ИСТОРИЯ КРИПТОГРАФИИ

Дергай В.С.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

С древнейших времён предки, греки и римляне, арабы и европейцы, цезари и короли использовали всевозможные простые и сложные шифры в первую очередь для того, чтобы хранить в секрете военные и государственные тайны. Первые шифры применялись для обеспечения сохранности военных тайн от неприятеля. Посла, который нёс важный приказ командира солдатом на поле битвы, могли взять в плен, а сообщение оказалось бы в руках врага. Такая ситуация могла не только угрожать жизням других солдат, но и предопределять исход всей битвы. Однако если приказ зашифровать, то его содержание с высокой степенью вероятности останется скрытым от противника.В дальнейшем шифры придумывались и для того,чтобы хранить государственные тайны.

Первым известным применением криптографии принято считать использование специальных иероглифов около 4000 лет назад в Древнем Египте.

Один из самых простых и наиболее широко известных методов шифрования древних времен – Шифр Цезаря, также известный как шифр сдвига, код Цезаря или сдвиг Цезаря. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций. Шифр Цезаря можно классифицировать как шифр подстановки, при более узкой классификации – шифр простой замены. Например, в шифре со сдвигом 3 А была бы заменена на Г, Б станет Д, и так далее.

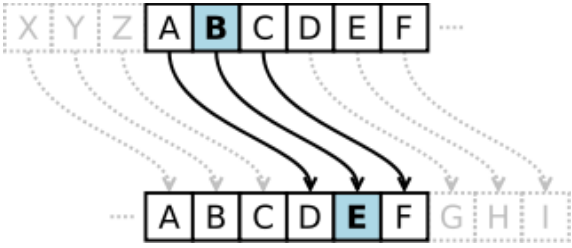

Рисунок 1. Шифр Цезаря

Значительный шаг вперёд криптография сделала благодаря труду Леона Альберти. Известный философ, живописец, архитектор, в 1466 году написал труд о шифрах. В этой работе был предложен шифр, основанный

на использовании шифровального диска. Сам Альберти называл его шифром, «достойным королей».

Шифровальный диск представлял собой пару соосных дисков разного диаметра. Больший из них – неподвижный, его окружность разделена на 24 равных сектора, в которые вписаны 20 букв латинского алфавита в их естественном порядке и 4 цифры (от 1 до 4). Меньший диск – подвижный, по его окружности, разбитой также на 24 сектора, были вписаны все буквы смешанного латинского алфавита. Имея два таких прибора, корреспонденты догадывались о первой индексной букве на подвижном диске. При шифровании сообщения отправитель ставил индексную букву против любой буквы большого диска.

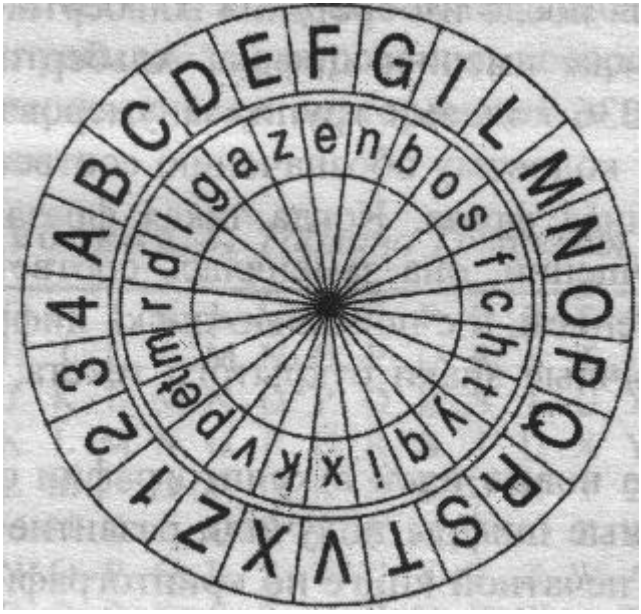

Рисунок 2. Диск Альберти

В период первой мировой войны в качестве полевых шифров широко использовались ручные шифры, в первую очередь шифры перестановки с различными усложнениями. Это были вертикальные перестановки, усложнённые перекодировкой исходного алфавита, а также двойные вертикальные перестановки. Первая мировая война явилась поворотным пунктом в истории криптографии: если до войны криптография представляла собой достаточно узкую область, то после войны она стала

широким полем деятельности. Причина этого состояла в необычайном росте объёма шифрпереписки, передаваемой по различным каналам связи. Криптоанализ стал важнейшим элементом разведки.

В семидесятых годах произошло два события, серьёзно повлиявших на дальнейшее развитие криптографии. Во-первых, был принят и опубликован первый стандарт шифрования данных (DES), "легализовавший" принцип Керкгоффса в криптографии. Во-вторых, после работы американских математиков У. Диффи и М. Хеллмана родилась "новая криптография"– криптография с открытым ключом.

Появление в середине двадцатого столетия первых электронно-вычислительных машин кардинально изменило ситуацию в области шифрования (криптографии).В результате развития компьютерных технологий огромное количество информации должно быть скрыто от несанкционированного доступа.Процесс шифрования информации при её передаче или хранении заключается в том, что открытый текст с помощью алгоритма шифрования и шифровального ключа преобразуется в зашифрованное сообщение. Данное правило в полной мере распространяется и на компьютерные системы шифрования, в которых в качестве ключа используется вполне определённая последовательность нулей и единиц.

Литература

1. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов. – М.: ДМК Пресс, 2012. – 256 с.

2. А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин Основы Криптографии. — М.: Гелиос, 2005., с.5 – 53.