

Популярно о криптографии

Основные понятия

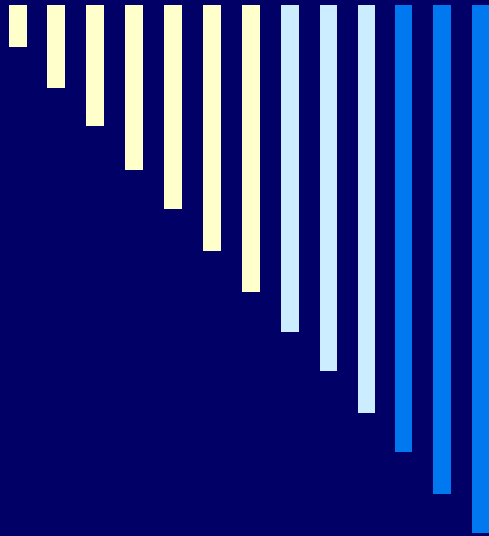


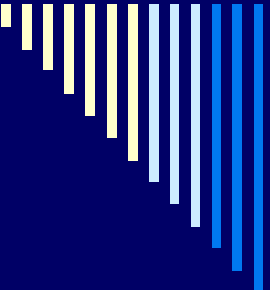
Когда и зачем нужно защищать информацию?

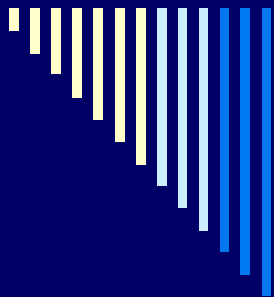
- Когда? В тех случаях, когда есть опасения, что информация станет доступной посторонним, которые могут обратить ее во вред законному пользователю.
 - Зачем? Чтобы предотвратить возможный вред от разглашения информации.
-

Информация – основное

понятие научных направлений, изучающих процессы передачи, переработки и хранения различных данных. Суть понятия информации обычно поясняется на примерах. Формальное определение не дается, поскольку понятие информации относится к таким же фундаментальным понятиям, как материя.



- 
- Информация может содержать тайну или являться защищаемой, приватной, конфиденциальной или секретной. Для наиболее типичных, часто встречающихся ситуаций такого типа введены даже специальные понятия:
 - - **государственная тайна;**
 - - **военная тайна;**
 - - **коммерческая тайна;**
 - - **юридическая тайна;**
 - - **врачебная тайна.**
-



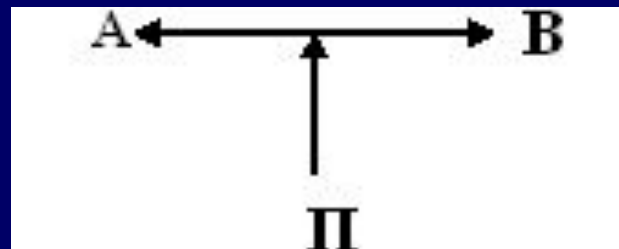
- **Криптография** – наука о методах преобразования информации с целью ее защиты от незаконных пользователей.
- **Стеганография** – набор средств и методов скрытия факта передачи сообщения.
- **Шифр** – способ, метод преобразования информации с целью ее защиты от незаконных пользователей.
- Еще одна важная проблема: соотношения цены информации, затрат на ее защиту и добывание. При современном уровне развития техники сами средства связи, а также разработка средств перехвата и защиты информации требуют очень больших затрат.

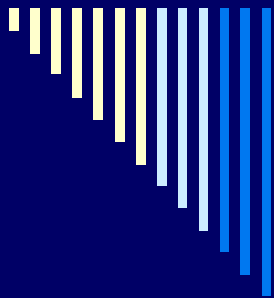


- Известен метод *микрочки*: сообщение записывается с помощью современной техники на очень маленький носитель – микрочку, которая пересылается с обычным письмом, например, под маркой или где-нибудь в другом заранее обусловленном месте.
- В настоящее время в связи с широким распространением компьютеров известно много тонких методов «запрятывания» защищаемой информации внутри больших объемов информации, хранящейся в компьютере.

Как можно представить основной объект криптографии

- Можно представить так:
- Здесь A и B – удаленные законные пользователи защищаемой информации; они хотят обмениваться информацией по общедоступному каналу связи. Π – незаконный пользователь, который может перехватывать передаваемые по каналу связи сообщения и пытаться из них интересующую его информацию.
- Приведенную схему также можно считать моделью типичной ситуации, в которой применяются криптографические методы защиты информации.





- **Вскрытие шифра** – процесс получения информации из зашифрованного сообщения без знания примененного шифра.
- **Шифрование** – процесс применения шифра к защищаемой информации, то есть преобразование защищаемой информации в зашифрованное сообщение с помощью определенных правил, содержащихся в шифре.
- **Дешифрование** – процесс, обратный шифрованию, то есть преобразование зашифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре.



Шифр «Сциталь».





Шифр Цезаря

Н У А Т Х С Ё У Г Ч А В



Шифр Виженера

ВАЗА означает следующую
последовательность сдвигов
букв открытого текста

3 1 9 1 3 1 9 1 3 1 9 1 3 1 9 1...



Что такое ключ

- Под *ключом* в криптографии понимают сменный элемент шифра, который применен для шифрования конкретного сообщения.
- В шифре «Сциतालъ» ключом является диаметр сциतालъ. При этом, не меняя принцип построения шифра, можно для шифрования различных сообщений пользоваться сциतालъами разных диаметров.
- В шифрах типа шифра Цезаря ключом является величина сдвига букв шифртекста относительно букв открытого текста.
- Зачем же нужен ключ? Из предыдущего изложения понятно, что придумывание хорошего шифра – дело трудоемкое. Поэтому желательно увеличить «время жизни» хорошего шифра и использовать его для шифрования как можно большего количества сообщений.

Атака на шифр. Стойкость шифра

Атака на шифр. Стойкость шифра
Под атакой на шифр понимают попытку
вскрытия этого шифра.

Под атакой на шифр понимают попытку
под стойкостью шифра понимают
вскрытия этого шифра
способность шифра противостоять

Под стойкостью шифра понимают
всевозможным атакам на него.
способность шифра противостоять
всевозможным атакам на него.



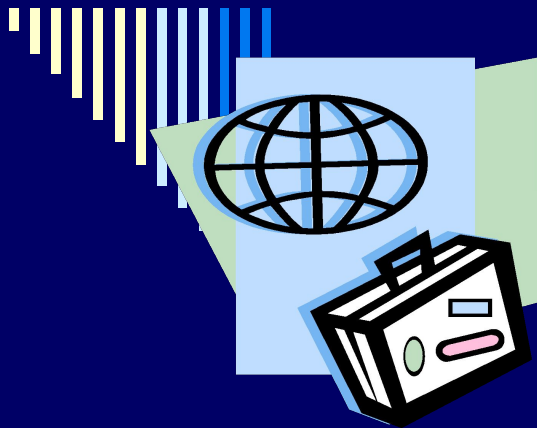


- **Криптология** – наука, состоящая из двух ветвей: криптография и криптоанализа.
- **Криптография** – наука о способах преобразования информации с целью ее защиты от незаконных пользователей.
- **Криптоанализ** – наука о методах и способах вскрытия шифра.



Случайность и закономерность в двоичных последовательностях

- Понятие последовательности известно еще со школьных лет. Однако последовательности, которые изучаются в школе, являются *детерминированными* – они однозначно восстанавливаются по их нескольким этапам. Так, арифметическая и геометрическая прогрессии восстанавливаются по любым двум своим подряд идущим членам.
- Но существуют и другие последовательности, так называемые *случайные*. Для них, в отличие от детерминированных, вообще говоря, нельзя определить очередной член последовательности, зная предыдущие.



Заключение

- Если вам захотелось подробнее узнать историю криптографии, события и легенды, связанные с ней, то рекомендуется попытаться найти и прочесть книги, упомянутые в списке литературы.
- Школьникам, которые решили избрать информатику своей профессией, рекомендуется выбрать один из трех вузов:
 - -институт криптографии, связи и информатики Академии безопасности ФСБ Российской Федерации;
 - - механико – математический факультет Московского государственного университета им. В. М. Ломоносова (МГУ).
 - - факультет защиты информации Российского государственного гуманитарного университета (РГГУ).



Список литературы

- Соболева Т. А. Тайнопись в истории России.
 - Шеннон К. Работы по теории информации и кибернетики. – М.: ИЛ, 1963.
 - Диффи У., Хеллман М.Э. Защищенность и имитостойкость. Введение в криптографию. – ТИИЭР.
 - Фролов Г. Тайны тайнописи. – М.:1922.
 - Гарднер М. От мозаик Пенроуза к надежным шифрам. – М.: Мир, 1993.
 - Введение в криптографию/ Под ред. В. В. Яценко. СПб.: Питер, 2001
-