

Артём Музагафаров

**Шифрованный мир: азы
криптографии. Просто,
понятно и увлекательно**

«Издательские решения»

Музагафаров А.

Шифрованный мир: азы криптографии. Просто, понятно и увлекательно / А. Музагафаров — «Издательские решения»,

ISBN 978-5-44-903934-7

В этой книге я попытался простым языком увлекательно рассказать о наиболее популярных, интересных и понятных шифрах. Мы разберём девять занимательных шифров, поговорим и о стеганографии, квантовом шифровании и о многом другом.

ISBN 978-5-44-903934-7

© Музагафаров А.
© Издательские решения

Содержание

Шифрованный мир: азы криптографии. Просто, понятно и увлекательно	6
Криптография	7
Виды шифров	8
Приложение СуртоApp	10
Как разгадать шифр	11
Конец ознакомительного фрагмента.	12

Шифрованный мир: азы криптографии Просто, понятно и увлекательно

Артём Музагафаров

© Артём Музагафаров, 2024

ISBN 978-5-4490-3934-7

Создано в интеллектуальной издательской системе Ridero

Шифрованный мир: азы криптографии. Просто, понятно и увлекательно

В этой книге я попытался простым языком увлекательно рассказать о наиболее популярных, интересных и понятных шифрах. Ну что же, приступим! Начнём с небольшого экскурса в науку, которая занимается шифрованием, и продолжим ознакомлением с видами шифров.

Криптография

Криптография (от древнегреческих «криптос» – скрытый, тайна и «графо» – пишу) – наука о методах и инструментах обеспечения конфиденциальности и аутентичности информации

Как уже было сказано, криптография занимается вопросами конфиденциальности и аутентичности информации. Конфиденциальность, обеспечивающая невозможность прочтения информации несанкционированными пользователями, применимо к криптографии состоит в шифровании информации на основе условленного метода шифрования с секретной передачей ключей для шифровок. А аутентичность, подразумевающая целостность и подлинность авторства, а также невозможность отказа от авторства информации, применимо к криптографии состоит в применении асимметричного шифрования, электронной подписи, хеш-функций и много другого. Однако, криптография не занимается защитой от иррационального поведения и неадекватных действий санкционированных абонентов, кражи ключей и других угроз информации, возникающих в защищенных системах передачи данных. Этим вместо криптографии занимается теория и методология защиты информации, комплексная система защиты информации и сами организаторы и технологи защиты информации.

История криптографии насчитывает около четырех тысяч лет, что делает криптографию одной из старейших наук наряду с математикой, логикой, геометрией, астрономией и медициной. Более подробно о истории криптографии читайте в Википедии. Здесь же стоит лишь упомянуть, что с конца 1980-х годов активно развивается квантовая криптография, которая поставит крест на большинстве систем шифрования и изобретет собственные методы шифрования. Ничто не стоит на месте, даже такая старая наука как криптография.

Виды шифров

Разумеется за четыре тысячи лет криптография повидала не один шифр, так давайте попробуем разобраться во всем многообразии видов шифра

Популярные виды шифров

Популярными видами шифрования для изучения азов криптографии являются, по нашему мнению, Шифр простой замены, Шифр Виженера, Шифр Вернама.

Симметричный и асимметричный виды шифров

Самые первые (читай древние) виды шифров являлись симметричными шифрами. Отличительная черта симметричных шифров – это то, что ключ расшифрования и ключ зашифрования одинаковы. Функция у таких видов шифрования лишь одна – обеспечение конфиденциальности информации от несанкционированных лиц. И только недавно, в конце 20 века, были изобретены асимметричные виды шифров. При этом один из ключей может быть разглашен и не сохраняться в тайне, в таком случае шифрование в некотором смысле получается односторонним – кто угодно может зашифровать информацию (к примеру текст), но расшифровать могут только узкий круг лиц, или наоборот расшифровать кто угодно, но зашифровать только одно лицо (используется для создания электронной подписи). Функциональность данного вида шифров чрезвычайно широка от конфиденциальности до цифровой подписи и подтверждения аутентичности информации (свойство, гарантирующее, что субъект или ресурс идентичны заявленным). Примерами асимметричного шифрования могут служить такие шифры, сертификаты и протоколы, как RSA, SSL, HTTPS и SSH

Блочный и потоковый виды шифров

Симметричный вид шифров подразделяется на блочный и потоковый виды шифров. Отличительная особенность блочного вида шифров состоит в том, что они обрабатывают за одну итерацию сразу несколько байт (обычно по 8 или 16) открытой информации в отличие от потокового вида шифров, который обрабатывает по 1 байту (символу).

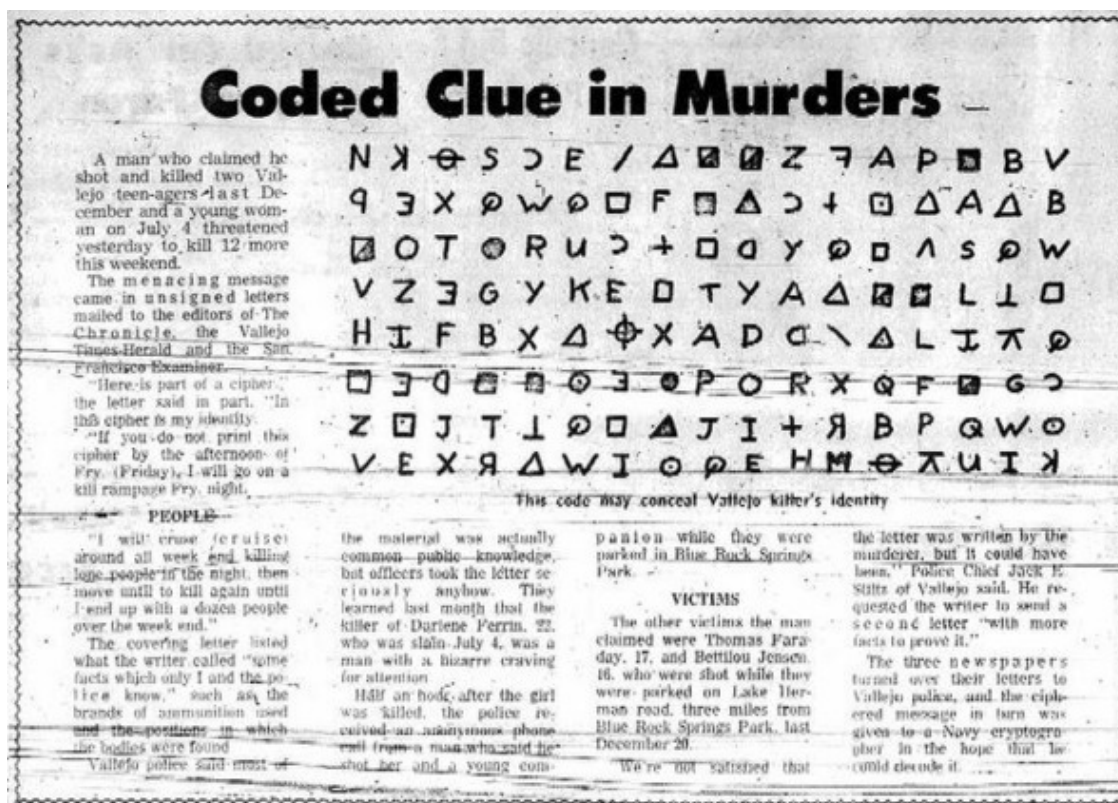
Шифры простой замены

Шифры замены меняют (что и является причиной их названия) части открытого текста на нечто другое. Шифр простой замены производят посимвольную замену, то есть однозначно заменяют каждый символ открытого текста на нечто своё, причем это нечто свое в процессе расшифрования однозначно заменяется на исходный символ. Примерами шифров простой замены могут служить такие шифры как Шифр Цезаря, Аффинный шифр, Шифр Атбаш, Шифр пляшущие человечки. Чтобы разобраться в виде шифров простой замены лучше, прочитайте соответствующую главу.

Однозвучные шифры подстановки

Однозвучные шифры подстановки полностью схожи с шифрами простой замены, за исключением того факта, что в процессе зашифрования символ открытого текста может быть заменен одним из нескольких вариантов, каждый из которых однозначно соответствует исходному. Однозвучный вид шифров подстановки, в отличие от вида шифров замены, не могут быть взломаны с помощью частотного криптоанализа, так как они маскируют частотную характеристику текста, хотя и не скрывают всех статистических свойств. Таким шифром, например, зашифровал свои послания серийный убийца Зодиак, действовавший в Северной

Калифорнии и Сан-Франциско (США) в конце 1960-х. Причём большинство его посланий так и остались нерасшифрованными.



Статья в американской газете с иллюстрацией шифровки Зодиака

Полиграммный шифр подстановки

Полиграммные вид шифров подстановки заменяют не по одному символу, а сразу по несколько. Так например, шифр Плейфера заменяет биграммы (две подряд идущих буквы), а Шифр Хилла по квадратному корню символов из длины ключа.

Многоалфавитный шифр подстановки

Многоалфавитный вид шифров подстановки заменяют одни и те же символы открытого текста каждый раз по разному, так как для каждой позиции открытого текста имеется ключ, определяющий на какой символ будет заменен тот или иной. Примерами многоалфавитного вида шифров могут служить такие шифры, как Шифр Виженера и Шифр Вернама.

Хорошо, понятно, так как же разгадать тот или иной шифр?

Приложение CryptoApp

CryptoApp – это приложение для Android, открывающее большие возможности автоматизированной работы при изучении шифров.

Приложение CryptoApp работает с шифрами простой замены (шифр Цезаря, Атбаш, пляшущие человечки) и полиалфавитными шифрами (Виженера, Бофора)

Скачать его можно в маркетплейсе **NashStore**

При необходимости в настройках разрешите установку из NashStore.

Также приложение CryptoApp может «расшифровывать» текст, набранный в неправильной раскладке, так как это частный случай простой замены.

Как разгадать шифр

Наверняка, если Вы получили (или перехватили☺) непонятную абракадабру, то первым вопросом будет «Как разгадать этот шифр?». Расшифровать шифр (когда знаешь ключ шифра и вид шифра) легко, а вот дешифровать шифр (когда не знаешь ключа шифра, взломать шифр то есть) ... Ну что ж начнём!

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.