**ЛЕКЦИОННЫЕ МАТЕРИАЛЫ**

|  |  |
| --- | --- |
| **Б2.В,ДВ.3.1 « Криптографические методы защиты информации»11504»** | |
| *(наименованиедисциплины (модуля) в соответствии с учебнымпланом)* | |
| Уровень | бакалавриат, специалитет |
|  | *(бакалавриат, магистратура, специалитет)* |
| Формаобучения | очная |
|  | *(очная, очно-заочная, заочная)* |
| Направление(-я)  подготовки | 10.05.02 «Информационнаябезопасность» |
|  | *(код(-ы) и наименование(-я))* |
|  |  |
| Институт | Кибербезопасности и цифровых технологий |
|  | *(полное и краткоенаименование)* |
| Кафедра КБ-8 | Информационное противоборство |
|  | *(полное и краткоенаименованиекафедры, реализующейдисциплину (модуль))* |
| Лектор | ДоцентДедовОлегПетрович |
|  | *(сокращенно – ученаястепень, ученоезвание; полностью – ФИО)* |

|  |  |  |
| --- | --- | --- |
| Используются в даннойредакции с учебногогода | 2020/2021 | |
|  | *(учебныйгодцифрами)* | |
| Проверено и согласовано «\_\_\_\_» \_\_\_\_\_\_\_\_20\_\_\_г. |  |  |
|  | *(подписьдиректораИнститута/Филиала с расшифровкой)* | |

Москва 2020 г.

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
|  | | |  |
|  | | |  |
|  | | | |
| **ЛЕКЦИЯ № 5** | | | |
| подисциплине: | | **Б2.В,ДВ.3.1 « Криптографические методы защиты информации»** | |
|  | | (шифр и наименованиеучебнойдисциплины) | |
| Потеме: | **Вычисление обратных значений. Расширенный алгоритм Евклида -для вычисление обратных значений . Вычисление инверсий с применением Теорем Ферма и Эйлера-Ферма.Афинный шифр.** | | |
|  | (наименованиетемылекции) | | |
|  | | |
|  | | |  |
| МИРЭА – 2020 г. | | | |

Темалекции: Вычисление обратных значений с применением а**лгоритма Евклида, теоремы Ферма и теоремы Эйлера-Ферма.ТестМерсена и тест Ферма. Афинный шифр.**

Учебные и воспитательныецели:

1. Сформировать у студентовпредставление о предмете, изучаемом в рамкахкурса «Математическиеосновыкриптологии».

2. Вычисление обратных значений с применением а**лгоритма Евклида -25 мин. 3.Вычисление обратных значений с применением теоремы Ферма и теоремы Эйлера-Ферма. Сравнительный анализ.- 30 мин.**

**4.Афинный шифр. Тест Мерсена и тест Ферма.-25мин.**

5. Привитьчувствоответственностизабудущуюпрофессию.

**Время:** 2 часа (90 мин.).

Литература:

а) Основная:

1. Рябко Б.Я.,Фионов А.Н. Криптография в современноммире.-М.: Горячаялиния-Телеком, 2018.-300с.:ил.

2. ГорбенкоА.О.,Основыинформационнойбезопасности: введение в профессию.Учебноепособие, СПб: ИЦ «Интермедия», 2016.‒ 224 с.

3. БутаковаН.Г.,Федоров Н.В. Криптографическиеметоды защитыинформации. Учебноепособие, СПб: ИЦ «Интермедия», 2016. ‒ 312 с.

4.Хорев А.А.,Защитаинформацииотутечкипотехническимканалам. Учебник. СПб: ИЦ «Интермедия», 2016. 920 с.

б) Дополнительнаялитература:

1. Зайцев А.П. и др. Техническиесредства и методызащитыинформации. Уч. пособие. М.:Горячаялиния – Телеком. 2009. – 615 с.

2. Романец Ю.В. и др. Защитаинформации в компьютерныхсистемах и сетях. М.:Радио и связь. 1999. – 376 с.

3. Лозовецкий В.В. Информационнаябезопасность. М.: Изд. ИУИ. 2011. – 169 с.

Учебно-материальноеобеспечение:

Наглядныепособия.

Техническиесредстваобучения: проектор.

Приложения: рисунки, таблицы, слайды.

ПЛАН ЛЕКЦИИ:

**Введение**– до 5 мин.

**Основнаячасть** (учебныевопросы) – до 80 мин.

1-й учебныйвопрос:Примененине алгоритма Евклида для вычисления обратных чисел.-30мин.

2-й учебныйвопрос: Вычисление инверсии при применении теоремы Ферма..-15 мин.

3-й учебныйвопрос: Вычисление инверсии с помощью теоремы Эйлера-Ферма -25 мин.

4- учебный вопрос-Афинный шифр-15 мин.

Заключение – до 5 мин.

Введение – до 5 мин.

Методическиерекомендации:

- показатьактуальностьтемы;

- довестицелевуюустановкучерезосновныеположениялекции;

- охарактеризоватьместо и значениеданнойтемы в курсе;

- описатьобстановку, в которойразрабатываласьтеоретическаяпроблема и шлаеепрактическаяреализация;

- датьобзорважнейшихисточников, монографий, литературыпотеме;

- вскрытьособенностиизучениястудентамиматериалапорассматриваемойпроблеме.

Основнаячасть – до 80 мин.

Введение

5\*1\5=1 x\*1\x=1

Для понимания вычисления инверсии рассмотрим пример:

Пусть необходимо вычислить 3(^(-1))mod 26.

Обозначим х=3(^(-1))mod 26.

Умножив обе части данного уравнения на 3 получим

**3х=1(mod 26)**

То есть 3 умноженное на х больше 26 на 1

Отсюда следует, что х=9.

**Инверсия по модулю m**

**Zm\*( 1,2,3,c,……..d,…..m-1)**

Вомногихзадачахкриптографиидлязаданныхчисел с, m требуетсянаходитьтакоечисло d < m, что

cd mod m = 1

Такое d существуеттогда и толькотогда, когдачисла с и m взаимнопростые. Число d, удовлетворяющееравенству cd mod m = 1, называется **инверсией** с **помодулю** m и частообозначается с-1 mod m. Данноеобозначениедляинверсиисвязано с тем, что *равенство* cd mod m = 1 можнопереписать в виде

cс-1mod m = 1.

Такимобразом, *умножение* на с-1 соответствуетделениюна с привычисленияхпомодулю m.

Инверсиюпомодулю m такжеможновычислять с помощьюобобщенногоалгоритмаЕвклида.

Покажем, какэтоделается. *Равенство*, приведенноенижеозначает, чтодлянекоторогоцелого k имеет *место* *равенство* cd – km = 1. Учитывая, что с и d взаимнопросты, можнопреобразоватьэто *равенство* следующимобразом:

m(-k) + cd = НОД(m,c).

Значит, мыможемвычислить с-1 mod m (илинайтичисло d ) с помощьюобобщенногоалгоритмаЕвклида. Приэтом *значение* переменной k наснеинтересует. Есличисло d получаетсяотрицательным, тонужноприбавить к нему m, таккакпоопределениючисло a mod m беретсяиз *множества* {0,1,..., m - 1}.

**Таблица № 7.Умножение a\*bпомодулю 7.(к вычислениюобратныхчисел).**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **a\b** | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
| **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** |
| **1** | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
| **2** | **0** | **2** | **4** | **6** | **1** | **3** | **5** |
| **3** | **0** | **3** | **6** | **2** | **5** | **1** | **4** |
| **4** | **0** | **4** | **1** | **5** | **2** | **6** | **3** |
| **5** | **0** | **5** | **3** | **1** | **6** | **4** | **2** |
| **6** | **0** | **6** | **5** | **4** | **3** | **2** | **1** |

**В таблице № 7 мывидим, чточисло 1 обратно1 ; 2 обратно 4; 3 обратно 5; 4 обратно 2; 5 обратно 3; 6 обратна 6.**

**Такимобразомподелить 3 на 5 эторавносильночисло 3 умножитьна 3**

**3:5= 3\*3=9 , учитывая, что 9=7+2 = 2(mod7). Тоесть 3:5=3\*3=9= 2 (mod7).**

Для модуля 7 все числа (1,2.3.4.5.6)- взаимно простые, то есть

НОД(7,1)=НОД(7,2)=НОД(7,3)=НОД(7,4)=НОД(7,5)=НОД(7,6)=1

Для m=10 существуют только 4 числа 1существуют только 4 числа 1,3,7,9 у которых есть обратное число .

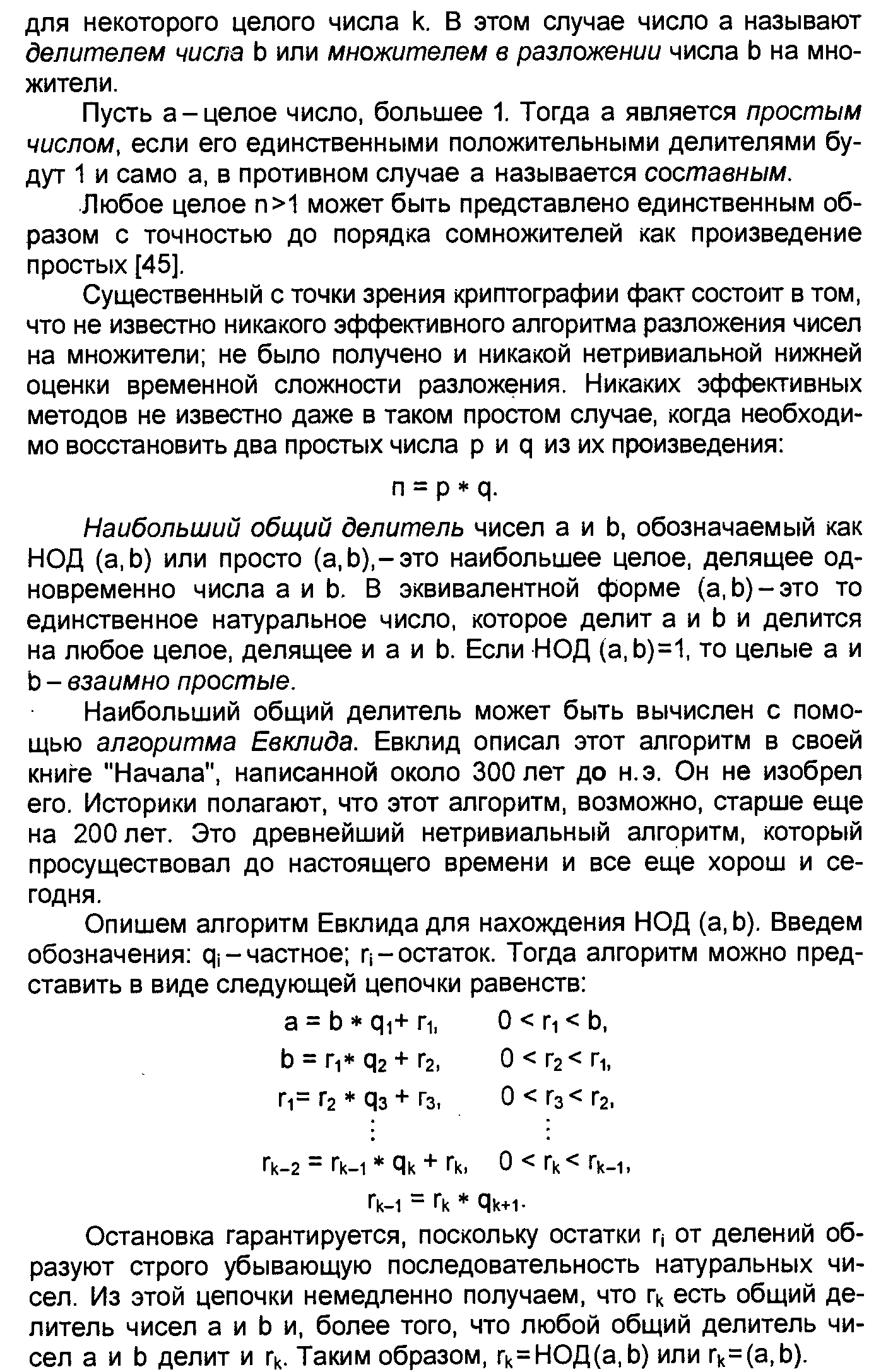
Общее у этих чисел:

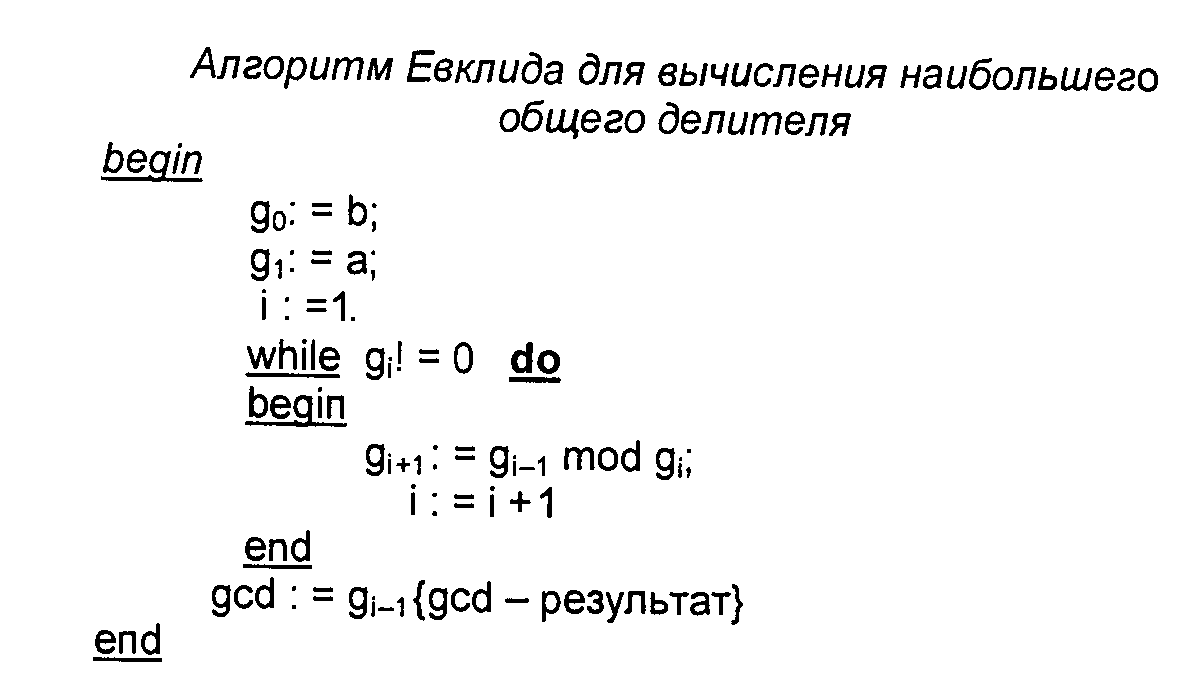
НОД(10,1)=НОД(10,3)=НОД(10,7)=НОД(10,9)=1

Алгоритм Евклида.

Целое число а делит без остатка другое целое число b, если , и только если

b = к\* a





ПримерыцифровойреализацииАлгоритмаЕвклида

**АлгоритмЕвклида** основаннаследующихдвухпростыхпримерах: 1. НОД (a, 0) = a;2. НОД (a, b) = НОД (b, r), где r — остатокотделения a на b

Первыйговорит, чтоесливтороецелоечисло — 0, то наибольшийобщийделительравенпервомучислу. Второйпозволяетнамизменятьзначение a на b, пока b нестанет 0. Например, вычисляя НОД (36, 10), мыможемиспользоватьвторойнесколькораз и одинразпервый, какпоказанониже.

НОД(36,10) = НОД(10,6) = НОД(6,4) = НОД(4,2) = НОД(2,0)

Другимисловами, НОД (36, 10) = 2, НОД (10, 6) = 2, и такдалее. Этоозначает, чтовместовычисления НОД (36, 10) мыможемнайти НОД (2, 0).

На[рис.](#image.2.7) 2.1 показанареализацияэтихпримероввычисления  НОД (a, b).

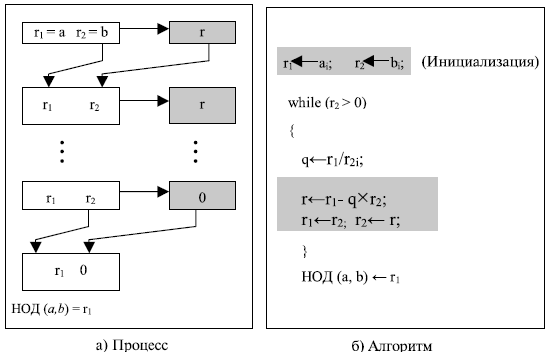


Рис. 2.1. АлгоритмЕвклидадлявычисления НОД (а, b)

Дляопределения НОД используютсядвепеременные, r1 и r2,чтобызапоминатьизменяющиесязначения в течениевсегопроцесса. Ониимеютначальноезначение a и b. Накаждомшагевычисляеетсяостатокотделения r1 на r2, хранится в видепеременной r. Потом r1, заменяетсяна r2 и r2 на r и расчётпродолжается, пока r нестанетравным 0. В этотмоментпроцессостанавливается и НОД (a, b) равен r1.

**Пример 1**

Нужнонайтинаибольшийобщийделитель 2740 и 1760.

**Решение**

Применимвышеупомянутуюпроцедуру, используятаблицу. Мыприсваиваемначальноезначение r1 2740 и r2 значение 1760. В таблицетакжепоказанызначения q накаждомшаге. Мыимеем НОД (2740, 1760) = 20.

|  |  |  |  |
| --- | --- | --- | --- |
| **q** | **r1** | **r2** | **r** |
| 1 | 2740 | 1760 | 980 |
| 1 | 1760 | 980 | 780 |
| 1 | 980 | 780 | 200 |
| 3 | 780 | 200 | 180 |
| 1 | 200 | 180 | 20 |
| 9 | 180 | 20 | 0 |
|  | 20 | 0 |  |

**Пример2**

Найтинаибольшийобщийделитель 25 и 60.

**Решение**

Этотконкретныйпримерпоказывает, чтодляалгоритмаЕвклидабезразлично, еслипервоечисломеньше, чемвторое. Всеравномыполучаемправильныйответ НОД (25, 60) = 5.

|  |  |  |  |
| --- | --- | --- | --- |
| **q** | **r1** | **r2** | **R** |
| 0 | 25 | 60 | 25 |
| 2 | 60 | 25 | 10 |
| 2 | 25 | 10 | 5 |
| 2 | 10 | 5 | 0 |
|  | 5 | 0 |  |

Пример 3. Применяя РАЕ найдем НОД чисел 1365и 77

( a) ( b) ( r) ( a) ( b) ( r)

1365:77=17(остаток 56) -------1365=17\*77+56

77:56=1 (остаток21) ------------77=1\*56 +21

56:21=2 (остаток 14) -------------56=2\*21 +14

21:14=1 ( остаток 7) --------------21=1\*14 +7

14:7= 2 ( остаток 0)---------------14= 2\*7 +0 НОД = 7

|  |  |  |  |
| --- | --- | --- | --- |
| q | a | b | r |
| 17 | 1365 | 77 | 56 |
| 1 | 77 | 56 | 21 |
| 2 | 56 | 21 | 14 |
| 1 | 21 | 14 | 7 |
| 2 | 14 | 7 | 0 |
|  | 7 | 0 |  |

Вычислим73-[[1]](#footnote-1)помодулю 1001, используя РАЕ(вариант № 1)

1001= 13\*73 + 52

73= 1\*52 + 21

52=2\*21 +10

21= 2\*10 +1

10=1\*10 +0 тоесть 73 и 1001 взаимнопростые.

Перенесемчлены в этихтождествахтакчтобыостаткиостались в правыхчастях

1001-13\*73 = 52 (1)

73-1\*52 =21 (2)

52-2\*21 =10 (3)

21-2\*10 =1 (4)

Подставимправуючасть = 10 извыражения (3) в (4)

21- 2\*(52-2\*21) = 21-2\*52+4\*21=1 (5)

**В** (5) сгруппируемслагаемые

5\*21- 2\*52 =1 (6)

Значениечисла 21 возьмемизправойчастиуравнения (2) подставим в выражение (6)

5\*(73-1\*52)-2\*52 =1 Раскрываяскобкиполучим 5\*73 -7\*52 = 1 (7)

Подставив 52 из (1) в (7) получим

5\*73- 7( 1001-13\*73) = 1 раскроемскобки

5\*73- 7\*1001+ 91\*73 =1 (8)

Сгруппируемслагаемые и получим

96\*73= 1 +7\*1001

Этозначает ,что 96 и естьобратныйэлемент к 73.

Пример 4.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Нод (161,28) | | | |  |
|  | q | r1 | r2 | r |
| 1 | 5 | 161 | 28 | 21 |
| 2 | 1 | 28 | 21 | 7 |
| 3 | 3 | 21 | 7 | 0 |
|  |  | 7 | 0 |  |

**Расширенный алгоритм Евклида - Sa + tb= НОД(а,b)**

**Sa + tb= НОД(а,b) a=161 , b= 28**

**s=s1-q\*s2, s1=1,s2=0. t=t1-q\*t2 t1=0, t2=1.**

**Пример 5.**

**Вычислить НОД( 161, 28) иs1, t1.**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **q** | **r1** | **r2** | **r** | **s1** | **s2** | **s** | **t1** | **t2** | **t** |
| **1** | **5** | **161** | **28** | **21** | **1** | **0** | **1** | **0** | **1** | **-5** |
| **2** | **1** | **28** | **21** | **7** | **0** | **1** | **-1** | **1** | **-5** | **6** |
| **3** | **3** | **21** | **7** | **0** | **1** | **-1** | **4** | **-5** | **6** | **-23** |
|  |  | **7** | **0** |  | **-1** |  |  | **6** |  |  |

**Проверка:**

**(-1)\*161 +6\* 28 = 7.**

**Пример 6.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Нод(2740, 1760)** | | | | |
|  | | **q** | **r1** | **r2** |  |
| **1** | | **1** | **2740** | **1760** | 980 |
| **2** | | **1** | **1760** | **980** | 780 |
| **3** | | **1** | **980** | **780** | 200 |
| **4** | | **3** | **780** | **200** | 180 |
| **5** | | **1** | **200** | **180** | 20 |
| **6** | | **9** | **180** | **20** | 0 |
|  | |  | **20** | **r2** |  |

**Пример 7. (73-1)**

**Вычисление обратных значений с помощью алгоритма Евклида**

**При а=nполучаем ,Sn=0 и следовательно bt= НОД (n,b).(вариант №2)73-1 =96 по модулю 1001**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **q** | **r1** | **r2** | **r** | **t1** | **t2** | **t** |
| **1** | **13** | **1001** | **73** | **52** | **0** | **1** | **-13** |
| **2** | **1** | **73** | **52** | **21** | **1** | **-13** | **14** |
| **3** | **2** | **52** | **21** | **10** | **-13** | **14** | **-41** |
| **4** | **2** | **21** | **10** | **1** | **14** | **-41** | **96** |
| **5** | **10** | **10** | **1** | **0** | **-41** | **96** | **-1001** |
|  |  | **1** |  |  | **96** |  |  |

73\*96= 7008 7008:1001=7 +1(в остатке)

73-1 =96 по модулю 1001

2. Вычисление обратных значений с помощью теоремы Ферма.

Давайте вспомним теоремы Ферма и Эйлера –Ферма, а потом рассмотрим как можно использовать данные теоремы для вычисления обратных значений. Мы разбирали данные теоремы в предыдущих лекциях, но не выделяли как можно с помощью данных теоремвычислять обратные значения.

**Малая теорема Ферма** играет очень важную роль в теории чисел и криптографии. Ниже мы приводим две версии теоремы.

**Первая версия**

Первая версия говорит, что если **p** — простое число и **a**— целое число, такое, что p не является делителем a, {a^{p - 1}} \equiv 1{\text{ }}\bmod {\text{ }}pтогда .

Умножив обе части даного уравнения на а ((^-1)) получим

**ap-2 = a-1 mod p**

a((^-1)) mod p, тоесть**a-1mod p = ap-2 mod p.**

**Приложение( изложенный ниже материал рассмотрен в предыдущей лекции)**

**Вторая версия**

Вторая версия вводит ограничивающие условие на a. Она утверждает, что если p — простое число и a — целое число, то {a^p} \equiv a{\text{ }}\bmod {\text{ }}p.

**Возведение в степень.**Малая теорема Ферма иногда полезна для того, чтобы быстро найти решение при возведении в степень. Следующие примеры показывают это.

**Пример 7.12**

Найдите результат 610 mod 11.

**Решение**

Мы имеем {6^{10}}{\text{ }}\bmod {\text{ }}11 \equiv 1. Это первая версия малой *теоремы Ферма*, где p = 11.

**Пример 7.13**

Найдите результат 312 mod 11.

**Решение**

Здесь степень (12) и модуль (11) не соответствуют условиям *теоремы Ферма*. Но, применяя преобразования, мы можем привести решение к использованию малой *теоремы Ферма*.

{3^{12}}\bmod {\text{ }}11 \equiv ({3^{11}} \times 3)\bmod {\text{ }}11 \equiv ({3^{11}}\bmod {\text{ }}11)(3{\text{ }}\bmod {\text{ }}11) \equiv (3 \times 3)\bmod {\text{ }}11 = 9

**Мультипликативные инверсии.**Очень интересное приложение теорема Ферма находит для некоторых мультипликативных *инверсий*, если модуль — простое число. Если **p** — простое число и **a** — целое число, такое, что p не является его делителем, **тогда a-1mod p = ap-2 mod p. Это может быть легко доказано, если мы умножим обе стороны равенства на a и используем первую версию малой *теоремы Ферма*.**

Это приложение позволяет не использовать расширенный *алгоритм Евклида* для нахождения мультипликативных *инверсий*.

**Пример 7.14**

*Инверсии* по модулю простого числа могут быть найдены, без использования расширенного Евклидова алгоритма:

1. **8-1 mod 17 = 817-2 mod 17 = 815 mod 17 = 15 mod 17**

**8\*8\*8=512; 512 mod 17=2; 2\*2\*2\*2\*2=15mod17.**

1. **5 –1 mod 23 = 523-2 mod 23 = 521 mod 23 = 14 mod 23**

**5\*5\*5=125 mod23=10. 1000mod23=11. 121mod23=6. 60mod23=14.**

**c. 60101 mod 101 = 60101-2 mod 101 = 6099 mod 101 = 32 mod 101**

**d. 22 -1 mod 211 = 22 211-2 modа 211 = 22209 mod 211 = 48 mod 211**

Давайте вычислим примеры a и b с помощью алгоритма Евклида:

а). На первом этапе в ячейку r1 записываем значение -17, а в ячейку r2 -8, в t1-0, в t2-1, а далее начинаем вычислять q=r1\r2, r= r1-q\*r2 , t=t1-q\*r2 .

На втором этапе производим сдвиг значение r2 в r1, t2 в t1 , t в t2 и продолжаем производить вычисления как и на первом этапе и тд. Пока значение в ячейке r станет равным нулю

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| q | R1 | R2 | r | T1 | T2 | t |
| 2 | 17 | 8 | 1 | 0 | 1 | -2 |
| 8 | 8 | 1 | 0 | 1 | -2 | 17 |
|  | 1 |  |  | -2 |  |  |

Таким образом, мы видим, что НОД(17,8)=1, а обратное значение будет равно (-2)+17=15.

b).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| q | R1 | R2 | r | T1 | T2 | t |
| 4 | 23 | 5 | 3 | 0 | 1 | -4 |
| 1 | 5 | 3 | 2 | 1 | -4 | 5 |
| 1 | 3 | 2 | 1 | -4 | 5 | -9 |
| 2 | 2 | 1 | 0 | 5 | -9 | 23 |
|  | 1 |  |  | -9 |  |  |

Так как результат отрицательный, то прибавив модуль получим +14.

3.Вычисление обратных значений с помощью теоремы Эйлера-Ферма.

**Мультипликативные инверсии.***Теорема Эйлера* может использоваться, чтобы найти мультипликативную *инверсию* по простому модулю. *Теорема Эйлера* может применяться, чтобы найти мультипликативные *инверсии* по составному модулю. Если **n** и **a** – взаимно простые, то {a^{ - 1}}\bmod n = {a^{\varphi (n) - 1}}\bmod n. Это может быть легко доказано умножением обеих сторон равенства на a.


a^{-1} \mod\ n = a \times  a^{\varphi (n)-1} \mod\ n = a^{\varphi (n)} \mod\ n = 1 \mod\ n 

**Пример 7.17**

Мультипликативная инверсия по составному модулю может быть найдена без использования расширенного евклидова алгоритма, если мы знаем разложение на множители *составного объекта*:

1. {8^{ - 1}}\bmod 77 = {8^{\varphi (77) - 1}}\bmod 77 = {8^{59}}\bmod 77 = 29\bmod 77

8\*8\*8=512; 512 mod77=50; 2500 mod77=36; 36\*36 mod77=64; 64\*64mod77=15;

225\*64 mod 77=1; 50\*36 mod 77=29.

b. {7^{ - 1}}\bmod 15 = {7^{\varphi (15) - 1}}\bmod 15 = {7^{7}}\bmod 15 = 13\bmod 15

7\*7\*7=343 mod15=13. 13\*13=169 mod15= 4. 4\*7=28 mod15=13.

c. {6^{ - 1}}\bmod 187 = {7^{\varphi (187) - 1}}\bmod 187 = {60^{159}}\bmod 187 = 53\bmod 187

d. {71^{ - 1}}\bmod 100 = {71^{\varphi (100) - 1}}\bmod 100 = {71^{39}}\bmod 100 = 31\bmod 100

**Рассмотрим пример а и проведем вычисление с помощью алгоритма Евклида:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| q | R1 | R2 | r | T1 | T2 | t |
| 9 | 77 | 8 | 5 | 0 | 1 | -9 |
| 1 | 8 | 5 | 3 | 1 | -9 | 10 |
| 1 | 5 | 3 | 2 | -9 | 10 | -19 |
| 1 | 3 | 2 | 1 | 10 | -19 | 29 |
| 2 | 2 | 1 | 0 | -19 | 29 | -77 |
|  |  | 1 |  | 29 |  |  |

**Так же можно вычислить и остальные примеры b, c,d.**

**Таким образом вычисление обратных значений(инверсий)возможно различными методами, но при вычислении Примера №7 с помощью Теорем Ферма, Эйлера-Ферма могут возникнуть значительные временные затруднения.**

**Генерация простых чисел**

Два математика, Мерсенна и Ферма, попытались получить формулу, которая могла бы генерировать простые числа.

**Простые числа Мерсенны**

Мерсенна предложил следующую формулу, которую называют **номера Мерсенны.**Он предполагал, что формула перечисляет все простые числа.

**M**p**= 2**p**–1**

Если p в приведенной выше формуле — простое число, то, как предполагали, Mp должно быть простым числом. Годы спустя было доказано, что не все числа, полученные по формуле Мерсенны, — простые числа. Ниже приведен список некоторых номеров Мерсенны.

\tt\parindent0pt

$M_{2} = 2^{2} – 1 = 3$

$M_{3} = 2^{3} – 1 = 7$

$M_{5} = 2^{5} – 1 = 31$

$M_{7} = 2^{7} – 1 = 127$

$M_{11} = 2^{11} – 1 = 2047$     Непростое число ($2047 = 23 \times  89$)

$M_{13} = 2^{13} – 1 = 8191$

$M_{17} = 2^{17} – 1 = 131071$ 

Оказалось, что M11 — не простое число. Однако было найдено, что 41 число по формуле Мерсенны — простые; одно из последних найденных чисел Мерсенны — М124036583, наибольшее число содержит 7 253 733 цифр. Поиск продолжается.

Ферма пробовал найти формулу, которая генерирует простые числа. Следующая формула — для **чисел Ферма:**

**Простые числа Ферма**

Ферма попытался найти формулу для генерации простых чисел. Он предложил следующую формулу, которая теперь называется формулой Ферма, и проверил номера от F0 (n=0,1,…) до F4, но оказалось, что уже F4 — не простое число.

{F_n} = {2^{{2^n}}} + 1

F0 = 3

F1 = 17

F2 = 257

F3 = 65537

F_{4} = 4294967297 =  641 \times  6700417. Не простое число

Фактически было доказано, что многие номера до F24 — составные числа

**Аффинный шифр.**

**Аффинный шифр**— это частный случай более общего моноалфавитного [шифра подстановки](https://ru.wikipedia.org/wiki/Шифр_подстановки). К [шифрам подстановки](https://ru.wikipedia.org/wiki/Шифр_подстановки) относятся также [шифр Цезаря](https://ru.wikipedia.org/wiki/Шифр_Цезаря), [ROT13](https://ru.wikipedia.org/wiki/ROT13) и [Атбаш](https://ru.wikipedia.org/wiki/Атбаш). Поскольку аффинный [шифр](https://ru.wikipedia.org/wiki/Шифр) легко дешифровать, он обладает слабыми [криптографическими](https://ru.wikipedia.org/wiki/Криптография) свойствами

В аффинном шифре каждой букве алфавита размера m ставится в соответствие число из диапазона { 0..m-1}0..m-1. Затем при помощи [модульной арифметики](https://ru.wikipedia.org/wiki/Модульная_арифметика) для каждого числа, соответствующего букве исходного алфавита, вычисляется новое число, которое заменит старое в шифротексте.

Функция [шифрования](https://ru.wikipedia.org/wiki/Шифрование)[[2]](#cite_note-multiple01-2) для каждой буквы

**E(x)= (aх+b) modm**, где m-размер алфавита, a, b -ключ, **a и m- взаимнопростые числа**.

Функция рас[шифрования](https://ru.wikipedia.org/wiki/Шифрование)[[2]](#cite_note-multiple01-2) для каждой буквы

**D(x)=a(^(-1))((E(x)-b) modm = xmodm**, где

1= a(^(-1))\*a.

Примеры шифрования и расшифрования.

В следующих примерах используются латинские буквы от A до Z, соответствующие им численные значения приведены в таблице.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

**Шифрование**.

В этом примере необходимо зашифровать сообщение "ATTACK AT DAWN", используя упомянутое выше соответствие между буквами и числами, и значения a=3 , b=4a=3,b=4, так как в используемом алфавите 26 букв. Только на число a=3 aaaaf наложены ограничения, так как оно должно быть взаимно простым с 26. Возможные значения a:**1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 и 25**[]](#cite_note-multiple02-3). Значение b может быть любым, только если a не равно единице, так как это сдвиг шифра. Итак, для нашего примера функция шифрования y=E(x)=(3x+4)mod {26}. Первый шаг шифрования — запись чисел, соответствующих каждой букве сообщения.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| сообщение | A | T | T | А | C | K | A | T | D | A | W | N |
| xx | 0 | 19 | 19 | 0 | 2 | 10 | 0 | 19 | 3 | 0 | 22 | 13 |

Теперь, для каждого значения x x найдем значение  **(3x+4)} 3x+4**. После нахождения значения (3x+4) для каждого символа возьмем остаток от деления (3x+4) на 26. Следующая таблица показывает первые четыре шага процесса шифрования.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| сообщение | A | T | T | А | C | K | A | T | D | A | W | N |
| xx | 0 | 19 | 19 | 0 | 2 | 10 | 0 | 19 | 3 | 0 | 22 | 13 |
| 3x+43x+4 | 4 | 61 | 61 | 4 | 10 | 34 | 4 | 61 | 13 | 4 | 70 | 43 |
| (3x+4)mod26 (3x+4)mod {26} | 4 | 9 | 9 | 4 | 10 | 8 | 4 | 9 | 13 | 4 | 18 | 17 |

Последний шаг процесса шифрования заключается в подстановке вместо каждого числа соответствующей ему буквы. В этом примере шифротекст будет "EJJEKIEJNESR". Таблица ниже показывает все шаги по шифрованию сообщения аффинным шифром.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| сообщение | A | T | T | А | C | K | A | T | D | A | W | N |
| xx | 0 | 19 | 19 | 0 | 2 | 10 | 0 | 19 | 3 | 0 | 22 | 13 |
| 3x+43x+4 | 4 | 61 | 61 | 4 | 10 | 34 | 4 | 61 | 13 | 4 | 70 | 43 |
| (3x+4)mod (26)(3x+4)mod26 | 4 | 9 | 9 | 4 | 10 | 8 | 4 | 9 | 13 | 4 | 18 | 17 |
| шифротекст | E | J | J | E | K | I | E | J | N | E | S | R |

**Расшифрование**

Для расшифрования возьмем шифротекст из примера с шифрованием. Заменим букву х на букву у – для лучшего понимания методики расшифрования.Функциярасшифрования будет D(y){\displaystyle b=4}a(^(-1))(y+m- b) {\displaystyle m=26}.D(y)=a^{-1}(y+m-b) mod m , где a=9, b=4 a^{-1}=9, b=4, m=26.(+ m –для ухода от отрицательных чисел).

Замечание: если каждая y больше или равно b y больше чем b , то функция расшифрование принимает вид D(y){\displaystyle b=4}a(^(-1))(y-b)  D(y)=a^{-1}(y-b)mod m.

Точно так же, как и в обозреваемом примере, но разберём общий вариант.

Для начала запишем численные значения для каждой буквы шифротекста, как показано в таблице ниже.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| шифротекст | E | J | J | E | K | I | E | J | N | E | S | R |
| yy | 4 | 9 | 9 | 4 | 10 | 8 | 4 | 9 | 13 | 4 | 18 | 17 |

Теперь для каждого y необходимо рассчитать 9(y+m-4) и взять остаток от деления этого числа на 26. Следующая таблица показывает результат этих вычислений.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| шифротекст | E | J | J | E | K | I | E | J | N | E | S | R |
| yy | 4 | 9 | 9 | 4 | 10 | 8 | 4 | 9 | 13 | 4 | 18 | 17 |
| 9(y+26-4)9\*(y+26-4) | 234 | 279 | 279 | 234 | 288 | 270 | 234 | 279 | 315 | 234 | 360 | 351 |
| 9(y+26-4)mod269(y+26-4)mod (26) | 0 | 19 | 19 | 0 | 2 | 10 | 0 | 19 | 3 | 0 | 22 | 13 |

Последний шаг операции расшифрования для шифротекста — поставить в соответствие числам буквы. Сообщение после расшифрования будет "ATTACKATDAWN". Таблица ниже показывает выполнение последнего шага.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| шифротекст | E | J | J | E | K | I | E | J | N | E | S | R |
| yy | 4 | 9 | 9 | 4 | 10 | 8 | 4 | 9 | 13 | 4 | 18 | 17 |
| 9(y+26-4)9\*(y+26-4) | 234 | 279 | 279 | 234 | 288 | 270 | 234 | 279 | 315 | 234 | 360 | 351 |
| 9(y+26-4)mod269(y+26-4)mod (26) | 0 | 19 | 19 | 0 | 2 | 10 | 0 | 19 | 3 | 0 | 22 | 13 |
| сообщение | A | T | T | A | C | K | A | T | D | A | W | N |

Заключение – до 5 мин.

Методическиерекомендации:

- обобщитьнаиболееважные, существенныевопросылекции;

- сформулироватьобщиевыводы;

- поставить задачидлясамостоятельнойработы;

- ответитьна вопросыстудентов.

Лекцияразработана «\_\_\_»\_\_\_\_\_\_\_\_20\_\_г.

\_\_\_\_\_\_\_\_\_\_\_\_ /Дедов О.П,/

1. [↑](#footnote-ref-1)