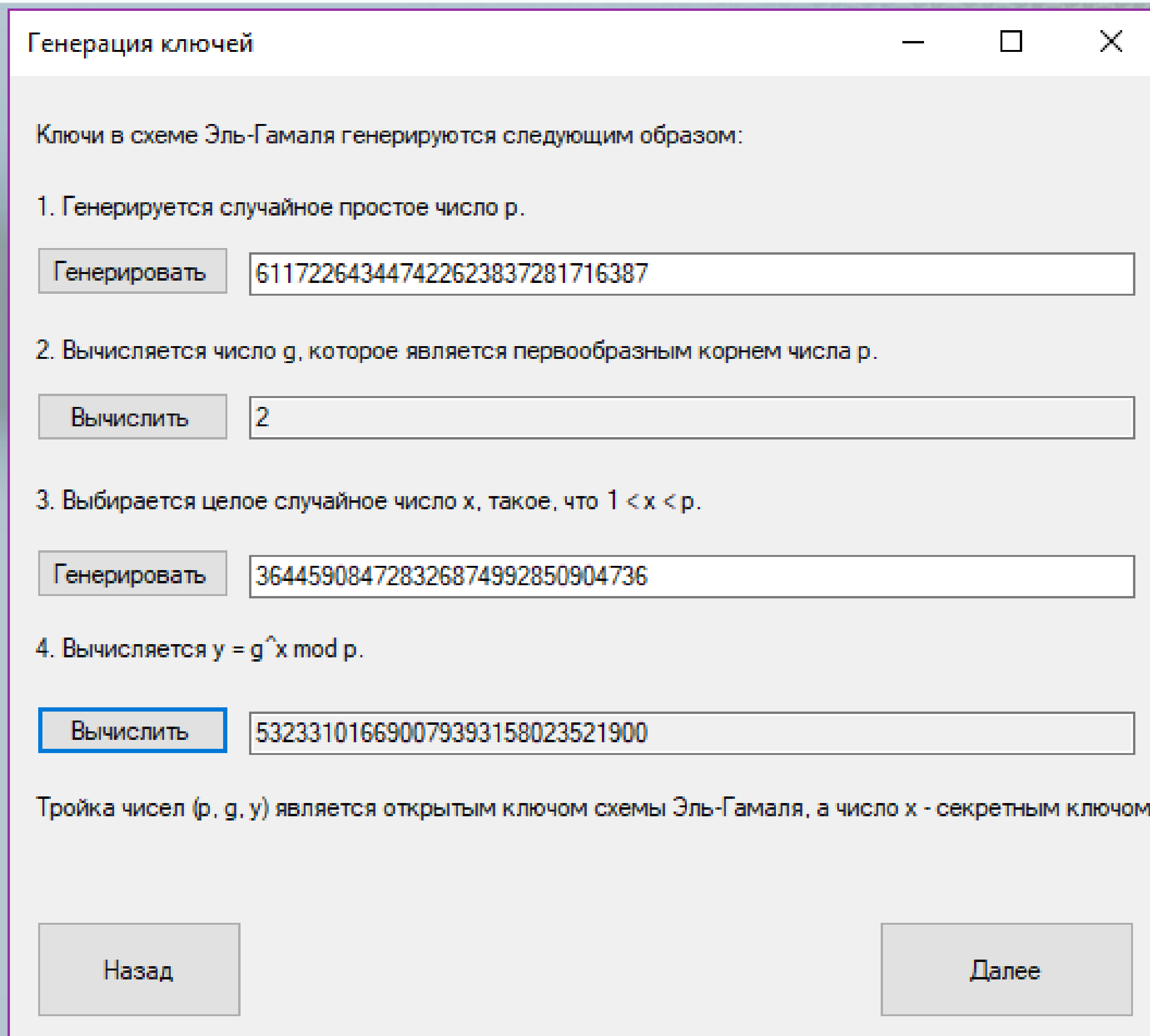
Схема Эль-Гамаля (Elgamal) – криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Криптосистема включает в себя алгоритм шифрования и алгоритм цифровой подписи.
Схема Эль-Гамаля лежит в основе бывших стандартов электронной цифровой подписи в США (DSA) и России (ГОСТ Р 34.10-94).
Схема была предложена Тахером Эль-Гамалем в 1985 году.

В настоящее время криптосистемы с открытым ключом считаются наиболее перспективными. К ним относится и схема Эль-Гамаля, криптостойкость которой основана на вычислительной сложности проблемы дискретного логарифмирования, где по известным p, g и y требуется вычислить x, удовлетворяющий сравнению:
y = g^x (mod p)
ГОСТ Р34.10-1994, принятый в 1994 году в Российской Федерации, регламентировавший процедуры формирования и проверки электронной цифровой подписи, был основан на схеме Эль-Гамаля. С 2001 года использовался новый ГОСТ Р 34.10-2001, использующий арифметику эллиптических кривых, определенных над простыми полями Галуа.
Существует большое количество алгоритмов, основанных на схеме Эль-Гамаля: это алгоритмы DSA, ECDSA, KCDSA, схема Шнорра.

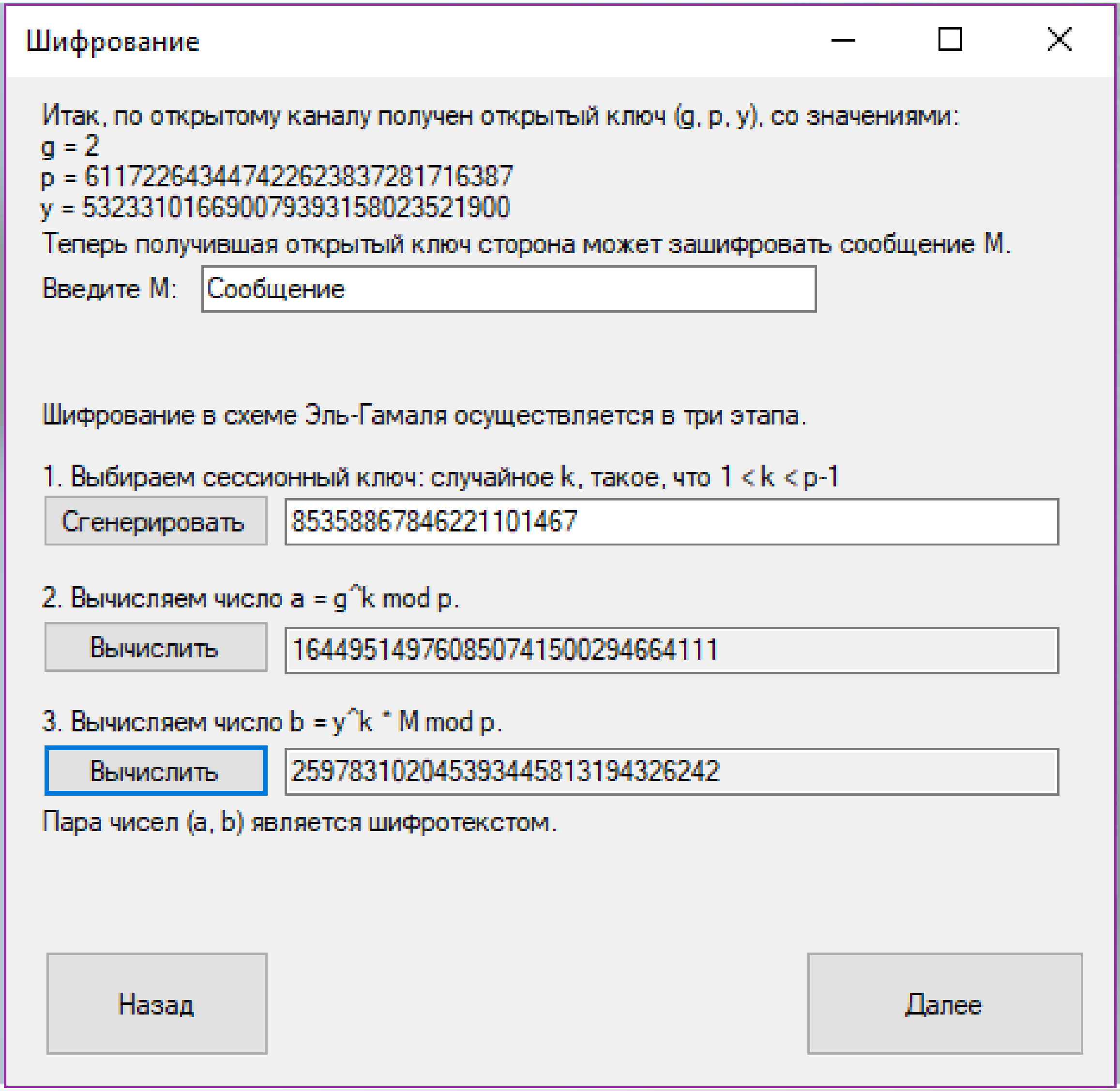
Назад

Далее

Режим обучения: 6-ой шаг



Режим обучения: 7-ой шаг



Режим обучения: 8-ой шаг

Расшифрование

Итак, мы получили шифротекст:
a = 164495149760850741500294664111
b = 259783102045393445813194326242
Также у нас есть открытый ключ:
g = 2
p = 611722643447422623837281716387
y = 532331016690079393158023521900
и секретный ключ
x = 364459084728326874992850904736
Сообщение M можно получить по формуле: M = b*(a^x)^-1 mod p

Вычислить 4241088717127167176401

Или, если перевести в текст: Сообщение

Таким образом, мы провели все этапы шифрования
по схеме Эль-Гамаля.

Назад Далее

Режим обучения: 9-ый шаг

Дискретное логарифмирование

Для дешифрования (криптоанализа) перехваченных сообщений, зашифрованных по криптосистеме Эль-Гамаля, необходимо также перехватить открытый ключ и подобрать секретный ключ x, такой, что g^x mod p = y. Задача вычисления такого числа называется задачей дискретного логарифмирования. В данном случае нам необходимо найти логарифм по основанию g от числа y по модулю p.

Попробуйте найти логарифм по основанию 2 и модулю 5 от числа 1:

Ответ: 4

Логарифм по основанию 5 и модулю 7 от числа 4:

Ответ: 2

Задача дискретного логарифмирования обладает большой вычислительной сложностью и является одной из основных задач, на которых базируется криптография с открытым ключом. На сегодняшний день не существует алгоритмов, позволяющих вычислить дискретный логарифм в конечном поле за полиномиальное время.
Существующие алгоритмы решения этой задачи - такие, как алгоритм Шенкса (он же алгоритм больших и малых шагов), решают задачу за экспоненциальное время.
Одна из теоретических возможностей эффективного решения задачи вычисления дискретного логарифма связана с квантовыми вычислениями.

Назад

Далее

Режим обучения: 10-ый шаг

Алгоритмы решения задачи дискретного ло...

Примерами экспоненциальных алгоритмов дискретного логарифмирования являются такие методы как алгоритм полного перебора, алгоритм Гельфонда-Шенкса и ро-метод Полларда. Сложность алгоритма полного перебора можно оценить в O(p^2) операций, что делает его неприемлемым для криптоанализа даже сравнительно небольших ключей. Для наглядной демонстрации вычислительной трудоёмкости перебора, реализуйте на любом языке программирования алгоритм полного перебора для задачи дискретного логарифмирования и найдите x в следующих задачах:

79560^x = 182693 mod 68831671

Ответ: 61204888

72547^x = 22520254 mod 58656431

Ответ: 14521334

Назад

Далее

Режим обучения: 11-ый шаг

Алгоритм Гельфонда-Шенкса

Алгоритм Гельфонда – Шенкса (алгоритм больших и малых шагов) – детерминированный алгоритм дискретного логарифмирования в мульпликативной группе кольца вычетов по модулю простого числа. Был предложен советским математиком Александром Гельфондом в 1962 году и независимо Дэниэлем Шенксом в 1972 году.

Теоретически упрощает решение задачи дискретного логарифмирования, на вычислительной сложности которой построены многие криптосистемы с открытым ключом.

На предположении о чрезвычайно высокой вычислительной сложности решения задачи дискретного логарифмирования основаны такие криптоалгоритмы как DSA, Elgamal, Diffie-Hellman, ECDSA, ГОСТ Р 34.10-2001, Rabin и другие. В них криптоаналитик может получить закрытый ключ путём взятия дискретного логарифма от открытого ключа и с его помощью преобразовать шифротекст в текст сообщения.

Одним из способов повысить сложность нахождения ключа является создание криптосистемы, основанной на группе с большим порядком (где логарифмирование будет происходить по модулю большого простого числа).

В общем случае такая задача решается полным перебором, данный же алгоритм позволяет в некоторых случаях упростить нахождения показателя степени (уменьшить количество шагов) при вычислении по модулю простого числа, в самом благоприятном случае в квадратный корень раз, но этого сокращения всё равно недостаточно для решения задачи на электронно-вычислительной машине за разумное время.

Александр Осипович Гельфонд

Назад

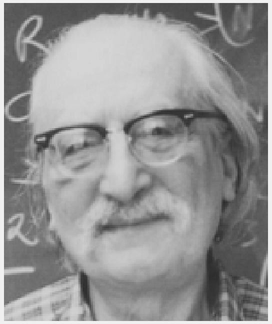
Далее

Режим обучения: 12-ый и 13-ый шаги

Теория алгоритма Гельфонда-Шенкса

Идея алгоритма состоит в выборе оптимального соотношения времени и памяти, а именно в усовершенствованном поиске показателя степени. Задача сводится к нахождению целого числа x, для которого выполняется
α^x = β mod n. (1)

Алгоритм Гельфонда – Шенкса основан на представлении x в виде
x = i · m – j, где m = √n + 1, и переборе 1 ≤ i ≤ m и 0 ≤ j < m. Ограничение на i и j следует из того, что порядок группы не превосходит m, а значит указанные диапазоны достаточны для получения всех возможных x из полуинтервала [0 ; m). Такое представление равносильно равенству
α^im=βα^j
Алгоритм предварительно вычисляет α^im для разных значений i и сохраняет их в структуре данных, позволяющей эффективный поиск, а затем перебирает всевозможные значения j и проверяет, если βα^j соответствует какому-то значению i. Таким образом находятся индексы i и j, которые удовлетворяют соотношению (1) и позволяют вычислить значение x = i * m – j



Дэниэль Шенкс

Назад Далее

Шаги алгоритма Гельфонда-Шенкса

Алгоритм
Вход: α, β, n.

Выход: Число x, удовлетворяющее α^x= β mod n.

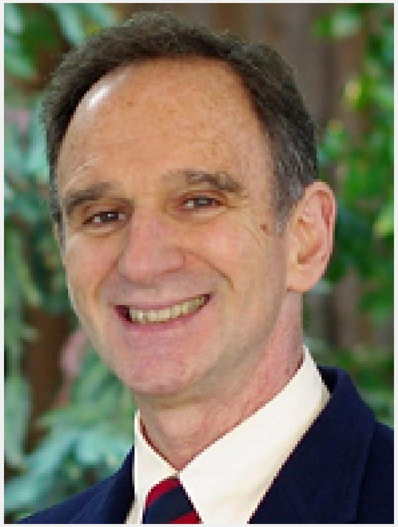
1. m = [√n] + 1
2. Вычислить γ = α^m.
Для i от 0 до m:
    Записать в таблицу (i, γ).
    γ = γ·α^m.
Для любого j где 0 ≤ j < m:
    Проверить, содержится ли βα^j в таблице.
    Если да, вернуть i · m – j.
    Если нет, продолжить выполнение цикла.
    Если цикл завершён и значения не найдено, то такого x не существует.

Назад Далее

Режим обучения: 14-ый шаг

Алгоритм Полига-Хеллмана

Другим субэкспоненциальным алгоритмом дискретного логарифмирования является Алгоритм Полига – Хеллмана (также называемый алгоритм Силвера – Полига – Хеллмана) - детерминированный алгоритм дискретного логирифмирования в кольце вычетов по модулю простого числа. Для модулей специального вида данный алгоритм является полиномиальным. Данный алгоритм был впервые описан американскими математиками Роланом Силвером (Roland Silver), Стефаном Полигом (Stephan Pohlig) и Мартином Хеллманом (Martin Hellman) в 1978 году в статье "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance". Важной особенностью этого метода является то, что для простых чисел специального вида, можно находить дискретный логарифм за полиномиальное время.
Суть алгоритма заключается в том, что для решения сравнения a^x = b mod p можно разложить p на простые множители q_i в степенях α_i, после чего достаточно найти x по модулям q_i ^ α_i для всех i, а затем решение исходного сравнения можно найти с помощью китайской теореме об остатках.
Алгоритм чрезвычайно эффективен если p раскладывается на небольшие простые множители. Это необходимо учитывать в выборе ключей при проектировании криптосистем.



Мартин Хеллман

Назад

Далее

Режим обучения: 15-ый и 16-ый шаги

Частный алгоритм Полига-Хеллмана

Ниже рассмотрен частный случай алгоритма Полига-Хеллмана для групп с простым порядком.

Алгоритм
Ввод: циклическая группа G порядка n = p^e с порождающим элементом g, элемент h из G, и разложение n на простые множители.
Вывод: такое x, что g^x = h mod n.

1. Инициализируем x = 0.
2. Вычисляем y = g^p^(e-1). По теореме Лагранжа, этот элемент имеет порядок p.
3. Для всех k = 0..e-1:
 h = (g^-x * h)^p^(e-1-k).
 Используя любой алгоритм дискретного логарифмирования, найти d, такое что y^d = h.
 Вычисляем x = x + p^k * d.
4. Вернуть x.

Назад | Далее

Общий алгоритм Сильвера-Полига-Хеллмана

Ниже рассмотрен общий алгоритм Полига-Хеллмана для полных групп. Он использует частный алгоритм и китайскую теорему об остатках.

Алгоритм
Ввод: циклическая группа G порядка n = p^e с порождающим элементом g, элемент h из G, и разложение n на r простых множителей p_i в степенях e_i.
Вывод: такое x, что g^x = h mod n.

1. Для всех i = 0..r:
 g_i = g^(n/(p_i ^ e_i))
 h_i = h^(n/(p_i ^ e_i))
 Используя частный случай алгоритма Полига-Хеллмана в группе g_i, вычислить x_i, такой, что g_i^x_i = h_i
2. Решить сравнение x ≡ x_i mod p_i^e_i для всех i ∊ {1, ... , r}
 Китайская теорема об остатках гарантирует существование решения x ∊ {0, ..., n-1}.
4. Вернуть x.

Назад | Далее

Режим обучения: 17-ый шаг

Ро-метод Полларда

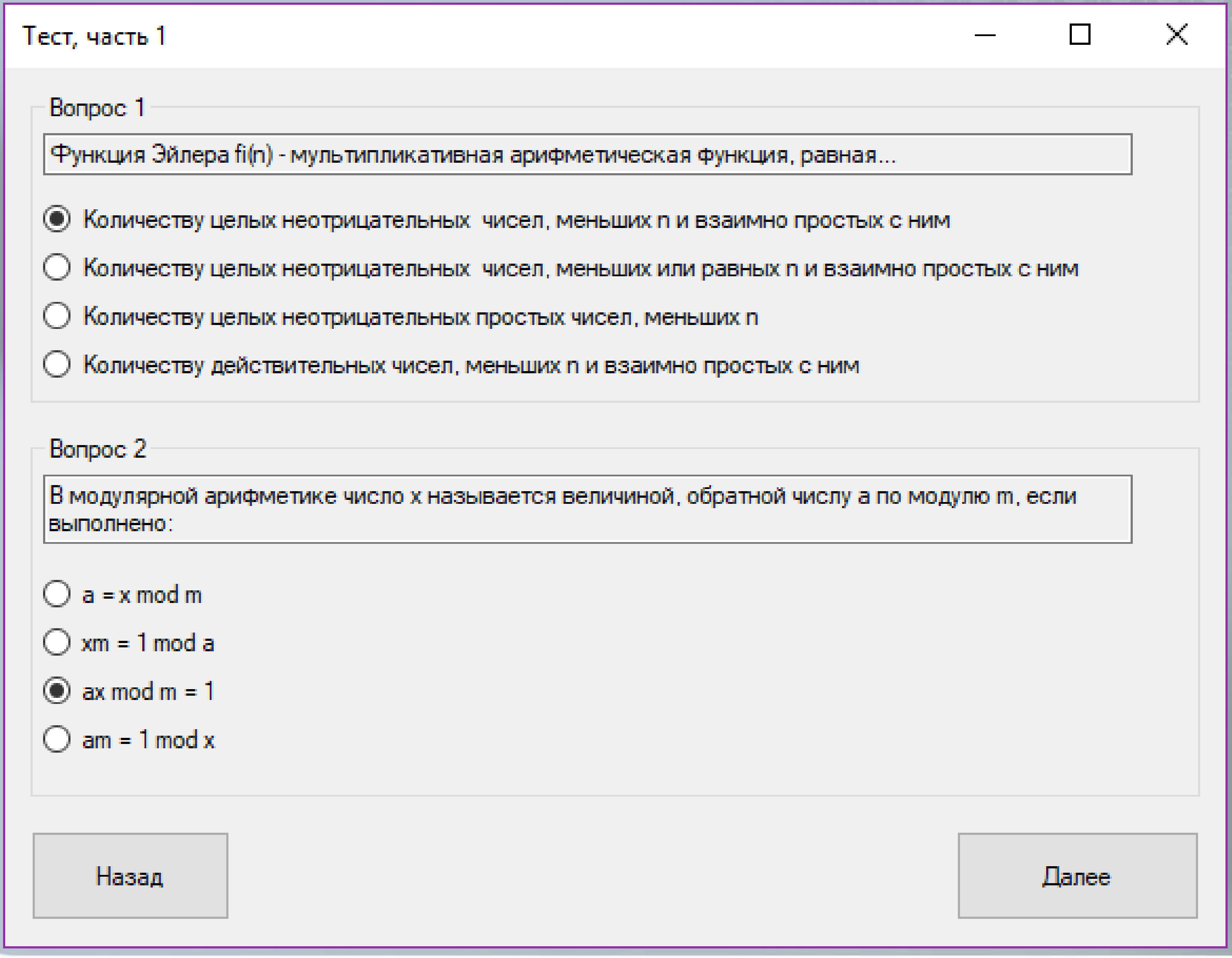
Ещё одним субэкспоненциальным алгоритмом дискретного логарифмирования является ро-метод Полларда для дискретного логарифмирования (Pollard's rho algorithm for logarithms) – алгоритм дискретного логарифмирования в кольце вычетов по простому модулю, имеющий субэкспоненциальную сложность. Предложен британским математиком Джоном Поллардом (англ. John Pollard) в 1978 году, основные идеи алгоритма очень похожи на идеи ро-алгоритма Полларда для факторизации чисел.
Данный метод рассматривается для группы ненулевых вычетов по модулю p, где p – простое число, большее 3.
Преимуществом алгоритма является фиксированный объём потребляемой памяти: между шагами поиска решения алгоритм не требует сохранения промежуточных результатов.
Ограничением алгоритма является то, что для его корректной работы порядок циклической группы элементов, порождённой основанием дискретного логарифма, должен быть простым.

Джон М. Поллард

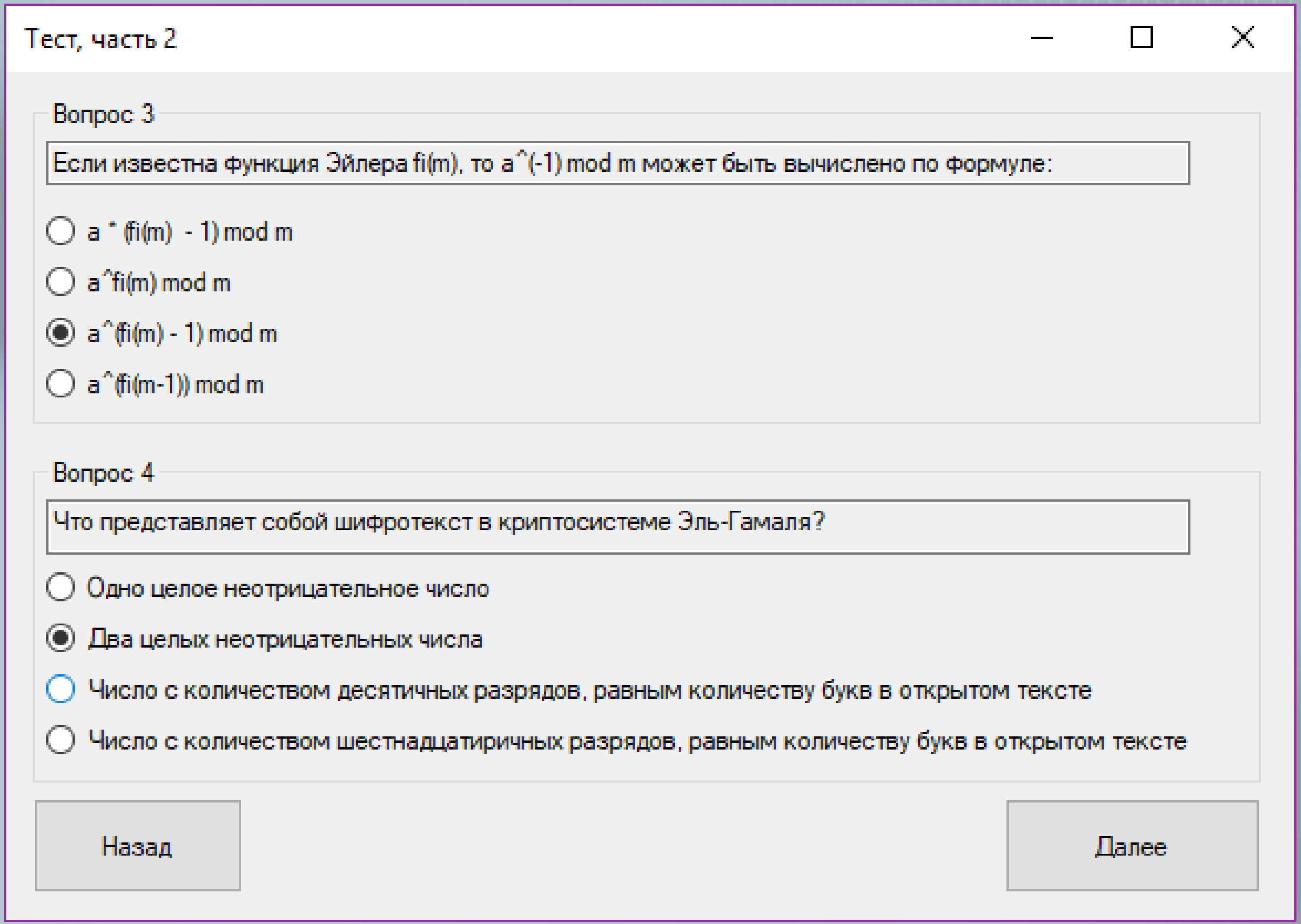
Назад

Далее

Режим обучения: Тест



Режим обучения: Тест



Режим обучения: Тест

Тест, часть 3

Вопрос 5

На какой вычислтельной проблеме основана криптостойкость схемы Эль-Гамаля?

- ( ) На сложности факторизации больших чисел
- ( ) На сложности вычисления первообразных корней в конечном поле
- ( ) На сложности вычисления дискретного логарифма в группе точек эллиптической кривой
- (•) На сложности вычисления дискретного логарифма в конечном поле

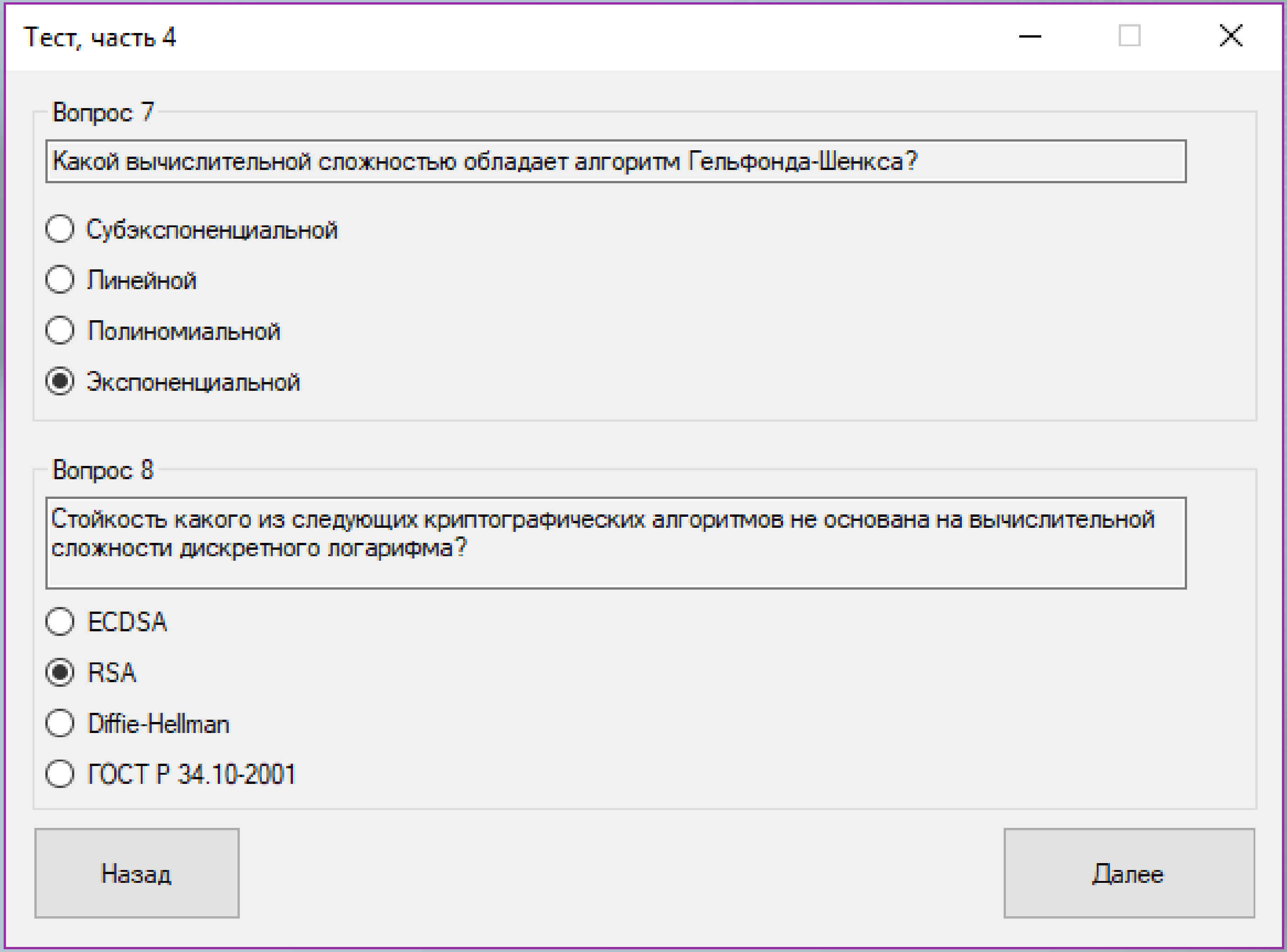
Вопрос 6

Для натурального числа n функция Эйлера может быть вычислена по формуле:

- ( ) $\varphi(\prod_{i=1}^{n-1} p_i^{k_i}) = \prod_{i=1}^{n-1}(p_i^{k_i} - p_i^{k_i-1})$
- ( ) $\varphi(\prod_{i=1}^{n} p_i^{k_i}) = \prod_{i=1}^{n}(p_i^{k_i} - p_i^{k_i+1})$
- ( ) $\varphi(\prod_{i=1}^{n} p_i^{k_i}) = \prod_{i=1}^{n}(p_i^{k_i} + p_i^{k_i-1})$
- (•) $\varphi(\prod_{i=1}^{n} p_i^{k_i}) = \prod_{i=1}^{n}(p_i^{k_i} - p_i^{k_i-1})$

Назад | Далее

Режим обучения: Тест



Режим обучения: Тест

Тест, часть 5

Вопрос 9

Какой из приведённых алгоритмов дискретного логарифмирования применим только для групп с порядком специального вида?

- ( ) Алгоритм Сильвера-Полига-Хеллмана
- (•) Ро-метод Полларда
- ( ) Алгоритм Гельфонда-Шенкса
- ( ) Ни один

Вопрос 10

Какой из следующих алгоритмов дискретного логарифмирования обладает полиномиальной сложностью в общем случае?

- ( ) Алгоритм Сильвера-Полига-Хеллмана
- ( ) Ро-метод Полларда
- ( ) Алгоритм Гельфонда-Шенкса
- (•) Ни один

Назад

Далее

Результаты ответов

Результаты

Задание 1: возведение в степень по модулю
- №1: Верно
- №2: Верно
- №3: Верно

Задание 2: вычисление функции Эйлера
- №1: Верно
- №2: Верно
- №3: Верно

Задание 3: нахождение обратного элемента по модулю
- №1: Верно
- №2: Верно

Задание 4: нахождение дискретного логарифма
- №1: Верно
- №2: Верно

Задание 5: алгоритмическое вычисление дискретного логарифма
- №1: Верно
- №2: Верно

Тест:

№1: Верно	№3: Верно	№5: Верно	№7: Верно	№9:Верно
№2: Верно	№4: Верно	№6: Верно	№8: Верно	№10:Верно

Итоговая оценка: 5

Готово!

Особенности программы

- Открытый исходный код
- Наглядность обучения
- Наличие системы проверки полученных знаний
- Наличие большого количества дополнительных функций
- Обучение не только принципам работы криптосистемы, но и базовым принципам её криптоанализа

Библиография

- Воронков Б. Н. Криптографические методы защиты информации: учебное пособие / Б. Н. Воронков. – Воронеж: Издательско-полиграфический центр Воронежского государственного университета, 2008. – 59 с.
- Схема Эль-Гамаля / Википедия [текст]. – (URL: https://ru.wikipedia.org/wiki/Схема_Эль-Гамаля) (дата обращения 13.05.2018).
- Воронков Б. Н. Обучающая компьютерная программа для изучения Российского стандарта криптографического преобразования / Б. Н. Воронков, И. И. Проскурин // Современные информационные технологии и ИТ-образование. Сборник избранных трудов 6-ой международной НПК (г. Москва, 12 – 14 декабря 2011 г.). – Москва: ИНТУИТ.РУ, 2011. – С. 121 – 127.
- Ковун В. А. Криптоанализ в обучающей программе El-Gamal_Tutor / В. А. Ковун, Б. Н. Воронков // Информатика: проблемы, методология, технологии: сборник материалов XVIII международной научно-методической конференции, г. Воронеж, 8 – 9 февраля 2018 г.: в 7-ти томах. – Воронеж: Издательство «Научно-исследовательские публикации» (ООО «Вэлборн»), 2018. – Т. 7. – С. 194 – 198.
- Ковун В. А. Алгоритм Эль-Гамаля. Лабораторная работа / В. А. Ковун, Б. Н. Воронков // Математика, информационные технологии, приложения: сборник трудов Межвузовский научной конференции молодых ученых и студентов, 23 апреля 2018 г. – Воронеж: Издательство «Научно-исследовательские публикации», 2018 – С. 46 – 60.

Спасибо за внимание !