Глава 1

История развития алгоритмов шифрования

Криптография – это наука о методах обеспечения конфиденциальности, целостности данных, аутентификации, а также невозможности отказа от авторства. Изначально криптография изучала способы обратимого преобразования текста на основе ключа или заданного алгоритма в шифрованный текст.

История криптографии началась более четырёх тысяч лет назад. Первые попытки шифрования текста были предприняты около третьего тысячелетия до н.э. Тогда были использованы моно алфавитные шифры, основная идея которых – замена букв исходного алфавита на другие буквы этого же алфавита, но со смещением, например: (n+3).

С греческого языка криптография переводится как – «тайнопись» и определятся как наука, позволяющая вести тайную коммуникацию. Первым известным человеком, написавшим работу о криптографии, считается Эней Тактик, завершивший свою исследовательскую деятельность ещё до н.э.. Также попытки шифровки различных дынных предпринимали Месопотамия и древняя Индия, однако первые работающие системы шифрования были изобретены в Китае. Также следует заметить, что часто различные шифры и изощрённые способы письма использовали писари Древнего Египта. Наиболее эффективное применения шифров, разумеется, в военных целях, так например, крайне успешен был применённый против Афин Спартой шифр - «Скитала». Подобные методы шифрования использовали вплоть до XV века.

Однако крипто анализ не стоял на месте и вскоре все документы стало крайне легко дешифровать. Поэтому в шестидесятых годах XV века итальянский учёный и архитектор Леон Баттиста Альберти, стремясь получить устойчивый к частотному крипто анализу шифр, изобрёл новый способ шифрования – поли алфавитный. Это означает что ключем к алгоритму является два и более секретных алфавита, переходы от одного к другому осуществлялись по некоторому заданному автором правилу. К сожалению, Баттисте не удалось довести эту систему до полноценной, это в скором времени предстояло его последователям.

Криптография особенно активно использовалась и развивалась в Средние века. Различными шифрами пользовались политики, военные дипломаты и даже купцы. Ярчайшим примером средневеково шифра является кодекс Copiale – это невероятно красиво оформленный рукописный текст (на котором были также имелись водяные знаки), дешифровка которого, до сих пор не увенчалась успехом. Эпоха Возрождения можно считать золотым веком криптографии: ее активным изучением занимались многие учёные наиболее успешным стал Фрэнсис Бэкон, которому удалось описать семь методов скрытого текста. Также он выдвинул идею двоичного способа шифрования, аналогичный использующемуся в современных компьютерных программах. Также весомое влияние на дальнейшее усовершенствование и развитие криптографии было оказало появлением первого телеграфа, поскольку факт передачи данных перестал быть секретным, что заставило отправителей сосредоточиться на шифровке данных.

[1]

С начала и до середины XX века активно практикуется внедрение электромеханических устройств в работу шифровальщиков. Однако при этом продолжалось использование поли и моно алфавитных шифров. Несомненно, Вторая мировая война послужила своеобразным толчком к развитию компьютерных систем — через криптографию. Использованные шифровальные машины (немецкая «Энигма», английская «Бомба Тьюринга») ясно показали жизненную необходимость информационного контроля. Также послевоенное время правительства многих стран наложили мораторий на использование криптографии. Необходимые исследования были опубликованы исключительно в виде секретных докладов — таких, как, например книга Клода Шеннона «Теория связи в секретных системах», подходящая к криптографии как к новой математической науке.

С середины семидесятых годов начинается переход к строгой математической криптографии, появляются совершенно конкретные определения количества информации, энтропии, передачи данных и функций шифрования. Также одними из необходимых этапов считаются изучения защиты шифра от атак – линейных и дифференциальным. Первым об этом упоминает в своей работе Шеннон.

В 1967 выход книги «взломщики кодов» Дэвида Кана, обозначил новую точку отсчёта. В книге подробно были описаны история развития криптографии и дешифрования. После выхода книги Дэвида Кана, в открытой печати стали появляться и другие работы по криптографии. Однако до 1975 года криптография оставалась «классической», или же, более корректно, криптографией с секретным ключом.

Но прогресс не стоял на месте, и вот уже был сформирован современный подход к науке, были четко определены основные требования к зашифрованной информации: конфиденциальность, защита и целостность. Криптография была разделена на две взаимодействующие части: криптосинтез и криптоанализ. То есть криптографы обеспечивают информации защиту, а криптоаналитики, напротив, ищут пути взлома системы.

[2]

[1] [<https://studopedia.org/9-187186.html>]

[2] <http://atlasprofdv.ru/index.php/prof3/703-2014-06-26-23-05-20?page=&print=1&tmpl=component>