Тема 18. ДЕШИФРУВАННЯ КЛАСИЧНИХ ШИФРІВ

1. Дешифрування шифру простої заміни

Введемо математичні моделі відкритих текстів, що використовуються при криптографічному аналізі шифрів, а також виділимо певні властивості відкритих текстів. Далі використаємо деякі з цих властивостей і акцентуємо увагу на ймовірнісно-статистичних закономірностях, які мають місце у відкритому тексті й використовуються при дешифруванні шифрів простої заміни та перестановки.

Існують стійкі закономірності відкритого тексту, які слід враховувати при дешифруванні шифрів простої заміни й перестановки. Можливість дешифрування певного шифру значною мірою залежить від того, наскільки криптографічні перетворення руйнують ймовірнісно-статистичні закономірності, наявні у відкритому тексті. До найбільш стійких закономірностей відкритого повідомлення належать такі:

1) в осмислених текстах кожної природної мови різні літери зустрічаються з різною частотою, при цьому відносні частоти вживання літер у різних текстах однієї мови є близькі поміж собою. Те ж саме можна стверджувати й по частоті вживаності пар, трійок літер відкритого тексту;

2) будь-яка природна мова має так звану надлишковість, що дозволяє з великою ймовірністю "вгадувати" зміст повідомлення, навіть якщо частина літер у повідомленні є невідома.

У таблиці 18.1 зазначено відносну частоту вживаності літер абетки російської мови.

Таблиця 5.1 - Частота вживаності літер абетки російської мови

1	а - 0,062	11	к - 0,028	21	ф - 0,002
2	б - 0,014	12	л - 0,035	22	х - 0,009
3	в - 0,038	13	м - 0,026	23	ц - 0,004
4	г - 0,013	14	н - 0,053	24	ч - 0,012
5	д - 0,025	15	о - 0,090	25	ш - 0,006
6	е - 0,072	16	п - 0,023	26	щ - 0,003
7	ж - 0,007	17	р - 0,040	27	ы - 0,016
8	з - 0,016	18	с - 0,045	28	ъ,ь - 0,014
9	и - 0,062	19	т - 0,053	29	э - 0,003
10	й - 0,010	20	у - 0,021	30	ю - 0,006
				31	я - 0,018

Подібні таблиці наводяться в багатьох джерелах. Їх побудовано па підставі підрахунків частоти вживаності певних літер на великих обсягах відкритого тексту. З огляду на те, що для експериментів залучається різний вихідний матеріал, значення ймовірностей дещо відрізняються поміж собою.

Якщо упорядкувати літери за спаданням ймовірностей, то дістанемо варіаційний ряд **О, Е, А, И, Н, Т, С, Р, В, Л, К, М, Д, П, У, Я, З, Ы, Б, Ь, Г, Ч, Й, Х, Ж, Ю, Ш, Ц, Щ, Д, Ф.**

Як запам'ятати перші 10 найчастіше вживаних літер російської абетки? Пригадуєте, як запам'ятовують основні кольори у фізиці? Треба запам'ятати фразу: *Каждый охотник желает знать, где сидит фазан*. Перші літери слів фрази вказують на основні кольори. У криптографії треба запам'ятати слово СЕНОВАЛИТР — у ньому наявні всі 10 найбільш вживаних літер.

Частотна діаграма вживаності літер, зрозуміло, залежить від мови. У таблиці 18.2 подано у відсотках відносні частоти найбільш уживаних літер деяких мов.

Таблиця 18.2 - Відносні частості найбільш уживаних літер деяких мов

Мова	Частість вживаності літер, %					
Англійська	e – 12,75	t – 9,25	r – 8,50	i – 7,75	h – 7,75	o – 7,50
Французька	e – 17,75	a – 8,25	s – 8,25	i – 7,25	n – 7,25	r – 7,25
Німецька	e – 18,50	n –11,50	I – 8,00	r – 7,50	s – 7,00	a – 5,00
Арабська	a – 17,75					
Грецька	a – 14,25					
Японська	p – 15,75					
Латина	a – 11,00					
Малайська	a – 20,25					
Санскрит	a – 31,25					

Частоти вживаності знаків абетки залежать не лише від мови, але й від характеру тексту. Наприклад, у тексті з криптографії буде вища ймовірність використання літер Ф, Ш (через часто вживані слова "шифр", "криптографія"). У математичному тексті ймовірніше буде більша частота використання літери Ф (через слова "функція, "функціонал" і т. п.).

У стандартних текстових файлах найчастіше вживається символ "прогалина"; в exe-файлах найчастіше вживається символ 0; в текстах,

написаних у текстовому процесорі ChiWriter, зручному для оформлення математичних текстів, перше місце посів символ "\" — backslash.

Частотна діаграма є стійкою характеристикою тексту. З теорії ймовірностей випливає, що за дуже слабких обмежень на ймовірнісні властивості випадкового процесу є справедливий закон великих чисел, тобто відносні частоти знаків збігаються за ймовірністю зі значеннями їхніх ймовірностей

$$P\left\{\left|\frac{\vartheta_k}{N} - p_k\right| > \varepsilon\right\} \xrightarrow[N\to\infty]{} 0.$$

Це справедливо для послідовності незалежних випробувань, дія кінцевого регулярного однорідного ланцюга Маркова. Експерименти засвідчують, що це справедливо й для відкритих текстів.

З позицій сучасної криптографії, шифри перестановки і простої заміни мають істотний недолік: вони не цілковито руйнують ймовірнісно-статистичні властивості, наявні у відкритому повідомленні.

При дешифруванні тексту, зашифрованого шифром простої заміни, використовують частотні характеристики відкритого тексту. Власне, якщо підрахувати частоти вживаності знаків у шифрованому тексті, упорядкувати їх за спаданням та порівняти з варіаційним рядом ймовірностей відкритого тексту, то ці дві послідовності будуть близькі. Найімовірніше перше місце посяде прогалина, далі слідуватимуть літери О, Е, А, И.

Зрозуміло, якщо текст не є надто довгий, то не є неодмінним повний збіг. На другому місці може бути літера О, а на третьому – Е, але в кожному разі в перших і других рядах однакові літери розташовуватимуться неподалік одна від одної, й що ближче до початку (що більше ймовірність вживання знаків), тим менше буде відстань поміж знаками.

Аналогічна картина спостерігається і для пар сусідніх літер (біграм) відкритого тексту (найчастіше зустрічається біграма російського відкритого тексту – СТ). Однак для здобуття стійкої картини довжина послідовності має бути істотно більше. На порівняно невеликих відрізках відкритого тексту ця картина є трохи розмита. Більш стійкою характеристикою біграм є відсутність в

осмисленому тексті, як говорять, певних біграм; наявність заборонних біграм, котрі мають імовірність, рівну практично нулю.

Чи бачили ви коли-небудь у відкритому тексті біграми ЪЬ, “ голосна” Ь, "прогалина" Ь? Знання й використовування зазначених особливостей відкритого тексту значно полегшує дешифрування шифрів перестановки й заміни.

Розглянемо приклад дешифрування шифру простої заміни. Нехай маємо такий шифротекст:

ДОЧАЛЬ ИЬЦИО ЛИОЙО ВНЫИЮШ ХЕМВЛНХЕИ ДОСОЛЬ ЧСО ИА" ТЬЖАТСР ЬАС АКЕИОЙО ДОКЩОКЗЖАЙО КПЗ РТАЩ ТПЬЧНАР ТДОТОУН ХЕМВОРНИЕЗ ЕИМОВЛНЯЕЕ РЮУОВ БВЕД СОЙВНМЕЧАТБОГ ТЕТСАЛЮ ЫНРЕТЕС ОС ОТОУ АИИОТСАГ ЕИМОВЛНЯЕЕ АА ЯАИИОТСЕ Е РОЫЛОЦИОТСАГ РПНКАПШЯАР ДО ЫНЖУСА ТРОАГ ЕИМОВЛНЯЕЕ ДВАЦКА РТАЙО ДОКЧАВБИАЛУОПШХОА ВНЫИООУ ВНЫЕА РЕКОР ЫНЖЕЖНАЛОГ ЕИМОВЛНЯАА КОБЬЛАИСНПШИНЗ САПАМОИИНЗ САПАРЕЫЕОИИНЗ БОЛДШЭСАВИНЗ БНЦКЮГ РНК ЕИМОВЛНЯЕЕ УЛААС ТРОЕ ТДАЯЕМЕЧАТБЕА ОТОУАИИОТСЕ Е ФСК ОТОЧАИИОТСЕ ТЕПШИО РПЕЗЭС ИН РЮУОВ ЛАСОКОР ХЕМВОРЙЙВЗ ЕИМОВЛНЯЕЕ УОПШХОА ЫИНЧАИЕА ЕЛАЭС ОУЪАЛЮ Е СВАУЬАЛНЗ ТБОВОТСШ ДАВАКНЧЕ ХЕМВОРНИИОГ

Роботу слід розпочати з підрахунку частоти вживаності символів у шифрованому тексті. Після того як здійснено підрахунок, упорядкуємо символи за спаданням частот: b_1, b_2, b_3, b_4, b_5 ...

Під цим рядом слід підписати варіаційний ряд ймовірностей знаків у відкритому тексті:

О Е А И Н Т С Р В Л К М Д П У Я З Ы Б Ь Г Ч Й Х Ж Ю Ш Ц Щ ЭФ

За дуже великої довжини шифротексту, для того аби з шифрованого отримати відкритий текст, потрібно замінити B на 0, B_2 – на Е, B_3 – на А й т. д. Принаймні саме така ситуація матиме місце для найбільш імовірних літер. У

нас матеріалу недостатньо. Переглянувши шифротекст після такої заміни, бачимо, що він не читається, – отже, матеріалу насправді є замало.

Що нам залишається? Вгадувати заміну. При цьому маємо все ж враховувати статистичні особливості відкритого тексту. У шифротексті через прогалину найімовірніше позначено прогалину; через літеру О – О чи А; через Е – О чи Е, чи А; через А – Е чи А, чи И й т. д.

Можна рекомендувати виписати шифротекст, а під ним у стовпець найбільш імовірні заміни для цих літер. У нашому прикладі заміну підібрано у такий спосіб, що літеру абетки замінено саме на найбільш імовірне для неї позначення. Тому сам шифротекст у даному прикладі виписувати немає потреби. Він збігається із середнім рядком послідовності стовпців найбільш імовірних замін.

Що рідше зустрічається літера, тим більшої глибини треба брати стовпець, аби була впевненість, що в стовпці міститься знак відкритого тексту. У нашому випадку стовпці взято однаковою глибиною в п'ять символів, але виписано їх лише для найчастіше вживаних літер.

При дешифруванні без використання засобів автоматизації далі треба вгадувати заміну. Якщо пильно придивитися до тексту, то зробити це не є дуже складно. В тексті є слово АА з двох часто вживаних літер. Що це може бути за слово? У російській мові немає слів ОО, ИИ, НН тощо. Так, перебираючи можливі слова, ми віднайдемо одне слово ЕЕ і дійдемо висновку, що літеру Е було замінено па А. Надто часто в шифротексті слова закінчуються біграмами ЕЕ. В російській мові типовими закінченнями є сполучення ЕЕ, ИИ. З огляду на те, що заміну для літери Е ми вже вгадали, дійдемо висновку, що в шифротексті літери И замінено на Е. Тоді усюди в шифротексті можна провести зворотну заміну. Тепер ми вже можемо вгадувати окремі слова. У такий спосіб, добряче поламавши голову, ми, як у грі "Поле чудес", зрештою відновимо увесь текст.

У стовпцях найбільш імовірних замін літери, котрі відповідають правильним зворотним замінам, має бути позначено як великі. Прочитавши відкритий текст, ви переконаєтесь, що він являє собою одну з кількох

пропозицій з книги С.А. Дориченка та В.В. Ященка «25 этюдов о шифрах», М., 1994.

Для дешифрування в автоматизованому режимі насамперед слід занести до пам'яті комп'ютера словник відповідної мови.

Програма дешифрування повинна, переглядаючи шифротекст, здійснювати спробні зворотні заміни, у припущенні, що на даному фіксованому місці у відкритому тексті перебувало слово, що перевірялося. Після кожної заміни програма частково відновлює ключове підставляння, частково розшифровує текст і відкидає варіант підставляння, якщо в певному місці відновленого тексту виникає літеросполучення, якого не може бути у відкритому тексті розглядуваної мови. Після відновлення певної кількості замін у тексті виникають ділянки, в яких віднайдено значну кількість літер. Решта літер добираються шляхом перебирання словника і підставляння до тексту слів, які не суперечать відновленим попередньо замінам.

Слід зазначити, що практичних навичок з дешифрування шифру простої заміни можна набути лише після проведення самостійних дослідів з дешифрування. [5]

2. Дешифрування шифру перестановки

Для відновлення відкритого тексту шифру перестановки слід переставити стовпці у такий спосіб, аби в рядках з'явився осмислений текст.

Розглянемо приклад дешифрування шифру перестановкою восьми стовпців.

Нехай шифротекст має вигляд, наведений в таблиці 18.3.

Таблиця 18.3 – Шифротекст російською мовою

1	2	3	4	5	6	7	8
п	а	я		в		и	м
0	ч	ш	г		У		е
е	б	ж	л		е		0
м		ч	–	0	т	0	я
	е	г	е		У	с	Щ
	а	к	ь	З	а	т	т
я	Р	е		е	п		ь
	ю	З	в	а	н	в	
0	и	а	в	е	ш	л	
	е	е	я	м		п	н
ь	Р	Р	н	З	е	е	е
З	а	м	а	н		а	к
ч	с	т	а		ь	а	н
0	я	л	м		а	л	
0	ь	ч	х	т	а	т	
в		е	0	а	я	е	я
0	е	Р	м	т	ь	е	
д	с	г	ы		0	а	т
е	б	в	н		ы		
	а	у	и	н	З	н	л
	г	и	а	0	к	к	д
	а	0	б	д	г	н	
	ж	а	У	е	д	я	д
х	л	и		е	м	0	а
к	Р	т	д		ь	0	е
	ь	х	в	т	0	н	
р	л	е		е	д	а	ю
р		З	е	в		е	д
ш		в	а	е	н	е	н
т	и	и	е	в			д
		в		с	д		

Зіставимо перестановці стовпців таблицю 8х8; при цьому поставимо на перетині і-того рядка й j-того стовпця одиницю, якщо j-ий стовпець після зворотної перестановки має слідувати за і-тим. Наше завдання – відновити таблицю, відповідну правильному переставленню стовпців.

Далі попарно прилаштовуватимемо один стовпець до одного. Якщо при цьому в певних рядках виникатимуть заборонені біграми, то стовпці не зможуть у відкритому тексті слідувати один за одним, – й відповідна клітинка закреслюється. В нашому прикладі шостий стовпець не може слідувати за четвертим, тому що інакше в тексті в першому рядку йтимуть дві прогалини

поспіль. Переглянемо, наприклад, шостий рядок. Якби четвертий стовпець слідував за першим, то в тексті були б слова, які розпочинаються з Ь. Після перегляду всіх рядків ми отримаємо таблицю 18.4.

Таблиця 18.4 – Дешифрування шифру перестановки

	1	2	3	4	5	6	7	8
1	X	X		X	X	X		X
2		X		X		X		
3			X					X
4	X	X		X		X	X	X
5	X				X	X	X	X
6	X	X		X		X	X	
7	X			X	X	X	X	X
8	X	X			X	X	X	X

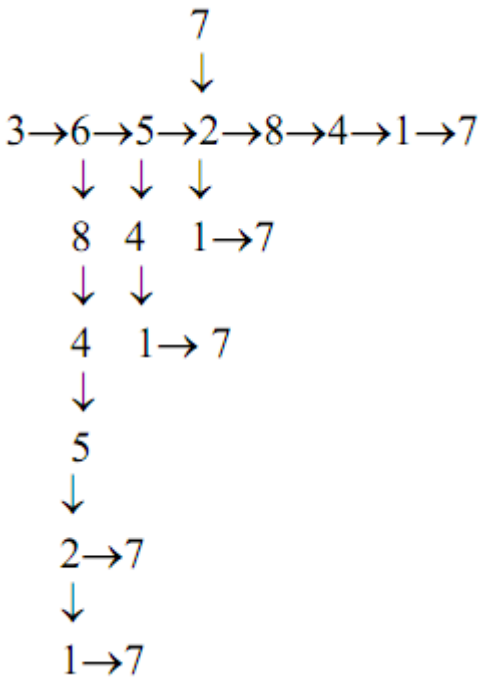
Якби текст був довшим і мав більше рядків, то в кожному рядку й у кожному стовпці залишилося б лише по одній незакресленій клітинці – і перестановку було б відновлено. Стосовно нашої таблиці ми можемо лише стверджувати, що шостий стовпець слідує за третім (позначимо цю подію як 3 —» 6), якщо шостий стовпець не є останнім. Для шостого стовпця можливі два варіанти продовження:

$$\begin{array}{ccccc} & & 8 & & \\ & & \downarrow & & \\ 3 & \rightarrow & 6 & \rightarrow & 5 \end{array}$$

Нам треба розглянути обидва варіанти й спробувати відкинути хибний. Якщо це не вдасться, то слід продовжувані обидва варіанти:

$$\begin{array}{ccccccccc} & & 8 & \rightarrow & 4 & & 1 & & \\ & & \uparrow & & & & \uparrow & & \\ 3 & \rightarrow & 6 & \rightarrow & 5 & \rightarrow & 2 & \rightarrow & 7 \end{array}$$

У підсумку отримаємо певне дерево можливого слідування стовпців у відкритому тексті:



Кожній гілці дерева відповідає певна перестановка стовпців. Далі перевіряємо кожен варіант на осмисленість і дістаємо правильний варіант :

$$3\to6\to5\to2\to8\to4\to1\to7$$

Зауважимо, що не обов'язково було будувати дерево до кінця. Наприклад, гілку $3\to6\to8\to4\to5$ можна було відкинути одразу. Хіба можна визнати за осмислений фрагмент тексту

3	6	8	4	5
я		м		в
ш	У	е	г	
ж	е	0	л	
ч	т	я		0
г	У	Щ	е	3
к	а	т	ь	е
е	а	т		а

Така процедура відкидання гілок була б необхідна, якби рядків було дещо менше й дерево було, відповідно, набагато більш розгалуженим. Запропоновану процедуру легко автоматизувати і зробити придатною для реалізації на ЕОМ.

Алгоритм дешифрування має складатися з таких етапів.

1. Попередня робота. Аналізуючи потужний обсяг відкритих текстів, побудувати множину заборонених біграм.
2. Попередня робота. Скласти словник усіляких *v*-грам для v = 2, 3, *d*, які можуть зустрітися у відкритому тексті. Число *d* обирається виходячи з

можливостей обчислювальної техніки. Побудувати таблицю 8x8. При цьому перебираються послідовно всі помітні біграми і для кожної спробуваної біграми – послідовно всі рядки. Якщо хоча б в одному рядку перший символ біграми зустрічається в і-тому стовпці, а другий – у *j*-тому, то клітинка *іxj* таблиці закреслюється.

3. Обрати певний стовпець за вихідний.
4. Розпочати процедуру побудови дерева шляхом прилаштовування до вихідного стовпця усіх варіантів стовпців.
5. Для кожного отриманого варіанта додати ще один з решти стовпців. Якщо хоча б в одному з рядків таблиці зустрінеться триграма, відсутня у словнику розміщених триграм, – то варіант від кидається.
6. Для кожного з не відкинутих варіантів додаємо ще одного стовпця і проводимо відкидання хибних варіантів за словником дозволених чотириграм.

Якщо словник побудовано лише для $d < 3$, то відкидання проводиться шляхом перевірки на припустимість триграм, які зустрілися в останніх трьох стовпцях кожного рядка. Продовжуємо цей процес до здійснення повної перестановки. Нижче наведено відновлений для нашого прикладу текст.

Таблиця 18.5 – Відновлений текст

	1	2	3	4	5	6	7	8
1	я		в	а	м		п	и
2	ш	у		ч	е	г	0	
3	ж	е		б	0	л	е	
4	ч	т	0	1	я		М	0
5	г	У		е	Щ	е		с
6	к	а	З	а	т	ь		т
7	е	п	е	Р	ь		я	
8	З	н	а	ю		в		в
9	а	ш	е	и		в	0	л
10	е		м	е	н	я		п
11	Р	е	З	Р	е	н	ь	е
12	м		н	а	к	а	З	а
13	т	ь		с	н	а	ч	а
14	л	а		я		м	0	л
15	ч	а	т	ь		х	0	т
16	е	л	а		п	0	в	е
17	Р	ь	т	е		м	0	е
18	г	0		с	т	ы	д	а
19	в	ы		б		н	е	
20	у	З	н	а	л	и		н
21	е	к	0	г	д	а		к
22	0	г	Д	а		б		н
23	а	д	е	ж	д	У		я
24	и	м	е	л	а		х	0
25	т	ь		Р	е	д	к	0
26	х	0	т	ь		в		н
27	е	д	е	л	ю		Р	а
28	З		в		д	е	Р	е
29	в	н	е		н	а	ш	е
30	и		в	и	д	е	т	ь
31	в	а	с					

Зауваження стосовно ступеня неоднозначності відновлення відкритого тексту. В обох прикладах нам вдалося, хоча й за певних зусиль, відновити відкриті тексти. Робота з дешифрування значно полегшується зі збільшенням довжини шифротексту (чи, як говорять, обсягу наявного в розпорядженні матеріалу перехоплення). Якби обсяг матеріалу було збільшено кількаразово, то в другому прикладі в таблиці 8x8 з великою ймовірністю було б закреслено всі клітинки, окрім відповідних справжньому порядку слідування один за одним стовпців у відкритому тексті. У першому прикладі варіаційний ряд частоти вживаності літер відкритого тексту майже повністю збігався б з варіаційним рядом ймовірностей знаків відкритого тексту і нам залишалося підписати один варіаційний ряд під іншим і здійснити зворотну заміну. Окремі

помилки легко усувалися б при першому ж прочитуванні дешифрованого варіанта тексту. З іншого боку, при зменшенні обсягу матеріалу завдання дешифрування істотно ускладнюється. Насправді, уявіть собі, що вам запропоновано дешифрувати зашифрований за допомогою простої заміни шифртекст, складений з одного першого слова нашого першого прикладу – ДОЧАЛЬ. Для кожного слова з шести різних літер віднайдеться проста заміна, застосовуючи яку ми отримаємо даний шифротекст. Проблема полягає не в тому, як віднайти ключову підстановку, а в тому, як обрати з численної кількості варіантів відновлених відкритих текстів саме той, котрий було зашифровано.

Отже, важливою характеристикою ефективності криптографічного захисту є ступінь неоднозначності відновлення відкритою тексту за шифрованим. Подамо якісне означення цього поняття. Під ступенем неоднозначності природно розуміти математичне сподівання кількості варіантів відкритих текстів, які може бути отримані за допомогою застосовування алгоритму дешифрування. Якщо припустити, що за випадкового вибору хибного ключа (ключа, розбіжною зі справжнім ключем, із застосуванням якого було отримано шифротекст, відновлений при розшифровуванні) і розшифровування на цьому випадковому хибному ключі, розшифрований текст не відрізняється від випадкового тексту, то ймовірність того, що отриманий текст довжини N буде осмисленим (за класичним означенням ймовірностей), дорівнює відношенню кількості сприятливих завершень – кількості $A(N)$ осмислених відкритих текстів довжини N до загальної кількості текстів довжини N, котра дорівнює n^N, де n – кількість літер в абетці відкритих текстів. Для того аби дістати ступінь неоднозначності, слід помножити отримане відношення на кількість K варіантів ключів, звідки дістаємо формулу

$$r = r(N) = KA(N)n^{-N}$$

для обчислення ступеня неоднозначності L відновлення відкритого тексту. Отже, шифрування забезпечує надійний захист повідомлення, якщо неоднозначність відновлення відкритого тексту за шифрованим є надто велика.

Ступінь неоднозначності дозволяє класифікувати шифри за ступенем їхньої криптографічної стійкості. Якісні міркування тут є такі. Якщо неоднозначність дешифрування (можлива кількість отриманих відкритих текстів) є *r(N),* а мета дешифрування визначена отриманням відкритого справжньою тексту, то ймовірність отримання саме його оцінюється величиною *l/r(N)*. Шифри, для яких *r(N) = A(N),* називаються ***абсолютно (теоретично) стійкими*** (для абсолютно стійкого шифру застосування будь-якого алгоритму дешифрування не надає жодної інформації про відкритий текст). До останньої формули, її висновку та її трактувань слід ставитися надто обережно. Насправді для отримання абсолютної стійкості шифру досить мати n^N, ключів.

Шифри, які теоретично не є стійкими, для яких надійність криптографічного захисту забезпечується надто великою складністю реалізувування відомих алгоритмів дешифрування, називають ***практично стійкими.***

Шифри, котрі не належать до класів теоретично стійких чи практично стійких шифрів, називають ***шифрами тимчасової стійкості.***

Кількість осмислених відкритих текстів довжини *N* для великих значень *N* зазвичай вважається 2^{HN}, де *H* – ентропія (в бітах) на знак відкритого тексту. Для літературного тексту, як засвідчують експериментальні розрахунки, величина *H* є наближена до одиниці. Для більш формалізованих текстів (організаційно-розпорядчих листів, документів тощо) величина *H* перебуває в межах від 0,5 до 0,8.

Повертаючись до аналізу шифру простої заміни, зауважимо, що ступінь неоднозначності відновлення відкритого тексту для цього шифру має вигляд

$$r(N) = \frac{n!2^{HN}}{n^N},$$

де *H* – ентропія на літеру відкритого тексту.

Шифр простої заміни є теоретично стійким при шифруванні літературного тексту *(n* = 32) довжиною в одне-два слова і забезпечує лише тимчасову стійкість за великого обсягу матеріалу,

Експерименти засвідчують, що практичне дешифрування шифру простої заміни для літературного тексту є можливе в разі, якщо довжина шифротексту вдвічі-втричі перевищує розмір абетки відкритою тексту, тобто дорівнює 60... 100 літерам. [5]