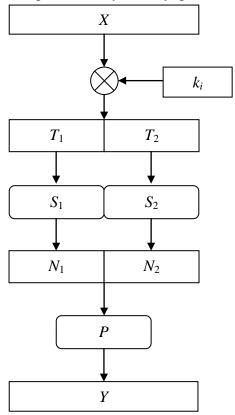
## Лабораторная работа №2. Блочно-итерационные криптосистемы.

## 1. *SP*-подстановка.

Необходимо реализовать (программно или вручную) блочно-итерационных шифр, состоящий из применения 3 итераций следующей упрощенной *SP*-подстановки:



На вход поступает сообщение длины 8 бит, исходный ключ имеет длину 12 бит. Это сообщение «складывается» с раундовым ключом. Вид «сложения» и способ генерации раундовых ключей будет указан в описании варианта. Результат «сложения» разбивается на 2 блока по 4 бита каждый:  $T_1$ ,  $T_2$ . Каждый из получившихся блоков поступает на вход соответствующего S-блока. Сами S-блоки будут заданы в варианте задания. Результаты применения S-блоков  $N_1$  и  $N_2$  снова собираются в один блок из 8 бит, к которому применяется операция перестановки бит (P-блок). P-блок будет задан в каждом варианте. Выход P-блока — это результирующий выход SP-подстановки.

2. Сначала X выбирается как  $(7*N)_2$ , где N — номер студента в списке группы, запись () $_2$  означает, что число необходимо представить в двоичной системе счисления. Ключ k выбирается, как  $(4096-11*q*r)_2$ , где q — количество символов в имени, r — количество символов в фамилии. Для указанного сообщения X найти результат зашифрования. При этом выводить не только окончательный результат, но и промежуточные результаты после 1-ой и 2-ой итерации. Затем заменить один бит сообщения (любой на выбор). Провести зашифрование и посмотреть насколько сильно изменился результат на каждой из итераций (лавинный эффект). Поскольку параметры вариантов специально не выбирались, то лавинный эффект может не наблюдаться.

## Бонусные задания

3. Реализовать (программно или вручную) систему шифрования, использующую подстановку Фейстеля для сообщения длиной 16 бит, где в качестве функции  $F_k$  используется реализуемая SP-подстановка. Всего 6 итераций. Раундовые ключи на 4-6 раундах совпадают с раундовыми ключами на 1-3 раундах. Открытый текст и ключ

возьмите произвольными. Проведите расшифрование и убедитесь, что получается исходный открытый текст.

## Варианты заданий:

*S*-блоки берутся из <u>статьи на википедии</u> из таблицы с идентификатором <u>id-Gost28147-89-</u> <u>СтуртоРго-A-ParamSet</u>. В варианте указаны номера *S*-блоков, которые надо брать из таблицы в статье.

№	Вид	Раундовые ключи – номера битов	Блок $S_1$	Блок $S_2$	Блок Р
Варианта	«Сложение»	из общего ключа			
1	Круглый плюс	1 – (1, 2, 3, 4, 5, 6, 7, 8)	1	2	Циклический сдвиг
		2 – (1, 2, 3, 4, 9, 10, 11, 12) 3 – (5, 6, 7, 8, 12, 11, 10, 9)			на 3 бита влево
2	Квадратный	1 – (1, 2, 3, 4, 5, 6, 7, 8)	1	7	Циклический сдвиг
	плюс	2 – (6, 7, 8, 9, 10, 11, 12, 1)		·	на 6 бит влево
		3 – (11, 12, 1, 2, 3, 4, 5, 6)			
3	Круглый плюс	1 – (1, 3, 5, 7, 2, 4, 6, 8)	1	8	(1, 3, 5, 7, 2, 4, 6, 8)
		2 – (5, 7, 9, 11, 6, 8, 10, 12)			
4	Квадратный	3 – (12, 10, 4, 2, 1, 3, 9, 11) 1 – (10, 12, 2, 5, 8, 6, 9, 4)	4	1	(1, 4, 7, 2, 5, 8, 3, 6)
4	плюс	2 – (10, 12, 2, 3, 8, 6, 9, 4)	4	1	(1, 4, 7, 2, 3, 6, 3, 0)
	illioc	3 – (7, 1, 2, 6, 12, 3, 9, 11)			
5	Круглый плюс	1 – (1, 4, 7, 10, 2, 5, 8, 11)	3	2	(4, 3, 2, 1, 6, 5, 8, 7)
		2 – (2, 5, 8, 11, 3, 6, 9, 12)			
		3 – (3, 6, 9, 12, 10, 4, 7, 1)			
6	Квадратный	1 – (1, 2, 3, 4, 5, 6, 7, 8)	6	7	Циклический сдвиг
	плюс	2 – (1, 2, 3, 4, 9, 10, 11, 12)			на 5 бит влево
7	Круглый плюс	3 – (5, 6, 7, 8, 12, 11, 10, 9) 1 – (1, 2, 3, 4, 5, 6, 7, 8)	2	5	Циклический сдвиг
/	круглый плюс	2-(6, 7, 8, 9, 10, 11, 12, 1)	2	3	на 3 бита влево
		3 – (11, 12, 1, 2, 3, 4, 5, 6)			na b enra briebe
8	Квадратный	1 – (1, 3, 5, 7, 2, 4, 6, 8)	5	4	Циклический сдвиг
	плюс	2 – (5, 7, 9, 11, 6, 8, 10, 12)			на 6 бит влево
		3 – (12, 10, 4, 2, 1, 3, 9, 11)			
9	Круглый плюс	1 – (10, 12, 2, 5, 8, 6, 9, 4)	2	6	(1, 3, 5, 7, 2, 4, 6, 8)
		2 – (2, 9, 10, 5, 1, 12, 6, 4) 3 – (7, 1, 2, 6, 12, 3, 9, 11)			
10	Квадратный	1 – (1, 4, 7, 10, 2, 5, 8, 11)	7	8	(1, 4, 7, 2, 5, 8, 3, 6)
10	плюс	2 – (2, 5, 8, 11, 3, 6, 9, 12)	,	o o	(1, 1, 7, 2, 3, 6, 3, 6)
		3 - (3, 6, 9, 12, 10, 4, 7, 1)			
11	Круглый плюс	1 – (1, 2, 3, 4, 5, 6, 7, 8)	5	2	(4, 3, 2, 1, 6, 5, 8, 7)
		2 – (1, 2, 3, 4, 9, 10, 11, 12)			
12	Квадратный	3 – (5, 6, 7, 8, 12, 11, 10, 9)	6	2	Циклический сдвиг
12	плюс	1 - (1, 2, 3, 4, 5, 6, 7, 8)  2 - (6, 7, 8, 9, 10, 11, 12, 1)	O	2	на 5 бит влево
	111100	3 – (11, 12, 1, 2, 3, 4, 5, 6)			ina y oni i mieno
13	Круглый плюс	1 – (1, 3, 5, 7, 2, 4, 6, 8)	8	4	Циклический сдвиг
		2 – (5, 7, 9, 11, 6, 8, 10, 12)			на 3 бита влево
		3 – (12, 10, 4, 2, 1, 3, 9, 11)			
14	Квадратный	1 – (10, 12, 2, 5, 8, 6, 9, 4)	5	4	Циклический сдвиг
	плюс	2 – (2, 9, 10, 5, 1, 12, 6, 4)			на 6 бит влево
15	Круглый плюс	3 – (7, 1, 2, 6, 12, 3, 9, 11) 1 – (1, 4, 7, 10, 2, 5, 8, 11)	3	8	(1, 3, 5, 7, 2, 4, 6, 8)
13	круглый плос	2 – (2, 5, 8, 11, 3, 6, 9, 12)	3	O	(1, 3, 3, 7, 2, 4, 0, 0)
16	Квадратный	3 – (3, 6, 9, 12, 10, 4, 7, 1) 1 – (1, 2, 3, 4, 5, 6, 7, 8)	3	4	(1, 4, 7, 2, 5, 8, 3, 6)
	плюс	2 – (1, 2, 3, 4, 9, 10, 11, 12)			
1.7	7.0	3 – (5, 6, 7, 8, 12, 11, 10, 9)	2		(4.2.2.1.6.5.0.7)
17	Круглый плюс	1 - (1, 2, 3, 4, 5, 6, 7, 8)  2 - (6, 7, 8, 9, 10, 11, 12, 1)	8	7	(4, 3, 2, 1, 6, 5, 8, 7)
18	Квадратный	3 – (11, 12, 1, 2, 3, 4, 5, 6) 1 – (1, 3, 5, 7, 2, 4, 6, 8)	7	2	Циклический сдвиг
-	плюс	2 – (5, 7, 9, 11, 6, 8, 10, 12)		_	на 5 бит влево
		3 - (12, 10, 4, 2, 1, 3, 9, 11)			
19	Круглый плюс	1 - (10, 12, 2, 5, 8, 6, 9, 4)	4	2	Циклический сдвиг
		2 – (2, 9, 10, 5, 1, 12, 6, 4)			на 3 бита влево
		3 – (7, 1, 2, 6, 12, 3, 9, 11)			

20	Квадратный плюс	1 – (1, 4, 7, 10, 2, 5, 8, 11) 2 – (2, 5, 8, 11, 3, 6, 9, 12)	2	1	Циклический сдвиг на 6 бит влево
		3 – (3, 6, 9, 12, 10, 4, 7, 1)			na o oni biloso
21	Круглый плюс	1 - (1, 2, 3, 4, 5, 6, 7, 8)	8	5	(1, 3, 5, 7, 2, 4, 6, 8)
		2 - (1, 2, 3, 4, 9, 10, 11, 12)			
		3 - (5, 6, 7, 8, 12, 11, 10, 9)			
22	Квадратный	1 - (1, 2, 3, 4, 5, 6, 7, 8)	3	4	(1, 4, 7, 2, 5, 8, 3, 6)
	плюс	2 - (6, 7, 8, 9, 10, 11, 12, 1)			
		3 - (11, 12, 1, 2, 3, 4, 5, 6)			
23	Круглый плюс	1 - (1, 3, 5, 7, 2, 4, 6, 8)	5	7	(4, 3, 2, 1, 6, 5, 8, 7)
		2 - (5, 7, 9, 11, 6, 8, 10, 12)			
2.4	T. V	3 – (12, 10, 4, 2, 1, 3, 9, 11)	0		- TT
24	Квадратный	1 – (10, 12, 2, 5, 8, 6, 9, 4)	8	6	Циклический сдвиг
	плюс	2 – (2, 9, 10, 5, 1, 12, 6, 4)			на 5 бит влево
25	I/	3 – (7, 1, 2, 6, 12, 3, 9, 11)	4	7	TI
25	Круглый плюс	1 - (1, 4, 7, 10, 2, 5, 8, 11)	4	/	Циклический сдвиг на 3 бита влево
		2 – (2, 5, 8, 11, 3, 6, 9, 12)			на 3 бита влево
26	Квадратный	3 - (3, 6, 9, 12, 10, 4, 7, 1) $1 - (1, 2, 3, 4, 5, 6, 7, 8)$	4	6	Циклический сдвиг
20	плюс	2 - (1, 2, 3, 4, 9, 10, 11, 12)	4	O	на 6 бит влево
	innoc	3 – (5, 6, 7, 8, 12, 11, 10, 9)			на о онт влево
27	Круглый плюс	1 – (1, 2, 3, 4, 5, 6, 7, 8)	5	8	(1, 3, 5, 7, 2, 4, 6, 8)
		2 - (6, 7, 8, 9, 10, 11, 12, 1)		-	(-, -, -, -, -, -, -, -,
		3 - (11, 12, 1, 2, 3, 4, 5, 6)			
28	Квадратный	1 – (1, 3, 5, 7, 2, 4, 6, 8)	1	3	(1, 4, 7, 2, 5, 8, 3, 6)
	плюс	2 - (5, 7, 9, 11, 6, 8, 10, 12)			
		3 - (12, 10, 4, 2, 1, 3, 9, 11)			
29	Круглый плюс	1 – (10, 12, 2, 5, 8, 6, 9, 4)	7	6	(4, 3, 2, 1, 6, 5, 8, 7)
		2 - (2, 9, 10, 5, 1, 12, 6, 4)			
		3 - (7, 1, 2, 6, 12, 3, 9, 11)			
30	Квадратный	1 - (1, 4, 7, 10, 2, 5, 8, 11)	7	2	Циклический сдвиг
	плюс	2 - (2, 5, 8, 11, 3, 6, 9, 12)			на 5 бит влево
		3 - (3, 6, 9, 12, 10, 4, 7, 1)			

Пример:

k	1	1	0	1	0	0	1	1	0	1	1	0
номера бит	1	2	3	4	5	6	7	8	9	10	11	12

Пусть указаны раундовые ключи

1-(1, 2, 3, 4, 5, 6, 7, 8) 2-(1, 2, 3, 4, 9, 10, 11, 12) 3-(5, 6, 7, 8, 12, 11, 10, 9)

Тогда

k1 = 11010011

k2 = 11010110

k3 = 00110110

Р-блок задан (1, 3, 5, 7, 2, 4, 6, 8), тогда Если на вход пришло (1001 1110),

k	1	0	0	1	1	1	1	0
номер бит	1	2	3	4	5	6	7	8

то выход (1011 0110).