НЕ ЗАБУДЬТЕ!!! Указать собственную фамилию, № группы, фамилию преподавателя, который проводит занятия по ЛР, пронумеровать страницы

Запишите значения чисел: **R, S, T**, где **R** - день рождения, **S** - месяц рождения, **T** - год рождения; (например, 15 мая 2002 г .: R = 15, S = 5, T = 2002). Вычислите произведение **RS = V**.

Задание 1. (5 баллов)

Найдите **НОД (T, V).** Охарактеризуйте используемый алгоритм и каждый его шаг.

Задание 2. (10 баллов)

Найдите значение числа $\mathbf{V}^{-1}$ (обратное к **V**) по модулю (**S+1**). Охарактеризуйте используемый алгоритм и каждый его шаг.

Задание 3. (15 баллов)

Зашифруйте и расшифруйте свое имя (хотя бы 2-3 начальных символа, в любом алфавите), используя аффинный шифр Цезаря при *a* = S; *b* обосновать и выбрать самостоятельно. Охарактеризуйте используемый алгоритм, каждый его шаг и криптостойкость.

Задание 4. (15 баллов)

Зашифруйте и расшифруйте 2-3 блока текста (ваше имя) с помощью алгоритма RSA: начальные числа p и q (для генерации ключей) - ближайшие к R и S большие числа соответственно, отвечающие необходимым требованиям. Охарактеризуйте используемый алгоритм, каждый его шаг и криптостойкость.

Задание 5. (15 баллов)

Представить в табличной форме содержимое каждого 32-битного расширенного подблока, входного сообщения (полные собственные фамилия и имя в кодах ASCII; таблица - справа) в алгоритме SHA1 (если фамилия начинается с буквы от A до M) или в алгоритм MD5 (если фамилия начинается с букв от H до Я). Охарактеризуйте используемый алгоритм расширения сообщения.

Bin	Знак
0100 0001	A
0100 0010	B
0100 0011	C
0100 0100	D
0100 0101	E
0100 0110	F
0100 0111	G
0100 1000	H
0100 1001	I
0100 1010	J
0100 1011	K
0100 1100	L
0100 1101	M
0100 1110	N
0100 1111	O
0101 0000	P
0101 0001	Q
0101 0010	R
0101 0011	S
0101 0100	T
0101 0101	U
0101 0110	V
0101 0111	W
0101 1000	X
0101 1001	Y
0101 1010	Z

Общая сумма баллов	Оценка
55-60	10
50-54	9
45-59	8
42-44	7
38-41	6
35-37	5
30-34	4