Краткий обзор развития методов криптографии

Шифр сдвига

Шифр Цезаря, также известный как шифр сдвига, код Цезаря или сдвиг Цезаря. Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

Шифр замены

Шифр простой замены, простой подстановочный шифр, моноалфавитный шифр — класс методов шифрования, которые сводятся к созданию по определённому алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифртекста. Само шифрование заключается в замене букв согласно таблице. Для расшифровки достаточно иметь ту же таблицу, либо знать алгоритм, по которому она генерируется.

К шифрам простой замены относятся многие способы шифрования, возникшие в древности или средневековье, как, например, Атбашь (также читается как этбаш) или шифр Цезаря.

Отметим, что шифр простой замены не всегда подразумевает замену буквы на какую-то другую букву. Допускается использовать замену буквы на число.

Полиалфавитный шифр

Полиалфавитный шифр (многоалфавитный шифр) — это совокупность шифров простой замены, которые используются для шифрования очередного символа открытого текста согласно некоторому правилу. Суть полиалфавитного шифра заключается в циклическом применении нескольких моноалфавитных шифров к определённому числу букв шифруемого текста.

Таблица Тритемия

Шифр Тритемия предполагал использование алфавитной таблицы. Он использовал эту таблицу для многоалфавитного зашифрования самым простым из возможных способов: первая буква текста шифруется первым алфавитом, вторая буква — вторым и т. д. В этой таблице не было отдельного алфавита открытого текста, для этой цели служил алфавит первой строк

Шифр Виженера

Шифр Виженера — это последовательность шифров Цезаря с различными значениями сдвига. Шифр Виженера является шифром подстановки, то есть шифром, в котором каждая буква исходного текста заменяется буквой шифр-текста.

Шифр Гронсфельда

Шифр Гронсфельда представляет собой модификацию шифра Цезаря числовым ключом. Для этого под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифртекст получают примерно, как в шифре Цезаря, но отсчитывают по алфавиту не третью букву, а выбирают ту букву, которая смещена по алфавиту на соответствующую цифру ключа.

Перестановочные шифры

Шифр перестановки — это метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами. Элементами текста могут быть отдельные символы, пары букв, тройки букв, комбинирование этих случаев и так далее.

В классической криптографии шифры перестановки можно разделить на два класса:

- Шифры одинарной (простой) перестановки — при шифровании символы открытого текста перемещаются с исходных позиций в новые один раз.
- Шифры множественной (сложной) перестановки — при шифровании символы открытого текста перемещаются с исходных позиций в новые несколько раз.

Квадрат Полибия

«Квадрат Полибия» представляет собой квадрат 5x5, столбцы и строки которого нумеруются цифрами от 1 до 5. В каждую клетку этого квадрата записывается одна буква. Буквы расположены в алфавитном порядке. В результате каждой букве соответствует пара чисел, и шифрованное сообщение превращается в последовательность пар чисел.
Расшифровывается путём нахождения буквы, стоящей на пересечении строки и столбца.

Магический квадрат

Магический, или волшебный квадрат — это квадратная таблица NxN, заполненная числами таким образом, что сумма чисел в каждой строке, каждом столбце и на обеих диагоналях одинакова. Если в квадрате равны суммы чисел только в строках и столбцах, то он называется полумагическим. Нормальным называется магический квадрат, заполненный натуральными числами от 1 до N^2 . Магический квадрат называется ассоциативным или симметричным, если сумма любых двух чисел, расположенных симметрично относительно центра квадрата, равна N^2 + 1.

Маршрут Гамильтона

Последовательность заполнения таблицы каждый раз соответствует нумерации ее элементов. Если длина шифруемого текста не кратна числу элементов, то при последнем заполнении в свободные элементы заносится произвольный символ. Выборка из таблицы для каждого заполнения может выполняться по своему маршруту, при этом маршруты могут использоваться как последовательно, так и в порядке, задаваемом ключом.

Решето Кардано

Решетка Кардано — это ключ к секретному посланию, как правило, специальная карточка, в которой в определенных местах имеются прорези — ячейки. Чтение зашифрованного послания происходит при наложении на кодированный текст.

Одноразовые блокноты

Шифр Вернама (одноразовый блокнот) - единственный известный абсолютно секретный шифр. Он основан на том, что сообщение кодируется побитовым xor с одноразовым ключом, длина которого не меньше длины передаваемого сообщения.

Шифр назван в честь телеграфиста Гильберта Вернама, который сконструировал телеграфный аппарат, автоматически кодирующий сообщения таким методом (ключ подавался на отдельной ленте).

Легко заметить, что нельзя использовать один и тот же ключ несколько раз - при кодировании одинаковых сообщений с одинаковым ключом, полученные сообщения также будут одинаковыми, что позволит анализировать передаваемые сообщения.

Шифровальный диск Альберти

«Диск Альберти» состоял из двух дисков — внешнего неподвижного (на нём были нанесены латинские буквы в алфавитном порядке и цифры 1, 2, 3, 4) и подвижного внутреннего диска, на котором буквы были переставлены. Диски крепились на одной оси так, чтобы внутренний мог вращаться. Окружность каждого диска разделена на 24 равные клетки. Скольжение алфавитов находится под контролем ключевых букв, включенных в тело криптограммы. Для того, чтобы расшифровать сообщение, написанное с использованием дисков Альберти вы должны были иметь соответствующий алфавит на ваш внутренний диск.

Принцип построения этого шифра заключается в следующем: для шифрования используются не один как в простой замене, а несколько шифр алфавитов. Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замене её на букву с внутреннего диска, стоящую под ней. После этого внутренний диск сдвигался на одну позицию и шифрование второй буквы производилось уже по новому шифр алфавиту. Ключом данного шифра являлся порядок расположения букв на внутреннем диске и его начальное положение относительно внешнего диска.

Шифровальная машина Enigma

«Энигма» — переносная шифровальная машина, использовавшаяся для шифрования и дешифрования секретных сообщений.

Машина Лоренца

«Лоренц» — немецкая шифровальная машина, использовавшаяся во время Второй мировой войны для передачи информации по телетайпу. Была разработана в Берлине. Принцип работы машины был основан на поточном шифре Вернама.

M-209

M-209, так же известная как CSP-1500 и C-38 — это портативная механическая шифровальная машина, первоначально использовавшаяся армией США во Второй мировой войне.