Домашняя работа №4
«Хэш-функции и ЭЦП в криптографии»

Задание 1: Найти хеш-образ сообщения «Погода сегодня ясная». Параметры p и q выбрать из таблицы согласно своему варианту. Вектор инициализации H_0 выбрать самостоятельно.

Варианты	p	q
1	101	11
2	103	13
3	107	17
4	109	19
5	113	23
6	127	29
7	131	31
8	137	37
9	139	41
10	149	43

Варианты	p	q
11	151	47
12	157	53
13	163	59
14	167	61
15	173	67
16	179	71
17	181	73
18	191	79
19	193	83
20	197	89

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

Задание 2: Используя хеш-образ сообщения, полученный в предыдущем задании, вычислить ЭЦП по схеме RSA. Закрытый ключ возьмите из таблицы простых чисел. Для вычисления открытого ключа **e** воспользуйтесь калькулятором: https://planetcalc.ru/3311/.

Простые числа

11	13	17	19	23
29	31	37	41	43
47	53	59	61	67
71	73	79	83	89
97	101	103	107	109
113	127	131	137	139
149	151	157	163	167
173	179	181	191	193
197	199	211	223	227
229	233	239	241	251
257	263	269	271	277
281	283	293	307	311
313	317	331	337	347
349	353	359	367	373
379	383	389	397	401
409	419	421	431	433
439	443	449	457	461
463	467	479	487	491
499	503	509	521	523
541	547	557	563	569
571	577	587	593	599

Задание 3: Для заданной пары простых чисел p и q и открытого текста M, согласно своему варианту определить самостоятельно остальные параметры схемы ЭЦП RSA и осуществить подписание сообщения. Проверить правильность цифровой подписи. Число **e** взять из таблицы простых чисел, а ключ **d** найти по калькулятору из задания 2.

Варианты	**p**	**q**	**M**
1	349	239	42
2	347	233	41
3	337	229	40
4	331	227	39
5	317	223	38
6	313	211	37
7	311	199	36
8	307	197	35
9	293	193	34
10	283	191	33

Варианты	**p**	**q**	**M**
11	409	293	52
12	401	283	51
13	397	281	50
14	389	277	49
15	383	271	48
16	379	269	47
17	373	263	46
18	367	257	45
19	359	251	44
20	353	241	43

Задание 4: Для заданного простого числа p, числа g и открытого текста M, согласно своему варианту, определить самостоятельно остальные параметры схемы ЭЦП Эль-Гамаля и осуществить подписание сообщения. Проверить правильность цифровой подписи. Число **e** взять из таблицы простых чисел, а число **x** и **k** выбрать самостоятельно. Помните, что числа x и k должны удовлетворять определенным условиям! Для просмотра этих условий воспользуйтесь Практической работой 4.

Варианты	**p**	**g**	**M**
1	353	3	43

Варианты	**p**	**g**	**M**
12	421	2	54

2	349	2	42
3	347	2	41
4	337	10	40
5	317	2	38
6	331	3	39
7	313	10	37
8	311	17	36
9	307	5	35
10	293	2	34
11	283	3	33

13	419	2	53
14	409	21	52
15	401	3	51
16	389	2	49
17	397	5	50
18	383	5	48
19	379	2	47
20	373	2	46
21	367	6	45
22	359	7	44