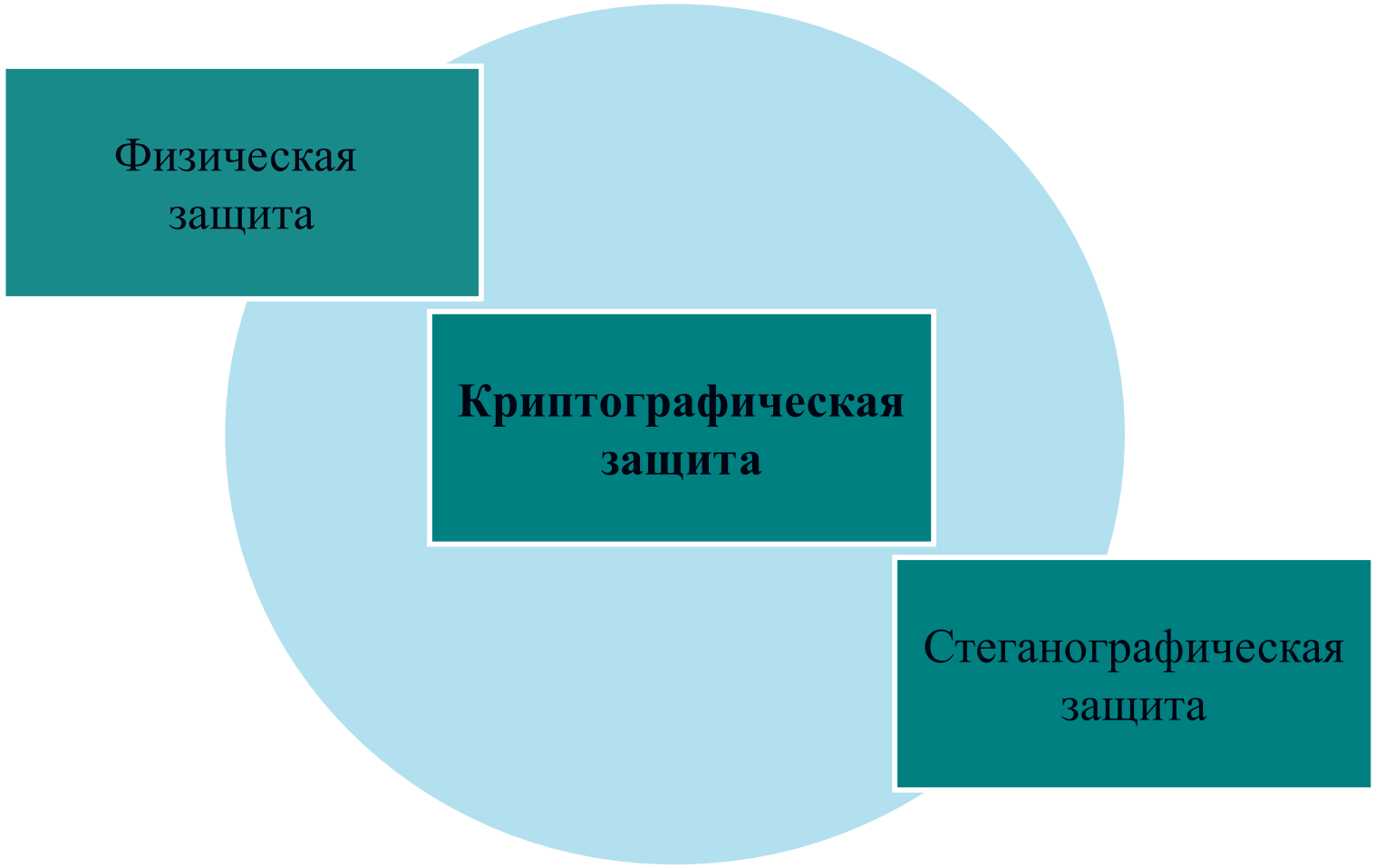
Основы криптографии

Лекция №2

Способы защиты



Криптография

Криптогра́фия (от др.-греч. κρυπτός «скрытый» + γράφω «пишу») — наука о методах обеспечения:

- **конфиденциальности** (невозможности прочтения информации посторонним),
- **целостности данных** (невозможности незаметного изменения информации),
- **аутентификации** (проверки подлинности авторства или иных свойств объекта),
- а также **невозможности отказа от авторства**

Основные определения

- **Шифр** – совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты.
- **Символ** - это любой знак, в том числе буква, цифра или знак препинания
- **Алфавит** - конечное множество используемых для кодирования информации символов
- **Ключ** – *информация*, необходимая для шифрования и расшифрования сообщений
- **Система шифрования**, или **шифрсистема**, – это любая система, которую можно использовать для обратимого изменения текста сообщения с целью сделать его непонятным для всех, кроме тех, кому оно предназначено.

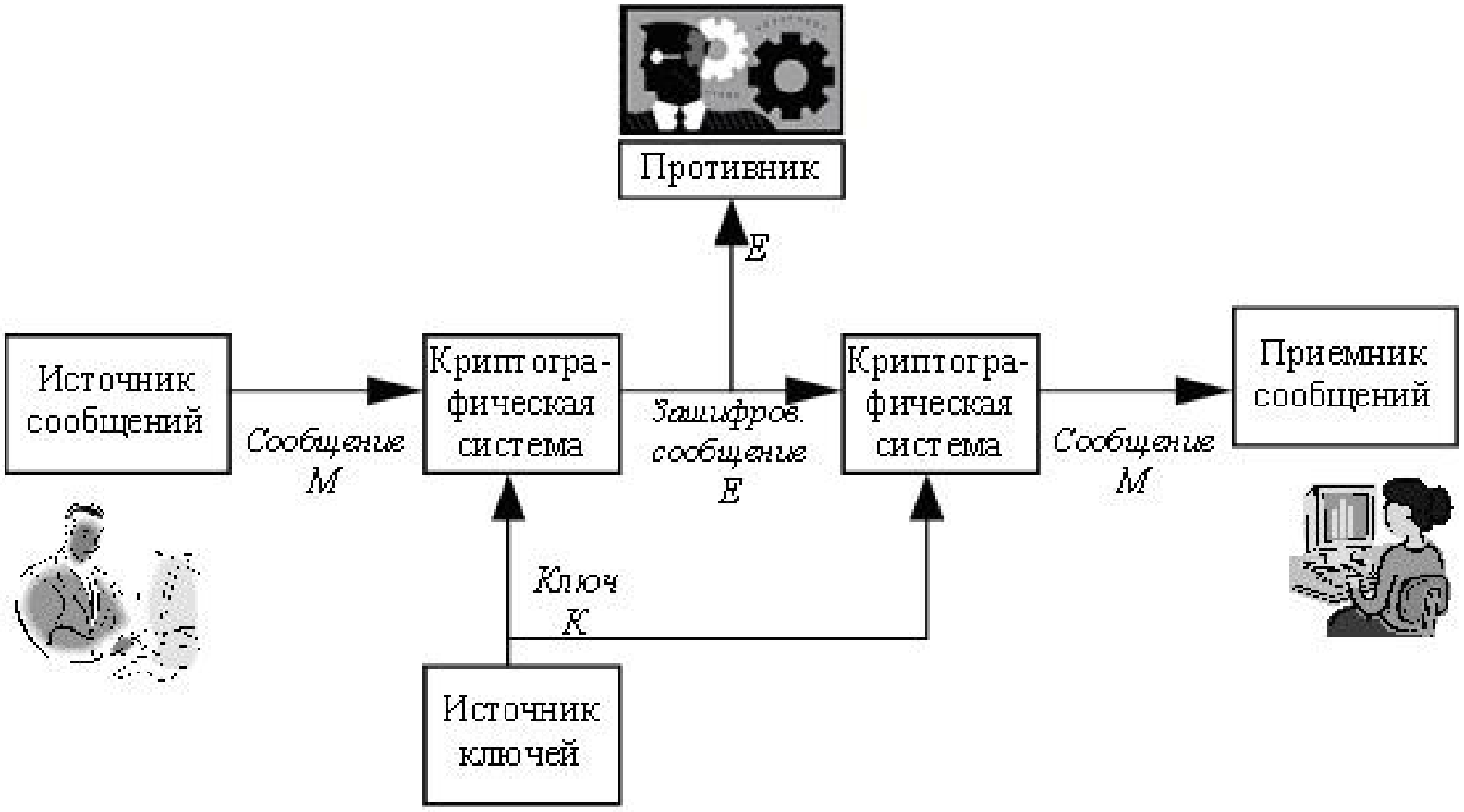
Основные определения

- **Криптостойкостью** называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. способность противостоять криптоанализу)
- **Электронной (цифровой) подписью** называется обычно присоединяемый к сообщению *блок данных*, полученный с использованием криптографического преобразования. *Электронная подпись* позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.
- **Криптографическая система защиты информации** – система защиты информации, в которой используются криптографические методы для шифрования данных.

Требования к криптографическим системам защиты информации

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа
- знание алгоритма шифрования не должно влиять на надежность защиты
- любой ключ из множества возможных должен обеспечивать надежную защиту информации
- алгоритм шифрования должен допускать как программную, так и аппаратную реализацию

Криптографическая система



Криптографическая система

Если **M** – сообщение, **K** – ключ, **E** – зашифрованное сообщение (криптограмма) , то:

$$\boldsymbol{E = f(M, K)}$$

т.е. **E** является функцией от **M** и **K**, однако удобнее понимать эту функцию, не как функцию двух переменных, а как однопараметрическое семейство операций или отображений

$$\boldsymbol{E = T_i M}$$

Отображение T_i примененное к сообщению M дает криптограмму E, а индекс соответствует конкретному использованному ключу

Имеется лишь конечное число возможных ключей, каждому из которых соответствует вероятность $\boldsymbol{P_i}$

Число возможных сообщений также конечно и эти сообщения $M_1,...,M_n$ имеют **априорные вероятности** $q_1,...,q_n$

Криптографическая система

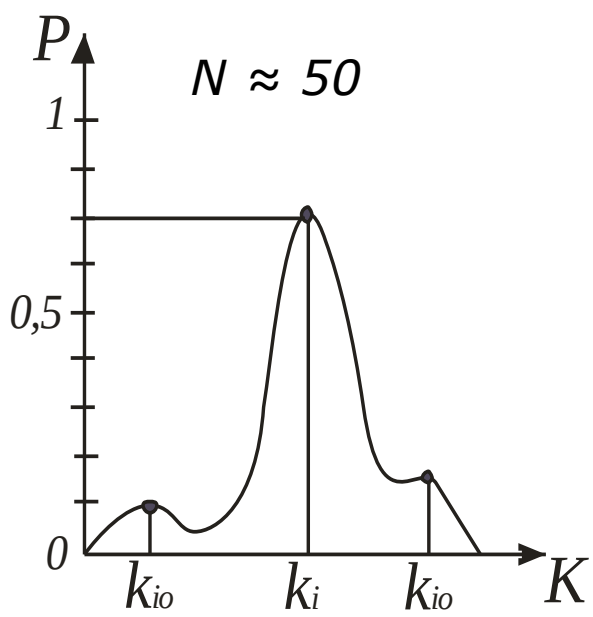
Также должна иметься возможность восстанавливать **M** на приемном конце, когда известны **E** и **K**. Поэтому отображение T_i из нашего семейства должно иметь единственное обратное отображение T_i^{-1}:

$$M = T_i^{-1} E$$

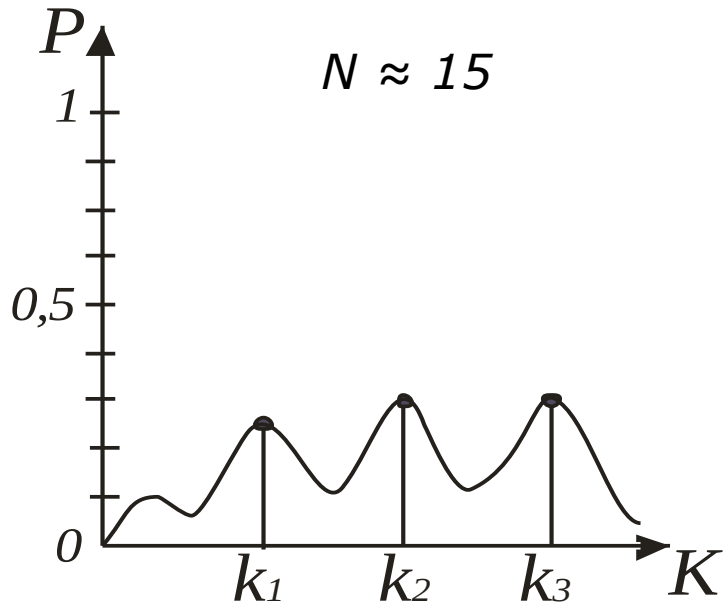
Определение: **Секретная система** есть семейство однозначно обратимых отображений T_i множества возможных сообщений во множество криптограмм, при этом отображение T_i имеет вероятность P_i

Секретную систему можно представлять себе как некоторую машину с одним или более переключающими устройствами. Последовательность букв (сообщение) поступает на вход машины, а на выходе ее получается другая последовательность. Конкретное положение переключающих устройств соответствует конкретному используемому ключу. Для выбора ключа из множества возможных ключей должны быть заданы некоторые статистические методы.

Апостериорная вероятность



$P(K_i) >> P(Koi)$



$P(K1) \approx P(K2) \approx P(K3) \approx \ldots \approx P(Kт)$

Вычисление **апостериорных вероятностей** является общей математической задачей дешифрования

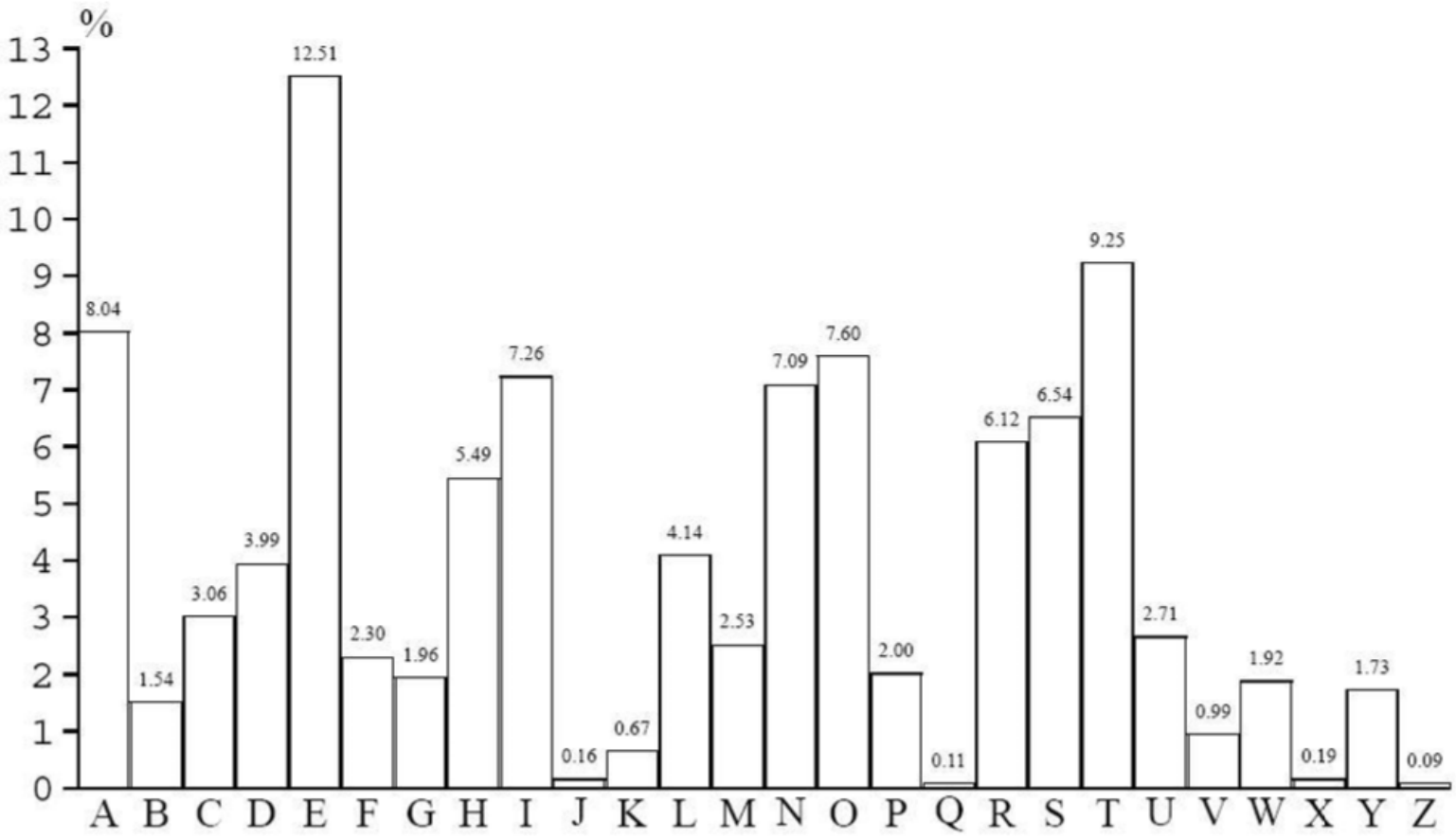
Пример вычисления апостериорных вероятностей

P(A) = 50%, P(B) = 20%, P(C) = 30%.

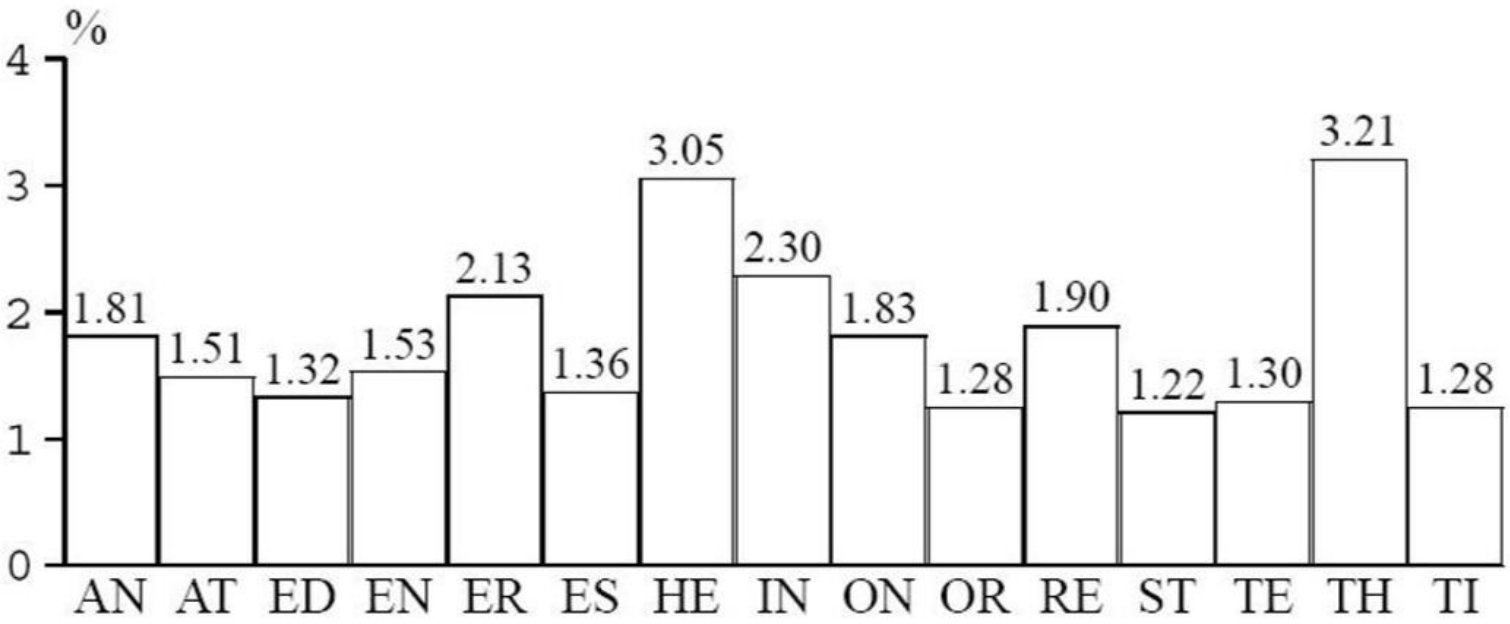
Исходное сообщение «ABACACABCA»

№	Множество возможных криптограмм	*P(A)*, %	*P(B)*, %	*P(C)*, %
1	A B A C A C A B C A	50	20	30
2	B A B C B C B A C B	20	50	30
3	B C B A B A B C A B	30	50	20
4	C B C A C A C B A C	30	20	50
5	C A C B C B C A B C	20	30	50
6	A C A B A B A C B A	50	30	20

Частотный анализ



Частотный анализ биграмм



Что может усложнить ситуацию?

1. Информация об источнике сообщений неполная или ее вообще нет
2. Мощность множества возможных ключей настолько велика, что перебор всех возможных значений займет слишком много времени (для алфавита в 256 символов мощность множества ключей в алгоритме простой перестановки составит $256! \approx 8.578 \cdot 10^{506}$)
3. Вероятность использования символов может быть либо неизвестной (неизвестный язык источника сообщений), либо выражаться нечетко (имитовставки)
4. Схема, по которой осуществлялось шифрование, неизвестна, либо достаточно сложна

Взвешенная сумма

T и *R* – секретные системы

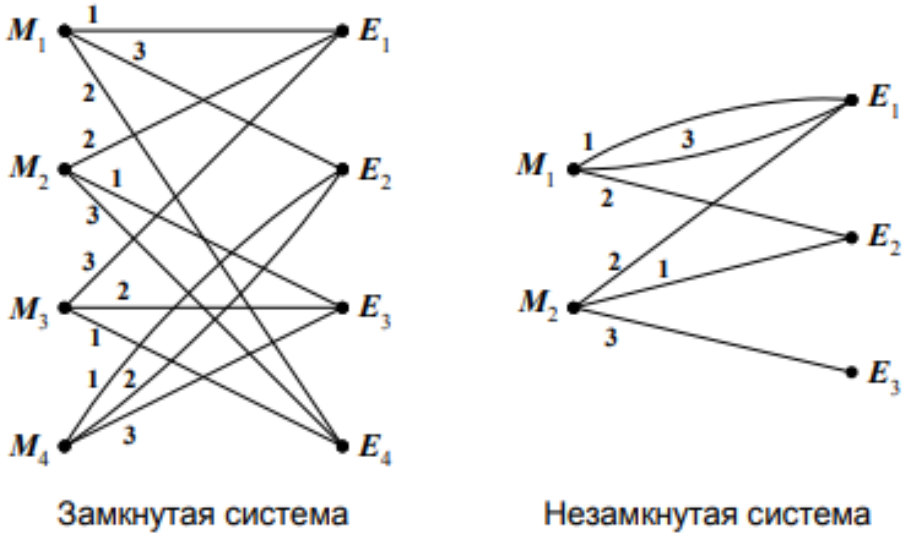
p – Вероятность использования системы T
q – Вероятность использования системы R

Произведение

$$S = TR$$

Замкнутость систем

Возможные сообщения представляются точками слева, а возможные криптограммы – точками справа. Если некоторый ключ, скажем, ключ 1, отображает сообщение $\mathbf{M_2}$ в криптограмму $\mathbf{E_2}$, то $\mathbf{M_2}$ и $\mathbf{E_2}$ соединяются линией, обозначенной значком 1 и т.д.



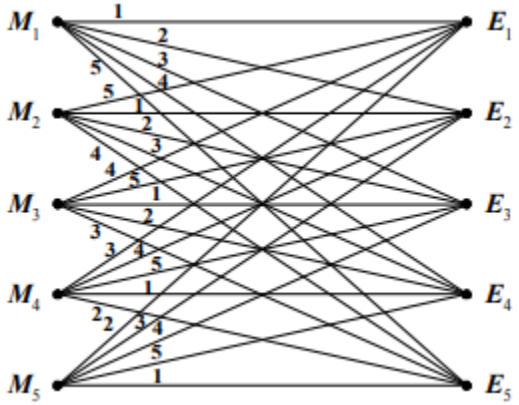
Замкнутая система

Незамкнутая система

Для каждого ключа из каждого сообщения должна выходить ровно одна линия. Если это же верно и для каждой криптограммы, то система является **замкнутой**, в противном случае – **незамкнутой**.

Совершенная секретность

Если шифровальщик противника перехватил некоторую криптограмму **E**, он может вычислить, по крайней мере в принципе, апостериорные вероятности различных сообщений $\mathbf{P_E(M)}$. Естественно определить совершенную секретность с помощью следующего условия: для всех **E** апостериорные вероятности равны априорным вероятностям независимо от величины этих последних



Совершенно секретные системы, в которых число криптограмм равно числу сообщений, а также числу ключей, характеризуются следующими двумя свойствами:

1) каждое **M** связывается с каждым **E** только одной линией
2) все ключи равновероятны

Шифр Вермана

Типичным примером реализации абсолютно стойкого шифра является шифр, который осуществляет побитовое сложение n-битового открытого текста и n-битового ключа:

$$y_i = x_i \oplus k_i, \quad i = 1, \ldots, n.$$

Для абсолютной стойкости необходимо чтобы было выполнено три условия:

1. **Полная случайность** (равновероятность) ключа (это, в частности, означает, что ключ нельзя вырабатывать с помощью какого-либо детерминированного устройства)
2. **Равенство** длины ключа и длины открытого текста
3. **Однократность** использования ключа

Использование шифров

- Чаще всего пользователи вынуждены использовать **неабсолютно** стойкие шифры. Такие шифры, по крайней мере теоретически, могут быть вскрыты. Вопрос только в том, хватит ли у противника сил, средств и времени для разработки и реализации соответствующих алгоритмов.

- Обычно эту мысль выражают так: «Противник с неограниченными ресурсами может вскрыть любой **неабсолютно** стойкий шифр»

Принцип Кирхгофа

Шифр – параметризованный алгоритм, состоящий из *процедурной части*, и *параметров* — различных элементов данных, используемых в преобразованиях.

Раскрытие только процедурной части не должно приводить к увеличению вероятности успешного дешифрования сообщения злоумышленником выше допустимого предела.

Особого смысла хранить процедурную часть в секрете нет. В секрете держится некоторая часть параметров алгоритма, которая называется *ключом* шифра.

Классификация шифров