МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ІМЕНИ СЕМЕНА КУЗНЕЦЯ

Лабораторна робота №3

“Тема №3”

з дисципліни «Математичні основи криптології»

Виконав:

Студент групи 6.04.125.010.21.2

факультету Інформаційних технологій

спеціальності 125

П.І.П. Бойко В.В.

Перевірив:

Чугай А.М.

Харків – 2022

1. Призначимо числові значення для великих літер латинського алфавіту   
   (A = 0, B = 1... Z = 25). Ми можемо створити модульну арифметику, використовуючи модуль 26.
   * Що є(A+N) mod 26у цій системі? 13 mod 26 = 13 = N
   * Чому одно(A + 6) mod 26у цій системі? 6 mod 26 = 6 = G
   * Чому одно(Y – 5) mod 26у цій системі? 21 mod 26 = 21 = V
   * Чому одно(C – 10) mod 26у цій системі? -7 mod 26 = 7 = H
2. Перерахуйте всі пари адитивної інверсії за модулем 20.

(0; 0)

(1; 19)

(2; 18)

(3; 17)

(4; 16)

(5; 15)

(6; 14)

(7; 13)

(8; 12)

(9; 11)

(10; 10)

1. Перерахуйте всі мультиплікативні зворотні пари за модулем 20.

(1; 1) => (1 \* 1) mod 20 = 1

(3; 7) => (3 \* 7) mod 20 = 1

(9; 9) => (9 \* 9) mod 20 = 1

(11; 11) => (11 \* 11) mod 20 = 1

(13; 17) => (13 \* 17) mod 20 = 1

(19; 19) => (19 \* 19) mod 20 = 1

1. Знайдіть мультиплікативну інверсію кожного з наступних цілих чисел Z180, використовуючи розширений алгоритм Евклід.
   * 38

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| q | r1 | r2 | R | t1 | t2 | t |
| 4 | 180 | 38 | 28 | 0 | 1 | -4 |
| 1 | 38 | 28 | 10 | 1 | -4 | 5 |
| 2 | 28 | 10 | 8 | -4 | 5 | -14 |
| 1 | 10 | 8 | 2 | 5 | -14 | 19 |
| 4 | 8 | 2 | 0 | -14 | 19 | -90 |
|  | 2 | 0 |  | 19 | -90 |  |

НСД (180; 38) = 2 – отже число 38 в Z180 не має мультиплікативної версії

* + 7

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| q | r1 | r2 | R | t1 | t2 | t |
| 25 | 180 | 7 | 5 | 0 | 1 | -25 |
| 1 | 7 | 5 | 2 | 1 | -25 | 26 |
| 2 | 5 | 2 | 1 | -25 | 26 | -77 |
| 2 | 2 | 1 | 0 | 26 | -77 | 180 |
|  | 1 | 0 |  | -77 | 180 |  |

НСД (180; 7) = 1 – отже число 7 в Z180 має мультиплікативної версії

(-77) mod 180 = 103

* + 132

|  |  |  |  |
| --- | --- | --- | --- |
| q | r1 | r2 | R |
| 1 | 180 | 132 | 48 |
| 2 | 132 | 48 | 36 |
| 1 | 48 | 36 | 12 |
| 3 | 36 | 12 | 0 |
|  | 12 | 0 |  |

НСД (180; 132) = 12 – отже число 132 в Z180 не має мультиплікативної версії

* + 24

|  |  |  |  |
| --- | --- | --- | --- |
| q | r1 | r2 | R |
| 7 | 180 | 24 | 12 |
| 2 | 24 | 12 | 0 |
|  | 12 | 0 |  |

НСД (180; 24) = 12 – отже число 24в Z180 не має мультиплікативної версії