Криптографические методы защиты информации

Лабораторно-практическая работа № 1
«Аффинный шифр»

Основные сведения

В аффинном шифре шифрование происходит посимвольно с помощью преобразования:

$$E_k(M)=aM+b \bmod m,$$

где a - число взаимно простое с m, b - любое целое, M - код символа. Ключом шифрования служит пара чисел k=(a,b).

Расшифрование происходит с помощью преобразования

$$D_k(C)=a^{-1}(C-b) \bmod m.$$

Задание к работе

1. Реализуйте программу выполняющую шифрование файла с помощью аффинного шифра с параметрами указанными для вашего варианта.
2. Реализуйте программу выполняющую расшифрование файла с помощью аффинного шифра с параметрами указанными для вашего варианта.

Варианты

1-1. m=256, k=(7,18).
1-2. m=256, k=(5,23).
1-3. m=256, k=(11,24).
1-4. m=256, k=(13,12).
1-5. m=256, k=(9,16).
1-6. m=256, k=(15,15).
1-7. m=256, k=(17,87).
1-8. m=256, k=(19,56).
1-9. m=256, k=(21,57).
1-10. m=256, k=(23,16).
1-11. m=256, k=(25,64).
1-12. m=256, k=(27,43).
1-13. m=256, k=(29,34).
1-14. m=256, k=(31,21).
1-15. m=256, k=(33,91).
1-16. m=256, k=(35,43).
1-17. m=256, k=(37,21).
1-18. m=256, k=(39,14).
1-19. m=256, k=(41,75).
1-20. m=256, k=(43,51).
1-21. m=256, k=(45,32).
1-22. m=256, k=(47,61).

1-23. m=256, k=(49,59).
1-24. m=256, k=(51,37).
1-25. m=256, k=(53,76).

Лабораторно-практическая работа № 2
«Шифр простой перестановки»

Основные сведения

В шифре простой перестановке шифрование происходит блоками из n символов которые перемешиваются согласно ключевой подстановке k(i):

$$E_k(x_1,x_2,x_3,\ldots,x_n)= (x_{k(1)},x_{k(2)},x_{k(3)},\ldots,x_{k(n)})$$

Расшифрование происходит с помощью обратной подстановки.

Задание к работе

1. Реализуйте программу, выполняющую шифрование файла с помощью шифра простой перестановки с ключевой подстановкой, указанной для вашего варианта.
2. Реализуйте программу, выполняющую расшифрование файла.

Варианты

2-1.

1	2	3	4	5	6
6	5	1	2	3	4

2-2.

1	2	3	4	5	6
6	1	2	5	3	4

2-3.

1	2	3	4	5	6
6	5	4	3	2	1

2-4.

1	2	3	4	5	6
5	4	2	3	6	1

2-5.

1	2	3	4	5	6
2	1	4	3	6	5

2-6.

1	2	3	4	5	6
6	3	2	5	4	1

2-7.

1	2	3	4	5	6
3	4	1	2	6	5

2-8.

1	2	3	4	5	6
3	5	1	6	2	4

2-9.

1	2	3	4	5	6
2	3	1	6	4	5

2-10.

1	2	3	4	5	6
2	5	4	3	6	1

2-11.

1	2	3	4	5	6
3	1	4	6	2	5

2-12.

1	2	3	4	5	6
3	4	6	5	2	1

2-13.

1	2	3	4	5	6
3	4	6	5	1	2

2-14.

1	2	3	4	5	6
3	6	2	1	4	5

2-15.

1	2	3	4	5	6
3	6	5	2	4	1

2-16.

1	2	3	4	5	6
4	6	1	5	3	2

2-17.

1	2	3	4	5	6
4	6	1	5	2	3

2-18.

1	2	3	4	5	6
4	5	2	3	6	1

2-19.

1	2	3	4	5	6
4	3	5	2	6	1

2-20.

1	2	3	4	5	6
5	3	4	6	2	1

2-21.

1	2	3	4	5	6
5	3	4	6	1	2

2-22.

1	2	3	4	5	6
5	4	3	1	6	2

2-23.

1	2	3	4	5	6
6	4	5	1	2	3

2-24.

1	2	3	4	5	6
6	4	5	3	2	1

2-25.

1	2	3	4	5	6
6	3	1	5	2	4

Лабораторно-практическая работа № 3
«Криптоанализ шифра ключевой перестановки»

Основные сведения

Перестановочный шифр с ключевым словом действует следующим образом. Буквы открытого текста записываются в клетки прямоугольной таблицы по ее строчкам. Буквы ключевого слова пишутся над столбцами и указывают порядок этих столбцов (по возрастанию номеров букв в алфавите). Чтобы получить зашифрованный текст, надо выписывать буквы по столбцам с учетом их нумерации:

Открытый текст: Прикладная математика Ключ: Шифр

Ш	И	ф	р
4	1	3	2
П	р	и	к
л	а	д	н
а	я	м	а
т	е	м	а
т	и	к	а

Криптограмма: Раяеикнаааидммкплатт
Ключевое слово(последовательность столбцов) известно адресату, который легко сможет расшифровать сообщение.

При криптоанализе перестановочных шифров полезной является информация о сочетаемости букв, то есть о предпочтительных связях букв друг с другом, которую легко извлечь из таблиц частот биграмм. В данной таблице слева и справа от каждой буквы расположены наиболее предпочтительные «соседи» (в порядке убывания частоты соответствующих биграмм). В таких таблицах обычно указывается также доля гласных и согласных букв (в процентах), предшествующих (или следующих за) данной букве. Сочетаемость букв русского языка:

Г	**С**	**Слева**		**Справа**	**Г**	**С**
3	97	л, д, к, т, в, р, н	**А**	л, н, с, т, р, в, к, м	12	88
80	20	я, е, у, и, а, о	**Б**	о, ы, е, а, р, у	81	19
68	32	я, т, а, е, и, о	**В**	о, а, и, ы, с, н, л, р	60	40
78	22	р, у, а, и, е, о	**Г**	о, а, р, л, и, в	69	31
72	28	р, я, у, а, и, е, о	**Д**	е, а, и, о, н, у, р, в	68	32
19	81	м, и, л, д, т, р, н	**Е**	н, т, р, с, л, в, м, и	12	88
83	17	р, е, и, а, у, о	**Ж**	е, и, д, а, н	71	29
89	11	о, е, а, и	**З**	а, н, в, о, м, д	51	49
27	73	р, т, м, и, о, л, н	**И**	с, н, в, и, е, м, к, з	25	75
55	45	ь, в, е, о, а, и, с	**К**	о, а, и, р, у, т, л, е	73	27
77	23	г, в, ы, и, е, о, а	**Л**	и, е, о, а, ь, я, ю, у	75	25
80	20	я, ы, а, и, е, о	**М**	и, е, о, у, а, н, п, ы	73	27
55	45	д, ь, н, о	**Н**	о, а, и, е, ы, н, у	80	20
11	89	р, п, к, в, т, н	**О**	в, с, т, р, и, д, н, м	15	85

65	35	в, с, у, а, и, е, о	**П**	о, р, е, а, у, и, л	68	32
55	45	и, к, т, а, п, о, е	**Р**	а, е, о, и, у, я, ы, н	80	20
69	31	с, т, в, а, е, и, о	**С**	т, к, о, я, е, ь, с, н	32	68
57	43	ч, у, и, а, е, о, с	**Т**	о, а, е, и, ь, в, р, с	63	37
15	85	п, т, к, д, н, м, р	**У**	т, п, с, д, н, ю, ж	16	84
70	30	н, а, е, о, и	**Ф**	и, е, о, а, е, о, а	81	19
90	10	у, е, о, а, ы, и	**Х**	о, и, с, н, в, п, р	43	57
69	31	е, ю, н, а, и	**Ц**	и, е, а, ы	93	7
82	18	е, а, у, и, о	**Ч**	е, и, т, н	66	34
67	33	ь, у, ы, е, о, а, и, в	**Ш**	е, и, н, а, о, л	68	32
84	16	е, б, а, я, ю	**Щ**	е, и, а	97	3
0	100	м, р, т, с, б, в, н	**Ы**	л, х, е, м, и, в, с, н	56	44
0	100	н, с, т, л	**Ь**	н, к, в, п, с, е, о, и	24	76
14	86	с, ы, м, л, д, т,, р, н	**Э**	н, т, р, с, к	0	100
58	42	ь, о, а, и, л, у	**Ю**	д, т, щ, ц, н, п	11	89
43	57	о, н, р, л, а, и, с	**Я**	в, с, т, п, д, к, м, л	16	84

Пример выполнения

Пусть дан шифр-текст: СВПООЗЛУЙЬСТЬ_ЕДПСОКОКАЙЗО
Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5x5. Могут быть и другие таблицы. В случае неудачи с таблицей 5x5 следует попробовать другое количество столбцов. Известно, что шифрование производилось по столбцам, следовательно, расшифрование следует проводить, меняя порядок столбцов.

С	В	П	О	О
З	Л	У	Й	Ь
С	Т	Ь	_	Е
Д	П	С	О	К
К	А	Й	З	О

Необходимо произвести анализ совместимости символов (Таблица сочетаемости букв русского алфавита, а также таблицы частот биграмм представлена выше). Во втором и третьем столбце сочетание ВП является крайне маловероятным для русского языка,

следовательно, такая последовательность столбцов быть не может. Рассмотрим другие запрещенные и маловероятные сочетания букв: ВП (2,3 столбцы), ПС (3,1 столбцы), ПВ (3,2 столбцы). Перебрав их все, получаем наиболее вероятные сочетания биграмм по столбцам:

В	О	С	П	О
Л	Ь	З	У	Й
Т	Е	С	Ь	_
П	О	Д	С	К
А	З	К	О	Й

Получаем осмысленный текст: ВОСПОЛЬЗУЙТЕСЬ_ПОДСКАЗКОЙ

Задание к работе

1. Расшифровать фразу, зашифрованную столбцовой перестановкой.

Варианты

3-1. ОКЕСНВРП_ЫРЕАДЕЫН_В_РСИКО
3-2. ДСЛИЕЗТЕА_Ь_ЛЬЮВМИ_ _АОЧХК
3-3. НМВИАИ_НЕВЕ_СМСТУОРДИАНКМ
3-4. ЕДСЗЬНДЕ_МУБД_УЭ_КРЗЕМНАЫ
3-5. СОНРЧОУО_ХДТ_ИЕИ_ВЗКАТРРИ
3-6. _ОНКА_БНЫЕЦВЛЕ_К_ТГОАНЕИР
3-7. НЗМАЕЕАА_Г_НОТВОССОТЬЯАЛС
3-8. РППОЕААДТВЛ_ЕБЬЛНЫЕ_ПА_ВР
3-9. ОПЗДЕП_ИХРДОТ_И_ВРИТЧ_САА
3-10. ВКЫОСИРЙУ_ОЬВНЕ_СОАПНИОТС
3-11. ПКТИРАОЛНАОИЧ_З_ЕСЬНЕЛНЖО
3-12. ИПКСОЕ_ТСМНАЧИ_ОЕН_ГДЕЛА_
3-13. АМВИННЬТЛЕАНЕ_ЙОВ_ОПХАРТО
3-14. АРЫКЗЫ_КЙТНЛ_ААЫ_ОЛБКЫТРТ
3-15. _ПАРИИВИАРЗ_БРА_ИСТЬЛТОЕК
3-16. П_ЛНАЭУВКАА_ЦИИВР_ОКЧЕДРО
3-17. ЖВНОАН_АТЗОЬСН_ЫО_ФВИИКИЗ
3-18. ОТВГОСЕЬЬТАДВ_С_ЬЗАТТЕЫАЧ
3-19. ЯАМРИТ_ДЖЕХ_СВЕД_ТСУВЕТНО
3-20. УЬБДТ_ОЕГТВ_ОЫКЭА_ВКАИУЦИ
3-21. ЛТБЕЧЛЖЫЕ_ _ОАПТЖРДУ_ЛМНОА
3-22. ИТПРКРФАГО_АВЯИА_ЯНЖУАКАН
3-23. ПКЕЕРРПО_ЙУСТ_ИТПСУТЛЯЕИН
3-24. ИЬЖЗНСД_ТДН_ЕТ_НУВЕУРЫГОЫ
3-25. ЕОУРВА_НЬРИАДИЦЕПИ_РНШВЫЕ

Лабораторно-практическая работа № 4
«Криптоанализ аффинного шифра»

Основные сведения

В аффинном шифре шифрование происходит посимвольно с помощью преобразования:

$$C=E_k(M)=aM+b \bmod m,$$

где a - число взаимно простое с m, b - любое целое, M - код символа. Ключом шифрования служит пара чисел k=(a,b).

Расшифрование происходит с помощью преобразования

$$M=D_k(C)=a^{-1}(C-b) \bmod m.$$

При криптоанализе аффинного шифра необходимо произвести частотный анализ текста и выявить две наиболее часто встречающиеся буквы. Для русского языка частоты (в порядке убывания) знаков алфавита, в котором отождествлены *Е* с*Ё*, *Ь* с *Ъ*, а также имеется знак пробела (-) между словами, приведены в следующей таблице

- 0.175	**О** 0.090	**Е, Ё** 0.072	**А** 0.062
И 0.062	**Т** 0.053	**Н** 0.053	**С** 0.045
Р 0.040	**В** 0.038	**Л** 0.035	**К** 0.028
М 0.026	**Д** 0.025	**П** 0.023	**У** 0.021
Я 0.018	**Ы** 0.016	**З** 0.016	**Ь, Ъ** 0.014
Б 0.014	**Г** 0.013	**Ч** 0.012	**Й** 0.010
Х 0.009	**Ж** 0.007	**Ю** 0.006	**Ш** 0.006
Ц 0.004	**Щ** 0.003	**Э** 0.003	**Ф** 0.002

С учетом данных таблицы две наиболее часто встречающиеся буквы О и Е. Сопоставляя их двум наиболее частым буквам текста можем составить систему из двух уравнений. Решение системы уравнений дает ключ шифрования.

Примечания:

1) Во всех заданиях используется следующая кодировка

а	**б**	**в**	**г**	**д**	**е**	**ж**	**з**	**и**	**й**	**к**	**л**	**м**	**н**	**о**	**п**	**р**	**с**	**т**	**у**	**ф**

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
ф		**х**		**ц**		**ч**		**ш**		**щ**	**ь**	**ы**	**ъ**	**э**	**ю**	**я**				
20		21		22		23		24		25	26	27	28	29	30	31				

2) В некоторых текстах наиболее частыми могут быть другие буквы, поэтому иногда приходится предпринимать несколько попыток, прежде чем расшифрованный текст будет осмысленным.

3) Далее во всех заданиях предполагается, что текст записан на русском языке без пробелов и знаков препинания только маленькими буквами.

Пример:

Пусть в тексте наиболее частыми буквами будут Й и П. Выдвигаем два предположения:

$$Ek(Й)=О,\ Ek(П)=Е$$

или

$$Ek(Й)=Е,\ Ek(П)=О.$$

Используя таблицу кодировок получаем две системы уравнений:

$(9a+b) \bmod 32=14,\ (15a+b) \bmod 32=5$

либо

$(9a+b) \bmod 32=5,\ (15a+b) \bmod 32=14.$

В обоих системах в качестве модуля взято число 32, так как используется алфавит из 32 символов. Решая эти две системы уравнений получаем возможные ключи шифрования. Какой из них правильный можно определить только расшифровав текст.

Задание к работе

1. Дешифруйте текст, представленный в Вашем варианте, если известно, что это аффинный шифр. Текст написан на русском языке без пробелов и знаков препинания только маленькими буквами.

Варианты

4-1. мьчнтздретчкнатчыктэкькбкечнтчюмыщисжэлшгсгнщнчиклтчкыщектэкгсгактщюдщжл чюгбсжчлш

4-2. бцияхъпаххъпкцмлчлпежмьктлжцднрльклзнэияхиглякцяльгксняжмкгицияпкхмрлглжшлц ктажбглыкйнслйихажмциягайль

4-3. гмажуиткфйъшяюсжламяютймяфгкдтякещйжлйшкттяюйтфйщлйлрщядтиюфйжягяюжуя суяэстгягжкюгжкшкттяю

4-4. ыщчщряжщмкстгткладгтжкьотютхьгчтымтплгчдфичтмтжхкьоищчзэчзжзеясзичщжкя жлщ

хэчщожщцыэкдхьктфщоерщчь

4-5. шкчцуъвхедьшхсчхьщйпмчпидьндтьсчкщцщхсзсюйьчгхдзюзйхьщщхюзжвзоьщсзслпщц

4-6. вхэбфыэбацявнрюншлзцрмчбтячзюнвьашцзцзмюдзаыцрюмбаьцраыюнмюдзаыцбвэюнбц

4-7. гсюэзюшбънягсюэзющянстдчяюжкфнузчэжъжунжчсмишбъшбюжлсшьюитаснсчэнстяд

соэяьжкеяжкшжми
4-8. ъиъщящснэршисвнутсхреопсзовднврвфщсшиычдщядбоыишидрбнспирщртяыиэчещя ещиэсзоэшсъощдслидргожишид
4-9. бсиьбжгаоялплцкщдцаэглшнокжцкшгезогльнглщишияжржгишкдгибжшксицкщгляябц ерлкгэхицкъглскокшгкзихлояигдшазяокэкяжкхс
4-10. уоьшзчиьйбхдорсэзшотпсчоязнъиьшгсяигдогоьйитчязарябэотэоэйотпсьитйоьитйовпж ьбафдбйг
4-11. цвйфиоицчякчвоицгяшфяечвоицшифвгочвэюгошяоабюигюсщфаюабагэцвчяечвфвгифв лпбифчвювшщк
4-12. обмхжузллвнлмхзбьфлхкаъмишлснлмхихбжебфбзибифюнлнывтбзихбинбатъвшбнбсоъ кевхеихылфвялъмнвсимякмбшълнл
4-13. ьштнюьшэшцнояйбяебягрябоэернгэвтнмсмршъябыяжрямшэшьэябрнокхемывилшыгни мршзряпгнфбяфэнмокмыетемсгемыеьштяфьниэябя
4-14. узьучуэхднэукнрудузнитжэжручфйчжвждфйирфяуйхлмэнчдхшжандщоушэуджзнимло жлнджгзтудщежохуяуй
4-15. фдлцакстходлвпскэкятхцзэлщктядкцтфъслюнпрощлцпьндэлюнайтлоцплылжксткознсф юхъахцпяложкэкь
4-16. цжпуешвкэпйебъьйпбтпквдвяпфлныекэвфсылэеоыаойъдаэаошцушнйжэвйпблажкелбнл аэефлнэпьтэвфлс
4-17. ьутъьвьурсалочфкстлцхялтфэфхресысьфхжъревыфжсяяфыйурчзсцйуюьчъялтлццфшфь фьлхфэжсрелыфт
4-18. вчсчщчфчхчотъъззоытптолнхищидюачъзытлсчэолсдвблнйоэчлстлнгбгъбхстьгчзстптлы чхиойъззочаъябочвб
4-19. зщшымзсвщзмжсипбмисиьсщмзбжчубсмзчичиоисаиеюикиаыфчимаъмыкауимбнщзмж юбтысъкимщмзъисытюыкызыфчъцкъчбизкваъ
4-20. фщчуюэбвфьажцфбаурнусьпжхьфвфьртсбйщябшуфьхвяпяущмюцбъбмоящэьцхусьтуцж мбгиььюуцоажхуюфьх
4-21. ьдзхцдпьдкяыоьдвцхъоыидвеярбдлухуишдцжфтшцяьйбжщоытбхьйткяцялящяфыхъдьь жртьдшобошяцйэдщяцябжщ
4-22. чьфбрхытырзбпьыюыаыеыжытзйвелбхгефрфтвирегрхжлбныхгтырзпъльыцртыеыохбжб дыаьгнцгрныьпытгрх
4-23. мэиэщэоэиэчцэюиацшмыдыоэиюыцчлыуиюйбэфоэлэгэвлэчущятлючудэбэфрэиавэъуиы тбэйэътщлыцш
4-24. цчтхзчгяцчндъщкгяыхъчгяюзхщомвъчрущзхючыдздйдмуйянвъдряйдждзмддюхъкгояха йящкисзчюяйхиюъдщдму
4-25. ктчешюфснмщнфбшзъжчуксфъциаожнслзоюяпязнщнмснжанмзчтжяжнфкснщзою

Лабораторно-практическая работа № 5
«Элементы блочных шифров. S-блоки»

Основные сведения

S-блоки алгоритма DES имеют следующий вид:

S1:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**1**	**1**	**1**	**1**	**1**	**1**

0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S5:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S6:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S7:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1

1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S8:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Шифрование с помощью S-блоков осуществляется следующим образом. Сообщение разбивается на блоки из 6 бит. Два из этих битов используются для определения номера строки, а остальные четыре для определения номера столбца. Номер строки определяется как двоичная запись числа, составленная из заданных битов. Для получения шифр-текста будем записывать сначала два бита, означающие номер строки, а затем значение в найденной ячейке S-блока.

Задание к работе

1. Реализуйте программы, осуществляющие шифрование и расшифрование с помощью S-блоков по алгоритму, описанному выше. В варианте указан номер S-блока, который нужно использовать, n и номера битов определения номера строки a и b.

Например, если указано n=3, a=1, b=2, то надо использовать блок S3, а для определения номера строки в нем брать биты первый и второй в виде двоичного числа ab.

Варианты

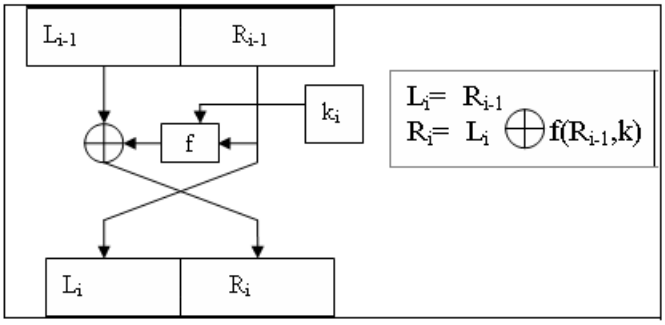
5-1. n=1, a=1, b=2.
5-2. n=2, a=1, b=3.
5-3. n=3, a=1, b=4.
5-4. n=4, a=1, b=5.
5-5. n=5, a=1, b=6.
5-6. n=6, a=2, b=1.
5-7. n=7, a=2, b=3.
5-8. n=8, a=2, b=4.
5-9. n=1, a=2, b=5.
5-10. n=2, a=2, b=6.
5-11. n=3, a=3, b=1.
5-12. n=4, a=3, b=2.
5-13. n=5, a=3, b=4.
5-14. n=6, a=3, b=5.

5-15. n=7, a=3, b=6.
5-16. n=8, a=4, b=1.
5-17. n=1, a=4, b=2.
5-18. n=2, a=4, b=3.
5-19. n=3, a=4, b=5.
5-20. n=4, a=4, b=6.
5-21. n=5, a=5, b=1.
5-22. n=6, a=5, b=2.
5-23. n=7, a=5, b=3.
5-24. n=8, a=5, b=4.
5-25. n=1, a=5, b=6.

Лабораторно-практическая работа № 6
«Элементы блочных шифров. Сеть Фейстеля»

Основные сведения

При шифровании с помощью сети Фейстеля входной блок разбивается на левую L и правую R части. Далее производятся преобразования, показанные на схеме



Задание к работе

1. Реализуйте программы, осуществляющие шифрование и расшифрование с помощью сети Фейстеля с использованием функции f, заданной в Вашем варианте. Все сеансовые ключи необходимо брать одинаковыми, равными ключу шифрования длиной 8 бит. Шифрование производить блоками по 8 бит. Необходимо выполнить три раунда шифрования.

Варианты

6-1. f(x,k)=(x<<1)⊕(x<<2)⊕k,
6-2. f(x,k)=(x<<1)⊕(x<<3)⊕k,
6-3. f(x,k)=(x<<1)⊕(x<<4)⊕k
6-4. f(x,k)=(x<<1)⊕(x<<5)⊕k
6-5. f(x,k)= (x<<1)⊕(x<<6)⊕k
6-6. f(x,k)= (x<<1)⊕(x<<7)⊕k
6-7. f(x,k)= (x<<2)⊕(x<<3)⊕k
6-8. f(x,k)= (x<<2)⊕(x<<4)⊕k
6-9. f(x,k)= (x<<2)⊕(x<<5)⊕k
6-10. f(x,k)= (x<<2)⊕(x<<6)⊕k
6-11. f(x,k)= (x<<2)⊕(x<<7)⊕k
6-12. f(x,k)= (x<<3)⊕(x<<4)⊕k
6-13. f(x,k)= (x<<3)⊕(x<<5)⊕k
6-14. f(x,k)= (x<<3)⊕(x<<6)⊕k
6-15. f(x,k)= (x<<3)⊕(x<<7)⊕k
6-16. f(x,k)= (x<<4)⊕(x<<5)⊕k
6-17. f(x,k)= (x<<4)⊕(x<<6)⊕k
6-18. f(x,k)= (x<<4)⊕(x<<7)⊕k
6-19. f(x,k)= (x<<5)⊕(x<<6)⊕k
6-20. f(x,k)= (x<<5)⊕(x<<7)⊕k
6-21. f(x,k)= (x<<6)⊕(k<<7)⊕k

6-22. f(x,k)= (x<<3)⊕(k<<2)⊕k
6-23. f(x,k)= (x<<4)⊕(k<<3)⊕k
6-24. f(x,k)= (x<<5)⊕(k<<1)⊕k
6-25. f(x,k)= (x<<6)⊕(k<<5)⊕k

Лабораторно-практическая работа № 7
«Модель открытого текста»

Основные сведения

Энтропией открытого текста T называется величина Σ

$$H_k(T)= \Sigma p(x)\log_2 p(x),$$

где x – k-граммы открытого текста T, p(x) – частота встречаемости k-граммы в открытом тексте T, суммирование производится по всем k-граммам. Для криптоанализа интерес представляет величина H_k/k.

Задание к работе

1. Для текста, представленного в вашем варианте, рассчитайте H_k/k для значений k от 1 до 5. Учитывать необходимо только буквы русского алфавита, опуская пробелы и знаки препинания. Большие и маленькие буквы считать эквивалентными.
2. Постройте график зависимости H_k/k от k для вашего текста.

Варианты

7-1. Мильоны - вас. Нас - тьмы, и тьмы, и тьмы. Попробуйте, сразитесь с нами! Да, скифы - мы! Да, азиаты - мы, С раскосыми и жадными очами! Для вас - века, для нас - единый час. Мы, как послушные холопы, Держали щит меж двух враждебных рас Монголов и Европы!

7-2. Летун отпущен на свободу. Качнув две лопасти свои, Как чудище морское в воду, Скользнул в воздушные струи. Его винты поют, как струны... Смотри: недрогнувший пилот К слепому солнцу над трибуной Стремит свой винтовой полет...

7-3. Гул затих. Я вышел на подмостки. Прислонясь к дверному косяку, Я ловлю в далеком отголоске, Что случится на моем веку. На меня наставлен сумрак ночи Тысячью биноклей на оси. Если только можно, Авва Отче, Чашу эту мимо пронеси.

7-4. Я был разбужен спозаранку Щелчком оконного стекла. Размокшей каменной баранкой В воде Венеция плыла. Все было тихо, и, однако, Во сне я слышал крик, и он Подобьем смолкнувшего знака Еще тревожил небосклон.

7-5. Глухая пора листопада, Последних гусей косяки. Расстраиваться не надо: У страха глаза велики. Пусть ветер, рябину занянчив, Пугает ее перед сном. Порядок творенья обманчив, Как сказка с хорошим концом.

7-6. Я пропал, как зверь в загоне. Где-то люди, воля, свет, А за мною шум погони, Мне наружу ходу нет. Темный лес и берег пруда, Ели сваленной бревно. Путь отрезан отовсюду. Будь что будет, все равно.

7-7. Снег идет, снег идет. К белым звездочкам в буране Тянутся цветы герани За оконный переплет. Снег идет, и всё в смятеньи, Всё пускается в полет,- Черной лестницы ступени, Перекрестка поворот.

7-8. Я сразу смазал карту будня, плеснувши краску из стакана; я показал на блюде студня косые скулы океана. На чешуе жестяной рыбы прочел я зовы новых губ. А вы ноктюрн сыграть могли бы на флейте водосточных труб?

7-9. Разворачивайтесь в марше! Словесной не место кляузе. Тише, ораторы! Ваше слово, товарищ маузер. Довольно жить законом, данным Адамом и Евой. Клячу истории загоним. Левой! Левой! Левой!

7-10. Вашу мысль, мечтающую на размягченном мозгу, как выжиревший лакей на засаленной кушетке, буду дразнить об окровавленный сердца лоскут:
досыта изъиздеваюсь, нахальный и едкий.
7-11. Послушайте! Ведь, если звезды зажигают - значит - это кому-нибудь нужно? Значит - кто-то хочет, чтобы они были? Значит - кто-то называет эти плевочки жемчужиной?
7-12. Я волком бы выгрыз бюрократизм. К мандатам почтения нету. К любым чертям с матерями катись любая бумажка. Но эту... По длинному фронту купе и кают чиновник учтивый движется. Сдают паспорта, и я сдаю мою пурпурную книжицу.
7-13. Скажи-ка, дядя, ведь не даром Москва, спаленная пожаром, Французу отдана? Ведь были ж схватки боевые, Да, говорят, еще какие! Недаром помнит вся Россия Про день Бородина!
7-14. Скажи мне, ветка Палестины: Где ты росла, где ты цвела, Каких холмов, какой долины Ты украшением была? У вод ли чистых Иордана Востока луч тебя ласкал, Ночной ли ветр в горах Ливана Тебя сердито колыхал?
7-15. Выхожу один я на дорогу; Сквозь туман кремнистый путь блестит; Ночь тиха. Пустыня внемлет богу, И звезда с звездою говорит. В небесах торжественно и чудно! Спит земля в сияньи голубом... Что же мне так больно и так трудно? Жду ль чего? жалею ли о чём?
7-16. Белеет парус одинокой В тумане моря голубом!.. Что ищет он в стране далекой? Что кинул он в краю родном?.. Играют волны - ветер свищет, И мачта гнется и скрыпит... Увы! он счастия не ищет И не от счастия бежит!
7-17. Погиб поэт!- невольник чести - Пал, оклеветанный молвой, С свинцом в груди и жаждой мести, Поникнув гордой головой!.. Не вынесла душа поэта Позора мелочных обид, Восстал он против мнений света Один, как прежде... и убит!
7-18. Несчастная кошка порезала лапу - Сидит, и ни шагу не может ступить.
Скорей, чтобы вылечить кошкину лапу Воздушные шарики надо купить!
И сразу столпился народ на дороге - Шумит, и кричит, и на кошку глядит.
А кошка отчасти идет по дороге, Отчасти по воздуху плавно летит!
7-19. Когда вода всемирного потопа Вернулась вновь в границы берегов, Из пены уходящего потока На берег тихо выбралась любовь И растворилась в воздухе до срока, А срока было сорок сороков.
7-20. Средь оплывших свечей и вечерних молитв, Средь военных трофеев и мирных костров Жили книжные дети, не знавшие битв, Изнывая от мелких своих катастроф. Детям вечно досаден Их возраст и быт,- И дрались мы до ссадин, До смертных обид. Но одежды латали Нам матери в срок, Мы же книги глотали, Пьянея от строк.
7-21. Живописцы, окуните ваши кисти в суету дворов арбатских и в зарю, чтобы были ваши кисти словно листья. Словно листья, словно листья к ноябрю. Окуните ваши кисти в голубое, по традиции забытой городской, нарисуйте и прилежно и с любовью, как с любовью мы проходим по Тверской.
7-22. В раннем детстве верил я, что от всех болезней капель Датского короля не найти полезней. И с тех пор горит во мне огонек той веры... Капли Датского короля пейте, кавалеры!
7-23. Надоело говорить и спорить, И любить усталые глаза... В флибустьерском дальнем море Бригантина подымает паруса... Капитан, обветренный, как скалы, Вышел в море, не дождавшись нас... На прощанье подымай бокалы Золотого терпкого вина.
7-24. Если я заболею, к врачам обращаться не стану, Обращаюсь к друзьям (не сочтите, что это в бреду): постелите мне степь, занавесьте мне окна туманом, в изголовье поставьте ночную звезду.

7-25. По крутой тропинке горной Шел домой барашек черный И на мостике горбатом Повстречался с белым братом. И сказал барашек белый: "Братец, вот какое дело: Здесь вдвоем нельзя пройти, Ты стоишь мне на пути."