Студент: Боженко Анна

Група: КМ-01

Арифметичні операції зійснювалися за допомогою терміналу python

Завдання 1. (див. таблицю) Користуючись заданими параметрами алгоритму RSA, обчислити: 1) значення функції Ейлера; 2) зашифроване число С;  3) встановити, чи може бути число d секретним ключем?

Дані: n = 40247, e = 65537, d = 22913, p = 241, q = 167, M = 91

1. Знайдемо значення функції Ейлера від n:

Phi(n) = phi(40247) = (p – 1)\*(q – 1) = (241 – 1)\*(167 – 1) = 39840

1. Зашифруймо М:

C = M^e mod n = 91^65537 mod 40247 = 17198

1. Розшифруймо С, щоб переконатися, що d може бути секретним ключем:

M = C^d mod n = 17198^22913 mod 40247 = 91

Отже, отримавши початкове М, встановлено, що d може бути секретним ключем.

Відповідь: 1) значення функції Ейлера = 39840,

2) С = 17198,

3) d може бути секретним ключем

Завдання 2. (див. таблицю) За алгоритмом Діффі-Хеллмана обчислити  спільний секретний ключ Аліси і Боба.

Дані: генератор - g = 2, модуль - p = 251, секретне число Аліси - a = 256, секретне число Боба -b = 229

1. Зімітуймо дії Аліси: А = g^a mod p = 2^256 mod 251 = 64
2. Зімітуймо дії Боба: В = g^b mod p = 2^229 mod 251 = 235
3. Боб та Аліса обмінюються згенерованими А та В
4. Аліса обраховує К = B^a mod p = 235^256 mod 251 = 125
5. Боб обраховує К = А^b mod p = 64^229 mod 251 = 125

Отже, отрмали значення К = 125

Відповідь: 125

Завдання 3. (див. таблицю) Розшифрувати повідомлення за алгоритмом Ель-Гамаля.

Дані: g = 3, p = 239, x = 139, y = 17, k = 170, a = 10, b = 16

1. Розшифруймо повідомлення: М = (a^(p-1-x)\*b) mod p = 10^(239 – 1 – 139)\*16) mod 239 = 10^1584 = 100

Відповідь: початкове повідомлення = 100