Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Факультет компьютерных технологий и прикладной математики**

**Кафедра вычислительных технологий**

**Отчёт**

**по лабораторной работе №2**

**Дисциплина: КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ**

**Тема: «Китайская теорема об остатках»**

Работу выполнил \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ К. А. Корнилов

Направление подготовки 02.03.02 Фундаментальная информатика и

информационные технологии

Направленность (профиль) Математическое и программное обеспечение

компьютерных технологий

Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А. А. Крамаренко

**Тема:** Теорема об остатках

**Цель:** Изучение теоремы об остатках для решения систем линейных сравнений.

**Ход работы:**

1. Найти решение системы сравнений

Решим задачу с помощью китайской теоремы об остатках.

* 1. Нод(5, 17, 12) = 1 =>взаимно простые модули
  2. M = 5 \* 17 \* 12 = 60 \* 17 = 1020
  3. M1 = 17 \* 12 =204 M2=5 \* 12 = 60 M3 = 5 \* 17 = 85
  4. Решаем отдельно каждое из сравнений и получаем следующие значения b1,b2,b3:
  5. X = (3 \* 204 + 60 \* 10 + 5 \* 85) mod 1020 = 617 + 1020K

1. Найти решение системы сравнений

Решим задачу с помощью китайской теоремы об остатках.

* 1. Нод(6, 35, 11) = 1 =>взаимно простые модули
  2. M = 6 \* 35 \* 11 = 2310
  3. M1 = 385 M2=66 M3 = 210
  4. Решаем отдельно каждое из сравнений и получаем следующие значения b1,b2,b3:
  5. X = (2 \* 385 + 23 \* 66 + 4 \* 210) mod 2310 = 818 + 2310K

1. Решены следующие примеры
   1. Дано НОД(a,b) = 24. Найти НОД(a,b,16)

НОД(a,b,16) <= 16. НОД(a,b) должен делиться на НОД(a,b,16) => Найдем НОД(24,16) => НОД(24,16) = 8 => **НОД(a,b,16) = 8**

* 1. Дано НОД(a,b,c) = 12. Найти НОД(a,b,c,16)

НОД(a,b,16) <= 16. НОД(a,b,c) должен делиться на НОД(a,b,c,16) => Найдем НОД(12,16) => НОД(12,16) = 4 => **НОД(a,b,c,16) = 4**

* 1. Найти НОД(200,180,450)

НОД(200,180) = 20 => НОД(200,180,450) = НОД(20,450) = **10**

* 1. Найти НОД(200,180,450,610)

Из предыдущей задачи НОД(200,180,450) = 10 => НОД(200,180,450,610) = НОД(10, 610) = 10

1. Предположим, что n >=0
   1. Найти НОД(2n+1, n) = 1

|  |  |  |  |
| --- | --- | --- | --- |
| q | R1 | R2 | R |
| 2 | 2n+1 | n | 1 |
| n | n | 1 | 0 |
| 0 | **1** | 0 | 0 |

* 1. Используя результат 4.1. найти:

НОД(201,100) = 1

НОД(81,40) = 1

НОД(501,250) = 1

1. Предположим, что n >=0
   1. Найти НОД(3n+1, 2n+1) = 1

|  |  |  |  |
| --- | --- | --- | --- |
| q | R1 | R2 | R |
| 1 | 3n+1 | 2n+1 | т |
| 2 | 2n+1 | n | 1 |
| n | n | 1 | 0 |
| 0 | **1** | 0 | 0 |

* 1. Используя результат 5.1. найти:

НОД(301,201) = 1

НОД(81,121) = 1

1. Используя расширенный алгоритм Евклида найти НОД и коэффициенты s и t
   1. R1 = 7 R2 = 4

|  |  |  |  |
| --- | --- | --- | --- |
| Q | R1 | R2 | R |
| 1 | 7 | 4 | 3 |
| 1 | 4 | 3 | 1 |
| 0 | 3 | 1 | 0 |

Обратный ход для нахождения коэффициентов s и t:

1 = 4 -3 = 4 – (7 – 4) = 4\*2 – 7

Тогда: Нод(1)

S = -1 + 4k

T = 2 – 7k

* 1. R1 = 291 R2 = 42

|  |  |  |  |
| --- | --- | --- | --- |
| Q | R1 | R2 | R |
| 6 | 291 | 42 | 39 |
| 1 | 42 | 39 | 3 |
| 13 | 39 | 3 | 0 |

Обратный ход для нахождения коэффициентов s и t:

3 = 42 - 39 = 42 – (291 – 42 \* 6) = 42 \* 7 – 291

Тогда: Нод(291,42) = 3

S = -1 + 42k

T = 7 – 291k

* 1. R1 = 320 R2 = 84

|  |  |  |  |
| --- | --- | --- | --- |
| Q | R1 | R2 | R |
| 3 | 320 | 84 | 68 |
| 4 | 68 | 16 | 4 |
| 4 | 16 | 4 | 0 |

Обратный ход для нахождения коэффициентов s и t:

4 = 68 – 16 \* 4 = 68 – 4 \* (84 – 68) = 320 – 3 \* 84 – 4\* ( 84 – 320 + 3 \* 84) = -19\*84 + 5 \* 320

Тогда: Нод(320,84) = 4

S = 5 + -84k

T = -18 + 320k

* 1. R1 = 400 R2 = 60

|  |  |  |  |
| --- | --- | --- | --- |
| Q | R1 | R2 | R |
| 6 | 400 | 60 | 40 |
| 1 | 60 | 40 | 20 |
| 2 | 40 | 20 | 0 |

Обратный ход для нахождения коэффициентов s и t:

20 = 60 – 40 = 60 – (400 – 6 \* 60) = -400 + 7 \* 60

Тогда: Нод(1)

S = -1 + 60k

T = 7 – 400k

1. Перечислите все пары аддитивной инверсии по модулю 20

(1,19), (2,18), (3,17), (4,16), (5,15), (6,14), (7,13), (8,12), (9,11), (10,10)

1. Перечислите все пары мультипликативной инверсии по модулю 20

20 = 2 \* 2 \* 5 => инверсию будут иметь элементы взаимно простые с 20

(1,1), (3,7), (9,9), (11,11), (13,17), (19,19)

1. Найти мультипликативную инверсию каждого из следующих целых чисел в Z180, используя расширенный алгоритм Евклида
   1. 38

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| q | R1 | R2 | r | S1 | S2 | s | T1 | T2 | T |
| 2 | 100 | 38 | 24 | 1 | 0 | 1 | 0 | 1 | -2 |
| 1 | 38 | 24 | 14 | 0 | 1 | -1 | 1 | -2 | 3 |
| 1 | 24 | 14 | 10 | 1 | -1 | 2 | -2 | 3 | -5 |
| 1 | 14 | 10 | 4 | -1 | 2 | -3 | 3 | -5 | 8 |
| 2 | 10 | 4 | 2 | 2 | -3 | 8 | -5 | 8 | -21 |
| 2 | 4 | **2** | 0 |  |  |  |  |  |  |

Так как НОД(38,180) = 2, то инверсии нет

* 1. 7

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Q | R1 | R2 | r | S1 | S2 | s | T1 | T2 | T |
| 25 | 100 | 38 | 24 | 1 | 0 | 1 | 0 | 1 | -2 |
| 1 | 38 | 24 | 14 | 0 | 1 | -1 | 1 | -2 | 3 |
| 2 | 24 | 14 | 10 | 1 | -1 | 2 | -2 | 3 | -5 |
| 2 | 14 | 10 | 4 | -1 | 2 | -3 | 3 | -5 | 8 |

Так как НОД(38,180) = 2, то инверсии нет