Лабораторная работа №3
«Асимметричная криптография»

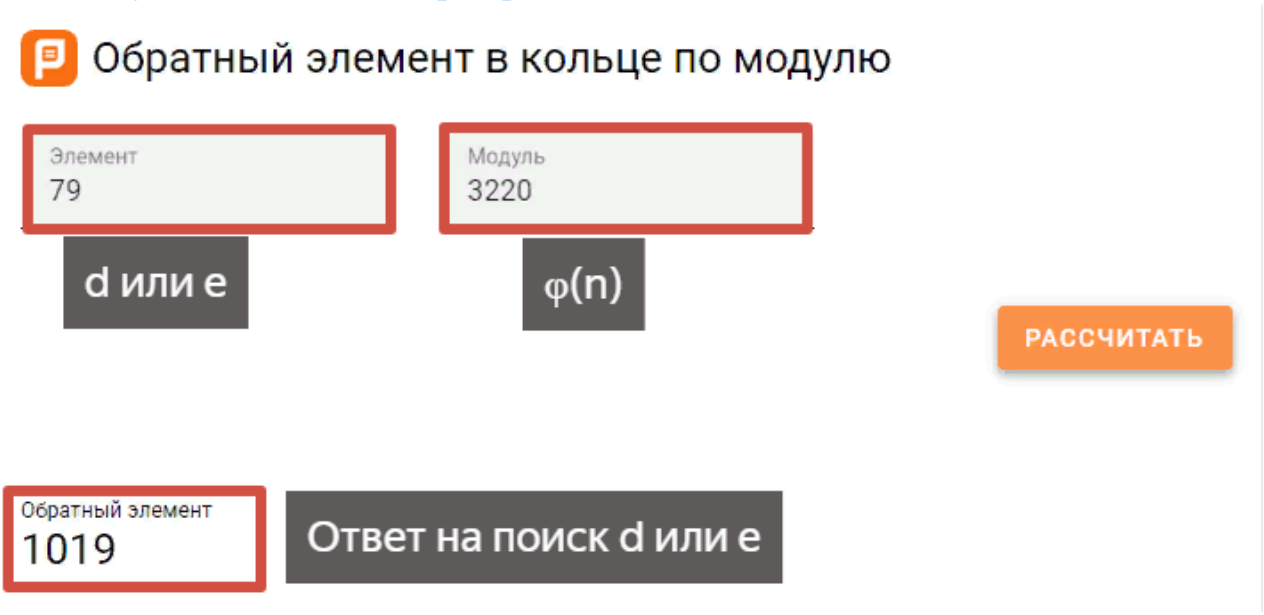
Цель: получить навыки кодирования и декодирования информации при помощи алгоритмов RSA и Эль-Гамаля.

ПРАКТИЧЕСКАЯ ЧАСТЬ

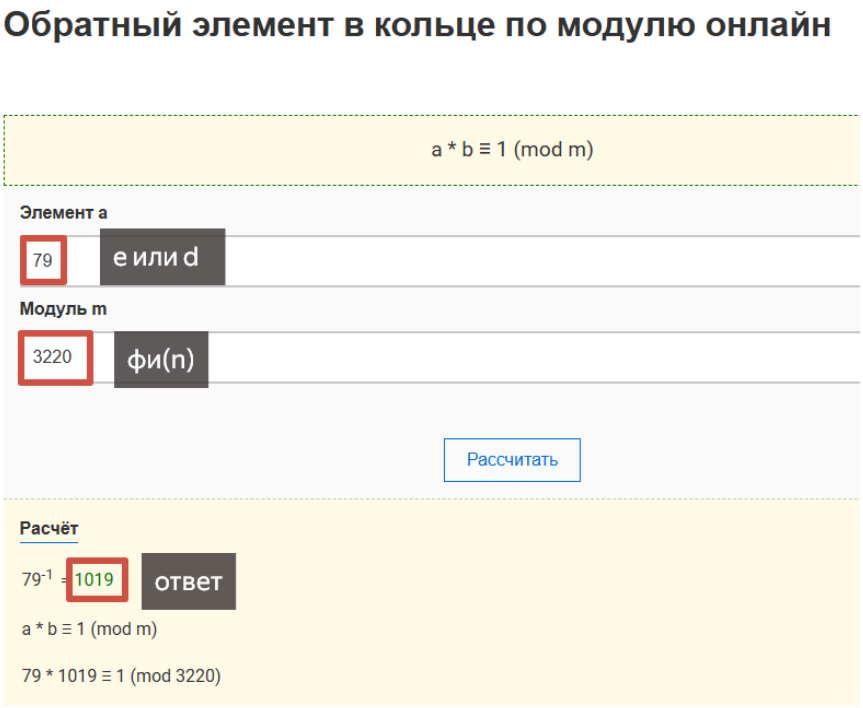
Задача 1: Используя алгоритм RSA зашифровать сообщение M = 6423897233, если известно: p = 47 и q = 71, e = 79 и r = 2.

Примечание 1: Задание аналогично задаче из последнего примера лекции по RSA.

Примечание 2: Для вычисления обратного элемента ключа d воспользуйтесь ссылкой: https://planetcalc.ru/3311/.



или другой сайт https://dzodzo.ru/calc-obratnyj-element-v-kolcze-po-modulyu-onlajn/:



Задача 2: Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA при простых числах p = 17 и q = 23, d = 41, k = 29. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.

ТАБЛИЦА ПРЯМОГО СЧЁТА РУССКОГО ЯЗЫКА (АЛФАВИТА)

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

Пример выполнения задачи 2:

Шифрование:

Шифруемое сообщение «МЕП» как последовательность целых чисел. Пусть буква «М» соответствует числу 14, буква «Е» - числу 6 и буква «П» - числу 17.

Зашифруем сообщение, используя открытый ключ (e, n):

C_1 = /решение скрыто/= 88

C_2 = /решение скрыто/= 164

C_3 = /решение скрыто/= 204

C = (88, 164, 204)

Расшифровывание: Расшифруем сообщение (88, 164, 204), пользуясь секретным ключом (d, n):

M_1 = /решение скрыто/= 14 = М

M_2 = /решение скрыто/= 6 = Е

M_3 = /решение скрыто/ = 17 =П

Задача 3: Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p и q из первой сотни. Зашифруйте сообщение, состоящее из вашей даты рождения (дд мм гг).

Примечание: Задание аналогично задаче 2. Числа p и q взять другие!!!

Задача 4: Даны 2 простых числа p = 7, q = 17. Часть ключа e = 5. Определите d и зашифруйте и расшифруйте сообщение M = 19 по алгоритму RSA.

Задача 5: Найти алгоритмом Евклида элемент *d* такой, что $e \cdot d \equiv 1 \bmod n$, если:

1. e = 15, ϕ(n) = 82
2. e = 58, ϕ(n) = 115
3. e = 29, ϕ(n) = 86
4. e = 24, ϕ(n) = 95

Задача 6: Зашифруйте и расшифруйте сообщения (свои фамилию, инициал имени, инициал отчества) с использованием алгоритма Эль-Гамаля для ключевых значений, представленных следующей таблицей.

Вариант	*p*	*g*	x_A	x_B	Вариант	*p*	*g*	x_A	x_B
1	23	11	14	21	**16**	23	14	17	16
2	29	11	14	21	**17**	29	14	17	16
3	31	11	14	21	**18**	31	14	17	16
4	37	11	14	21	**19**	37	14	17	16
5	43	11	14	21	**20**	43	14	17	16
6	23	12	15	19	**21**	23	15	18	13
7	29	12	15	19	**22**	29	15	18	13
8	31	12	15	19	**23**	31	15	18	13
9	37	12	15	19	**24**	37	15	18	13
10	43	12	15	19	**25**	43	15	18	13
11	23	13	16	18	**26**	23	16	21	12
12	29	13	16	18	**27**	29	16	21	12
13	31	13	16	18	**28**	31	16	21	12
14	37	13	16	18	**29**	37	16	21	12
15	43	13	16	18	**30 для всех**	43	16	21	12