

Тема: Основы криптографической защиты

Санкт-Петербургский
политехнический
университет Петра Великого

Шергин Илья Викторович 4731204/50001
Петров Алексей Геннадьевич 4731204/50001
Ху Тунцзэ 4731204/50001

Введение

В современном цифровом мире информация стала одним из самых ценных активов. Ее передача и хранение сопровождаются постоянными угрозами со стороны злоумышленников: перехватом, кражей, модификацией или уничтожением. В этих условиях обеспечение конфиденциальности, целостности и аутентичности данных является критически важной задачей. Ключевым инструментом для ее решения стала криптография — наука о методах обеспечения конфиденциальности и аутентичности информации.



Криптографическая защита информации



ПОЛИТЕХ

Криптографическая защита информации — это совокупность методов и средств, преобразующих данные (шифрующих их) для того, чтобы они стали недоступны для прочтения лицам, не обладающим специальным ключом

- Исходный текст (открытый текст)
- Шифрованный текст (криптограмма)
- Шифрование
- Дешифрование
- Ключ



Рис 2.
“Замок
И ключи”



Цели криптографии:

- **Конфиденциальность**
- **Целостность**
- **Аутентичность**
- **Неотрекаемость (Non-repudiation)**

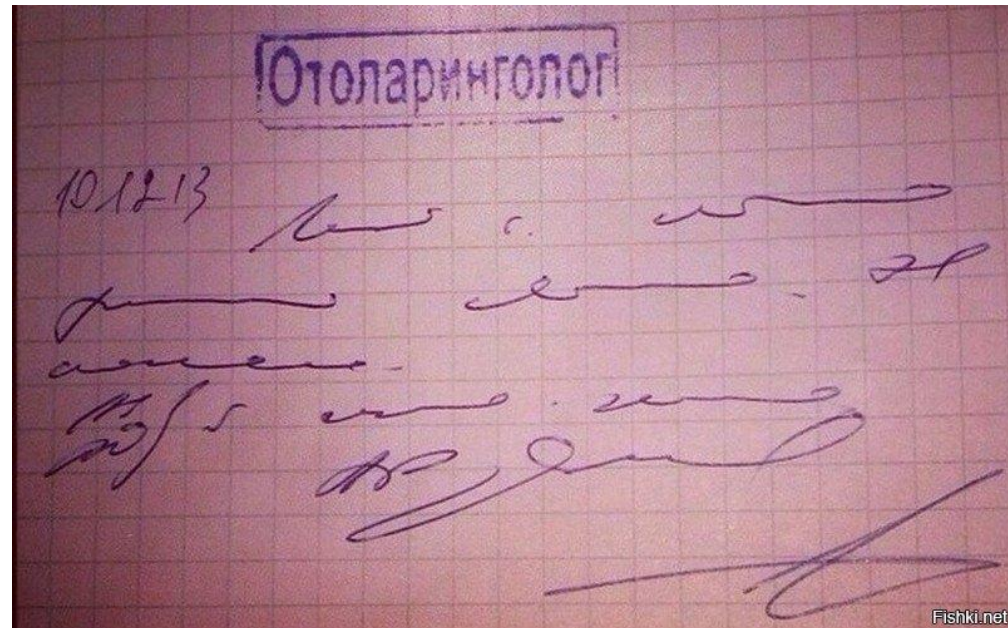


Рис 3. “Шифр
отоларинголога”

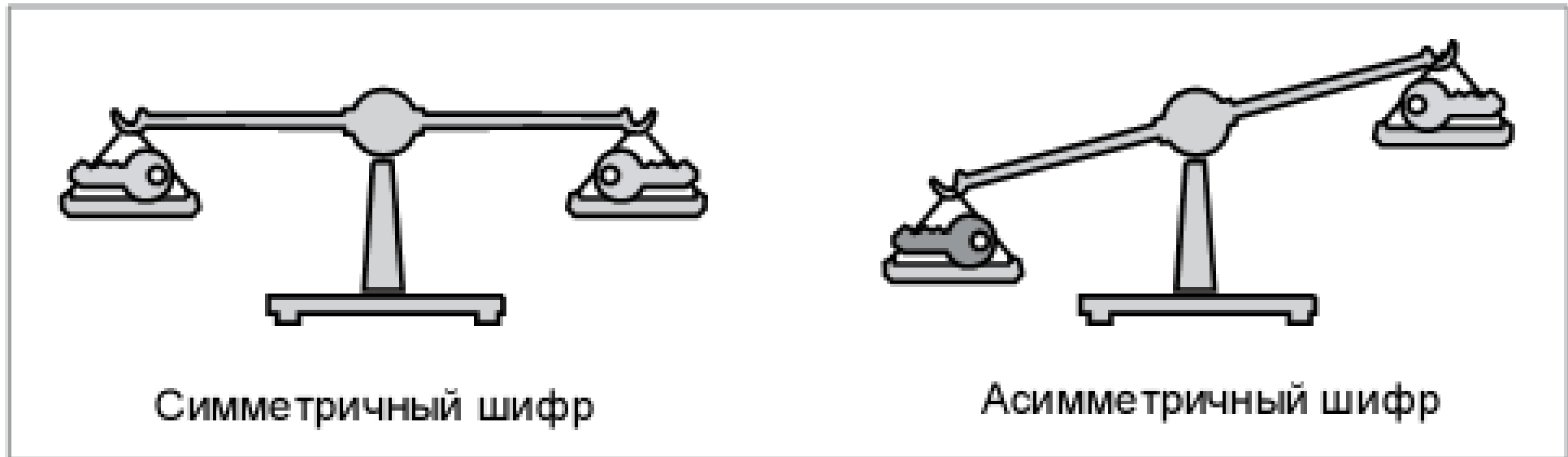
Типы криптографических алгоритмов

Симметричное шифрование

1 общий ключ

Асимметричное шифрование

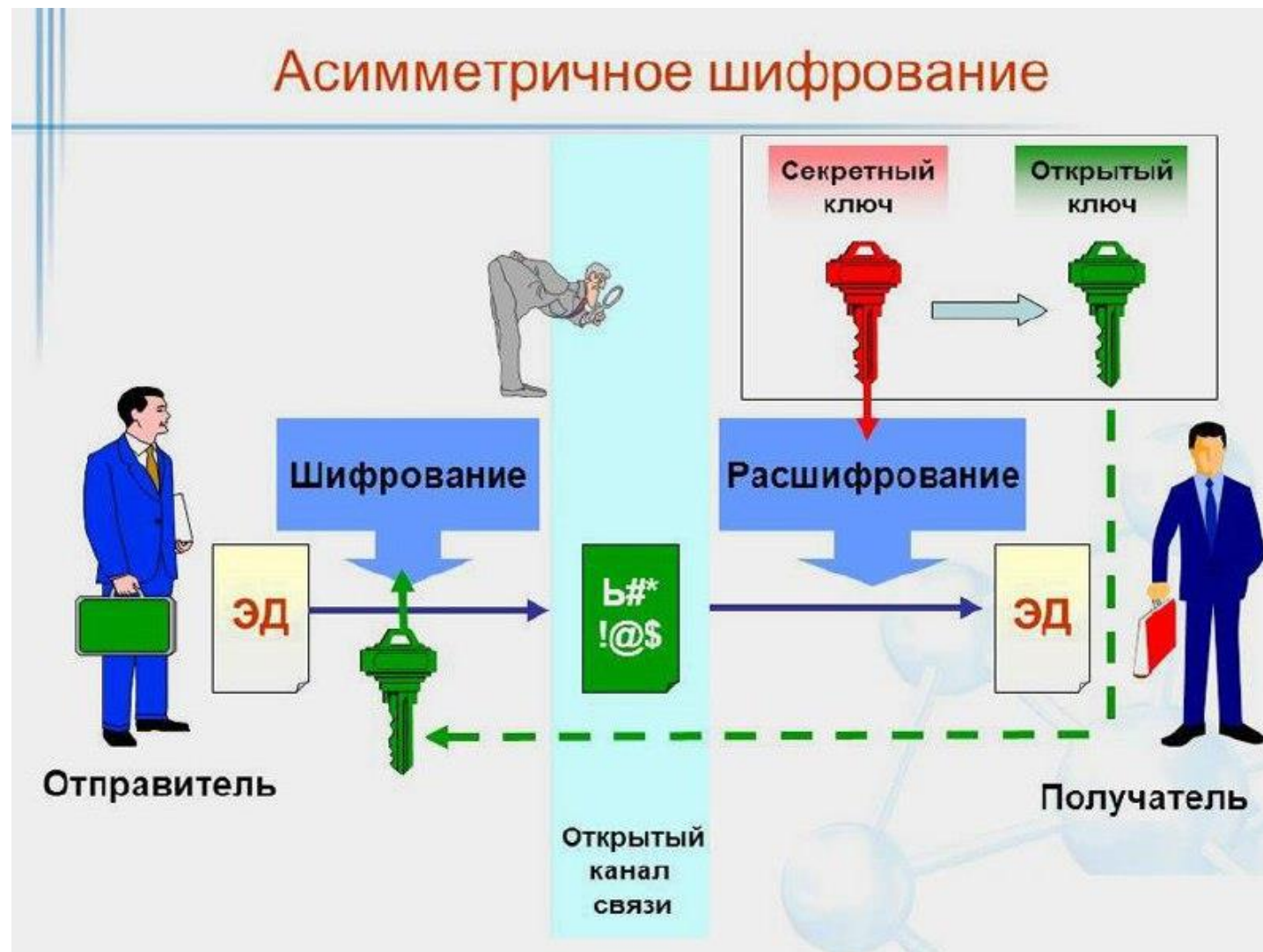
Закрытый и открытый ключ



Симметричное шифрование



Ассиметричное шифрование



Сравнение криптографических алгоритмов

Симметричное шифрование

- **Преимущества:**

- Высокая скорость работы.
- Относительная простота реализации.

- **Недостатки:**

- **Проблема распределения ключей:** Как безопасно передать ключ всем участникам обмена?
- **Масштабируемость:** Для общения N пользователей попарно требуется $N(N-1)/2$ уникальных ключей.

DES AES ChaCha20

Ассиметричное шифрование

- **Преимущества:**

- Решает проблему распределения ключей — нет необходимости заранее обмениваться секретом.
- Обеспечивает основу для создания электронных цифровых подписей.

- **Недостатки:**

- Значительно более медленное по сравнению с симметричным шифрованием.

RSA ECDSA

Дополнительные криптографические механизмы:

Хеширование

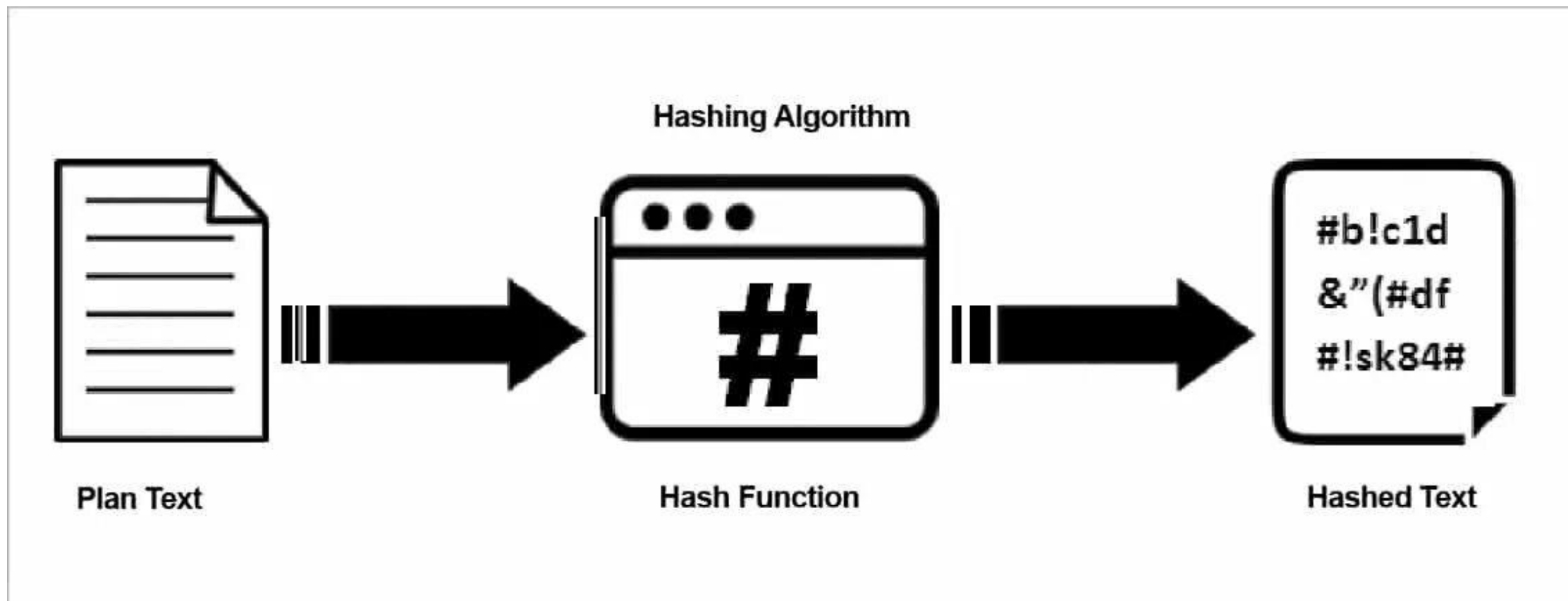


Рис 7. “Хеширование”

Дополнительные криптографические механизмы:

Электронная цифровая подпись ЭЦП



Рис 8. “Электронная цифровая подпись”

Применение криптографии на практике

- Защищенные интернет-соединения (HTTPS, TLS/SSL)
- Криптовалюты и блокчейн
- Защита данных на дисках (Full Disk Encryption)

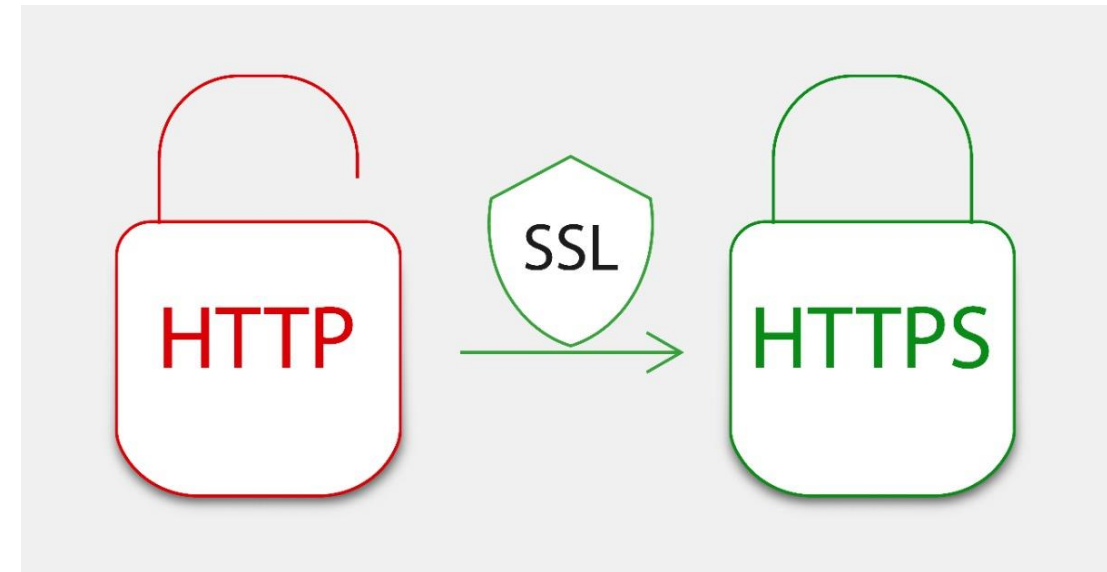


Рис 8. “Протокол http”

Рис 9. “Криптовалюта”

Заключение

Криптография является краеугольным камнем информационной безопасности в цифровую эпоху. Она предоставляет надежный математический фундамент для обеспечения конфиденциальности, целостности и аутентичности информации. Понимание основ симметричного и асимметричного шифрования, хеш-функций и электронной подписи необходимо не только специалистам по безопасности, но и всем, кто использует современные технологии. По мере роста вычислительных мощностей и появления новых угроз (например, квантовых компьютеров) криптография продолжает развиваться, создавая все более стойкие алгоритмы для защиты наших данных в будущем.