Криптография: вчера, сегодня, завтра

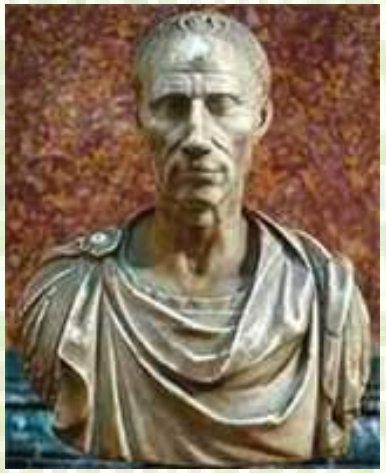
Содержание

1. Древний Рим: шифр Цезаря
2. Шифры простой замены
3. Частотный метод дешифровки, частотный анализ
4. «Пляшущие человечки»
5. Теоретико-числовые результаты (теорема Эйлера)
6. Алгоритмический прогресс XX в.
7. Криптосистема RSA
8. Криптография будущего: квантовая криптография

1. Древний Рим: шифр Цезаря

Широко известен метод шифрования, который применял римский император Гай Юлий Цезарь для секретной переписки с генералами своей армии:

каждая буква послания заменялась буквой, находящейся в алфавите на 3 позиции правее неё



Гай Юлий Цезарь (102–44 до н. э.)

Таким образом, таблица замены выглядит так:

буквы

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 Ъ Ы Ь Э Ю Я

заменяются соответственно на

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

Б	В	Г	Д	Е	Ж	З
В	Г	Д	Е	Ж	З	И
Г	Д	Е	Ж	З	И	К
Д	Е	Ж	З	И	К	Л
Е	Ж	З	И	К	Л	М
Ж	З	И	К	Л	М	Н
З	И	К	Л	М	Н	О
И	К	Л	М	Н	О	П
К	Л	М	Н	О	П	Р
Л	М	Н	О	П	Р	С
М	Н	О	П	Р	С	Т
Н	О	П	Р	С	Т	У
О	П	Р	С	Т	У	Ф

Для шифровки и расшифровки удобно пользоваться двумя дисками разного диаметра на одной оси с нарисованными по краям дисков алфавитами

Шифр Цезаря легко взламывается: например, для этого можно использовать заранее заготовленные полоски с алфавитом

Дешифровку можно провести и непосредственно:

Я Э О Ъ

А Ю П Э

Б Я Р Ю

В А С Я

2. Шифры простой замены

Шифр Цезаря – один из примеров *шифров простой замены.*

Принцип шифра простой замены состоит в замене букв согласно таблице: каждой букве сопоставляется буква или символ так, чтобы соответствие было однозначным.

Для расшифровки достаточно знать ту же таблицу.

Шифры простой замены были описаны в нескольких художественных произведениях: «Пляшущие человечки» Артура Конан Дойла (см. далее), «Золотой Жук» Эдгара По, «Путешествие к центру земли» Жюля Верна.

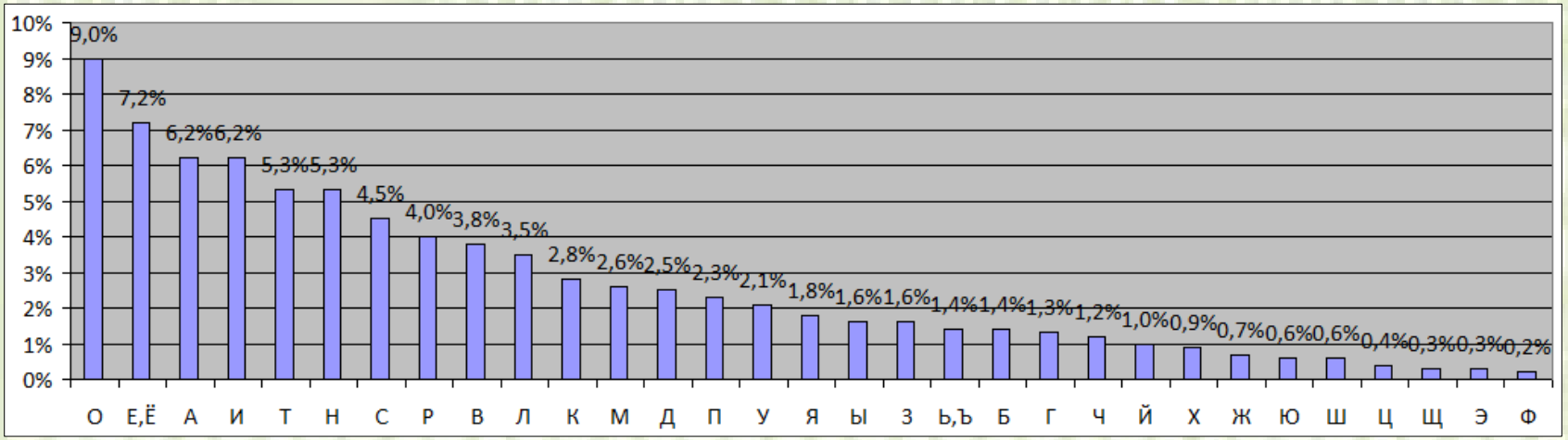
Все шифры простой замены также ненадёжны: они легко взламываются *методом частотного анализа*, так как не меняют частоты использования символов в тексте.

3. Частотный метод дешифровки. Частотный анализ

Для текстов на русском языке таблица средних частот букв такова:

А	6,2%	И	6,2%	Р	4,0%	Ш	0,6%
Б	1,4%	Й	1,0%	С	4,5%	Щ	0,3%
В	3,8%	К	2,8%	Т	5,3%	Ы	1,6%
Г	1,3%	Л	3,5%	У	2,1%	Ь,Ъ	1,4%
Д	2,5%	М	2,6%	Ф	0,2%	Э	0,3%
Е,Ё	7,2%	Н	5,3%	Х	0,9%	Ю	0,6%
Ж	0,7%	О	9,0%	Ц	0,4%	Я	1,8%
З	1,6%	П	2,3%	Ч	1,2%		

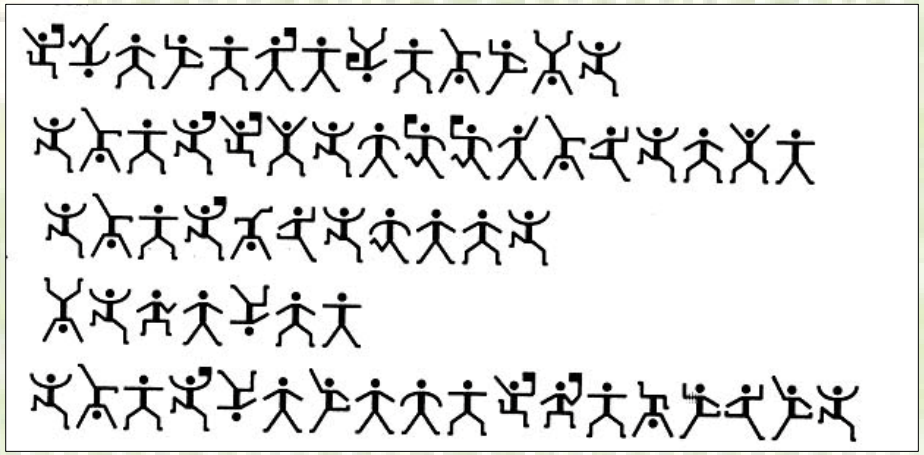
На графике:



Для восстановления таблицы шифровки достаточно сопоставить её с таблицей средних частот букв в зашифрованном тексте.

4. «Пляшущие человечки»

«Пляшущие человечки» – детективный рассказ Артура Конан Дойля, написанный в 1903 г., об очередном расследовании Шерлока Холмса и доктора Ватсона. Перед домом человека, обратившегося к ним за помощью, стали появляться такие рисунки:



С первого взгляда эти «пляшущие человечки» напоминают детские рисунки. Однако накопив достаточное количество рисунков, Шерлок Холмс догадался, что это сообщения, зашифрованные шифром простой замены, расшифровал их методом частотного анализа и раскрыл дело. «Флажки» у человечков означали границы слов.

Теоретико-числовая модель шифра Цезаря:

Обозначения:

$$y = x + k \bmod n$$

$$y \equiv x \,(\bmod n)$$

Шифрование (сдвиг на 3 в русском языке):

$$y = x + 3 \bmod 32$$

Расшифровка (обратная операция):

$$x = y - 3 \bmod 32$$

Таким образом, сложности выполнения операций шифрования и расшифровки одинаковы.

5. Теоретико-числовые результаты (теорема Эйлера)

Для разработки более надёжных способов шифрования используются математические (в частности, теоретико-числовые) методы.

Приведём некоторые известные теоретико-числовые факты, которые широко применяются в криптографии.

Функция Эйлера: $\varphi(n)$ – количество натуральных чисел, меньших n и взаимно простых с n.

Например, если p – простое число, то $\varphi(p) = p - 1$.

Если $n=pq$, где p, q – простые числа, то $\varphi(n) = (p-1)(q-1)$.

Теорема Эйлера: если числа x и n взаимно просты, то

$$x^{\varphi(n)} \equiv 1 \pmod{n}.$$

6. Алгоритмический прогресс XX в.

В 1970-х гг. был разработан принципиально новый метод шифрования, основанный на применении теории чисел и глубоком исследовании современных вычислительных алгоритмов. Он не предполагал ни наличия защищённого канала связи, ни необходимости «скрывать» число *n*.

В основе метода лежит понятие *односторонней функции* – такой функции *f*(*x*), что по известному *x* можно достаточно быстро вычислить значение *f*(*x*), тогда как нахождение *x* по заданному значению *f*(*x*) невозможно за обозримое время.

Односторонняя функция применяется для шифрования сообщения, но расшифровать его с её помощью нельзя. Для расшифровки же используется некоторый секретный ключ *y*, помогающий вычислить *x*, зная *f*(*x*).

7. Криптосистема RSA

RSA – это широко применяемая криптосистема с открытым ключом.

Её надёжность обусловлена тем, что возможность человечества находить большие простые числа (т. е. доказывать простоту конкретных больших чисел) значительно опережает возможности в области разложения на множители. Текущий рекорд разложения на множители произвольных чисел – менее 200 знаков, а проверить на простоту можно любое число вплоть до 10^{15000}.

Наибольшее известное простое число: $2^{43112609} – 1$ (найдено 23.08.2008 в университете UCLA в рамках проекта GIMPS).

Принцип действия криптосистемы RSA:

Можно считать, что сообщение – это натуральное число M.

- Выбираются два больших простых числа p, q (на сегодняшний день обычно выбирают числа, содержащие от 200 до 400 знаков) и вычисляется их произведение n, которое не может быть разложено на множители за разумное время (даже с использованием компьютеров ближайшего будущего).
- Вычисляется значение функции Эйлера $\varphi(n) = (p - 1)(q - 1)$.
- Выбирается целое число e ($1 < e < \varphi(n)$), взаимно простое со значением функции $\varphi(n)$. Обычно в качестве e берут простые числа, содержащие небольшое количество единичных битов в двоичной записи, например, простые числа Ферма 17, 257 или 65537. Число e называется *открытой экспонентой*.

- Вычисляется число *d*, обратное по умножению к числу *e* по модулю $\varphi(n)$, то есть число, удовлетворяющее условию

$$de \equiv 1 \pmod{\varphi(n)}$$

т. е. $de = 1 + k\varphi(n)$, где *k* – некоторое целое число. Число *d* называется *секретной экспонентой*.

- Пара $P = (e,n)$ публикуется в качестве открытого ключа системы RSA.
- Пара $S = (d,n)$ называется секретным ключом RSA и держится втайне.
- Шифрование и расшифровка происходят по стрелкам на схеме:

$$M \to C = M^e \bmod n \to S = C^d \bmod n = M.$$

Корректность расшифровки обеспечивается теоремой Эйлера:

$$S = C^d \bmod n = M^{de} \bmod n = M^{1+k\varphi(n)} \bmod n = M \cdot \left(M^{\varphi(n)}\right)^k \bmod n = M.$$

В рассматриваемой криптосистеме односторонней функцией является

$$f(x) = x^e \bmod n.$$

Оказывается, что при перехвате зашифрованного сообщения $C = M^e \bmod n$ восстановить значение *M*, не зная секретного ключа, практически невозможно: быстрый способ решения этой задачи неизвестен, а при умело выбранных больших числах любой перебор значений займёт слишком большое время.

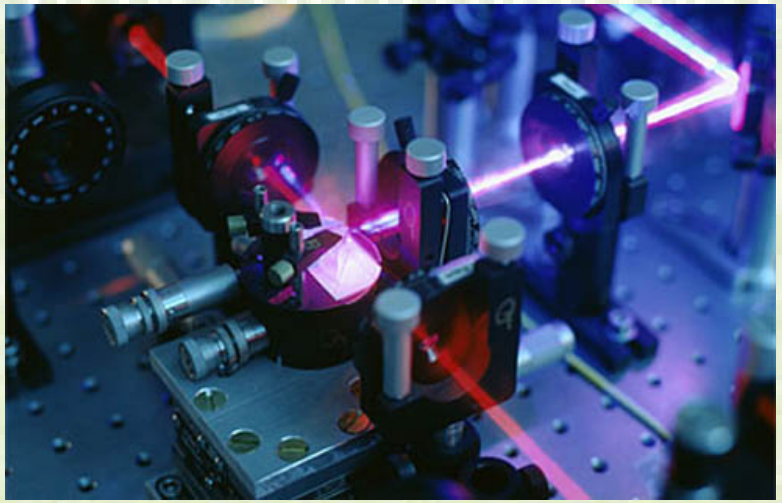
Отметим также, что знание секретного ключа позволяет провести расшифровку, применяя ту же операцию возведения в степень, что и при шифровании, но с другим показателем, а существующий алгоритм возведения в степень позволяет относительно быстро вычислять эти значения.

Взломать криптосистему можно, узнав значение функции $\varphi(n)$ или разложив число *n* на множители, но уже для 400-значных чисел это сегодня неподъёмные задачи.

Пример шифрования и расшифровки сообщения методом RSA

Этап	Описание операции	Результат операции
Генерация ключей	Выбор двух простых чисел	$p = 139, q = 157$
	Вычисление модуля	$n = pq = 139 \cdot 157 = 21823$
	Вычисление функции Эйлера	$\varphi(n) = (p-1)(q-1) = 21528$
	Выбор открытой экспоненты	$e = 7$
	Вычисление секретной экспоненты	$d = 6151 \quad (k = 2)$
	Публикация *открытого ключа*	$(e, n) = (7, 21823)$
	Сохранение *секретного ключа*	$(d, n) = (6151, 21823)$
Шифрование	Выбор текста для шифрования	$M = 2011$
	Вычисление шифротекст	$P(M) = M^e \bmod n = 2011^7 \bmod 21823 = 11295.$
Расшифровка	Вычисление исходного сообщения	$S(C) = C^d \bmod n = 11295^{6151} \bmod 21823 = 2011.$

8. Криптография будущего: квантовая криптография



Квантовая криптография — метод защиты информации, основанный на принципах квантовой физики.

В отличие от использования математических методов, для обеспечения секретности информации квантовая криптография сосредоточена на физических принципах и квантовой механике.

В такой системе невозможно захватить информацию, переданную через сеть, не нарушая при этом ее работы, поэтому легко обнаружить попытку прослушки информации и принять меры по её защите.