Криптографические методы защиты информации

Студент:

- Фролов Евгений ИУ7-55Б

Руководитель:

- Рудаков И. В.

Москва 2021

Цель работы - провести анализ наиболее распространенных методов защиты информации. Определить достоинства и недостатки каждого и их применимость в различных областях.

Рассматриваемые способы шифрования.

- Алгоритмы подстановки
- Алгоритмы гаммирования
- Комбинированные методы
- Асимметричные методы шифрования
- Симметричные методы шифрования

Криптографические методы в настоящее время являются базовыми для обеспечения надежной аутентификации сторон информационного обмена, защиты информации в транспортной подсистеме АС, подтверждения целостности объектов.

Криптографические алгоритмы преобразования информации реализуются с целью:

Защиты информации при ее обработке, хранении и передачи;

обеспечение достоверности и целостности информации;

выработки информации, используемой для идентификации и аутентификации субъектов АС.

Системы подстановок

- Шифр Цезаря - моноалфавитная подстановка, преобразующая n-грамму исходного текста (x0, x1, .., xn−1) в n-грамму шифрованного текста (y0, y1, ..., yn−1)

А →г	Й →м	Т →х	Ы →ю
Б →д	К →н	У →ц	Ь →я
В →е	Л →о	Ф →ч	Э →_
Г →ж	М →п	Х →ш	Ю →а
Д →з	Н →р	Ц →щ	Я →б
Е →и	О →с	Ч →ъ	_ →в
Ж →й	П →т	Ш →ы	
З →к	Р →у	Щ →ь	
И →л	С →ф	Ъ →э	

Асимметричное шифрование

Метод шифрования данных, предполагающий использование двух ключей — открытого и закрытого.

Криптосистемы на основе эллиптических уравнений

Проблемы ограничивающие использование метода:

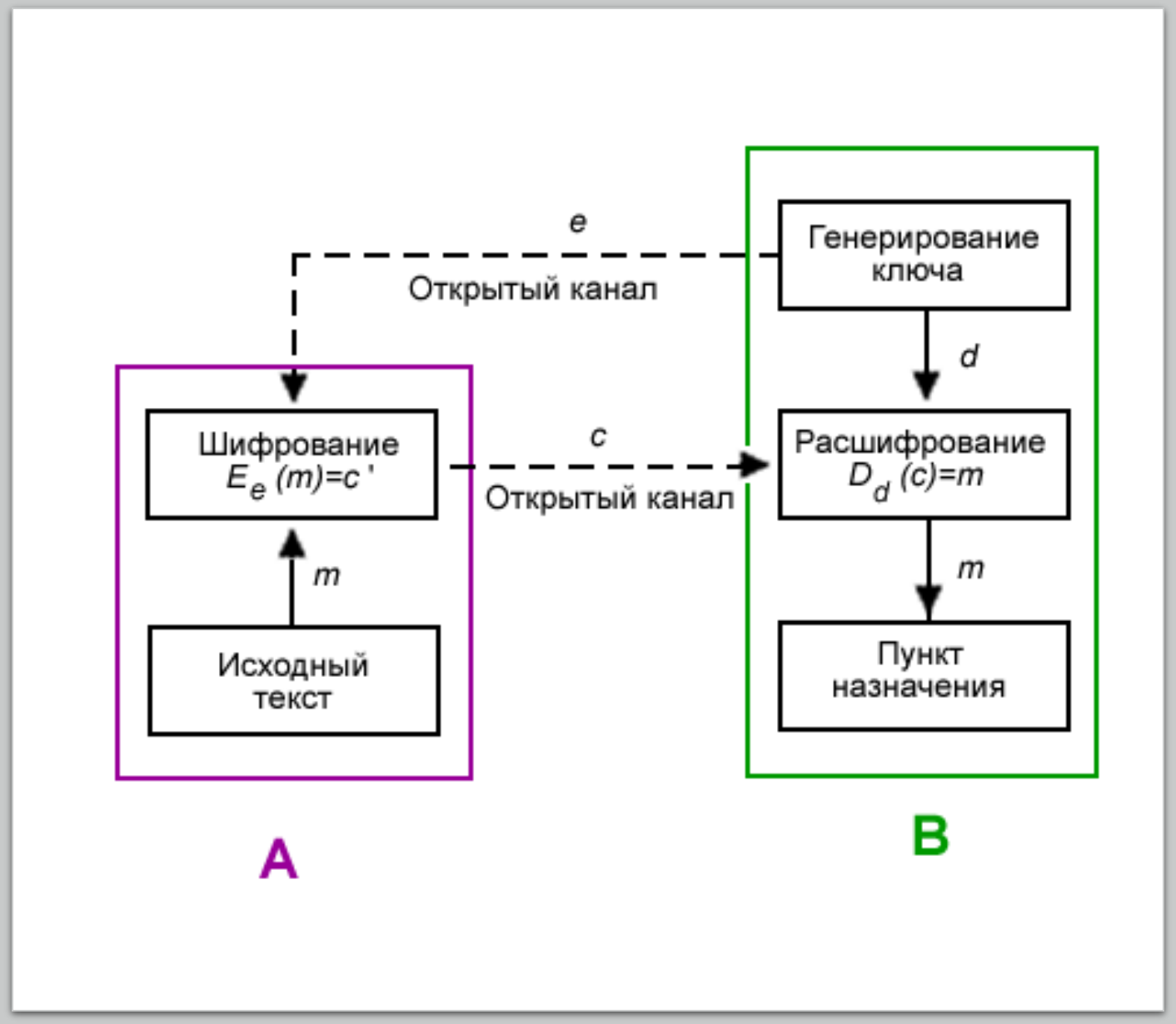
- Реальная безопасность таких систем все еще недостаточно осознана;
- трудность генерации подходящих кривых;
- несовместимость;
- лицензирование и патентование;
- относительно медленная проверка цифровой подписи

Области применения.

- m-commerce - мобильная торговля;
- смарт-карты;
- e-commerce - электронная торговля и банковские операции;
- интернет-приложения.

Криптосистемы с открытым ключом

- Система шифрования, при которой открытый ключ передаётся по открытому каналу и используется для проверки ЭП и для шифрования сообщения.



Алгоритмы гаммирования

- Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, которая называется гаммой.

По стойкости данные шифры относятся к классу совершенных.

НО

- если период гаммы превышает длину текста, то можно подобрать ключ;
- если известен фрагмент текста, то шифр раскрывается в два шага.

Комбинированный метод шифрования

- Сочетает преимущества секретности криптосистем с открытым ключом и высокой скорости работы криптосистемам с секретным ключом.

Шифрование - открытый ключ.

Передача и расшифровка - симметричная криптосистема.