**Прізвище, ім'я\_\_Козій\_Євгеній\_\_ІПС-41\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Тема: Обмін ключами за протоколом Діффі-Хелмана Варіант 8**

**Завдання**:

1. Для заданих простого числа p, генератора g, секретного числа Аліси a, секретного числа Боба b, знайти секретний ключ Аліси і Боба К.

p=53; g=4; a=35; b=38;

Відповідь: К=44

2. Знайти х як найменший додатній розвʼязок ріявняння A=gx mod p

A = 522

p = 19037

g = 8

Відповідь: х = 705

3. Для заданих простого числа p, генератора g, секретного числа Аліси a, секретного числа Боба b, знайти секретний ключ Аліси і Боба К та проаналізувати всі розвʼязки рівнянь A = gx mod p, B = gy mod p.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| p | g | a | b | A | B | K(A) | K(B) |
| 31 | 7 | 24 | 27 | 8 | 16 | 2 | 2 |

|  |  |  |
| --- | --- | --- |
| **x,y** | **A** | **B** |
| x1 = 9 | 8 | 8 |
| y1 = 12 | 16 | 16 |
| x2 = 24 | 8 | 8 |
| y2 = 27 | 16 | 16 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| x | y | xy | K =g^(xy) mod p | xy mod (p-1) |
| 9 | 12 | 108 | 2 | 18 |
| 9 | 27 | 243 | 2 | 3 |
| 24 | 12 | 288 | 2 | 18 |
| 24 | 27 | 648 | 2 | 18 |