ШИФРОВАНИЕ НА ОСНОВЕ ТАБЛИЦЫ С УПРАВЛЯЮЩИМИ СИМВОЛАМИ

Представленная вам система шифрования является симметричной. При симметричном шифровании используется один и тот же ключ и для шифрования, и для расшифровки. Симметричные системы имеют как ряд достоинств, так и ряд недостатков. К достоинствам можно отнести скорость и простоту реализации, а к недостаткам — сложность обмена и управления ключами.

В рассматриваемой системе шифрования ключом является прямоугольная таблица, содержащая некоторый набор символов. По договоренности двух сторон, эти символы могут представлять собой что угодно: буквы, цифры, знаки. Так же имеются служебные символы, которые не имеют печатного представления. О них будет рассказано позже.

Рассмотрим следующий текст для зашифровки: «Нападаем в полночь. Не забудьте взять с собой агента! Ваш Юстас». В тексте встречается только кириллица, так что занесем в таблицу только символы этого алфавита. Также нам понадобится символ пробела, точки и восклицательного знака. Цифры, латиница и различные дополнительные знаки нам не понадобятся. Таким образом, мы должны занести в таблицу минимум 69 символов.

Главной особенностью данной системы шифрования является использование управляющих символов. Они влияют на сам процесс шифрования, и, соответственно, дешифрования

CC1 — Указывает на необходимость расшифровывания последующего текста. При повторном вызове указывает на конец шифрованного текста. Благодаря этому служебному символу мы можем внедрять в произвольные места шифротекста бессмысленные куски, для того, чтобы усложнить процесс несанкционированной расшифровки.

CC2 — Указывает на смещение всех символов в таблице шифровки вперед на строку. Первая строка становится второй, вторая — третьей, и так далее. Последняя строка становится первой. После этого шифротекст нужно будет расшифровывать с помощью обновленного ключа.

CC3 — Указывает на смещение всех символов в таблице шифровки назад на строку. Первая строка становится последней, вторая — первой, и так далее. После этого шифротекст нужно будет расшифровывать с помощью обновленного ключа.

CC4 — Указывает на смещение всех символов в таблице шифровки вперед на столбец. Первый столбец становится вторым, второй — третьим, и так далее. Последний стоблец становится первым. После этого шифротекст нужно будет расшифровывать с помощью обновленного ключа.

CC5 — Указывает на смещение всех символов в таблице шифровки назад на столбец. Первый столбец становится последним, второй — первым, и так далее. После этого шифротекст нужно будет расшифровывать с помощью обновленного ключа

Прибавляем эти пять управляющих символов, и получаем, что нужно занести в таблицу 74 символа. Возьмем таблицу 11*7, что даст нам возможность занести 77 символов.

Так как заполнять таблицу желательно случайным образом, можно использовать генератор псевдослучайных чисел. Оставшиеся три ячейки заполним пробелом, как самым часто используемым при письме, а так же буквами «о» и «а»

	1	2	3	4	5	6	7
А	Д	У	Ц	п	н	х	е
Б	с	П	Э	л	Ы	и	Т
В	Н	Ъ	Ю	ь	А	.	Б
Г	ы	Ж	б	СС4	Г	ч	СС2
Д	Ф	Щ	я	В	СС3	_	С
Е	Е	_	О	т	Ч	м	а
Ж	ф	К	Л	Й	И	а	Ь
З	о	ю	ш	в	а	З	р
И	Х	э	!	СС5	Ш	ж	Я
К	г	Р	М	ъ	у	щ	ё
Л	ц	Ё	СС1	д	з	к	й

Процесс шифрования заключается в том, что мы требуемый нам символ ищем в таблице, находим букву столбца и номер строки, который соответствует символу, и ставим пару букву+число, или число+букву. При шифровании мы будем использовать управляющие символы. Из заданного текста: «Нападаем в полночь. Не забудьте взять с собой агента! Ваш Юстас» получаем следующее:

3ЛВ16ЖА4Л36Ж7Е1Б53Л534Л357А6
ЕЕ2Г74И6ЕБ45Е13Б45А136Г4ВВ66Д1
ВА7Е2Л57ЕГ35К4ЛВ44ЕА72Е345Л3Д
4Е4ВД61БД61Б313Г137Л2Е4Г7Ж4ЛЛ
5А1Г5Г5Е64Л2КА1А65Е7ЖИ43Е5И4Д
5З336Д3В1Б4Е7Е1Б3ЛД1Е2Л4Л2Г7

Основной проблемой данного шифрования является передача ключа. Нужен защищенный канал передачи ключа.

Плюсом же можно отметить стойкость к взлому с помощью частотных таблиц, благодаря замене ключа, в случае, если мы передаем не обычный текст, а, например, пароли или другие ключи

Данное шифрование удобно реализовать программно. Программа будет по заданному ключу шифровать и дешифровать текст, а также сможет генерировать новые ключи.

Спасибо за внимание!