ЗАДАНИЯ НА КРИПТОАНАЛИЗ КЛАССИЧЕСКИХ ШИФРОВ

1. ШИФР СТОЛБЦОВОЙ ПЕРЕСТАНОВКИ

При решении заданий на криптоанализ шифров перестановки необходимо восстановить начальный порядок следования букв текста. Для этого используется анализ совместимости символов, в чем может помочь таблица сочетаемости.

Таблица 1. 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, а, и, е	**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

Таблица 2. Сочетаемость букв английского языка

Г	С	Слева		Справа	Г	С
19	81	l,c,d,m,n,s,w,t,r,e,h	**A**	n,t,s,r,l,d,c,m	6	94
55	45	y,b,n,t,u,d,o,s,a,e	**B**	e,l,u,o,a,y,b,r	70	30

61	39	u,o,s,n,a,i,l,e	**C**	h,o,e,a,i,t,r,l,k	59	41
52	48	r,i,l,a,n,e	**D**	e,i,t,a,o,u	54	46
8	92	c,b,e,m,v,d,s,l,n,t,r,h	**E**	r,d,s,n,a,t,m,e,c,o	21	79
69	31	s,n,f,d,a,i,e,o	**F**	t,o,e,i,a,r,f,u	52	48
36	64	o,d,u,r,i,e,a,n	**G**	e.h.o.r.a.t.f.w.i.s	42	58
7	93	g,e,w,s,c,t	**H**	e,a,i,o	90	10
13	87	f,m,w,e,n,l,d,s,r,h,t	**I**	n,t,s,o,c,r,e,m,a,l	17	83
28	72	y,w,t,s,n,e,c,b,a,c	**J**	u,o,a,e,m,w	88	12
53	47	y,u,i,n,a,r,o,c	**К**	e,i,n,a,t,s	68	32
52	48	m,p,t,i,b,u,o,e,l,a	**L**	e,i,y,o,a,d,u	65	35
69	31	s,d,m,r,i,a,o,e	**M**	e,a,o,i,p,m	71	29
89	11	u,e,o,a,i	**N**	d,t,g,e,a,s,o,i,c	32	68
21	79	o,d,l,p,h,n,e,c,f,s,i,r,t	**O**	n,f,r,u,t,m,l,s,w,o	18	82
47	53	r,l,t,n,i,p,m,a,o,u,e,s	**P**	o,e,a,r,l,u,p,t,i,s	59	41
20	80	o,n,l,e,d,r,s	**Q**	u	100	0
70	30	p,i,u,t,a,o,e	**R**	e,o,a,t,i,s,y	61	39
48	52	d,t,o,u,r,n,s,i,a,e	**S**	t,e,o,i,s,a,h,p,u	41	59
43	57	u,o,d,t,f,e,i,n,s.a	**T**	h,i,o,e,a,t,r	38	62
35	65	p,f,t,l,b,d,s,o	**И**	n,s,t,r,l,p,b,c	8	92
88	12	r,u,o,a,i,e	**V**	e,i,o,a	99	1
48	52	g,d,y,n,s,t,o,e	**W**	a,h,i,e,o,n	80	20
95	5	u,n,i,e	**X**	p,t,i,a,u,c,k,o	38	62
24	76	b,n,a,t,e,r,l	**Y**	a,o,s,t,w,h,i,e,d,m	38	62
88	12	o,n,a,i	**Z**	e,i,w	86	14

При анализе сочетаемости букв друг с другом следует иметь в виду зависимость появления букв в открытом тексте от значительного числа предшествующих букв. Для анализа этих закономерностей используют понятие условной вероятности.

Систематически вопрос о зависимости букв алфавита в открытом тексте от предыдущих букв исследовался известным русским математиком А.А.Марковым (1856 — 1922). Он доказал, что появления букв в открытом тексте нельзя считать независимыми друг от друга. В связи с этим А. А. Марковым отмечена еще одна устойчивая закономерность открытых текстов, связанная с чередованием гласных и согласных букв. Им были подсчитаны частоты встречаемости биграмм вида гласная-гласная (*г,г*), гласная-согласная (*г,с*), согласная-гласная (*с,г*), согласная-согласная (*с,с*) в русском тексте длиной в 10^5 знаков. Результаты подсчета отражены в следующей таблице:

Таблица 3. Чередование гласных и согласных

	Г	С	Всего
Г	6588	38310	44898
С	38296	16806	55102

Пример решения:

Дан шифр-текст: СВПООЗЛУЙЬСТЬ_ЕДПСОКОКАЙЗО

Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5х5. 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 и английского алфавита, а также таблицы частот биграмм представлена выше). В первом и третьем столбце сочетание СП 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: Расшифровать фразу, зашифрованную столбцовой перестановкой.

1. ОКЕСНВРП_ЫРЕАДЕЫН_В_РСИКО
2. ДСЛИЕЗТЕА_Ь_ЛЬЮВМИ_ _АОЧХК
3. НМВИАИ_НЕВЕ_СМСТУОРДИАНКМ
4. ЕДСЗЬНДЕ_МУБД_УЭ_КРЗЕМНАЫ
5. СОНРЧОУО_ХДТ_ИЕИ_ВЗКАТРРИ
6. _ОНКА_БНЫЕЦВЛЕ_К_ТГОАНЕИР
7. НЗМАЕЕАА_Г_НОТВОССОТЬЯАЛС
8. РППОЕААДТВЛ_ЕБЬЛНЫЕ_ПА_ВР
9. ОПЗДЕП_ИХРДОТ_И_ВРИТЧ_САА
10. ВКЫОСИРЙУ_ОЬВНЕ_СОАПНИОТС
11. ПКТИРАОЛНАОИЧ_З_ЕСЬНЕЛНЖО

12.ИПКСОЕ_ТСМНАЧИ_ОЕН_ГДЕЛА_
13.АМВИННЬТЛЕАНЕ_ЙОВ_ОПХАРТО
14.АРЫКЗЫ_КЙТНЛ_ААЫ_ОЛБКЫТРТ
15._ПАРИИВИАРЗ_БРА_ИСТЬЛТОЕК
16.П_ЛНАЭУВКАА_ЦИИВР_ОКЧЕДРО
17.ЖВНОАН_АТЗОЬСН_ЫО_ФВИИКИЗ
18.ОТВГОСЕЬЬТАДВ_С_ЬЗАТТЕЫАЧ
19.ЯАМРИТ_ДЖЕХ_СВЕД_ТСУВЕТНО
20.УЬБДТ_ОЕГТВ_ОЫКЭА_ВКАИУЦИ
21.ЛТБЕЧЛЖЫЕ_ _ОАПТЖРДУ_ЛМНОА
22.ИТПРКРФАГО_АВЯИА_ЯНЖУАКАН
23.ПКЕЕРРПО_ЙУСТ_ИТПСУТЛЯЕИН
24.ИЬЖЗНСД_ТДН_ЕТ_НУВЕУРЫГОЫ
25.ЕОУРВА_НЬРИАДИЦЕПИ_РНШВЫЕ

2. ШИФР ДВОЙНОЙ ПЕРЕСТАНОВКИ

Пример решения:

Дан шифр-текст: ЫОЕЧТТОУ_СНСОРЧТРНАИДЬН_Е

Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5х5. известно, что шифрование производилось сначала по столбцам, а затем по строкам, следовательно, расшифрование следует проводить тем же способом.

Ы	О	Е	Ч	Т
Т	О	У	_	С
Н	С	О	Р	Ч
Т	Р	Н	А	И
Д	Ь	Н	_	Е

Производим анализ совместимости символов. Если в примере столюцовой перестановки можно было легко подобрать нужную комбинацию путем перебора, то здесь лучше воспользоваться таблицей частот букв русского языка (см. приложение). Для оптимизации скорости выполнения задания можно проверить все комбинации букв только в первой строке. Получаем ОЕ-15, ОЧ-12, ЕТ-33, ТЕ-31, ЧО-х, ЕО-7, ЧЫ-х, ОЫ-х, ТЫ-11, ТЧ-1, ЧЕ-23 (где х-запрещенная комбинация).

Из полученных результатов можно предположить следующую комбинацию замены столбцов **2 4 3 5 1:**

О	Ч	Е	Т	Ы
О	_	У	С	Т
С	Р	О	Ч	Н

Р	А	Н	И	Т
Ь	_	Н	Е	Д

Теперь необходимо переставить строки в нужном порядке. **3 2 4 5 1:**

С	Р	О	Ч	Н
О	_	У	С	Т
Р	А	Н	И	Т
Ь	_	Н	Е	Д
О	Ч	Е	Т	Ы

Получаем осмысленный текст: СРОЧНО_УСТРАНИТЬ_НЕДОЧЕТЫ

Задание: Расшифровать фразу, зашифрованную двойной перестановкой (сначала были переставлены столбцы, затем строки)

1. СЯСЕ_ _ЛУНЫИАККННОГЯДУЧАТН
2. МСЕЫ_ЛЫВЕНТОСАНТУЕИ_РЛПОБ
3. АМНРИД_УЕБСЫ_ЕЙРСООКОТНВ_
4. ОПЧУЛС_БООНЕВ_ОЖАЕОНЕЩЕИН
5. ЕШИАНИРЛПГЕЧАВРВ_СЕЫНА_ЛО
6. АРАВНРСВЕЕОАВ_ЗАНЯА_КМРЕИ
7. А_ЛТАВЙООЛСО_ТВ_ШЕЕНЕСТ_Ь
8. ФИ_ЗИММУЫНУУБК_Е_ДЬШЫИВЧУ
9. ВР_ЕСДЕИ_ТПХРОИ_ЗБУАДНУА_
10. ЦТААЙПЕЕ_ТБГУРРСВЬЕ_ОРЗВВ
11. АВАРНСЧАА_НЕДВЕДЕРПЕОЙ_ИС
12. ДОПК_СОПАЛЕЧНЛ_ГИНЙОИЖЕ_Т
13. ЛУАЗИЯНСА_ДТДЕАИ_ШРФЕОНГ_
14. С_ОЯНВ_СЬСЛААВРЧЕАРТОГДЕС
15. ЗШАФИПРАЛОЕНЖ_ОЬН_ДАРВОНА
16. КЭЕ_ТДУМБ_ЬСЗЕДНЕЗМАОР_ТУ
17. _ЕАЛЯРАНВЯАЧДА_ЕРПЕСАНВ_Ч
18. _И_ЕНТРЗИ_ОКЕВНОДЛЕША_ИМП
19. РОБДОЕВПС_МСХЬА_ _ИВПСНИОТ
20. ЕСДНОГТЕАНН_НЕОВМР_ЕУНПТЕ
21. _ЙЕСТОВО_НИИНЛАЕТИЖДСОПВ_
22. НДИАЕОЫЛППНЕ_ _НВЕАНГТ_ИЗЛА
23. П_БИРДЛЬНЕВ_ОП_ОПЗДЕВЫГЕА
24. МДООИТЕЬ_СМТ_НАДТЕСУБЕХНО
25. АИНАЛЖНОЛЕШФ_ЗИ_УАРОЬСНЕ_