Задача дискретного логарифмирования и основанные на ней криптосистемы: система Диффи-Хеллмана обмена ключами, системы Мэсси-Омура и Эль-Гамаля

Задача 1.

Пусть $G = \mathbb{Z}_{29}^*$, $g = 2$. Размер группы достаточен, чтобы закодировать все буквы латинского алфавита, а также пробел и точку. Закодируем их при помощи следующей таблицы:

a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
t	**u**	**v**	**w**	**x**	**y**	**z**		**.**										
20	21	22	23	24	25	26	27	28										

Вам прислали открытый ключ $g^b = 12$. Вы выбрали закрытый ключ $a = 10$, вычислили g^a и послали в ответ.

Найдите общий секрет $s = g^{ab}$. Найдите s^{-1}. Расшифруйте сообщение, в котором каждый символ был умножен вашим корреспондентом на s, при помощи найденного вами s^{-1}:

$$24, 9, 24, 11, 15, 28, 17, 2, 6, 28, 15, 25, 24, 11, 24, 11, 1.$$

Решение 1.

$$s = g^{ab} = (g^b)^a = 12^{10} = 28$$

Найдем обратный:

$$ss^{-1} = 1 \pmod{29}$$

$$28s^{-1} = 1 \pmod{29}$$

$$-s^{-1} = -28 \pmod{29}$$

$$s^{-1} = 28 \pmod{29}$$

Расшифруем сообщение, домножив каждый элемент на s^{-1}:

eternal wanderer.

Задача 2.

Пусть $G = \mathbb{Z}_{29}^*$, $g = 2$, латинский алфавит закодирован при помощи таблицы из прошлого задания. Вы перехватили зашифрованное сообщение $<$ 6 24 20 25 21 1 $>$. К сожалению, вы не знаете секретные ключи. Каким могло быть истинное сообщение? Перебирайте все возможные s^{-1} по возрастанию, начиная от 2 и пока не найдёте осмысленное английское слово.

Решение 2. Переберем s^{-1}:

```
from alph import alph


encrypted = [6, 24, 20, 25, 21, 1]
for descr in range(2, 29):
    print(descr, end=': ')
    for el in encrypted:
        print(alph[el * descr % 29], end='')
    print()
```

При $s^{-1} = 5$ Получилось осмысленное слово:

admire

Задача 3.

Алиса хочет получить от Сири сообщение, состоящее из секретного (неизвестного нам) числа M. Для общения с Сири она использует схему Эль-Гамаля. Она сгенерировала случайное простое число $p = 149$ и его первообразный корень $g = 59$, а также случайное целое число $x = 41$ (на интервале от 1 до $p-1$, взаимно простое с $p-1$). После этого она вычислила $y = g^x \bmod p \ = 134$. Таким образом, открытым ключом является $(p, g, y) = (149, 59, 134)$, а закрытый ключ равен $x = 41$. Сири при шифровании своего сообщения M получила пару чисел $(M \cdot g^{xt}, g^t) = (83, 57)$.

Выступая в роли Алисы, расшифруйте сообщение, то есть найдите M. Все вычисления производятся в группе $\mathbb{Z}_p^*$, то есть мультипликативной группе поля $\mathbb{Z}_p$.

Решение 3. Алиса знает x. Тогда домножим $M \cdot g^{xt}$ на $(g^t)^{|\mathbb{Z}_p^*|-x}$:

$$M \cdot g^{xt} \cdot (g^t)^{|\mathbb{Z}_p^*|-x} = M \cdot g^{xt} \cdot (g^t)^{|\mathbb{Z}_p^*|} \cdot g^{-xt} = M \cdot g^{xt} \cdot e \cdot g^{-xt} = M \cdot e = M$$

С дргуой стороны:

$$M \cdot g^{xt} \cdot (g^t)^{|\mathbb{Z}_p^*|-x} = 83 \cdot 57^{149-1-41} = 83 \cdot 57^{107} = 83 \cdot 43 = 142$$

Получили:

$$M = 142$$