криптография

Криптография – математическая дисциплина, связанная с изучением методов и средств защиты информации, обеспечивающих конфиденциальность, имитозащиту, опознавание и ряд других функций.

Слово «криптография» имеет греческое происхождение и в буквальном переводе на русский язык означает «тайнопись». Цель криптографии состоит не в том, чтобы скрыть наличие сообщения, а в том, чтобы скрыть его смысл. Чтобы сделать сообщение непонятным, оно зашифровывается по определенному правилу.

Свои послания пытались шифровать еще в древних цивилизациях: Индии, Египте, Месопотамии. Чтобы запутать читателя, использовали методы кодирования и стеганографии, которые лишь косвенно относятся к криптографии. Шифрование обычно сводилось к перестановке и замене символов.

Ученые считают первым применением криптографии использование специальных иероглифов в Древнем Египте. Тогда у египтян была другая задача — не затруднить чтение, а превзойти друг друга в изобретательности передачи послания. Прежде всего, писцы хотели привлечь внимание к своим текстам, используя более редкие иероглифы для красноречия.

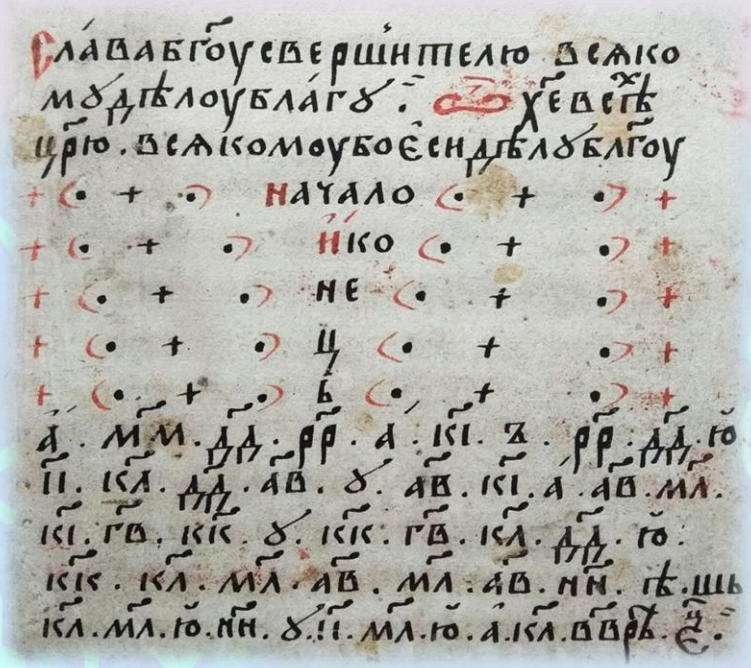
Самым древним свидетельством применения шифра (около 4000 до н.э.) ученые считают древнеегипетский папирус с перечислением монументов времен фараона Аменемхета II. Безымянный автор видоизменил известные иероглифы, но, скорее всего, не для сокрытия информации, а для более сильного воздействия на читателя.

Еще один известный шифр – древнесемитский атбаш, приблизительно 600 г. до н.э. Здесь информацию запутывали самым простым способом – с помощью подмены букв алфавита. Криптограммы на атбаше встречаются в Библии.

А в Древней Спарте пользовались скиталой – шифром из цилиндра и обвивающей его полоски пергамента. Текст писали в строку на пергаменте. После разматывания ленты текст превращался в шифр, прочитать который было возможно, только имея цилиндр такого же диаметра. Можно сказать, что спартанская скитала стала одним из первых криптографических устройств.

Шифрованием пользовались многие древние народы, но особенного успеха в криптографии уже в нашу эру достигли арабские ученые. Высокий уровень развития математики и лингвистики позволил арабам не только создавать свои шифры, но и заниматься расшифровкой чужих. Это привело к появлению первых научных работ по криптоанализу – дешифровке сообщений без знания ключа. Эпоха так называемой наивной криптографии, когда шифры были больше похожи на загадки, подошла к концу.

Интересно, что в Древней Руси тоже были свои способы тайнописи, например литорея, которая делилась на простую и мудрую.
В мудрой версии шифра некоторые буквы заменялись точками, палками или кругами. В простой литорее, которая еще называлась тарабарской грамотой, все согласные буквы кириллицы располагались в два ряда. Зашифровывали письмо, заменяя буквы одного ряда буквами другого.



Еще одним известным шифром Древней Руси была цифирь, когда буквы, слоги и слова заменялись цифрами. Иногда для усложнения в шифр добавлялись математические действия, и было непросто разгадать подобную загадку: «Десятерица сугубая и пятерица четверицею, единица четверицею сугубо и десятерица дващи».

В Средние века прорыва в шифровании не произошло. Новые и более сложные методы шифрования появлялись редко – старых было вполне достаточно.

Эпоха Возрождения дала криптографии намного больше, чем Средние века. В это время люди сосредоточились на изобретении шифров, а не шифровальных инструментов. Хотя именно этот инструмент и дал начало новому периоду в криптографии. Около 1466г. Итальянский ученый Леон Баттиста Альберти выдвинул идею двойного шифрования.

Он сконструировал шифровальный диск состоящий из двух частей: неподвижной внешней и внутренней, которая двигалась. Для шифрования, нужно было вращать внутренний диск через несколько слов. С каждым поворотом образовывалась новая комбинация.

Промышленная революция не обошла вниманием и криптографию. Около 1790 года один из отцов – основателей США Томас Джефферсон создал дисковый шифр, прозванный позже цилиндром Джефферсона. Этот прибор, основанный на роторной системе, позволил автоматизировать процесс шифрования и стал первым криптоустройством Нового времени.

Большое влияние на шифровальное дело оказало изобретение телеграфа. Прежние шифры вмиг перестали работать, при этом потребность в качественном шифровании только возрастала в связи с чередой крупных военных конфликтов. В XIX-XX веках основные импульсы для развития криптографии давала именно военная сфера. С 1854 года британские военные применяют шифр Плейфера, в основе которого – шифрование биграмм, или пар символов. Этот шифр использовался до начала Второй мировой войны.

Во время Второй мировой войны противники уже использовали мобильные электромеханические шифраторы, шифры которых считались нераскрываемыми. Сами устройства были роторными, как шифровальная машина «Энигма», и на цевочных дисках, как М-209. С помощью «Энигмы» сообщения шифровали войска Германии и ее союзники, при помощи М-209 — армия США. В СССР производили оба типа устройств.

Шифровальная машина «Энигма М-4»

Шифровальна машина М-209

Шифры «Энигмы» считались самыми стойкими для взлома, так как количество ее комбинаций достигало 15 квадриллионов. Однако код «Энигмы» все же был расшифрован, сперва польскими криптографами в 1932 году, а затем английским ученым Аланом Тьюрингом, создавшим машину для расшифровки сообщений «Энигмы» под названием «Бомба».

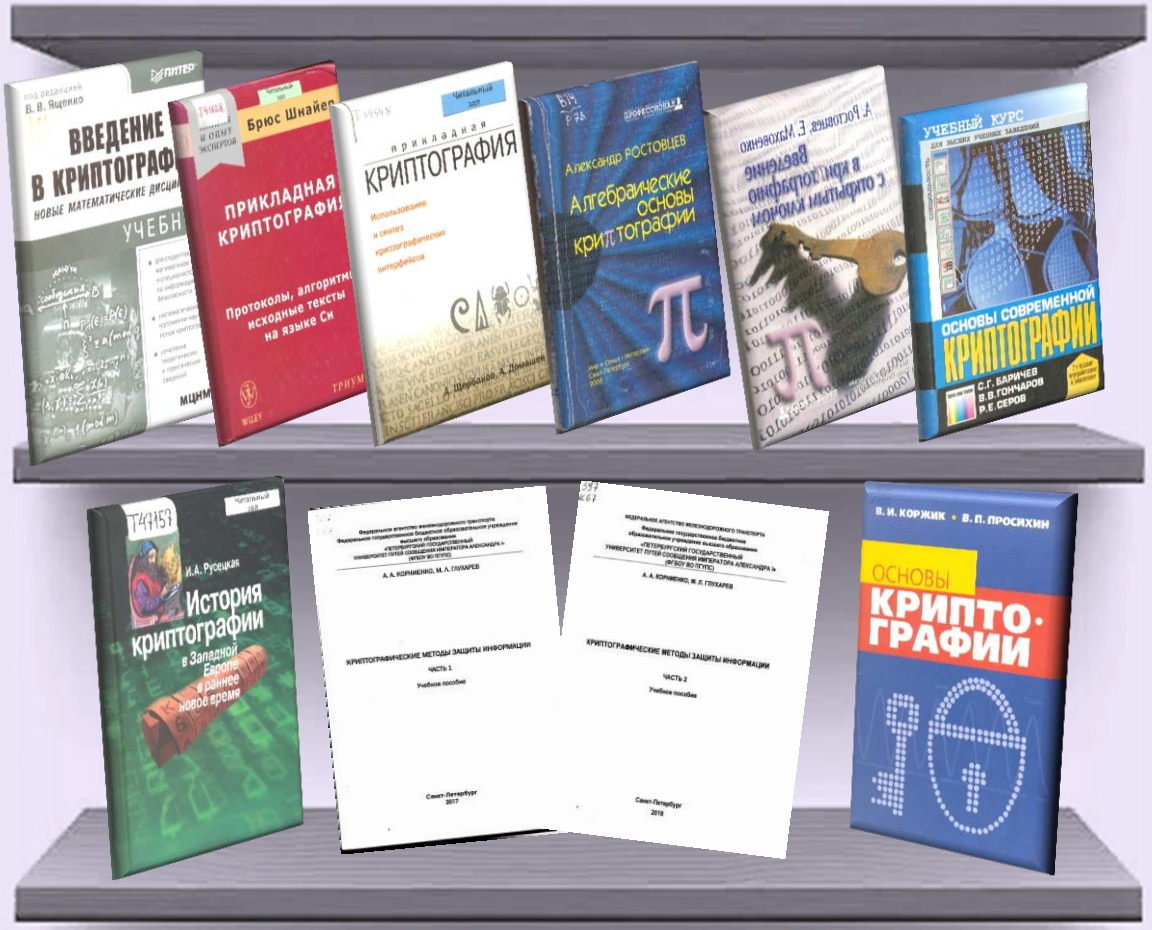
К концу 1960-х роторные шифровальные системы заменяются более совершенными блочными, которые предполагали обязательное применение цифровых электронных устройств.

С распространением компьютеров криптография выходит на новый уровень. Мощности новых устройств позволяют создавать на порядки более сложные шифры. Шифр или код становится языком общения между компьютерами, а криптография становится полноценной гражданской отраслью. В 1978 году разрабатывается стандарт шифрования DES, который стал основой для многих современных криптографических алгоритмов.

На протяжении многих веков послания засекречивались вручную и лишь в XX веке появились шифровальные машины. Но сфера применения шифров оставалась незначительной до компьютерной революции, которая ознаменовала новый этап в развитии криптографии. Из области интересов узкой прослойки общества шифрование перешло в нашу повседневную жизнь. Сегодня мы сталкиваемся с криптографией ежедневно, когда вводим пароль от почтового сервиса, узнаем статус покупки онлайн или делаем денежный перевод через приложение банка.

Криптография прошла гигантский путь от простых шифров древности к сложнейшим криптосистемам. Будущее этой науки творится на наших глазах – очередная революция в шифровании произойдет с появлением квантовых суперкомпьютеров, разработка которых уже ведется.

литература


ПИТЕР
под редакцией
В. В. Ященко
ВВЕДЕНИЕ
В КРИПТОГРАФ
НОВЫЕ МАТЕМАТИЧЕСКИЕ ДИСЦИ
УЧЕБН
Брюс Шнайер
ПРИКЛАДНАЯ
КРИПТОГРАФИЯ
Протоколы, алгоритм
исходные тексты
на языке Си
ТРИУМ
прикладная
КРИПТОГРАФИЯ
Использование
и синтез
криптографических
интерфейсов
А. Шокалов, А. Домашев
Александр РОСТОВЦЕВ
Алгебраические
основы
криптографии
Введение в криптографию
УЧЕБНЫЙ КУРС
ОСНОВЫ СОВРЕМЕННОЙ
КРИПТОГРАФИИ
С.Г. БАРИЧЕВ
В.В. ГОНЧАРОВ
Р.Е. СЕРОВ
И.А. Русецкая
История
криптографии
в Западной
Европе
в раннее
новое время
А. А. КОРМЕНЦКО, М. Л. ГЛУХАРЕВ
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ
ЧАСТЬ 1
Учебное пособие
Санкт-Петербург
2017
А. А. КОРМЕНЦКО, М. Л. ГЛУХАРЕВ
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ
ЧАСТЬ 2
Учебное пособие
Санкт-Петербург
2018
В. И. КОРЖИК • В. П. ПРОСИХИН
ОСНОВЫ
КРИПТО·
ГРАФИИ

1. Введение в криптографию: Новые математические дисциплины : учебное пособие / В. В. Ященко [и др.] ; ред. В. В. Ященко. - СПб. ; М. ; Харьков : Питер ; [Б. м.] : МЦНМО, 2001. - 287 с. : ил.

2. Шнайер, Брюс. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptjgraphy : пер. с англ. / Б.Шнайер. - М. : Триумф, 2003. - 815 с. : ил.

3. Щербаков, А. Ю. Прикладная криптография: Использование и синтез криптографических интерфейсов : к изучению дисциплины / А. Ю. Щербаков, А. В. Домашев. - М. : Русская редакция, 2003. - 404 с. : ил.

4. Ростовцев, А. Г. Алгебраические основы криптографии / А. Г. Ростовцев. - СПб : Мир и семья: Интерлайн, 2000. - 353 с.

5. Ростовцев, А. Г. Введение в криптографию с открытым ключом : учебное пособие / А. Г. Ростовцев, Е. Б. Маховенко. - СПб. : Мир и Семья ; [Б. м.] : Интерлайн, 2001. - 335 с. : ил.

6. Баричев, С. Г. Основы современной криптографии : Учебный курс / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. - 2-е изд., перераб. и доп. - М. : Горячая линия - Телеком, 2002. - 175 с. : ил.

7. Русецкая, И. А. История криптографии в Западной Европе в раннее новое время / И. А. Русецкая. - Санкт-Петербург : Центр гуманитарных инициатив ; [Б. м.] : Университетская книга-СПб, 2014. - 143 с.

8. Корниенко, А. А. Криптографические методы защиты информации: учебное пособие / А. А. Корниенко, М. Л. Глухарев. - Санкт-Петербург : ФГБОУ ВО ПГУПС.
Ч. 1. - 2017. - 61 с. : ил. - Библиогр.: с. 60.

9. Корниенко, А. А. Криптографические методы защиты информации [Текст] : учебное пособие / А. А. Корниенко, М. Л. Глухарев. - Санкт-Петербург : ФГБОУ ВО ПГУПС.
Ч. 2 / , ФГБОУ ВО ПГУПС. - 2018. - 63 с. : ил., табл. - Библиогр.: с. 61.

10. Коржик, В. И.
Основы криптографии : учебное пособие по спец. 210403 "Защищенные телекоммуникационные системы связи" / В. И. Коржик, В. П. Просихин. - СПб. : Линк, 2008. - 250 с. : ил.