Глава 1. Моноалфавитный и полиалфавитный методы шифрования.

Первую главу я решила посвятить моноалфавитному и полиалфавитному методам шифрования, которые использовались людьми до начала использования электромеханических устройств в шифровании. Эти методы являлись основоположниками современной криптографии.

Моноалфавитный шифр, или, как его по-другому называют, шифр простой замены, простой подстановочный шифр, являет собой самы простой и самый древний метод шифрования, который, по сути, появился вместе с зарождением письменности. Его принцип состоял и состоит по сей день в том, чтобы заменять одни символы другими, то есть тем самым сводился к созданию таблицы шифровния по определенному алгоритму.

Самыми известными моноалфавитными шифрами являются Атбаш и Шифр Цезаря.

Атбаш — это шифр подстановки, который изначально использовался только для иврита, но, в целом, применим к любому языку. Его суть состоит в том, что все буквы алфавита заменяются на буквы, имеющие тот же порядковый, но с конца.

То есть, данный шифр можно записать, как D(i)=n-i, где n — количество букв в алфавите, i — изначальный порядковый номер буквы, которую нам надо заменить, а D(i) — получаемый номер, который соответствует новому значению буквы, на которое мы ее заменяем. Получается, что алфавит выстраивается в обратном порядке.

История Атбаша насчитывает почти 20 веков, так как, предположительно, он появился примерно в 500 году до нашей эры и использовался вплоть до 1300 года нашей эры. Доподлинно не известно, кто изобрел Атбаш, но считается, что его придумала иудейская секта повстанцев, Ессеи. Ими было разработано множество различных шифров и кодов, так как это было важно, чтобы избежать преследования. Позже эти знания были переданы Гностикам (Гностицизм — условное название ряда позднеантичных религиозных течений, использующих мотивы Ветхого Завета, восточной мифологии и ряда раннехристианских учений), которые в последствии передали их Катарам (христианское религиозное движение). Позднее Катарские дворяне были завербованы Орденом Тамплиеров, которым, соответственно, были переняты знания шифров. Шифр перестал существовать с роспуском Ордена Тамплиеров.

Шифр Цезаря, по-другому именуемый код Цезаря или сдвиг Цезаря, является одним из самых простых и наиболее известных методов шифрования. Он заключается в том, что алфавит «сдвигается», а каждая конкретная буква соответствует другой букве с определенным интервалом. В классическом шифре Цезаря использовался сдвиг вправо на три. То есть в целом шифр сдвига можно записать, как D(i)=i+k, при |k|<n, где i — порядковый номер начальной буквы, k — любое выбранное целое число, n — количество букв в отдельно взятом алфавите, а D(i) — получаемый порядковый номер буквы, на которую мы заменяем старую букву.

Шифр, как не трудно догадаться, был назван в честь Гая Юлия Цезаря. Он был первым зафиксированным человеком, который использовал эту схему, как уже говорилось раннее, сдвигая буквы на три, хотя доподлинно известно, что другие шифры с подстановкой использовались еще до него. Согласно «Жизни двенадцати цезарей» Светония, он использовался в целях защиты военных сообщений,. Нельзя оценить, насколько эффективным был данный шифр во времена великого правителя, но разумно предположить, что он был достаточно надежен. Большинство врагов Цезаря были безграмотными, поэтому шифр мог восприниматься как сообщения на иностранном языке.

Так же этот шифр использовался племянником Цезаря, Августом.

“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 двенадцати цезарей, Книга вторая», гл. 88

Шифр подстановки так же использовался на мезузах (свиток определенного типа пергамента из кожи кошерного животного, содержащий часть текста молитва Шма, который прикреплялся к внешнему косяку двери в еврейском доме), чтобы зашифровать имя Бога. Есть предположение, что это делалось потому, что существовали времена, когда еврейскому народу не разрешали иметь мезузу.

В XIX веке были случаи, когда обычные любители, участвовали в секретных коммуникациях, которые были зашифрованы с помощью шифра Цезаря в «Таймс». Даже позднее, в 1915 году, данный шифр использовался в качестве аналога более сложным шифрам в российской армии.

Абу аль - Кинди первым предложил использовать многоалфавитный шифр. Наиболее распространенными полиафлавитными шифрами являются шифр Виженера и шифр Гронсфельда.

В целом, шифр Виженера изобретался неоднократно. Впервые он был описан итальянцем Джован Баттиста Беллазо в середине XVI веке. Немногим позже, в 1586 году Блез Виженер представил своё описание того же самого метода шифрования перед комиссией Генриха III во Франции.

Для более удобного шифрования используется так называемая таблица Виженера. Вот так она выглядит для русского и английского языков



Сверху по горизонтали записаны буквы шифруемые, а слева по вертикали написаны буквы ключа. В качестве ключа берется какое-либо слово или фраза. Чем больше символов будет в ключе, тем сложнее будет его расшифровать. Все символы шифруются циклически. То есть к символам по очереди применяется моноалфавитный метод шифрования. Когда ключ заканчивается, то к следующему символу кодируемого сообщения применяется вновь первый символ кода. Таким образом, если у нас есть ключ длиной в n символов, то мы применяем шифровальную строку первого символа ключа к первому символу кодируемого сообщения, строку второго символа ко второму и так далее. Когда мы доходим до n+1 символа кодируемого сообщения, то снова используем первый символ для кодирования. Таким образом, если мы хотим зашифровать слово «криптография» с помощью слова «ключ» для удобства мы можем нарисовать вот такую таблицу:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Кодируемое слово | к | р | и | п | т | о | г | р | а | ф | и | я |
| Ключ | к | л | ю | ч | к | л | ю | ч | к | л | ю | ч |
| Получаемый текст | х | ь | ж | ж | э | ъ | б | з | ч | а | ж | ц |

Естественно, что для дешифровки надо использовать данный алгоритм в обратном порядке.

Шифр Гронсвельда, который был гораздо более популярен в Европе, состоит примерно в том же. Единственное его отличие от шифра Виженера состоит в том, что вместо буквенного ключа в нем используется числовой. То есть все буквы слева заменяются на числа. Количество чисел зависит от количества букв в алфавите. Соответственно каждое из заданных чисел ключа и является сдвигом алфавита.

Во времена Первой мировой войны стали использоваться новые, более сложные методы шифрования, но о них будет рассказано в следующей главе.