Практическое занятие 6. Криптосистема Рабина

Цель работы

Закрепить знания, полученные на лекциях по теме “Криптосистема Рабина”.

Задание

1.Выполнить упражнения по расшифрованию криптограммы, полученной в криптосистеме Рабина.

2.Зашифровать сообщение в криптосистеме Рабина.

Порядок

1. Выбрать вариант задания в табл 1.
2. Зашифровать сообщение табл. 1
3. Расшифровать криптограмму табл.2

Таблица1

№	p	q	M	№	p	q	M
1	11	31	316	14	17	41	811
2	19	7	331	15	31	43	341
3	23	19	535	16	57	49	222
4	31	11	480	17	47	5	178
5	43	7	528	18	37	11	342
6	47	19	1129	19	11	17	300
7	5	43	455	20	19	23	457
8	11	31	445	21	29	11	638
9	17	19	427	22	37	7	233
10	13	47	29	23	17	53	452
11	19	31	759	24	19	31	743
12	23	17	541	25	23	29	690
13	29	5	223	26	47	13	876

Примечание 1. Если сообщение меньше модуля, то сообщение необходимо разбить на две части путем представления сообщения в двоичном виде .

Таблица2

№	M	C	№	M	C
1	144	128	14	18	2
2	17	128	15	31	156
3	22	1	16	57	29
4	21	119	17	48	50
5	30	95	18	37	116
6	43	76	19	110	25
7	47	116	20	19	39
8	40	151	21	29	36
9	15	64	22	56	77
10	25	142	23	87	2
11	34	29	24	39	72
12	29	36	25	23	46

13	26	32	26	49	147

Примечание 2.

1. При расшифровании использовать ключи p=23, q=7 для вариантов с 1-26.
2. Перед расшифрованием проверить есть ли решение у задачи.
3. После расшифрования сверить расшифрованное сообщение с исходным по табл.