БИБЛИОТЕКА "КНИГА БУДУЩЕГО ИНЖЕНЕРА"

ИНФОРМАЦИОННЫЙ МИР XXI ВЕКА

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ГРАЖДАНСКОЙ АВИАЦИИ

УДК 003.26
ББК 87.4
И74

Библиотека «Книга будущего инженера»

И74 **Информационный мир XXI века. Криптография – основа информационной безопасности** / Под ред. Э.А. Болелова; Московский государственный технический университет гражданской авиации. – 4-е изд. – М.: Издательско-торговая корпорация «Дашков и К°», 2020. – 126 с.

ISBN 978-5-394-03777-1

Книга посвящена криптографическим методам защиты информации. В ней даются советы, как защитить свое послание. Рассказывается об истории развития криптографии, ее математических основах. Рассмотрены современные криптосистемы.

Для учащихся инженерных классов общеобразовательных школ, учителей, ведущих занятия в этих классах, а также широкого круга читателей.

ISBN 978-5-394-03777-1

Содержание

1. Как защитить свое послание?

С тех пор как люди изобрели письменность, возникла потребность защищать свои послания от посторонних. В документах древних цивилизаций (Индии, Египта, Месопотамии, Греции) встречаются сведения о способах защиты посланий. Уже в те времена человек выработал три основных способа защиты информации.

Первый способ защиты информации – физическая защита от противника материального носителя информации (пергамента, бумаги), например передача информации специальным курьером с охраной, сундук с надежным замком для тайного послания и так далее.

Второй способ защиты информации – сокрытие от противника самого факта передачи информации. Интересен способ, описанный в трудах Геродота. На голове раба, которая брилась наголо, записывалось послание. Когда волосы раба достаточно отрастали, его отправляли к адресату, который снова брил голову раба и читал послание.

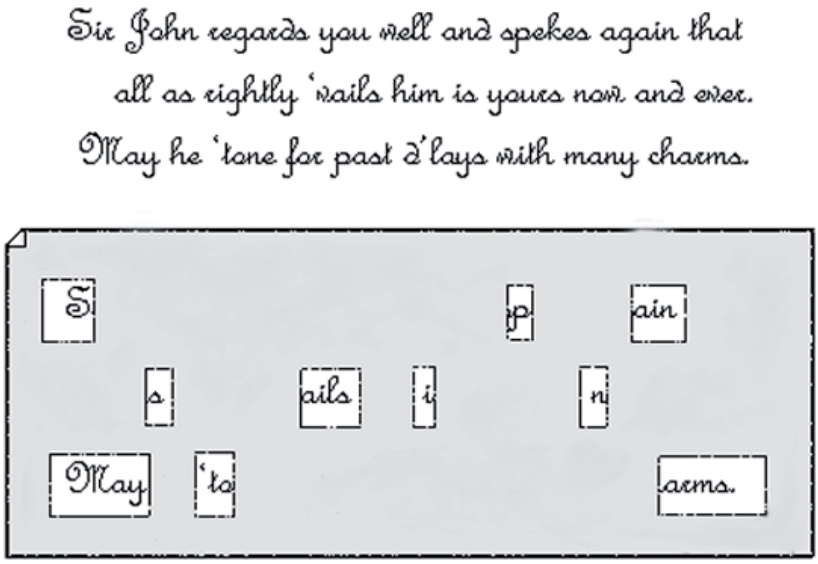
Для защиты посланий были широко распространены и сейчас используются симпатические или «невидимые» чернила. Между строк ничем не примечательного послания записывалось передаваемое сообщение. Адресат проводил термическую, химическую или другую обработку и читал передаваемое скрытое сообщение.

В XVI–XVIII веках пользовались популярностью различные «решетки», предназначенные для кодирования сообщений. Наиболее известна «решетка», которую называют «шифром Ришелье». Эта «решетка» вырезалась из листа картона или пергамента, или же из любого тонкого металла.

«Решетка» помещается на лист бумаги и затем записывается сообщение в ее прямоугольных

отверстиях, в которых помещается отдельный символ, слог или целое слово. Исходное сообщение оказывается разделенным на большое число маленьких фрагментов. Затем «решетка» убирается и пустые места на бумаге заполняются посторонним текстом так, чтобы скрываемый текст стал частью другого текста. Такое заполнение требует известного литературного таланта.

Для расшифровки у получателя сообщения должна быть такая же «решетка».



Подобной «решеткой» пользовался известный русский дипломат и писатель А.С. Грибоедов, будучи послом в Персии.

В настоящее время разработкой средств и методов сокрытия факта передачи сообщений занимается специальная наука – **стеганография**.

Третий способ защиты информации – преобразование информации, маскирующее ее содержание от посторонних лиц. Такое преобразование информации называется **криптографическим**, а наука о методах и способах преобразования информации с целью ее защиты от незаконных пользователей называется **криптографией**.

Далее мы будем рассматривать только криптографические способы защиты информации, потому что криптография является основой современных систем защиты информации и наиболее широко используется.

В целях понимания материала, изложенного в книге, дадим некоторые основные определения и понятия криптографии.

Криптография – наука, изучающая методы, алгоритмы и средства преобразования информации (шифрования) в целях сокрытия ее содержания.

Криптоанализ – наука, изучающая методы, алгоритмы и средства анализа криптосистем извлечения конфиденциальной информации.

Таким образом, криптография и криптоанализ составляют единое целое и образуют науку – **криптологию**.

Исторически центральным понятием криптографии является понятие шифра.

Шифром называется совокупность обратимых криптографических преобразований множества открытых текстов на множество зашифрованных текстов, проводимых с целью их защиты. Конкретный вид криптографического преобразования открытого текста определяется с помощью **ключа** шифрования.

Открытым текстом называют исходное сообщение, которое подлежит зашифрованию.

Под **зашифрованием** понимается процесс применения обратимого криптографического преобразования к открытому тексту, а результат этого преобразования называется **шифртекстом**, или **криптограммой**. Соответственно, процесс обратного криптографического преобразования криптограммы в открытый текст называется **расшифрованием**. Расшифрование нельзя путать с дешифрованием.

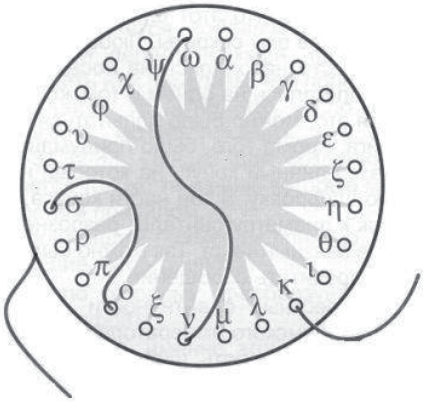
Дешифрование (**дешифровка**, **взлом**) – процесс извлечения открытого текста без знания криптографического ключа на основе перехваченных криптограмм.

2. Из истории криптографии

Вероятно, первые в истории человечества шифровальные устройства (шифраторы) появились в Древней Греции. Первое шифровальное устройство – скиталу создали в Спарте примерно в V–IX веках до н. э. **Скитала** (в переводе – «жезл» или «посох») представляет собой цилиндр заданного диаметра. На цилиндр наматывался ремень из пергамента, на который наносился текст сообщения вдоль оси цилиндра. Затем ремень сматывался и отправлялся получателю сообщения. Последний, имея аналогичный цилиндр, расшифровывал сообщение. Ключом шифра является диаметр скитала.

Изобретение дешифровального устройства приписывается Аристотелю. Он предложил использовать для дешифрования конусообразное «копье», на которое наматывался перехваченный ремень, до тех пор, пока не появлялся осмысленный текст. Скитала упоминается в трудах Аполлония Родосского (III век до н.э.), а также Плутарха (около 45–127 гг. н. э.), у которого описывается сам способ шифрования.

В античные времена в IV веке до н.э. древнегреческий полководец Эней Тактик предложил устройство, названное впоследствии **диском Энея**. Принцип был прост. На диске размером 10-15 см и толщиной 1-2 см высверливались отверстия по числу букв алфавита. В центре диска закреплена катушка с нитью. При зашифровании нитка последовательно протягивалась через отверстия, соответствующие буквам послания. Диск отсылался получателю, который вытягивал нитку из отверстий и получал сообщение в обратном порядке.



Другим устройством шифрования, предложенным Энеем Тактиком является **линейка Энея**. Здесь вместо диска использовалась линейка с числом отверстий, равным числу букв в алфавите. Буквы по отверстиям располагались в произвольном порядке. К линейке прикреплялась катушка с нитью. При шифровании нить протягивалась через отверстие, соответствующее букве шифруемого послания, при этом на нити в месте прохождения отверстия завязывался узелок. Таким образом, зашифрованное послание представляло собой нить

с узелками, в которой каждой букве ставилось в соответствие расстояние между узелками нити. Ключом шифра являлся порядок следования букв по отверстиям линейки.

Еще оно изобретение древних греков – **квадрат Полибия**. Полибий – греческий государственный деятель, полководец III века до н.э. Применительно к современному английскому алфавиту шифрование по этому квадрату заключалось в следующем. Шифруемая буква заменялась на координаты квадрата, в котором она записана. Так, буква R заменяется на DB. При расшифровании каждая пара букв определяет соответствующую букву сообщения. Например, TABLE – DDAAABCAAE. Ключом этого шифра является сам квадрат.

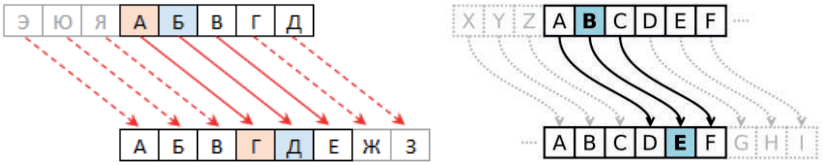
	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I,J	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Интересно отметить, что в несколько измененном виде квадрат Полибия дошел до наших дней и получил название «тюремный шифр». Для его использования достаточно знать только естественный порядок букв в алфавите. Стороны квадрата обозначаются не буквами, а цифрами.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Каждая цифра кодируется определенным количеством стуков. При передаче сообщения сначала «отстукивается» номер строки, а затем номер столбца. «Тюремный шифр» строго говоря не является шифром, это способ кодировки сообщения с целью его приведения к виду удобному для передачи по каналу связи (тюремная стена).

Значительный вклад в развитие криптографии внес Гай Юлий Цезарь – древнеримский государственный и политический деятель, диктатор. Суть метода шифрования заключается в следующем. Выписывается алфавит, а затем под ним выписывается тот же алфавит, но с циклическим сдвигом на три буквы влево.



Шифрование заключается в выборе буквы из первой строки и замену ее на букву второй строки, расшифрование представляет собой обратную операцию. Например, APPLE – DSSOH. Ключом шифра Цезаря является величина циклического сдвига. Гай Юлий Цезарь всю жизнь использовал один и тот же ключ – сдвиг на 3 буквы. Преемник Юлия Цезаря – Цезарь Август использовал тот же шифр, но со сдвигом на одну букву.

В эпоху раннего Средневековья мощная созидательная энергия арабской культуры, которую ислам лишил портретной живописи и скульптуры, дала плоды на ниве литературы, музыки и наук. Распространились различные ремесла, развивалась система государственного управления, которая потребовала создания различных методов защиты информации. Разумеется, не обошли своим вниманием арабы и криптографию. Получило широкое распространение составление словесных загадок, ребусов и каламбуров. Грамматика стала главным учебным предметом и включала в себя тайнопись. Тайнопись и ее значение упоминаются в сказках Шахерезады «Тысяча и одна ночь». Да и само слово «шифр» имеет корни в арабском слове صِفْر («сифр», т.е. ноль). Кстати, цифры, которыми сейчас пользуются в мире, называются «арабскими», хотя на самом деле они пришли в Европу через Ближний Восток из Индии. Сейчас арабы, как и все в мире, пользуются десятичной системой счисления, однако написание цифр серьезно отличается от принятого на Западе.

0 1 2 3 4 5 6 7 8 9

٠ ١ ٢ ٣ ٤ ٥ ٦ ٧ ٨ ٩

На Арабском Востоке появились книги не только с описаниями известных на тот момент систем шифрования, но и впервые в истории было