**Лекция 2. Шифры сложной замены и код. Способы их вскрытие. Весовой критерий.**

Шифры сложной замены называют многоалфавитными, так как для шифрования каждого символа исходного сообщения применяют свой шифр простой замены. Многоалфавитная подстановка последова­тельно и циклически меняет используемые алфавиты. При *r*-алфавитной подстановке символ *х0* исходного сообщения за­ме­няется символом из алфавита Во, символ *х1*символом из алфави­та B1, и так далее, символ *хr-1* заменяется символом из алфавита Br-1, символ *хr*  заменяется символом снова из алфавита Во, и т.д.

*Общая схема многоалфавитной подстановки* (*r*=4):

Входной символ *х0 х1 х2 х3 х4 х5 х6 х7 х8 х9*

Алфавит подстановки B0 B1 B2 B3 B0 B1 B2 B3 B0 B1

Эффект использования многоалфавитной подстановки за­ключается в том, что обеспечивается маскировка естественной статистики исходного языка, так как конкретный символ из исход­ного алфавита Х может быть преобразован в несколько различ­ных символов шифровальных алфави­тов В. Степень обеспечи­ваемой защиты теоретически пропорцио­наль­на длине периода *r*  в последо­ватель­ности используемых алфавитов В.

Для *многоалфавитной подстановки Ек* ключ подстановки *К* представляет собой последовательность подстановок из некоторого множества *Π*:

*К* = {(π*0,* π*1, … ,* π*n-1*)*,*  π*i* *Π* }*,* 1 *n* < 

В случае блочного шифра эта подстановкашифрует *п*-грамму (блок) открытого текста

(*х*0, *х*1, *х*2, … , *хn-1*) в *п*-грамму (*y*0, *y*1, *y*2, … , *yn‑1*) шифртекста в соответствии с формулой:

*yi* = π*i* (*хi*), 0  *i* < *n*, *п* = 1, 2, 3, ... .

При *n*→мы приближаемся к теоретически стойкой одноразовой системе шифрования.

Данный шифр может быть использован и для потокового шифрования, где открытый текст шифруется побуквенно (буква за буквой). При этом *i*-ая буква шифртекста является функцией только *i*-ой компо­ненты π*i* ключа К и *i*-ой буквы *хi*; открытого текста;

Диск Альберти. Многоалфавитные шифры замены предложил и ввел в практику криптографии Леон Батист Альберти, который также был известным архитектором и теоретиком искусства. Он же впервые выдвинул идею повторного шифрования, которая в виде идеи многократного шифрования лежит в основе всех современных шифров с секретным ключом. Кроме шифра многоалфа­витной замены, Альберти также подробно описал устройства для его реализации. Диск Альберти представляет собой систему из внешнего неподвижного и внутреннего подвижного дисков, на которые нанесены символы алфавита и цифры. На внешнем в алфавитном порядке, на внутреннем в произвольном. Ключом шифрования являются порядок букв на внутреннем диске и начальное положение внутреннего диска относительно внешнего. После шифрования слова внутренний диск сдвигался на один шаг. Количество алфавитов r в нем равно числу символов на диске.

Шифр Цезаря многоалфавитный. В отличие от простого шифра Цезаря, многоалфавит­ный или система шифрования Цезаря образуется множеством одноалфавитных подстановок, определяемых функциями шифрования Е*k* для различных значений ключа *k*, причем 0  *k* < *m,* где *m*-основание алфавита.

В соответствии с этой системой буква *x*∈*Zm* открытого текста преобразуется в букву *y*∈*Zm* шифртекста согласно следующему правилу:

Е*k* : *y* = (*x + k*) mod *m*,

где *x* - числовой код буквы открытого текста; *y* -числовой код соответствующей буквы шифртекста.

Концепция, заложенная в систему шифрования Цезаря, оказалась весьма плодотворной, о чем свидетельствуют ее многочисленные модификации.

Шифр Гронсфельда. Этот шифр сложной замены, называемый шифром Гронс­фельда, представляет собой модификацию шифра Цезаря число­вым ключом. Для этого под буквами исходного сообщения записы­вают цифры *числового ключа*. Если ключ короче сообщения, то его запись циклически повторяют.

Шифртекст получают аналогично, как в шифре Цезаря, но отсчитывают по алфавиту не третью букву (как это делается в шифре Цезаря), а выбирают ту букву, которая смещена по алфавиту на соответствующую цифру ключа. Напри­мер,

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Сообщение | В | О | С | Т | О | Ч | Н | Ы | Й |  | Э | К | С | П | Р | Е | С | С |
| Ключ | 2 | 7 | 1 | 8 | 2 | 7 | 1 | 8 | 2 |  | 7 | 1 | 8 | 2 | 7 | 1 | 8 | 2 |
| Шифртекст | Д | Х | Т | Ь | Р | Ю | О | Г | Л |  | Д | Л | Щ | С | Ч | Ж | Щ | У |

Чтобы зашифровать первую букву сообщения В, исполь­зуя первую цифру ключа 2 , нужно отсчитать вторую по порядку букву от В, получается первая буква шифртекста Д.

Следует отметить, что шифр Гронсфельда вскрывается относитель­но легко, если учесть, что в числовом ключе каждая цифра имеет только десять значений, а значит, имеется лишь де­сять вариантов прочтения каждой буквы шифртекста. Модификация шифра Гронсфельда *с буквенным ключом* предполагает смещение на величину, равную номеру буквы ключа в алфавите. При этом улучшается стой­кость, за счет увеличения размерности ключевого пространства. Шифр Гронсфельда представляет собой по существу ча­стный случай системы шифрования Вижинера.

Система шифрования Вижинера впервые была опубликована в 1586 г. и является одной из старейших и наиболее известных многоалфавитных систем. Свое название она получила по имени француз­ского дипломата XVI века Блеза Вижинера.

Этот шифр многоалфавитной замены можно описать таблицей шифрования, называемой таблицей (квадратом) Вижинера. Размер таблицы Вижинера равен длине алфавита. Первая строка имеет цифровой ключ «0» и заполняется всеми символами по алфавиту, вторая имеет цифровой ключ «1» и заполняется теми же символами, сдвинутыми вправо на один символ по кругу, и далее. *k*‑ая имеет цифровой ключ «*к-1*» и заполняется теми же символами, сдвинутыми вправо на (*к-1*) символ по кругу.

Приведем фрагмент таблицы Вижинера для русского алфавита.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **а** | **б** | **в** | **г** | **д** | **е** | **ж** | **з** | **и** | **й** | **к** | **л** | **м** | **н** | **о** | **п** | **р** | **с** | **т** | **у** | **ф** | **х** | **ц** | **ч** | **ш** | **щ** | **ь** |
| 0 | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь |
| 1 | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы |
| 2 | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ |
| 3 | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э |
| 4 | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю |
| 5 | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я |
| 6 | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а |

Таблица Вижинера используется для зашифрования и расшифрования. Она имеет два входа:

* верхнюю строку подчеркнутых символов, используемую для считывания очередной буквы исходного открытого текста;
* крайний левый столбец ключа.

Ключ представляет собой последовательность цифр или слово (чтобы ключ легче было запомнить), в последнем случае буквы ключевого слова заменяют на их порядковые номера в алфавите.

При шифровании исходного сообщения его выписывают в строку, а под ним записывают ключевое слово. Если ключ оказался короче сообщения, то его циклически повторяют. В процессе шифрования очередная буква шифртекста находится на пересече­нии столбца, определяемого шифруемой буквой, и строки, опре­деляемой значением ключа.

Рассмотрим пример получения шифртекста с помощью таблицы Вижинера. Пусть выбрано ключевое слово АМБРОЗИЯ. Необходимо зашифровать сообщение ПРИЛЕТАЮ СЕДЬМОГО.

Выпишем исходное сообщение в строку и запишем под ним ключе­вое слово с повторением. В третью строку выпишем шифртекст.

Сообщение П Р И Л Е Т А Ю С Е Д Ь М О Г О

Ключ АМ Б Р О З И Я А М Б Р О З И Я

Шифртекст П Ъ Й Ы УЩИ Э С С Е К Ь Х Л Н

Шифры Вижинера с коротким периодическим ключом используются и в наши дни в системах шифрования, от которых не требуется высокая криптостойкость. Так, например они использо­вались в программе-архиваторе ARJ в программе Word версии 6.

С развитием математики необходимость в таблицах шифрования отпала. Если заменить буквы на числа, то операции шифрования и дешифрования легко выражаются простыми математическими формулами. Так в шифре Вижинера используются операции циклического или модульного сложения (при шифровании) и вычитания (при дешифровании).

Пусть ключевая последовательность системы Вижинера имеет длину *r*, тогда ключ  *r*-алфавитной подстановки, который является строкой букв или цифр можно представить в виде последовательности подстановок

π =( π*0,* π*1, … ,* π*r-1*)*,*

Функция шифрования Вижинера Еπ: *х → y* преобразует

открытый текст *х*=(*х0*, *х1*, *х2*, … , *хn-1*) в шифртекст *y* = (*y0*, *y1*, *y2*, … , *yn-1*)

согласно правилу:

*y* = (*y0*, *y1*, *y2*, … , *yn-1*) = (π0(*х0*), π1(*х1*), … , π*n-1*(*хn-1*)), где π*i* =π(*i* mod *r*).

**Приведем таблицы частот биграмм** для русского языка. Для удобства они разбиты на четыре части по следующей схеме:

|  |
| --- |
| **Часть 1** |
|   | **А** | **Б** | **В** | **Г** | **Д** | **Е** | **Ж** | **З** | **И** | **Й** | **К** | **Л** | **М** | **Н** | **О** | **П** |
| **А** | 2 | 12 | 35 | 8 | 14 | 7 | 6 | 15 | 7 | 7 | 19 | 27 | 19 | 45 | 5 | 11 |
| **Б** | 5 |   |   |   |   | 9 | 1 |   | 6 |   |   | 6 |   | 2 | 21 |   |
| **В** | 35 | 1 | 5 | 3 | 3 | 32 |   | 2 | 17 |   | 7 | 10 | 3 | 9 | 58 | 6 |
| **Г** | 7 |   |   |   | 3 | 3 |   |   | 5 |   | 1 | 5 |   | 1 | 50 |   |
| **Д** | 25 |   | 3 | 1 | 1 | 29 | 1 | 1 | 13 |   | 1 | 5 | 1 | 13 | 22 | 3 |
| **Е** | 2 | 9 | 18 | 11 | 27 | 7 | 5 | 10 | 6 | 15 | 13 | 35 | 24 | 63 | 7 | 16 |
| **Ж** | 5 | 1 |   |   | 6 | 12 |   |   | 5 |   |   |   |   | 6 |   |   |
| **З** | 35 | 1 | 7 | 1 | 5 | 3 |   |   | 4 |   | 2 | 1 | 2 | 9 | 9 | 1 |
| **И** | 4 | 6 | 22 | 5 | 10 | 21 | 2 | 23 | 19 | 11 | 19 | 21 | 20 | 32 | 8 | 13 |
| **Й** | 1 | 1 | 4 | 1 | 3 |   | 1 | 2 | 4 |   | 5 | 1 | 2 | 7 | 9 | 7 |
| **К** | 24 | 1 | 4 | 1 |   | 4 | 1 | 1 | 26 |   | 1 | 4 | 1 | 2 | 66 | 2 |
| **Л** | 25 | 1 | 1 | 1 | 1 | 33 | 2 | 1 | 36 |   | 1 | 2 | 1 | 8 | 30 | 2 |
| **М** | 18 | 2 | 4 | 1 | 1 | 21 | 1 | 2 | 23 |   | 3 | 1 | 3 | 7 | 19 | 5 |
| **Н** | 54 | 1 | 2 | 3 | 3 | 34 |   |   | 58 |   | 3 |   | 1 | 24 | 67 | 2 |
| **О** | 1 | 28 | 84 | 32 | 47 | 15 | 7 | 18 | 12 | 29 | 19 | 41 | 38 | 30 | 9 | 18 |
| **П** | 7 |   |   |   |   | 15 |   |   | 4 |   |   | 9 |   | 1 | 46 |   |

|  |
| --- |
| **Часть 2** |
|   | **Р** | **С** | **Т** | **У** | **Ф** | **Х** | **Ц** | **Ч** | **Ш** | **Щ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |
| **А** | 26 | 31 | 27 | 3 | 1 | 10 | 6 | 7 | 10 | 1 |   |   | 2 | 6 | 9 |
| **Б** | 8 | 1 |   | 6 |   |   |   |   |   | 1 | 11 |   |   |   | 2 |
| **В** | 6 | 19 | 6 | 7 |   | 1 | 1 | 2 | 4 | 1 | 18 | 1 | 2 |   | 3 |
| **Г** | 7 |   |   | 2 |   |   |   |   |   |   |   |   |   |   |   |
| **Д** | 6 | 8 | 1 | 10 |   |   | 1 | 1 | 1 |   | 5 | 1 |   |   | 1 |
| **Е** | 39 | 37 | 33 | 3 | 1 | 8 | 3 | 7 | 3 | 3 |   |   | 1 | 1 | 2 |
| **Ж** |   | 1 |   |   |   |   |   |   |   |   |   |   |   |   |   |
| **З** | 3 | 1 |   | 2 |   |   |   |   |   |   | 4 |   |   |   | 4 |
| **И** | 11 | 29 | 29 | 3 | 1 | 17 | 3 | 11 | 1 | 1 |   |   | 1 | 3 | 17 |
| **Й** | 3 | 10 | 2 |   |   |   | 1 | 3 | 2 |   |   |   |   |   |   |
| **К** | 10 | 3 | 7 | 10 |   |   | 1 |   |   |   |   |   |   |   |   |
| **Л** |   | 3 | 1 | 6 |   | 4 |   | 1 |   |   | 3 | 20 |   | 4 | 9 |
| **М** | 2 | 5 | 3 | 9 | 1 |   |   | 2 |   |   | 5 | 1 | 1 |   | 3 |
| **Н** | 1 | 9 | 9 | 7 | 1 |   | 5 | 2 |   |   | 36 | 3 |   |   | 5 |
| **О** | 43 | 50 | 39 | 3 | 2 | 5 | 2 | 12 | 4 | 3 |   |   | 2 | 3 | 2 |
| **П** | 41 | 1 |   | 6 |   |   |   |   |   |   | 2 |   |   |   | 2 |

|  |
| --- |
| **Часть 3** |
|   | **А** | **Б** | **В** | **Г** | **Д** | **Е** | **Ж** | **З** | **И** | **Й** | **К** | **Л** | **М** | **Н** | **О** | **П** |
| **Р** | 55 | 1 | 4 | 4 | 3 | 37 | 3 | 1 | 24 |   | 3 | 1 | 3 | 7 | 56 | 2 |
| **С** | 8 | 1 | 7 | 1 | 2 | 25 |   |   | 6 |   | 40 | 13 | 3 | 9 | 27 | 11 |
| **Т** | 35 | 1 | 27 | 1 | 3 | 31 |   | 1 | 28 |   | 5 | 1 | 1 | 11 | 56 | 4 |
| **У** | 1 | 4 | 4 | 4 | 11 | 2 | 6 | 3 | 2 |   | 8 | 5 | 5 | 5 | 1 | 5 |
| **Ф** | 2 |   |   |   |   | 2 |   |   | 2 |   |   |   |   |   | 1 |   |
| **Х** | 4 | 1 | 4 | 1 | 3 | 1 |   | 2 | 3 |   | 4 | 3 | 3 | 4 | 18 | 5 |
| **Ц** | 3 |   |   |   |   | 7 |   |   | 10 |   | 2 |   |   |   | 1 |   |
| **Ч** | 12 |   |   |   |   | 23 |   |   | 13 |   | 2 |   |   | 6 |   |   |
| **Ш** | 5 |   |   |   |   | 11 |   |   | 14 |   | 1 | 2 |   | 2 | 2 |   |
| **Щ** | 3 |   |   |   |   | 8 |   |   | 6 |   |   |   |   | 1 |   |   |
| **Ы** |   | 1 | 9 | 1 | 3 | 12 |   | 2 | 4 | 7 | 3 | 6 | 6 | 3 | 2 | 10 |
| **Ь** |   | 2 | 4 | 1 | 1 | 2 |   | 2 | 2 |   | 6 |   | 3 | 13 | 2 | 4 |
| **Э** |   |   |   |   |   |   |   |   |   |   | 1 |   |   | 1 |   |   |
| **Ю** |   | 2 | 1 | 2 | 1 |   |   | 3 | 1 |   | 1 |   | 1 | 1 | 1 | 3 |
| **Я** | 1 | 3 | 9 | 1 | 3 | 3 | 1 | 5 | 3 | 2 | 3 | 3 | 4 | 6 | 3 | 6 |

|  |
| --- |
| **Часть 4** |
|   | **Р** | **С** | **Т** | **У** | **Ф** | **Х** | **Ц** | **Ч** | **Ш** | **Щ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |
| **Р** | 1 | 5 | 9 | 16 |   | 1 | 1 | 1 | 2 |   | 8 | 3 |   |   | 5 |
| **С** | 4 | 11 | 82 | 6 |   | 1 | 1 | 2 | 2 |   | 1 | 8 |   |   | 17 |
| **Т** | 26 | 18 | 2 | 10 |   |   |   | 1 |   |   | 11 | 21 |   |   | 4 |
| **У** | 7 | 14 | 7 |   |   | 1 |   | 8 | 3 | 2 |   |   |   | 9 | 1 |
| **Ф** | 1 | 1 |   |   |   |   |   |   |   |   |   |   |   |   |   |
| **Х** | 3 | 4 | 2 | 2 | 1 |   |   | 1 |   |   |   |   |   |   |   |
| **Ц** |   |   |   | 1 |   |   |   |   |   |   | 1 |   |   |   |   |
| **Ч** |   |   | 7 | 1 |   |   |   |   | 1 |   |   | 1 |   |   |   |
| **Ш** |   |   |   | 1 |   |   |   |   |   |   |   | 1 |   |   |   |
| **Щ** |   |   |   | 1 |   |   |   |   |   |   |   |   |   |   |   |
| **Ы** | 3 | 9 | 4 | 1 |   | 16 |   | 1 | 2 |   |   |   |   |   |   |
| **Ь** | 1 | 11 | 3 |   |   |   |   | 1 | 4 |   |   |   | 1 | 3 | 1 |
| **Э** |   | 1 | 9 |   |   |   |   |   |   |   |   |   |   |   |   |
| **Ю** | 1 | 1 | 7 |   |   |   | 1 | 1 |   | 4 |   |   |   |   |   |
| **Я** | 3 | 6 | 10 |   |   | 2 | 1 | 4 | 1 | 1 |   |   | 1 | 1 | 1 |



Рис.3

Хорошие таблицы *k*-грамм легко получить, используя тексты электронных версий многих книг, содержащихся на CD-дисках.

Для получения более точных сведений об открытых текстах можно строить и анализировать таблицы *k*-грамм при *k*>2, однако для учебных целей вполне достаточно ограничиться биграммами. Неравномерность *k*-грамм (и даже слов) тесно связана с характерной особенностью открытого текста – наличием в нем большого числа повторений отдельных фрагментов текста: корней, окончаний, суффиксов, слов и фраз. Так, для русского языка такими привычными фрагментами являются наиболее частые биграммы и триграммы:

**СТ, НО, ЕН, ТО, НА, ОВ, НИ, РА, ВО, КО
СТО, ЕНО, НОВ, ТОВ, ОВО, ОВА**

Полезной является информация о сочетаемости букв, то есть о предпочтительных связях букв друг с другом, которую легко извлечь из таблиц частот биграмм.

