Шифрованный мир:

Азы криптографии

Просто, понятно и увлекательно

9 занимательных шифров с примерами и задачами

+ приложение для шифрования

Артём Музагафаров

Артём Музагафаров

Шифрованный мир: азы криптографии. Просто, понятно и увлекательно

http://www.litres.ru/pages/biblio_book/?art=29607505
ISBN 9785449039347

Аннотация

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.

Содержание

Шифрованный мир: азы криптографии Просто, понятно и увлекательно

Артём Музагафаров

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 ассиметричного шифрования, электронной подписи, хеш-функций и много другого. Однако, криптография не занимается защитой от иррационального поведения и неадектватных действий санкционированных абонентов, кражи ключей и других угроз информации, возникающих в защищенных системах передачи данных. Этим вместо криптографии занимается теория и методология защиты информации, комплексая 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 собственые 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 ассиметричный 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 изобретен ассиметричный вид 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 ассиметричного 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).

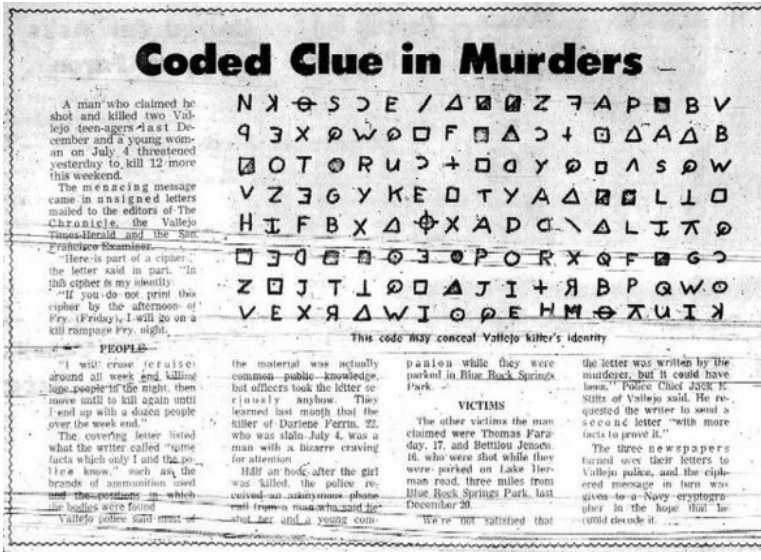
Шифры простой замены

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, шифровал 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.



Coded Clue in Murders

A man who claimed he shot and killed two Vallejo teen-agers last December and a young woman on July 4 threatened yesterday to kill 12 more this weekend.

The menacing message came in unsigned letters mailed to the editors of The Chronicle, the Vallejo Times-Herald and the San Francisco Examiner.

"Here is part of a cipher," the letter said in part. "In this cipher is my identity.

"If you do not print this cipher by the afternoon of Fry. (Friday), I will go on a kill rampage Fry. night.

PEOPLE

"I will cruse (cruise) around all week and killing some people of the night, then move until to kill again until I end up with a dozen people over the week end."

The covering letter listed what the writer called "some facts which only I and the police know," such as the brands of ammunition used and the positions in which the bodies were found.

Vallejo police said most of the material was actually common public knowledge, but officers took the letter seriously anyhow. They learned last month that the killer of Darlene Ferrin, 22, who was slain July 4, was a man with a bizarre craving for attention.

Hdff on hook, after the girl was killed, the police received an anonymous phone call from a man who said he shot her and a young companion while they were parked in Blue Rock Springs Park.

VICTIMS

The other victims the man claimed were Thomas Faraday, 17, and Bettilou Jensen, 16, who were shot while they were parked on Lake Herman road, three miles from Blue Rock Springs Park, last December 20.

We're not satisfied that

This code may conceal Vallejo killer's identity

the letter was written by the murderer, but it could have been," Police Chief Jack E. Stitz of Vallejo said. He requested the writer to send a second letter "with more facts to prove it."

The three newspapers turned over their letters to Vallejo police, and the ciphered message in turn was given to a Navy cryptographer in the hope that he could decode it.

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.