Криптография – история возникновения и математическое составляющее

проМан ученика

1(5) – В класса

Одесской Мариинской гимназии

Константина Артюшка

А) Наука о способах преобразования информации с целью ее защиты от посторонних.

Б) Область научных и инженерно-технических исследований и практической деятельности, которая занимается разработкой, анализом и обоснованием стойкости криптографических средств защиты информации от угроз со стороны противника.

Основные задачи криптографии – обеспечение секретности, целостности, аутентификации, невозможности отказа, неотслеживаемости

Что такое криптография?

История криптографии

- Способы тайного письма были известны уже древним цивилизациям Индии , Египта и Месопотамии . Были найдены множества примеров засекреченных посланий , рецептов и текстов . Первым применением криптографии принято считать использование специальных иероглифов в Древнем Египте около 5 000 000 лет до н.э.

История криптографии

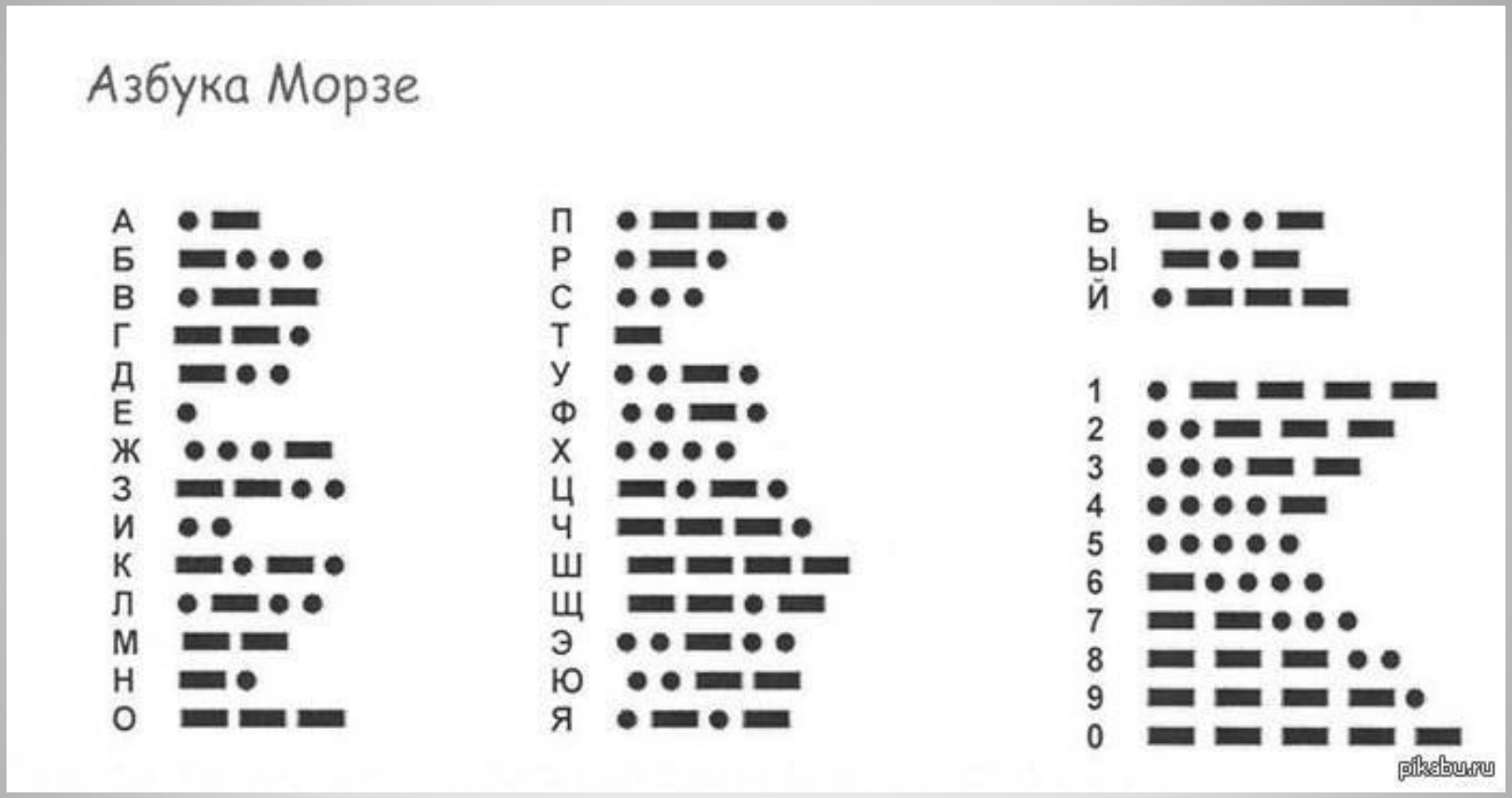
- Хотя никто не знает, когда появилась тайнопись, но глиняная табличка, сделанная приблизительно 1500 лет до нашей эры, содер-жит один из самых ранних ее примеров. Она содержит закодированную формулу изготовления глазури для покрытия сосудов. Греки применя- ли коды по крайней мере с 475 года до нашей эры, а высшие слои в Риме использовали простые шифры в период царствования Юлия Цеза- ря. В начале нашей эры интерес к криптографии (также, как и к другим интеллектуальным занятиям) упал; единственными, кто иногда применял ее, были монахи.

- С наступлением эпохи возрождения искусство криптографии стало расцветать. Во времена Луи XIV во Франции для правительственных сообщений использовалось шифрование, основанное на 587 произвольно набранных ключах.

История криптографии

- В XIX веке два фактора способствовали развитию криптографии. Первым фактором были истории Эдгара Алана По такие, как "Золотой жук", в которых фигурируют закодированные сообщения и которые волновали воображение многих читателей. Вторым фактором явилось изобретение телеграфа и азбуки Морзе. Азбука Морзе была первым двоичным представлением (точка и тире) алфавита, которое получило широкое распространение.

История криптографии



Азбука Морзе

- В первую мировую войну в ряде стран были разработаны "шифро- вальные машины", которые позволяют легко кодировать и декодиро- вать текст, используя сложный шифр. С этого момента история крип- тография становится историей дешифрации кодов.

История криптографии

- Во время второй мировой войны главный метод дешифровки кодов основывался на краже неприятельской дешифровальной машины, таким образом можно было избежать утомительного процесса расшифровки кодов. Фактически обладание службой Аллеса германской шифровальной машиной, что было не известно Германии, способствовало в оп- ределенной степени исходу войны.

История криптографии

Германская шифровательная машина

Криптография в литературе

- Шерлок Холмс был крупный специалист в области криптографии:
- **- Я превосходно знаком со всеми видами тайнописи и сам являюсь автором научного труда, в котором проанализировано сто шестьдесят различных шифров**. (**I am fairly familiar with all forms of secret writings, and am myself the author of a trifling monograph upon the subject, in which I analyze one hundred and sixty separate ciphers,..**)

Криптография в литературе

- «Пляшущие человечки» (англ. The Adventure of the Dancing Men) — один из 56 рассказов английского писателя Артура Конана Дойля о сыщике Шерлоке Холмсе, включённый писателем в сборник 13 рассказов «Возвращение Шерлока Холмса», опубликованных в журнале «Стрэнд».
- Сам писатель включал этот рассказ в число 12 своих лучших произведений о Холмсе. В рассказе великий сыщик Шерлок Холмс разоблачает загадку таинственного шифра, состоящего из изображений пляшущих человечков.
- Сюжет «Плящущих человечков» настолько схож с сюжетом «Золотого жука», что некоторые критики считают этот рассказ данью уважения Конан Дойля к Эдгарду Аллану По.

Шифр «Пляшущие человечки»

- Берем алфавит :

Практическая часть

- После этого поменяем буквы местами вот так :
- А + 1
- Б - 1
- В + 1
- Г - 1
- ……
- Э + 1
- Ю - 1
- и Я оставляем на месте .

Практичекая часть

- Мы получили такой «алгоритм»

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я
Б А Г В Е Д Ж Ё И З К Й М Л О Н Р П Т С Ф У Ц Х Ш Ч Ь Щ Ъ Ы Ю Э Я

Теперь присвоем новому алфавиту порядковый номер от одного до 33 + точка , запятая и пробел .

Практичекая часть

- Б - 1
- А - 2
- Г - 3
- В - 4
- ….
- Ъ - 28
- Ы - 29
- Ь - 30
- Ю - 31
- Э - 32
- Я - 33
- Точка (.) - 34
- Запятая (,) - 35
- Пробел (_) - 36 .

Практическая часть

- Теперь самая главная часть – замена . Все мы знаем , что существует такой язык как иврит . И там есть «свои цифры» . Так вот , мы смотрим как читаются цифры по еврейски и получается как-то так:

Практическая чать

- Б – ахат 1
- А – штайм 2
- Г –шалош 3
- В – арба 4
- Е – хамеш 5
- Д – шеш 6
- Ж – шэва 7
- Ё – шмноэ 8
- И – тейша 9
- З – эсэер 10

Практическая часть

- К – ахат эсрэ 11
- Й - штайм эсрэ 12
- М- шалош эстрэ13
- Л – арба эсрэ 14
- О - хамеш эсрэ 15
- Н – шеш эсрэ16
- Р – шэва эсрэ 17
- П – шмонэ эсрэ 18
- Т тейша эсрэ 19
- С – эсрим 20

Практическая часть

- Ф – эсрим ве ахат 21
- У – эсрим у штайм 22
- Ц – эсрим ве шалош 23
- Х – эсрим вэ арба 24
- Ш – эсрим вэ хамеш 25
- Ч – эсрим ва шеш 26
- Ь – эсрим ва шева 27
- Щ – эсрим у шмонэ 28
- Ъ – эсрим ва тейша 29
- Ы – шлошим 30
- Ю – шлошим вэ ахат 31
- Э – шлошим у штайм 32
- Я – шлошим вэ шалош 33
- . – шлошим вэ арба 34
- , - шлошим у хамеш 35
- _ - шлошим вэ шеш . 36

Практическая часть

ШИФРУЕМ !

- Зашифруем фамилию моего куратора :

  ЧЕРЕПЕНКО

Практическая часть

- Исспользуя схему МОЕГО шифра :

- **ЧЕРЕПЕНКО=ШДПДОИН=27 6 18 6 15 9 16 = эсрим ва шева шеш шмонэ эсрэ шеш хамеш эсрэ тейша шеш эсрэ .**

Практичекая часть

Спасибо за внимание