**Прізвище, ім'я\_\_Житарюк\_Юлія\_\_ІПС-41\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Тема: Обмін ключами за протоколом Діффі-Хелмана Варіант 7**

**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=47; g=8; a=15; b=42;

Відповідь: К=16

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

A = 600; p = 18913; g = 7

Відповідь: х = 628

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) |
| 23 | 5 | 6 | 7 | 8 | 17 | 12 | 12 |

|  |  |  |
| --- | --- | --- |
| **x,y** | **A** | **B** |
| x1 = 6 | 8 | 8 |
| y1 = 7 | 17 | 17 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| x | y | xy | K =g^(xy) mod p | xy mod (p-1) |
| 6 | 7 | 42 | 12 | 20 |