Коды и Шифры

Код и кодирование

Что такое код и кодирование? Кодирование - преобразование представления информации. Так например, различные кодировки интернет-страниц не шифруют информацию, а просто подразумевают определенное представление преобразования двоичной информации в символьную.

Шифр и шифрование

В отличие от кодирования шифрование выполняет определенную задачу криптографии, будь то сокрытие информации, сохранение аутентичности или что-нибудь еще. При этом различные виды шифров выполняют различные функции различными методами и с различной стойкостью.

Шифры

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 заменяюткаждый 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, щелкните на любую ссылку выше.

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.

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 корень квадратному 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.

Шифры

Популярные виды шифров

Популярными видами шифрования для изучения азов криптографии являются, по нашему мнению, Шифр простой замены, Шифр Виженера, Шифр Вернама. Работа с этими видами шифров, как в учебных целях, так и в практических.

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. Функциональность данного вида шифров чрезвычайно широка от конфиденциальности до цифровой подписи и подтверждения аутентичности информации.

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).

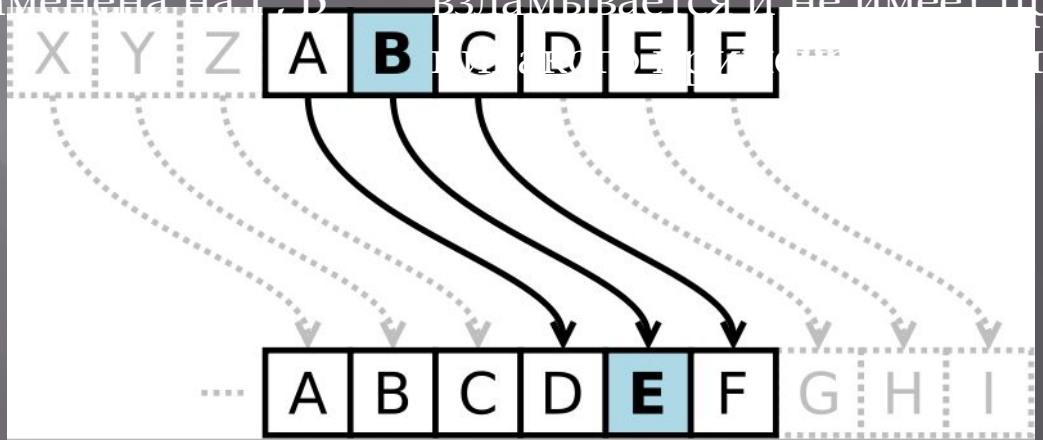
Шифр Цезаря

Шифр Цезаря, также известный как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется буквой находящейся на некоторое постоянное число позиций левее или правее него в алфавите. Например, в шифре со сдвигом 3, А была бы заменена на Г, Б станет Д, и так далее.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и все еще имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет практически [illegible] практике.



Математическая модель

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

$$y = (x + k) \mod n,$$
$$x = (y - k) \mod n.$$

где x — символ открытого текста, y — символ шифрованного текста, n — мощность алфавита, а k — ключ.

С точки зрения математики шифр Цезаря является частным случаем аффинного шифра.

Пример

Шифрование с использованием ключа k=3. Буква «С» «сдвигается» на три буквы вперед и становится буквой «Ф». Твердый знак, перемещённый на три буквы вперед, становится буквой «Э», и так далее:

Исходный алфавит:
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

Шифрованный:
ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВ

Оригинальный текст:

Съешь же ещё этих мягких французских булок, да выпей чаю.

Шифрованный текст получается путём замены каждой буквы оригинального текста соответствующей буквой шифрованного алфавита:

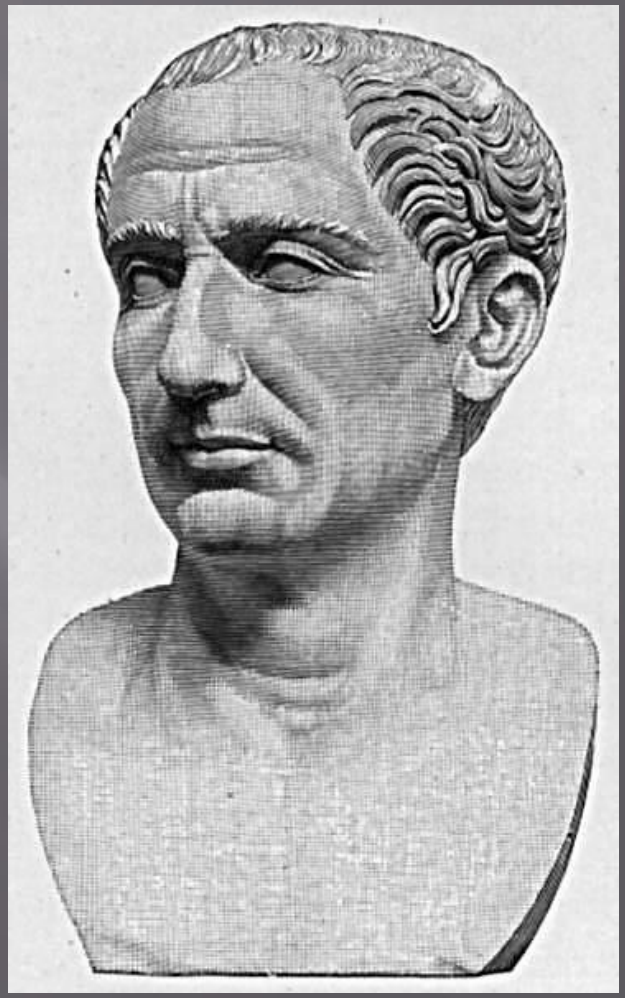
Фэзыя йз зьи ахлш пвёнлш чугрщцкфнлш дцосн, жг еютзм ъгб.

История и применение

Шифр Цезаря называют в честь Юлия Цезаря, который согласно «Жизни двенадцати цезарей» Светония использовал его со сдвигом 3, чтобы защищать военные сообщения. Хотя Цезарь был первым зафиксированным человеком использующим эту схему, другие шифры подстановки, как известно, использовались и ранее. Если у него было что-либо конфиденциальное для передачи, то он записывал это шифром, то есть так изменял порядок букв алфавита, что нельзя было разобрать ни одно слово. Если кто-либо хотел дешифровать его и понять его значение, то он должен был подставлять четвертую букву алфавита, а именно, D, для A, и так далее, с другими буквами.

Гай Светоний Транквилл

Жизнь двенадцати цезарей 56

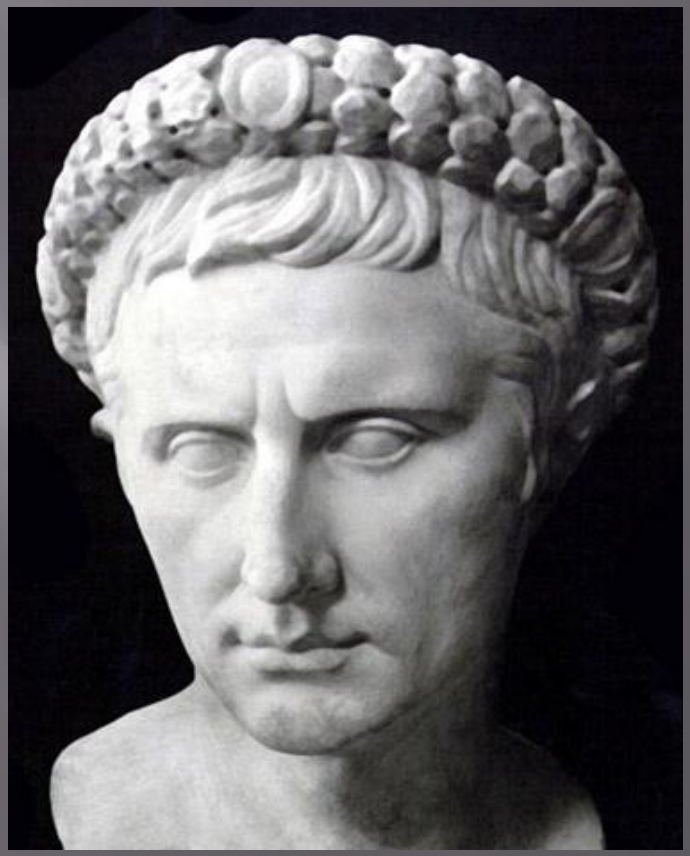


Октавиан Август

Его племянник, Август, также использовал этот шифр, но со сдвигом вправо на один, и он не повторялся к началу алфавита:

Всякий раз, когда он записывал шифром, он записал B для A, C для B, и остальной части букв на том же самом принципе, используя AA для X.

Гай Светоний Транквилл, Жизнь Августа 88



Есть доказательства, что Юлий Цезарь использовал также и более сложные схемы.

Неизвестно, насколько эффективным шифр Цезаря был в то время, но вероятно он был разумно безопасен, не в последнюю очередь благодаря тому, что большинство врагов Цезаря были неграмотными, и многие предполагали, что сообщения были написаны на неизвестном иностранном языке. Нет никаких свидетельств того времени касательно методов взлома простых шифров подстановки. Самые ранние сохранившиеся записи о частотном анализе — это работы Ал-Кинди 9-ого века об открытии частотного анализа.

Шифр Цезаря со сдвигом на один используется на обратной стороне мезузы, чтобы зашифровать имена Бога. Это может быть пережитком с раннего времени, когда еврейскому народу не разрешили иметь мезузы

В 19-ом столетии личная секция рекламных объявлений в газетах иногда использовалась, чтобы обмениваться сообщениями, зашифрованными с использованием простых шифров. Кан (1967) описывает случаи когда любители участвовали в секретных коммуникациях, зашифрованных с использованием шифра Цезаря в «Таймс». Даже позднее, в 1915, шифр Цезаря находил применение: российская армия использовала его как замену для более сложных шифров, которые оказались слишком сложными для войск; у немецких и австрийских криптоаналитиков были лишь небольшие трудности в расшифровке этих сообщений.

- Шифр Цезаря со сдвигм тринадцать также используется в алгоритме ROT13, простом методе запутывания текста, широко испольуемого в Usenet, и используется скорее как способ сокрытия спойлеров, чем как метод шифрования. Шифр Виженера использует шифр Цезаря с различными сдвигами в каждой позиции в тексте; значение сдвига определяется с помощью повторяющегося ключевого слова. Если ключевое слово такое же длинное как и сообщение, тогда этот шифр становится невзламываемым до тех пор пока пользователи поддерживают тайну ключевого слова.

- Ключевые слова короче чем сообщение (например, «Complete Victory», используемое Конфедерацией во время гражданской войны в США), вводят циклический образец, который мог бы быть обнаружен с помощью улучшенной версии частотного анализа.

- В апреле 2006, беглый босс Мафии Бернардо Провенцано был пойман в Сицилии частично из-за криптоанализа его сообщений, написанных с использованием вариации шифра Цезаря. Шифр Провенцано использовал числа, так, чтобы «A» была написана как «4», «B» как «5», и так далее.

Часто для удобство использования шифра Цезаря используют два диска разного диаметра с нарисованными по краям дисков алфавитами, насаженных на общую ось. Изначально диски поворачиваются так, чтобы напротив каждой буквы алфавита внешнего диска находилась та же буква алфавита малого диска. Если теперь повернуть внутренний диск на несколько символов, то мы получим соответствие между символами внешнего диска и внутреннего — шифр Цезаря. Получившийся диск можно использовать как для шифрования, так и для расшифровки.

Например, если внутреннее колесо повернуть так, чтобы символу A внешнего диска соответсвовал символ D внутреннего диска, то мы получим шифр со сдвигом 3 влево.

Взлом шифра

Шифр Цезаря может быть легко взломан даже в случае, когда взломщик знает только зашифрованный текст. Можно рассмотреть две ситуации:

взломщик знает (или предполагает), что использовался простой шифр подстановки, но не знает что это — схема Цезаря;

взломщик знает, что использовался шифр Цезаря, но не знает значение сдвига.

В первом случае шифр может быть взломан, используя те же самые методы что и для простого шифра подстановки, такие как частотный анализ и т. д., Используя эти методы взломщик вероятно быстро заметит регулярность в решении и поймет, что используемый шифр — это шифр Цезаря.

Во втором случае, взлом шифра является даже более простым. Существует не так много вариантов значений сдвига (26 для английского языка), все они могут быть проверены методом грубой силы.[Один из способов сделать это — выписать отрывок зашифрованного текста в столбец всех возможных сдвигов — техника, иногда называемая как «завершение простого компонента». Рассмотрим пример для зашифрованного текста «EXXEGOEXSRGI»; открытый текст немедленно опознается глазом в четвертой строке.

Другой способ применения этого метода — это написать алфавит под каждой буквой зашифрованного текста, начиная с этой буквы. Метод может быть ускорен, если использовать заранее подготовленные полоски с алфавитом. Для этого нужно сложить полоски так, чтобы в одной строке образовался зашифрованый текст, тогда в некоторой другой строке мы увидим открытый текст.

Для обычного текста на естественном языке, скорее всего, будет только один вариант декодирования. Но, если использовать очень короткие сообщения, то возможны случаи, когда возможны несколько вариантов расшифровки с различными сдвигами. Например зашифрованный текст MPQY может быть расшифрован как «aden» так и как «know» (предполагая что открытый текст написан на английском языке). Точно также «ALIIP» можно расшифровать как «dolls» или как «wheel»; «AFCCP» как «jolly» или как «cheer».

Многократное шифрование никак не улучшает стойкость, так как применение шифров со сдвигом a и b эквивалентно применению шифра со сдвигом a+b. В математических терминах шифрование с различными ключам образует группу.

Взлом шифра

Decryption shift	Candidate plaintext
0	exxegoexsrgi
1	dwwdfndwrqfh
2	cvvcemcvqpeg
3	buubdlbupodf
4	attackatonce
5	zsszbjzsnmbd
6	yrryaiyrmlac
23	haahjrhavujl
24	gzzgiqgzutik
25	fyyfhpfytshj