Автор:

Точилкин Михаил Владимирович

магистрант

ФГАОУ ВО «Южно-Уральский государственный университет (НИУ)»

г. Челябинск, Челябинская область

ШИФРОВАНИЕ ЭНИГМОЙ КАК ОДИН ИЗ ИСТОРИЧЕСКИХ ЭТАПОВ РАЗВИТИЯ КРИПТОГРАФИИ

Аннотация: *в статье рассмотрено развитие криптографии и её обзор. Автор отмечает, что в связи с развитием и широким распространением криптографии, растёт интерес к данному направлению науки, интерес к её становлению и развитию.*

Ключевые слова: *криптография, Энигма, шифрование.*

Разные люди понимают под шифрованием разные вещи. Дети играют в игрушечные шифры и секретные языки. Это, однако, не имеет ничего общего с настоящей криптографией. Настоящая криптография (strong cryptography) должна обеспечивать такой уровень секретности, чтобы можно было надежно защитить критическую информацию от расшифровки крупными организациями – такими как мафия, транснациональные корпорации и крупные государства. Настоящая криптография в прошлом использовалась лишь в военных целях. Однако сейчас, с становлением информационного общества, она становится центральным инструментом для обеспечения конфиденциальности.

По мере образования информационного общества, крупным государствам становятся доступны технологические средства тотального надзора за миллионами людей. Поэтому криптография становится одним из основных инструментов, обеспечивающих конфиденциальность, доверие, авторизацию, электронные платежи, корпоративную безопасность и бесчисленное множество других важных вещей.

Криптография не является более придумкой военных, с которой не стоит связываться. Настала пора снять с криптографии покровы таинственности и

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

использовать все ее возможности на пользу современному обществу. Широкое распространение криптографии является одним из немногих способов защитить человека от ситуации, когда он вдруг обнаруживает, что живет в тоталитарном государстве, которое может контролировать каждый его шаг.

История криптографии насчитывает около 4 тысяч лет. В качестве основного критерия периодизации криптографии возможно использовать технологические характеристики используемых методов шифрования.

Первый период (приблизительно с 3-го тысячелетия до н. э.) характеризуется господством моноалфавитных шифров (основной принцип – замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами). Второй период (хронологические рамки – с IX века на Ближнем Востоке (Ал-Кинди) и с XV века в Европе (Леон Баттиста Альберти) – до начала XX века) ознаменовался введением в обиход полиалфавитных шифров. Третий период (с начала и до середины XX века) характеризуется внедрением электромеханических устройств в работу шифровальщиков. При этом продолжалось использование полиалфавитных шифров.

Четвёртый период – с середины до 70-х годов XX века – период перехода к математической криптографии. В работе Шеннона появляются строгие математические определения количества информации, передачи данных, энтропии, функций шифрования. Обязательным этапом создания шифра считается изучение его уязвимости к различным известным атакам – линейному и дифференциальному криптоанализу. Однако до 1975 года криптография оставалась «классической», или же, более корректно, криптографией с секретным ключом.

Современный период развития криптографии (с конца 1970-х годов по настоящее время) отличается зарождением и развитием нового направления – криптография с открытым ключом. Её появление знаменуется не только новыми техническими возможностями, но и сравнительно широким распространением криптографии для использования частными лицами. Правовое регулирование использования криптографии частными лицами в разных странах сильно различается – от разрешения до полного запрета.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

Современная криптография образует отдельное научное направление на стыке математики и информатики – работы в этой области публикуются в научных журналах, организуются регулярные конференции. Практическое применение криптографии стало неотъемлемой частью жизни современного общества – её используют в таких отраслях как электронная коммерция, электронный документооборот (включая цифровые подписи), телекоммуникации и других.

18 февраля 1918 года немецкий инженер Артур Шербиус (Arthur Scherbius) запросил патент на шифровальную машину, использующую роторы (это диск, имеющий с двух сторон контакты (каждый контакт соответствует символу алфавита), контакты с разных сторон попарно соединены в случайном порядке.), и совместно с Рихардом Риттером (E. Richard Ritter) основал фирму Шербиус и Риттер (Scherbius & Ritter). Они пытались наладить отношения с германским военно-морским флотом и с Министерством иностранных дел, но на тот момент те не были заинтересованы в шифровальных машинах. В дальнейшем они зарегистрировали патенты на предприятие Геверкшафт Секуритас (Gewerkschaft Securitas), которое 9 июля 1923 года основало корпорацию производителей шифровальных машин Chiffriermaschinen Aktien-Gesellschaft. Шербиус и Риттер состояли в совете директоров этой корпорации.

Корпорация Chiffriermaschinen AG начала рекламировать роторную машину, Энигму модели «A», которая была выставлена на обозрение на конгрессе Международного почтового союза в 1923 и 1924 годах. Машина была тяжёлой и очень большой и напоминала печатную машину. Её размеры были 65×45×35 см, и весила она около 50 кг. Потом была представлена модель «B» подобной же конструкции. Первые две модели «A» и «B» были совсем не похожи на более поздние версии. Они были различных размеров и формы. Отличались они и с шифровальной точки зрения – в ранних версиях не хватало рефлектора.

Рефлектор – идея, предложенная коллегой Шербиуса Вилли Корном (Willi Korn) – впервые был внедрён в Энигме модели «C» (1926). Рефлектор был ключевой особенностью Энигмы.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

Модель «C» была меньше по размеру и более портативной, чем предшественники. В этой модели не хватало пишущей машинки, чтобы заменить дополнительного оператора, следящего за лампочками, отсюда и альтернативное название «Glowlamp Enigma», для отличия её от моделей «A» и «B». Энигма модели «C» вскоре устарела, уступая новой модели «D» (1927). Эта версия широко использовалась в Швеции, Нидерландах, Великобритании, Японии, Италии, Испании, США и Польше.

15 июля 1928 года немецкой армией была внедрена собственная модель Энигмы – «Энигма G», модифицированная в июне 1930 года в модель «Энигма I». «Энигма I», также известная как Энигма вермахта, или «войсковая» Энигма, широко использовалась немецкими военными службами и другими государственными организациями (например, железными дорогами) во время Второй мировой войны.

Список литературы

1. Tatu Ylonen. Introduction to Cryptography (Введение в криптографию) [Электронный ресурс]. – Режим доступа: http://www.infocity.kiev.ua/hack/content/hack014.phtml

2. Носов В.А. Краткий исторический очерк развития криптографии.

3. Сивтсев Д. Алгоритм Энигмы [Электронный ресурс]. – Режим доступа: http://habrahabr.ru/post/217331/

4. Tony Sale. Technical Specification of Enigma (Технические спецификации Энигмы) [Электронный ресурс]. – Режим доступа: http://www.codesandciphers.org.uk/enigma/rotorspec.htm

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)