МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ДГТУ)
Колледж экономики, управления и права

Реферат

на тему: Шифрование с использованием

Дисциплина: Информатика
Автор: Каплин С.Е
Учебная группа: СИС-11
Специальность 09.02.04 Информационные системы (по отраслям)
Руководитель: Пегливанова А.С

Ростов–на-Дону
2017

Цели и задачи

Цель реферата – рассмотреть различные методы шифрования.

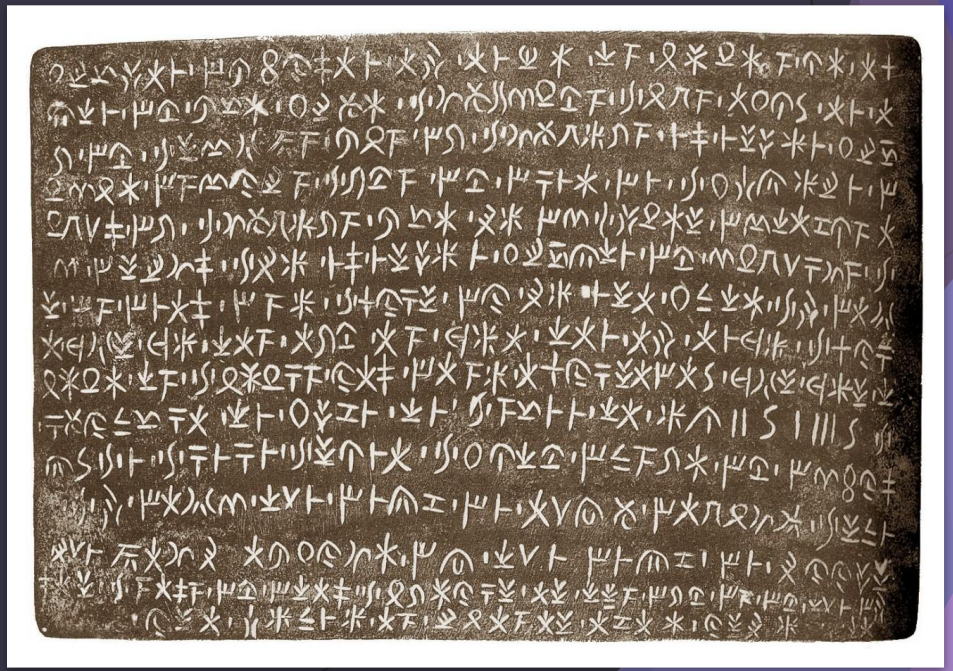
Данная цель обуславливает решение следующих задач:

- - история возникновения криптографии
- - эволюция криптографии;
- - проанализировать виды шифрования.

1 ИСТОРИЯ КРИПТОГРАФИИ

- Шифрование возникло именно как практический предмет, изучающий и разрабатывающий методы шифрования информации, то есть при трансфере сообщений - не скрывающий сам факт передачи, а делающий текст сообщения недоступным для прочтения непосвященными людьми

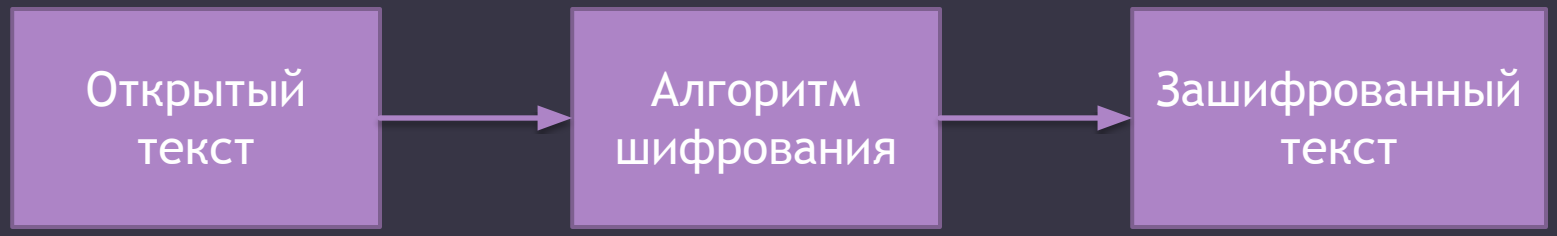
- Археологами был найден ряд глиняных клинописных табличек, в которых первая запись часто замазывалась толстым слоем глины, на котором и производилась вторая запись. Появление подобных странных табличек вполне могло быть обосновано и тайнописью, и утилизацией.



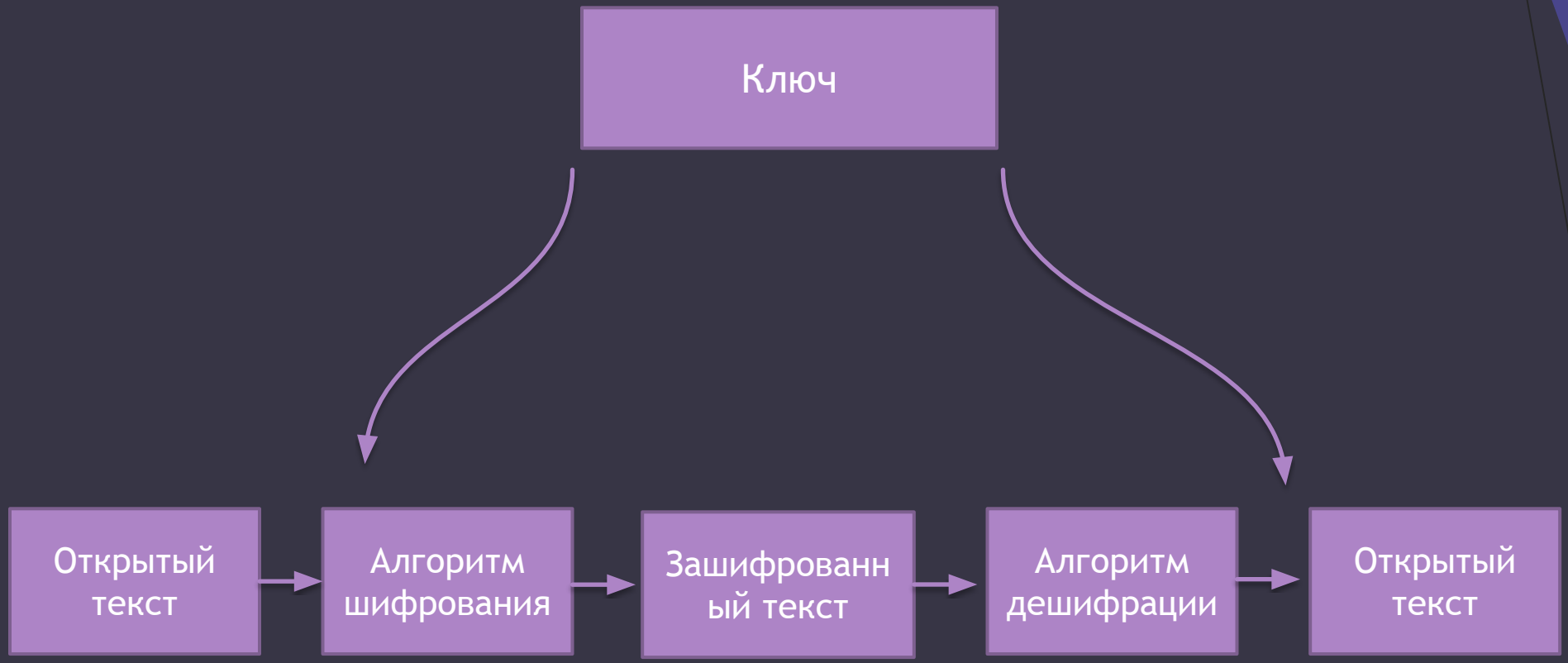
2 КРИПТОАНАЛИЗ

- Эни́гма - переносная шифровальная машина, использовавшаяся для шифрования и расшифрования секретных сообщений.
Более точно, «Энигма» — целое семейство электромеханических роторных машин, применявшихся с 20-х годов XX века.

3 ОСНОВЫ ШИФРОВАНИЯ



На рисунке процесс шифрования представлен в виде простой блок-схемы. Открытый текст загружается в механизм шифрования, который может быть даже механическим устройством наподобие машины Энигма, применявшейся во время второй мировой войны.

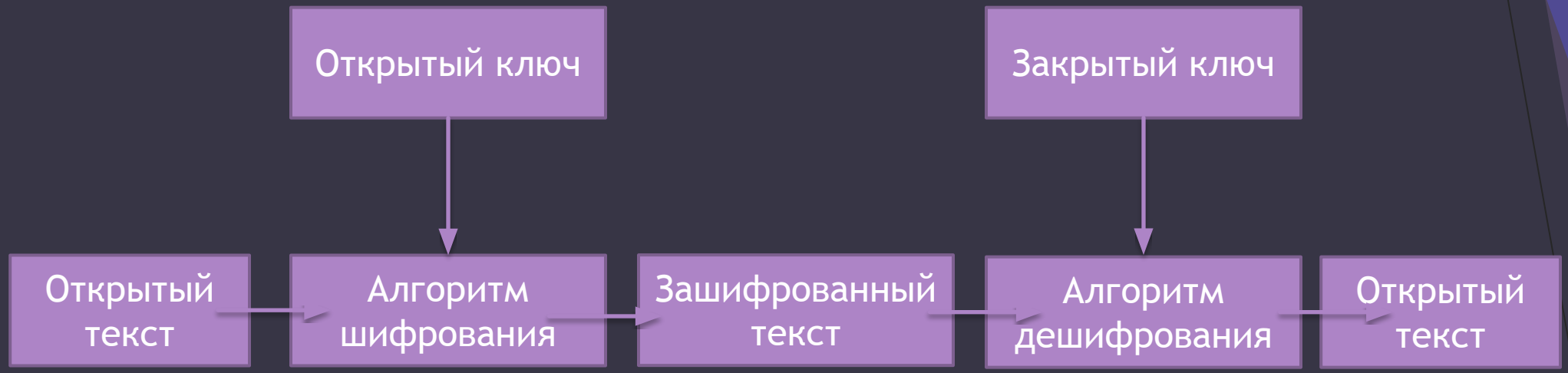


На рисунке ниже показан двунаправленный процесс шифрования.

4 ШИФРОВАНИЕ С ЗАКРТЫМ КЛЮЧОМ

Шифрование с закрытым ключом основано на том, что доступ к ключу имеет только авторизованный персонал. Этот ключ должен держаться в секрете.

5 ШИФРОВАНИЕ С ОТКРЫТЫМ КЛЮЧОМ



Шифрование с открытым ключом базируется на двух различных ключах — открытом и закрытом. Как показано на рисунке, открытый ключ используется для шифрования сообщений, а закрытый — для их дешифрации.

6 СИММЕТРИЧНОЕ ШИФРОВАНИЕ

- Симметричные криптосистемы (также симметричное шифрование, симметричные шифры) - способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ.

Заключение

- Итак, в этой работе был сделан обзор наиболее распространенных в настоящее время методов криптографической защиты информации и способов ее реализации.
- Выбор для конкретных систем должен быть основан на глубоком анализе слабых и сильных сторон тех или иных методов защиты. Обоснованный выбор той или иной системы защиты в общем-то должен опираться на какие-то критерии эффективности.