

Варианты заданий на лабораторную работу № 3

Пользуясь алгоритмом своего варианта, напишите программу, которая позволит зашифровать произвольный открытый текст, предварительно закодировав его согласно прилагаемым таблицам 1, 2, 3 и расшифровать его. Зашифрованный текст должен сохраняться в файле для пересылки своему другу.

При написании программы используйте алгоритм быстрого возведения в степень и алгоритмы Евклида.

Метод шифрования и необходимые параметры указаны в таблице вариантов (таблица 4).

Таблица 1 – Кодировка русского алфавита

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41

Таблица 2 – Кодировка латинского алфавита

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58

R	S	T	U	V	W	X	Y	Z
59	60	61	62	63	64	65	66	67

Таблица 3 – Дополнительные символы

Пробел	Запятая	Точка
68	69	70

Таблица 4 – Варианты заданий

№ варианта	Алгоритм	Параметры
1	RSA	$p = 761, q = 827, e = 17$
2	Шамира	$p = 87613$
3	Эль-Гамаля	$p = 21617, g = 56$
4	RSA	$p = 983, q = 643, e = 11$
5	Шамира	$p = 93761$
6	Эль-Гамаля	$p = 21841, g = 39$
7	RSA	$p = 919, q = 571, e = 7$
8	Шамира	$P = 93169$
9	Эль-Гамаля	$P = 22157, g = 29$
10	RSA	$p = 823, q = 659, e = 49$
11	Шамира	$P = 87641$
12	Эль-Гамаля	$P = 22391, g = 39$
13	RSA	$p = 751, q = 619, e = 13$
14	Шамира	$P = 68531$
15	Эль-Гамаля	$P = 23961, g = 30$
16	RSA	$p = 857, q = 673, e = 5$
17	Шамира	$P = 72431$
18	Эль-Гамаля	$P = 25951, g = 92$
19	RSA	$p = 937, q = 571, e = 13$
20	Шамира	$P = 76103$
21	Эль-Гамаля	$P = 23189, g = 23$
22	RSA	$p = 823, q = 673, e = 11$