# Лекция 4. Криптография (шифрование информации)

Приступаем к изучению одной из 64 техник, которой должна была владеть каждая уважающая себя индианка – ее основы изложены в Камасутре

## Термины

**Шифрование** (encryption) – преобразование открытого текста (plaintext) в зашифрованный (ciphertext) с целью защитить его конфиденциальность

Cipher – обозначать условным знаком, кодом.

Зашифрование (enciphering)/расшифрование (deciphering)

Письменность – шифрование, а уж запись на иностранном языке – тем более.

Демарт в 5 веке до н.э. при осаде города Ксерксом отправил деревянные таблички, покрытые воском в дружественный город

## Требования к алгоритмам шифрования:

1. Сложность расшифровки и модификации
2. Малое изменение исходного текста или ключа влечет значительное изменение шифртекста
3. Область значений ключа должна исключать его перебор
4. Стоимость дешифрации превышает стоимость данных

Правило Огюста Керкхоффа (голландец, 1835-1903 гг.): стойкость алгоритма определяется только секретностью ключа.

Алгоритм шифрования НЕ ЯВЛЯЕТСЯ СЕКРЕТНЫМ, а значит, можно вести открытое обсуждение достоинств и недостатков алгоритма, что переводит работы по криптологии в разряд ОТКРЫТЫХ научных работ, допускающих дискуссии, верификацию и публикации. (эмпирическая проверка)

Книга «Военная криптография» ("La cryptographie militaire") вышла в 1883 году.

Труды Керкхоффа - фламандская грамматика, английская грамматика, справочник немецких пословиц, лингвистические, историко-филологические работы.

Активно участвовал в общественной жизни: основал Общество содействия просвещению в Мелю, был членом Французского общества археологии, возглавлял Международную академию воляпюка и Французскую ассоциацию пропаганды воляпюка, был командиром католического Ордена Христа.

Принципы & desiderata (требования)

1. Массовость (постоянно используемый метод сложной защиты, а не шифрование время от времени писем ограниченного круга лиц)
2. Эмпирическая поддержка теоретической стойкости путем криптоатак

Не понятно, что заставило уже известного к тому времени лингвиста, гуманиста, космополита и сторонника развития международной торговли и мирного сосуществования наций, почти **в 50-летнем возрасте** обратиться к теме секретных военных коммуникаций. Можно было бы предположить в качестве причины франко-прусскую войну 1870-71 гг., однако известно, что еще десятью годами ранее он претендовал на кафедру немецкого языка в Высшей военной школе в Париже и не прошел конкурс лишь по недоразумению.

Керкхофф предсказал выход криптографии на широкие массы:

Криптология и криптография меняют основного потребителя - теперь это гражданские организации и частные лица (предыдущим было появление телеграфной связи).

Если бы немцы прочитали этот труд, энигму бы не взломали.

**Рассеивание** – влияние одного знака открытого текста на несколько знаков шифротекста.

## Симметричные алгоритмы

Это алгоритмы с единым секретным ключом (для шифрования и расшифровки)

Общая схема симметричного шифрования

Открытый текст M1M2M3

Шифрование

Открытый текст M1M2M3

Зашифрованный текст C1C2C3

Расшифровка

Ключ K

## Симметричные методы шифрования

* + Шифры перестановки (permutation, P-блоки);
  + Шифры замены (подстановки, substitution, S-блоки):
    1. моноалфавитные (код Цезаря);
    2. полиалфавитные (шифр Виженера, цилиндр Джефферсона, диск Уэтстоуна, Enigma);
  + составные (Lucipher (фирма IBM, США); DES (Data Encryption Standard, США); FEAL-1 (Fast Enciphering Algoritm, Япония); IDEA/IPES (International Data Encryption Algorithm); Improved Proposed Encryption Standard, фирма Ascom-Tech AG, Швейцария); B-Crypt (фирма British Telecom, Великобритания); ГОСТ 28147-89 (СССР); Skipjack (США)).

Перестановки

Древний метод шифрования «скитала»

На палку определенного диаметра наматывается лента, на которой построчно пишется сообщение. **Палка является ключом**.

Все сводится к **записи** сообщения в **матрицу**.

Перестановка по правилу

Текст: шифровка секрет

Правило: 3-1-2

Шифртекст: фшивро каксетре

Циклический сдвиг

Код символа сдвигается – первые коммерческие версии роторов Энигмы (A->K, B->L, C->M)

Подстановки (замены)

Одноалфавитные подстановки

Шифр Юлия Цезаря (100-44 гг. до н.э.)

Для исходного символа s, зашифрованным символом будет

C(s)=(ord(s)+shift) mod (длина алфавита + 1)

HELLO FRIENDS -> JGNNQBHTKGPFU

У Цезаря shift=3, а у Цезаря Августа - 4

Ключ можно подобрать простым перебором (так называемой силовой атакой).

Квадрат Полибия

Буквы алфавита записываются в прямоугольник, после чего каждый шифруемый символ заменяется на стоящий под ним в прямоугольнике.

Все варианты одноалфавитной подстановки букв сводятся к замене по формуле:

C(s)=(А(s)+B) mod D, где А-множитель, В-сдвиг, D-длина алфавита.

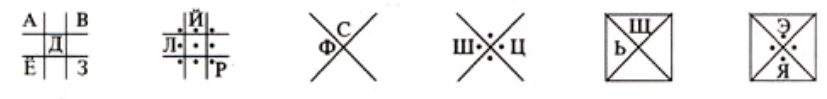
Дополнительно можно заполнять квадрат произвольно и менять его по ходу шифрования.

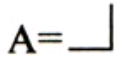
Двойной квадрат (шифрование биграммами)

Диграфы

Шифр PigPen

Алфавит составляется по следующему правилу:



Таким образом, и т.д.

Великий шифр Людовика XIV

Числом кодируется **сочетание символов**

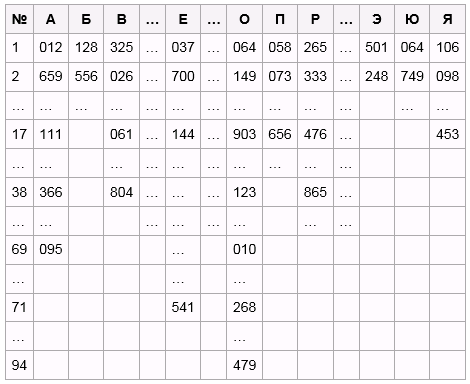
Добавлено специальное **число для удаления** предыдущегослова

Переходный алгоритм (статистику скрывает):

Таблица омофонов (омофоническая замена) (англ. Homophonic substitution cipher)

Подстановки, при которой каждый символ открытого текста заменяется на **один из нескольких символов шифралфавита**, причём количество заменяющих символов для одной буквы пропорционально частоте этой буквы.

Число замен для каждого символа берется пропорционально вероятности появления этого символа в открытом тексте. Например, если выбрать шифр 3 цифрами (и их общее количество равно 1000), то для самого частого символа будет много строк, а для самого редкого - 1



1 символ заменяется по очереди несколькими кодами (например, 3-циферными), число которых ~ частоте символа в языке

-> все новые коды образуют равномерное распределение

Скрывает настоящую частоту появления данной буквы в зашифрованном тексте

Индекс соответствия (ИС)

ИС=Сумма всех (F(f-1))/N\*(N-1), где f-встречаемость буквы, N-число букв.

Для английского языка ИС>0,066 – однозначный признак использования моноалфавитной подстановки. ИС>0,052 – двухалфавитная и т.д.

Многоалфавитные подстановки

Маскируют естественную частотную статистику языка

Для каждой буквы алфавита строится массив символов замены такие, что:

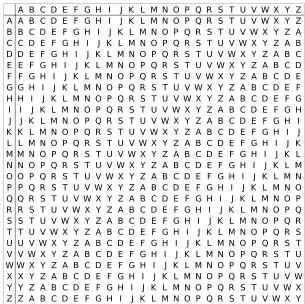
1) ни одна пара массивов не пересекается, т.е. не содержит одинаковых элементов.

2) количество символов замены в каждом массиве пропорционально частоте появления буквы в открытом тексте

Скрывается частота появления символа.

Шифр Виженера

Последовательность нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера (каждая следующая строка сдвигается на несколько позиций - 26 различных шифров Цезаря).



На каждом шаге используются различные алфавиты, выбираемые в зависимости от очередного символа ключевого слова Ki.

Символ ключа фиксирует строку

Символ сообщения задает столбец

Каждый символ Мi шифруется строкой Кi – зашифрованный символ находится на пересечении строки Кi и столбца Мi в таблице Виженера.

Использование вычислительной техники позволяет для любого алгоритма подстановки или перестановки использовать **группы бит любой длины**!

### Блочные

(шифрование данных поблочно без взаимосвязей между блоками):

Виды блочного шифрования:

* + Кодовая книга (простая замена), одноразовый блокнот
  + Сложение с одноразовым или бесконечным ключом (infinite-key cipher)

Сложение по модулю 2 (XOR): 0101 XOR 0011=0110 XOR 0011=0101

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 101100011101 | p | 100111101110 |
| k | 001011110011 | k | 001011110011 |
| p | 100111101110 | 1 | 101100011101 |

Рекомендуется только для коротких сообщений (1-несколько блоков).

* + на основе генератора псевдослучайных чисел (ПСЧ), гаммирование – наложение на открытые данные гаммы шифра (случайной или псевдослучайной последовательности единиц и нулей).

Генератор потока ключей f(K)

Порождающий ключ K

Шифруемое сообщение M

Зашифрованное сообщение C

* + Шифр Вернама (XOR текста с конечным ключом – система Vernam – повторяемым бесконечно (целиком или частично))

Использовался для шифрования телеграфных сообщений, которые представляли собой бинарные тексты, в которых открытый текст представляется в [коде Бодо](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%B4_%D0%91%D0%BE%D0%B4%D0%BE) (в виде пятизначных «импульсных комбинаций»). В этом коде, например, буква «А» имела вид (1 1 0 0 0). На бумажной ленте цифре «1» соответствовало отверстие, а цифре «0» — его отсутствие

Для произведения шифротекста открытый текст объединяется операцией «исключающее ИЛИ» с ключом. Операция выполнялась автоматически — надо было только подать на шифровальщик ленту с ключом.

Каждая **лента должна использоваться только один раз** и после этого уничтожаться, что трудноприменимо на практике. Аппарат был переделан на **несколько закольцованных лент с взаимно простыми периодами**.

### Поточное шифрование

Шифрование потока данных; используется в линиях связи – возможны помехи -> нужна избыточность

Сцепление блоков шифра – использование обратной связи дает рассеивание

Если подряд будут идти 2 одинаковых блока, в c2 будет синхропосылка.

Последний блок шифротекста зависит от синхросигнала, ключа и текста.

Синхропосылка с0

р1

р2

рN

Шифрование (с ключом)

с1

Шифрование (с ключом)

с2

Шифрование (с ключом)

сN

Для расшифровки – обратный порядок (XOR, расшифровка)

Шифр Фейстеля (Feistel)

L

R

F(k)

L

R

F(k) содержит **замены**

Обратная связь по шифротексту

s(0) длиной n бит; текст длиной t бит

Открытый текст р (блоки по t бит)

Зашифрованный текст с(i): t

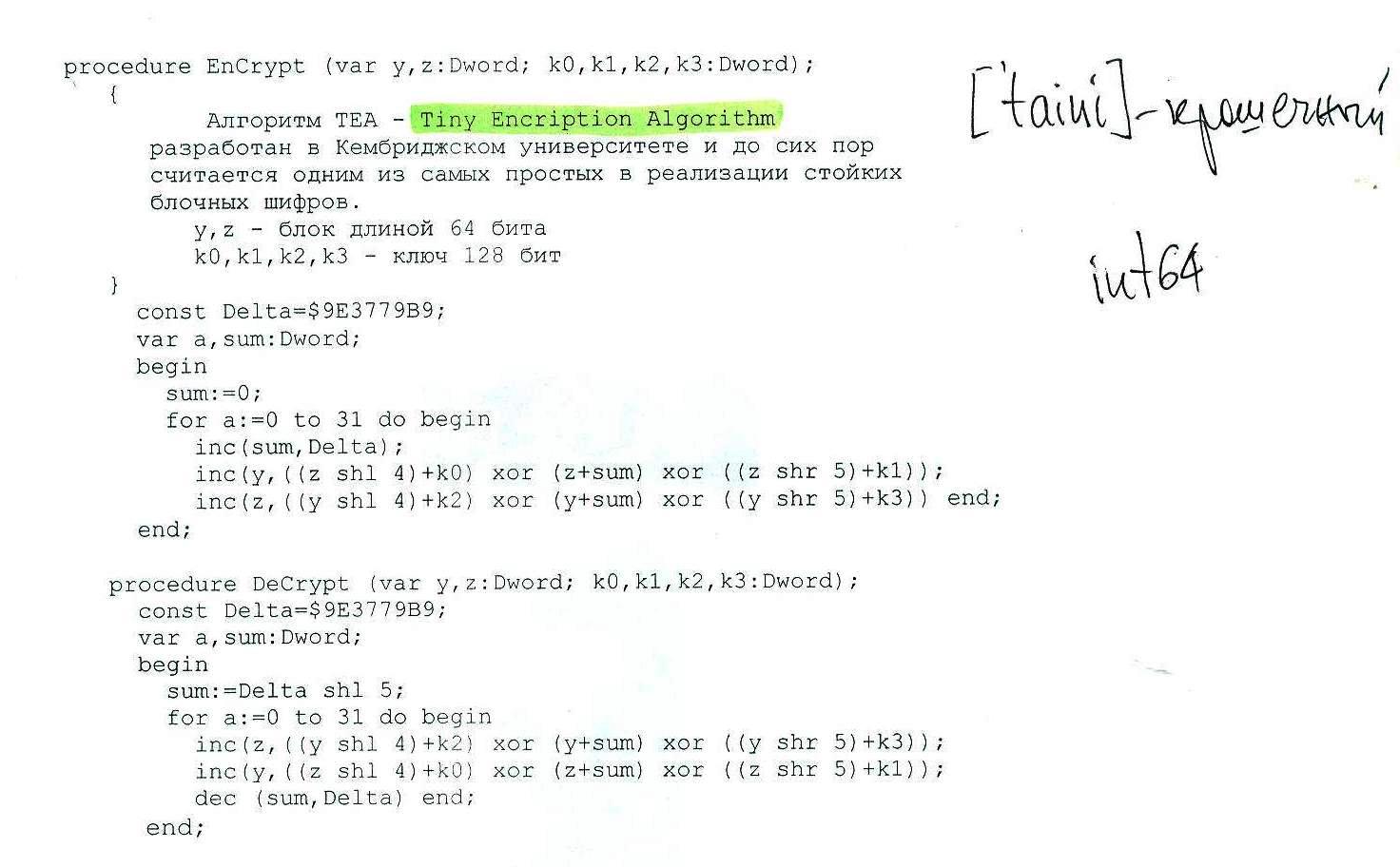
Входной блок s(i-1):

n-t vs t

Шифрование

Выходной блок:

t vs n-t



------------------------------------------------------ 45 минут ------------------------------------------------

### Энигма

Переносная электромеханическая машина, в которой электрическая схема меняется для каждой следующей буквы (многоалфавитный алгоритм)

<https://ru.wikipedia.org/wiki/%D0%AD%D0%BD%D0%B8%D0%B3%D0%BC%D0%B0>

Стадии:

- настройка (инициализация роторов/рефлектора)

- кодирование/раскодирование символа

- ступенчатое движение роторов

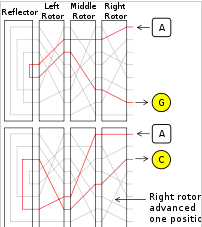
Ротор

Рефлектор

В результате ток течёт через роторы, «отражается» от рефлектора, затем снова через роторы.

Вращение

Перед расшифровкой роторы возвращаются в начальное состояние. Расшифровка идентична шифрованию



Серыми линиями показаны другие возможные электрические цепи внутри каждого ротора. Буква **A** шифруется по-разному при последовательных нажатиях одной клавиши, сначала в **G**, затем в **C**. Сигнал пошёл по другому маршруту за счёт поворота ротора.

Патент Артура Шербиуса 1918 – Модель А (весила 50 кг)

Рефлектор добавил Вилли Корн в 1926 – Модель С

Немцы создали 100 тыс. Экземпляров

Стандартная машина (для сухопутных войск) – 3 колеса

Военно-морская версия – 4 колеса

Схема использовалась в Италии, Испании, Швейцарии

Клоны реализованы в Японии, Британии, Голландии и США

<<взять из методички>>