**Успанова А.И.**

**Криптоанализшифров зашифрованных методом Виженера**

Аннотация

В статье раскрываются методы расшифровки шифра Виженера.**Шифр Виженера это**oдин из самых знаменитых и интересных шифров, призванных решить эту проблему, — это так называемый шифр Виженера. Названный именем французского дипломата XVI века, он был на самом деле изобретен независимо друг от друга разными людьми. Что интересно, БлезаВиженера при этом среди них не было, он лишь убедил в свое время Генриха III использовать его, а название это шифр получил уже в XIX веке.

Первое его описание можно найти еще в XVI веке в «Трактате о шифрах» Леона Баттиста Альберти, более известного тем, что он впервые изложил математические основы перспективы в живописи. Идея была довольно простой, однако все равно означала выход криптографии на новый уровень — полиалфавитные шифры.

**Ключевые слова:** криптография, криптоанализ, шифр, шифр Виженера, дешифровка, шифровка, частотный анализ, индекс совпадений

**Криптография** - наука о методах обеспечения конфиденциальности, целостности данных аутентификации, а также невозможности отказа от авторства.

Крип­то­гра­фи­че­ская сис­те­ма пред­став­ля­ет со­бой се­мей­ст­во T пре­об­ра­зо­ва­ний от­кры­то­го тек­ста. Чле­ны это­го се­мей­ст­ва ин­дек­си­ру­ют­ся, или обо­зна­ча­ют­ся сим­во­лом k ; па­ра­метр k яв­ля­ет­ся клю­чом . Про­стран­ст­во клю­чей K - это на­бор воз­мож­ных зна­че­ний клю­ча. Обыч­но ключ пред­став­ля­ет со­бой по­сле­до­ва­тель­ный ряд букв ал­фа­ви­та.

Криптосистемы разделяются на симметричные и с открытым ключом .

В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ .

В системах с открытым ключом используются два ключа - открытый и закрытый , которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Тер­ми­ны рас­пре­де­ле­ние клю­чей и управ­ле­ние клю­ча­ми от­но­сят­ся к про­цес­сам сис­те­мы об­ра­бот­ки ин­фор­ма­ции, со­дер­жа­ни­ем ко­то­рых яв­ля­ет­ся со­став­ле­ние и рас­пре­де­ле­ние клю­чей ме­ж­ду поль­зо­ва­те­ля­ми.

**Криптоанализ** (от [греч.](http://mind-control.wikia.com/wiki/%D0%93%D1%80%D0%B5%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA?redlink=1&action=edit&flow=create-page-article-redlink) κρυπτός — скрытый и [анализ](http://mind-control.wikia.com/wiki/%D0%90%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7?redlink=1&action=edit&flow=create-page-article-redlink)) — наука о методах получения исходного значения зашифрованной информации, не имея доступа к секретной информации ([ключу](http://mind-control.wikia.com/wiki/%D0%9A%D0%BB%D1%8E%D1%87_%28%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%29)), необходимой для этого. В большинстве случаев под этим подразумевается нахождение [ключа](http://mind-control.wikia.com/wiki/%D0%9A%D0%BB%D1%8E%D1%87_%28%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%29). Проще говоря, криптоанализ — это [взламывание кода](http://mind-control.wikia.com/wiki/%D0%92%D0%B7%D0%BB%D0%B0%D0%BC%D1%8B%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%BE%D0%B4%D0%B0?redlink=1&veaction=edit&flow=create-page-article-redlink), хотя этот термин имеет и строго технические значение. Термин был введён американским криптографом [Уильямом Ф. Фридманом](http://mind-control.wikia.com/wiki/%D0%A4%D1%80%D0%B8%D0%B4%D0%BC%D0%B0%D0%BD%2C_%D0%A3%D0%B8%D0%BB%D1%8C%D1%8F%D0%BC_%D0%A4%D1%80%D0%B5%D0%B4%D0%B5%D1%80%D0%B8%D0%BA)в [1920 году](http://mind-control.wikia.com/wiki/1920_%D0%B3%D0%BE%D0%B4?redlink=1&veaction=edit&flow=create-page-article-redlink).

Под термином «криптоанализ» также понимается попытка найти уязвимость в криптографическом алгоритме или протоколе. Хотя основная цель осталась неизменной с течением времени, методы криптоанализа претерпели значительные изменения, эволюционировав от использования лишь ручки и бумаги до широкого применения вычислительных мощностей компьютеров в наши дни. Если раньше криптоаналитиками были большей частью лингвисты, то в наше время это удел «чистых» математиков.

Результаты криптоанализа конкретного шифра называют криптографической атакой на этот шифр. Успешную криптографическую атаку, полностью дискредитирующую атакуемый шифр, называют взломом или вскрытием.

**Шифр Виженера**  — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.

Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал ДжованиБаттистаБеллазо в книге Lacifradel. Sig. GiovanBattistaBellasо в 1553 году, однако в XIX веке получил имя БлезаВиженера, французского дипломата. Метод прост для понимания и реализации, он является недоступным для простых методов криптоанализа.

Хотя шифр легко понять и реализовать, на протяжении трех столетий он сопротивлялся всем попыткам его сломать; чем и заработал название **lechiffreindéchiffrable** (с французского 'неразгаданный шифр'). Многие люди пытались реализовать схемы шифрования, которые по сути являлись шифрами Виженера.

**Как происходит шифрование методом Виженера?**

1. Взять квадрат Виженера

2. Придумать ключевое слово

3. Записать предложение без пробелов

4. Записать ключевое слово под сообщением, чтобы каждая буква соответствовала букве сообщения

5. Перейти к ряду первой буквы в ключевом слове на Квадрате Виженера и найти колонку с первой буквой изначального сообщения, а затем найти точку пересечения между рядом и колонкой

6. Продолжать делать тоже самое, пока не будет зашифрована вся фраза

А расшифровка происходит в обратном порядке.

**Криптоанализ методом Виженера**

Шифр Виженера «размывает» характеристики частот появления символов в тексте, но некоторые особенности появления символов в тексте остаются. Главный недостаток шифра Виженера состоит в том, что его ключ повторяется. Поэтому простой криптоанализ шифра может быть построен в два этапа:

1. Поиск длины ключа. Можно анализировать распределение частот в зашифрованном тексте с различным прореживанием. То есть брать текст, включающий каждую 2-ю букву зашифрованного текста, потом каждую 3-ю и т. д. Как только распределение частот букв будет сильно отличаться от равномерного (например, по энтропии), то можно говорить о найденной длине ключа.

2. Криптоанализ. Совокупность *l* шифров Цезаря (где *l* — найденная длина ключа), которые по отдельности легко взламываются.

**Тест Фридмана**

**Индекс совпадений**

Тест Фридмана (иногда называемый каппа-тест) был изобретен Вильямом Фридманом в 1920 году. Фридман использовал индекс совпадения, который измеряет частоты повторения символов, чтобы взломать шифр. Зная вероятность   того, что два случайно выбранных символа текста совпадают (примерно 0,067 для англ. языка) и вероятность совпадения двух случайно выбранных символов алфавита   (примерно 1 / 26 = 0,0385 для англ. языка), можно оценить длину ключа как:

Из наблюдения за частотой совпадения следует:

Где С — размер алфавита (26 символов для англ. языка), N — длина текста, и   до   — наблюдаемые частоты повторения символов зашифрованного текста. Однако, это только приблизительное значение, точность которого увеличивается при большем размере текста. На практике это было бы необходимо для перебора различных ключей приближаясь к исходному.

**Частотный анализ**

Как только длина ключа  становится известной, зашифрованный  текст можно записать во множество  столбцов, каждый из которых соответствует  одному символу ключа. Каждый столбец  состоит из исходного текста, который  зашифрован шифром Цезаря; ключ к шифру Цезаря является всего-навсего одним символом ключа для шифра Виженера, который используется в этом столбце. Используя методы, подобные методам взлома шифра Цезаря, можно расшифровать зашифрованный текст. Усовершенствование теста Касиски, известное как метод Кирхгофа, заключается в сравнении частоты появления символов в столбцах с частотой появления символов в исходном тексте для нахождения ключевого символа для этого столбца. Когда все символы ключа известны, криптоаналитик может легко расшифровать шифрованный текст, получив исходный текст. Метод Кирхгофа не применим, когда таблица Виженера скремблирована, вместо использования обычной алфавитной последовательности, хотя тест Касиски и тесты совпадения всё ещё могут использоваться для определения длины ключа для этого случая.

**Заключение**

 Криптография, особенно с открытым ключом, служит надёжной системой защиты информации в современном мире. И криптография, и криптоанализ - две взаимно стимулирующие друг друга области знаний. Любое продвижение в развитии одной даёт толчок к развитию другой. Следует заметить, что развитие криптографии и криптоанализа неразрывно связано с очень высоким уровнем развития вычислительной техники.

В заключение два слова о будущем криптографии. Ее роль будет возрастать в связи с расширением ее областей приложения (цифровая подпись, аутентификация и подтверждение подлинности и целостности электронных документов, безопасность электронного бизнеса, защита информации, передаваемой через Интернет и др.). Знакомство с криптографией потребуется каждому пользователю электронных средств обмена информацией, поэтому криптография в будущем станет "третьей грамотностью" наравне со"второй грамотностью" - владением компьютером и информационными технологиями.

**Список литературы:**

1. David Kahn, Remarks on the 50th Anniversary of the National Security Agency, November 1, 2002.
2. *Шнайер Б.* Криптоанализ // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = AppliedCryptography. Protocols, Algorithms and Source Code in C. - М.:Триумф, 2002. - С. 19 -22. 816 с.  3000 экз. — ISBN 5-89392-055-4
3. *Пилиди В. С.* Криптография. Вводные главы. - Ростов-на-Дону: ЮФУ, 2009. - 110 с.
4. *Alex Biryukov and EyalKushilevitz.: From Differential Cryptanalysis to Ciphertext-Only Attacks*