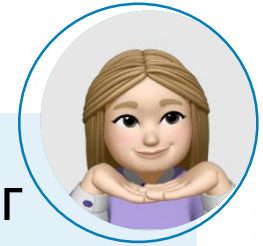
infotecs

Прикладная криптография. С чего начать и что учитывать.

Кто ты такая и зачем тебя слушать



Анкель Лихтенберг

Системный аналитик

АО «ИнфоТеКС», АНО НТЦ ЦК

Криптография и квантовые технологии

Шпаргалка по криптографии: что делать, если попал в проект с криптографами

Почему криптография нужна в разработке

Конфиденциальность

свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право

Целостность

термин, означающий, что данные не были изменены при выполнении какой-либо операции над ними, будь то передача, хранение или отображение

Аутентичность

подлинность, полнота и точность информации, означающая, что информация:
была создана законными участниками информационного процесса;
не подвергались случайным или преднамеренным искажениям

Неотказуемость

состояние информации, при котором субъект не может отказаться от того действия, которое имело место быть

Сценарии для разработки

- Защищённое хранение
  - как хранить данные
  - и почему только шифрования не достаточно
- Установление безопасного соединения
  - кому и почему можно доверять
  - что и как защищаем
- Подпись электронных документов
  - как и чем подписать, чтобы все поверили

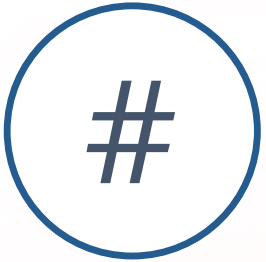
Я понял, что мне не сбежать

Какая бывает криптография

01. Симметричная

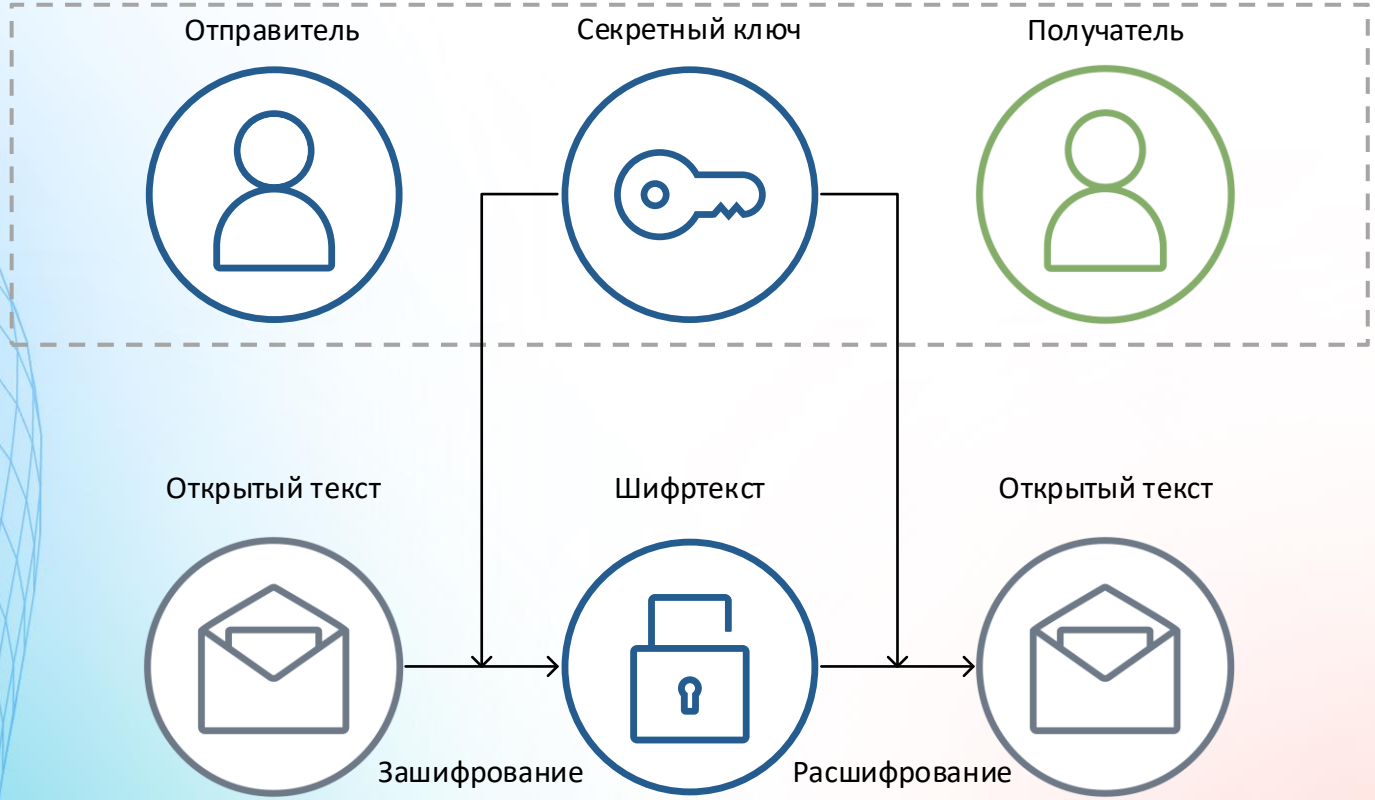
02. Асимметричная

03. Бесключевая - хэши



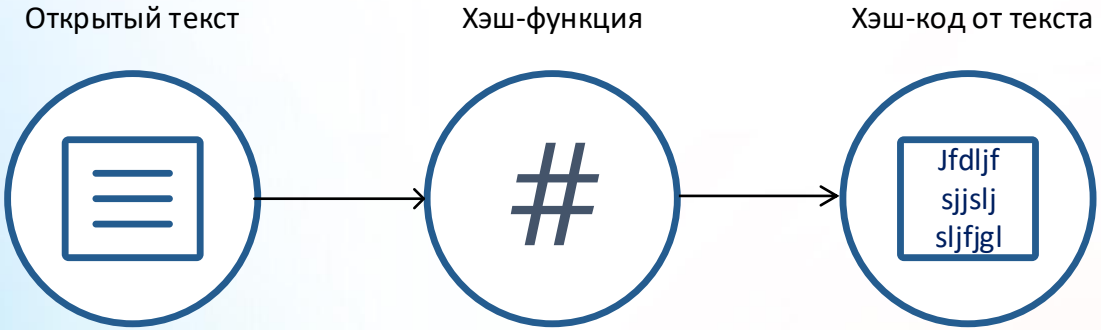
04. Выработка общего секрета

Симметричная криптография

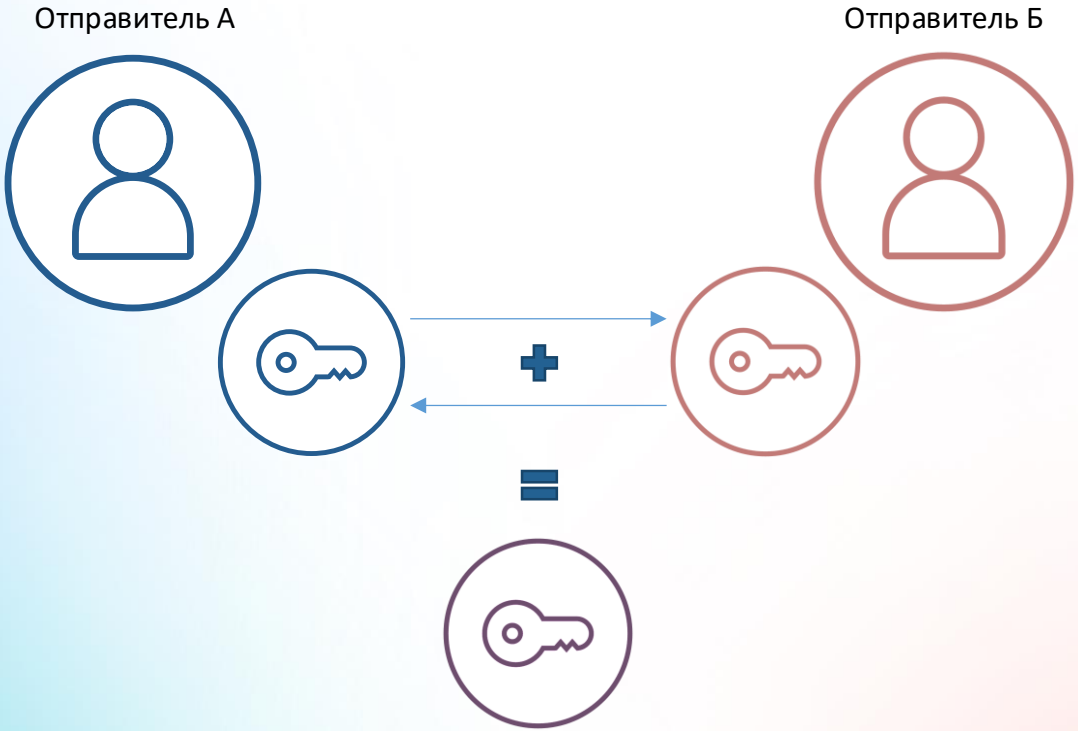


Асимметричная криптография

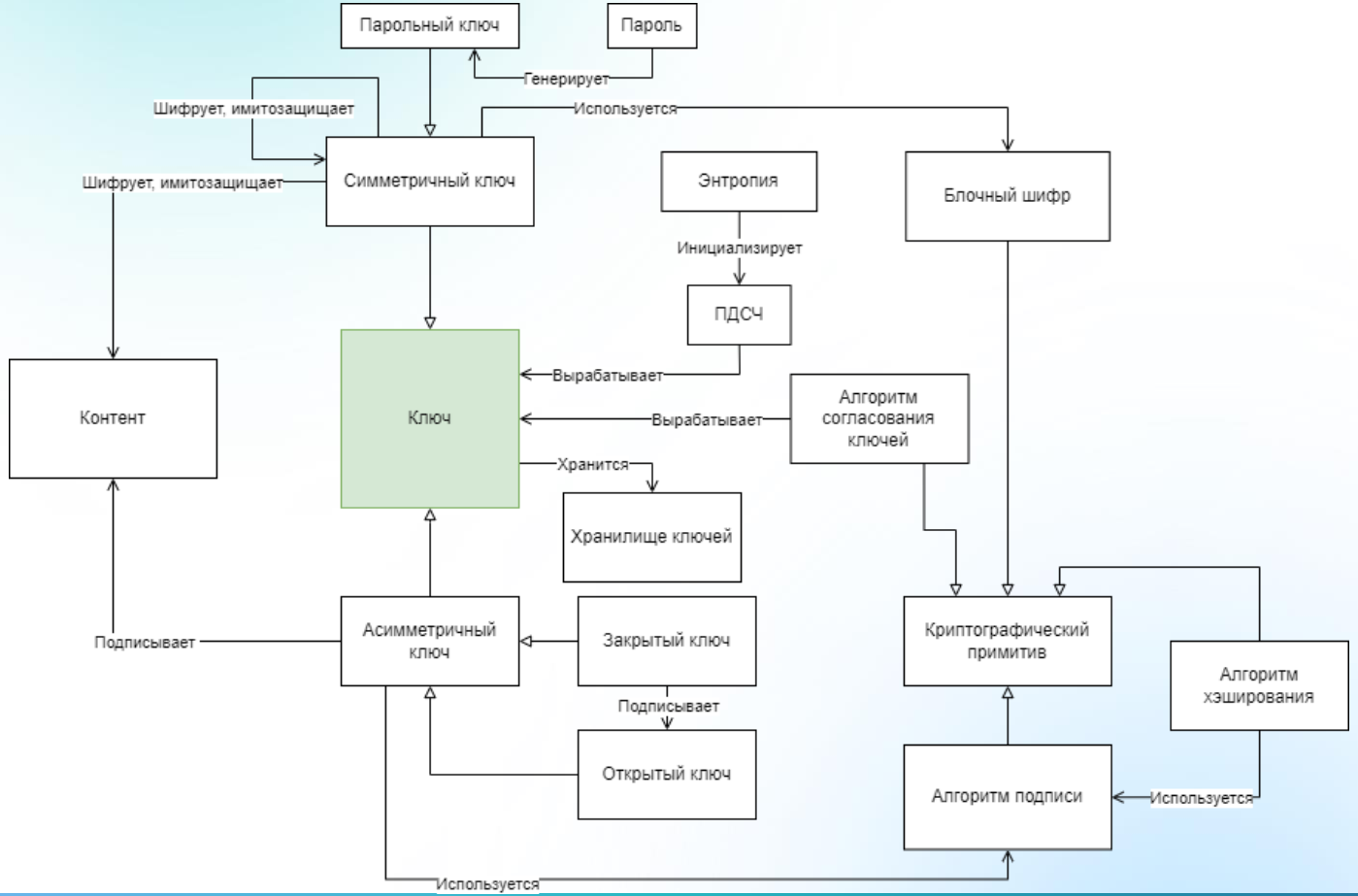
Бесключевая криптография



Выработка общего секрета



Как всё взаимосвязано



Случайность в криптографии

нужна, например, для генерации ключей

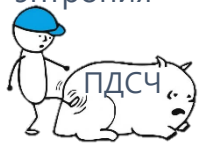
Физические датчики случайных чисел

Датчики случайных чисел

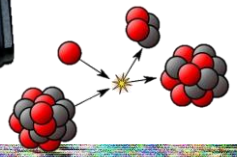
Биологические датчики случайных чисел

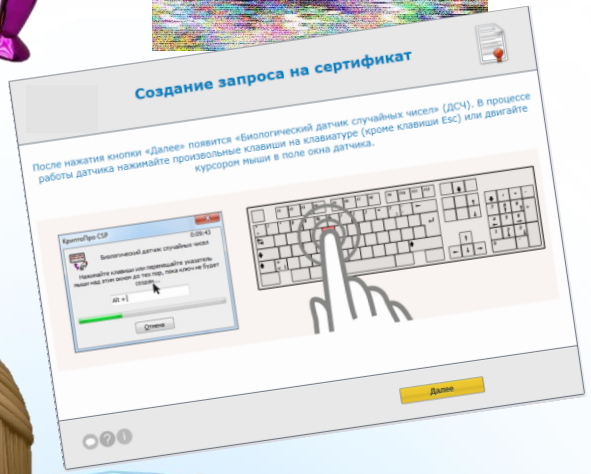
Программные датчики случайных чисел

энтропия

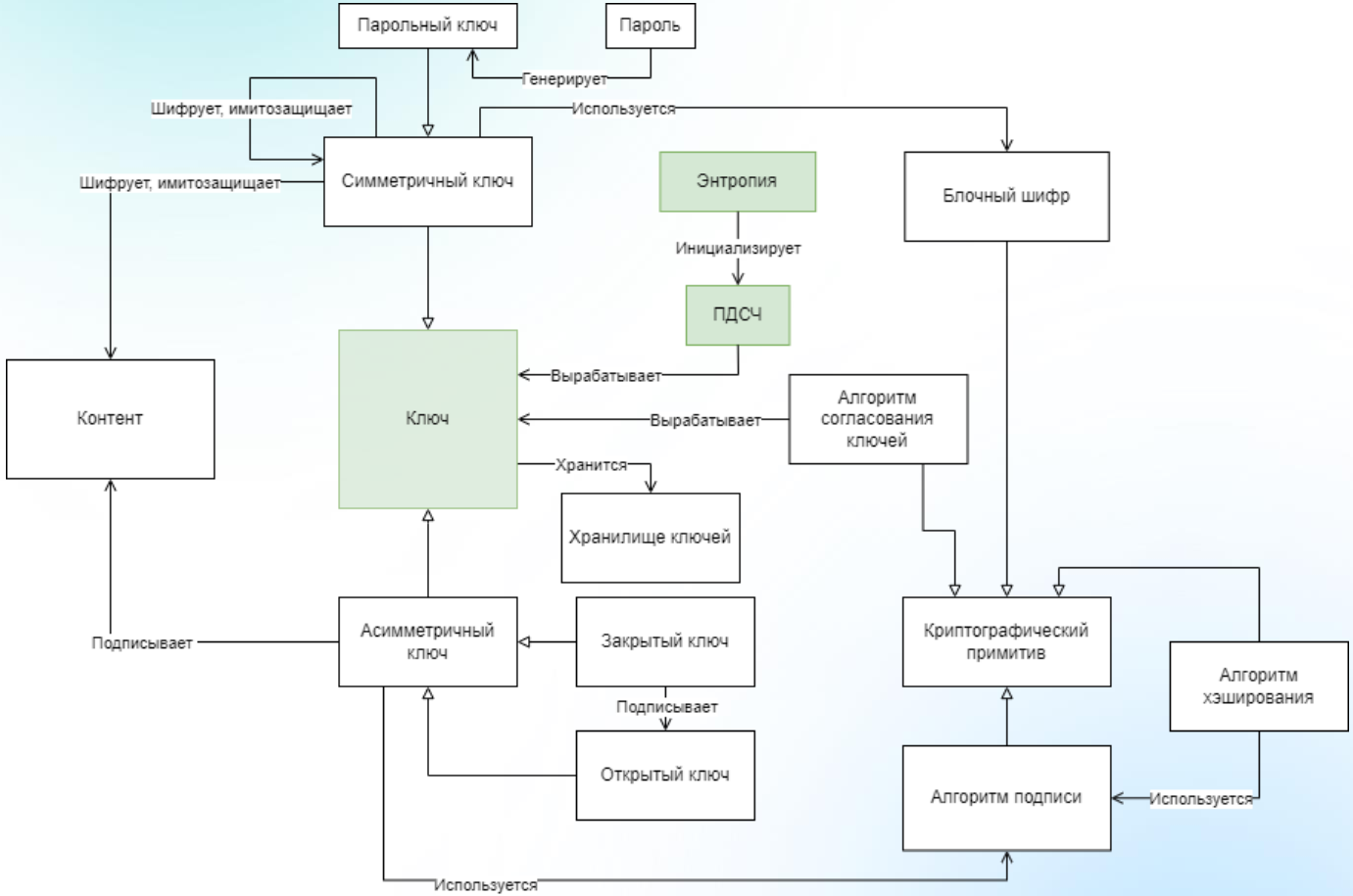


требуют для начала работы инициализирующую последовательность (энтропию)





Как всё взаимосвязано



Ключи и их перемещения

продвинутые технологий

infotecs

Хранилища сертификатов в ОС и браузерах

+ автоматический поиск ключей приложениями
+ легко настроить

- специфичны для каждой ОС или браузера

транспорт

Файлы .pfx, .p12

+ универсальны
+ всегда защищены паролем

± легко распространить

- слабая защита, которая зависит от человека

Токены и смарт-карты

+ повышенная безопасность
+ закрытый ключ не экспортируется

- привязка к вендору
- ограниченная производительность
- требуют СКЗИ каждому сотруднику

HSM

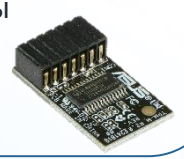
+ не нужны отдельные токены
+ поддержка легче, чем у токенов
+ использование ЭП во внутренних сценариях

- сложны в обслуживании

TPM и PUF

+ аппаратная защита ключей с помощью физических свойств

- реализация возможна только на устройствах, где есть необходимые компоненты



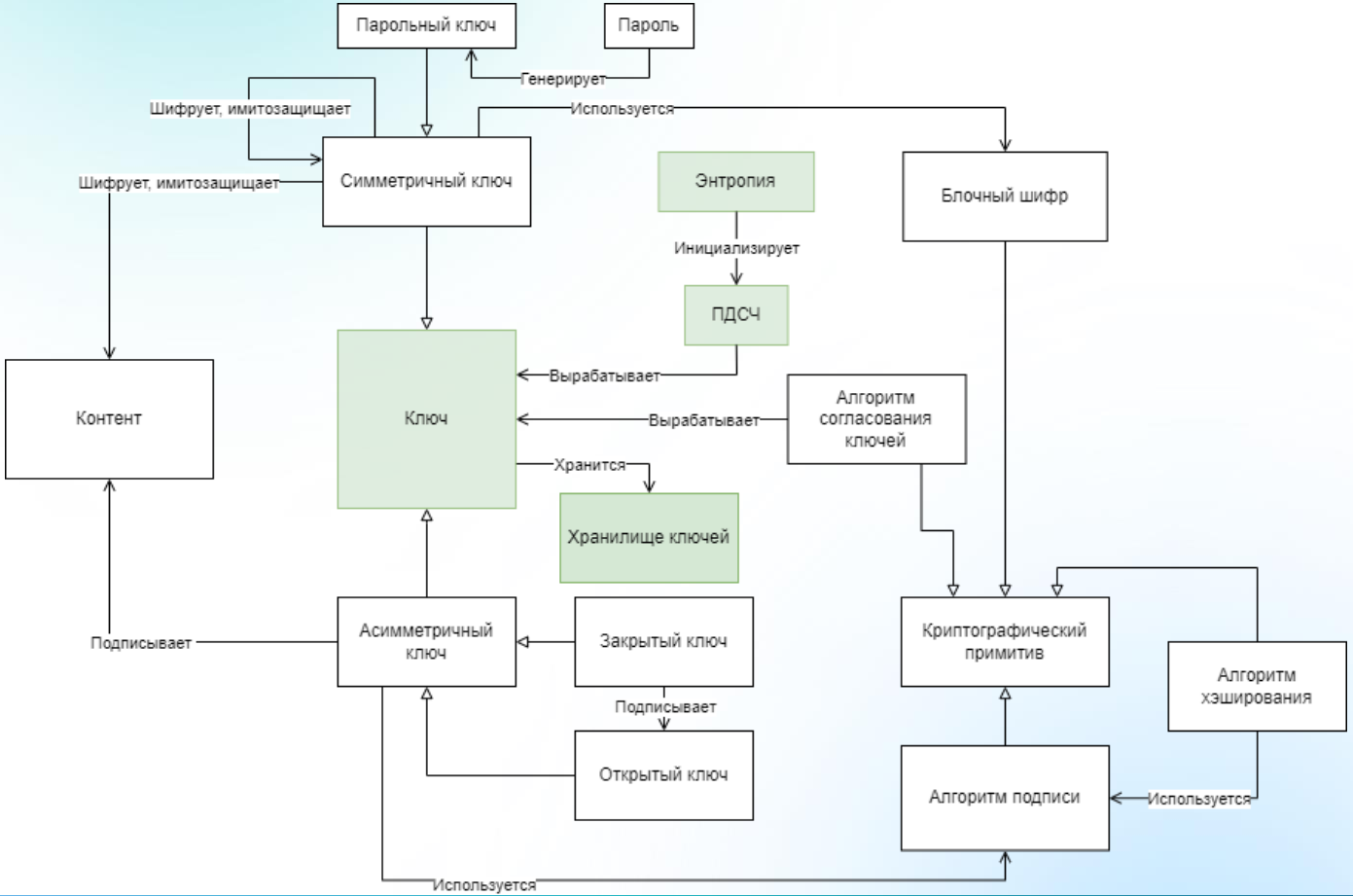
Физически неклонируемая функция — это **функция**, воплощённая в **физической** структуре, которую просто оценить, но трудно охарактеризовать, смоделировать или воспроизвести.

Хранение ключей в долговременной памяти

+ удобно пользователю
+ удобно в разработке
+ связь с хранилищем сертификатов

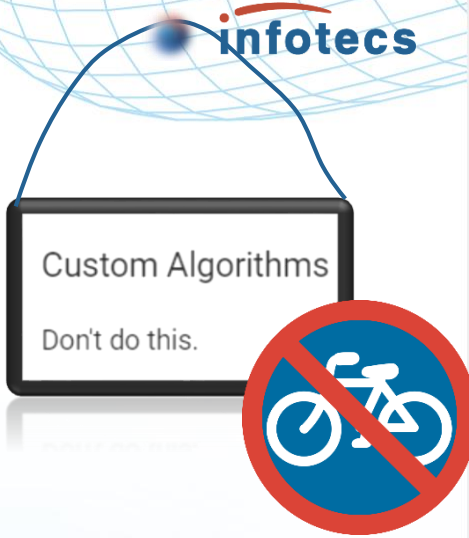
- ключ может появиться в оперативной памяти

Как всё взаимосвязано



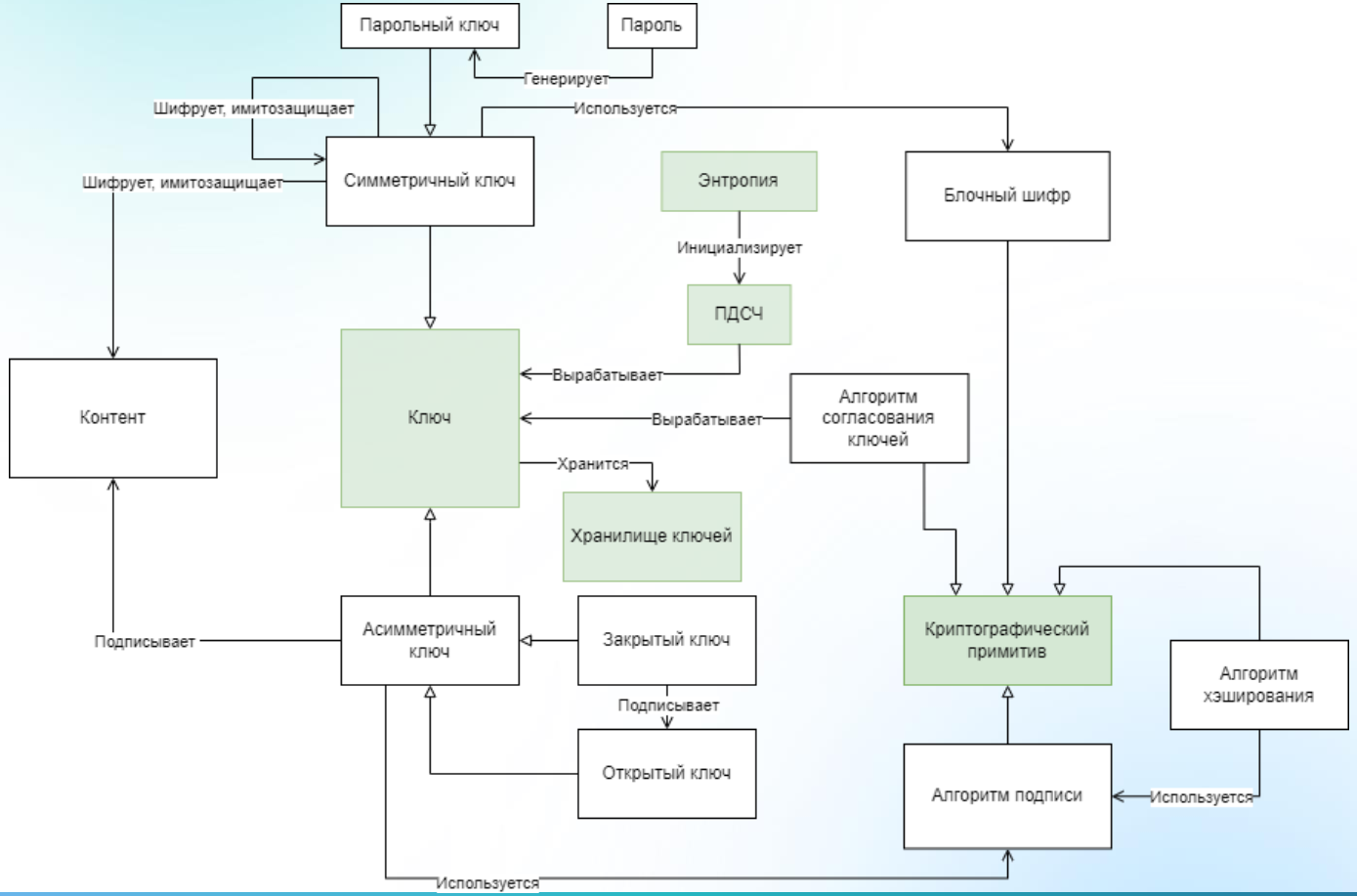
Реализация криптографии

Уровень абстракции	Язык/ Технология	Платформа	Решение
Функции низкого уровня: генерация ключей, шифрование, подпись	C++	Linux, Windows, macOS, Android, iOS	Botan
	Java, C#	JVM	Bouncy Castle
	C	Linux, Windows, macOS, Android, iOS	PKCS#11 решение вендора, OpenSSL
Прикладные функции: формирование запросов и сертификатов, создание ЭП	PKCS#11 API, OpenSSL API		PKCS#11 решение вендора, OpenSSL
	Microsoft Crypto API	Семейство Windows. Есть порт на GNU\Linux, OS X, iOS, Android	Криптопровайдеры под Windows: КриптоПро CSP, ViPNet CSP

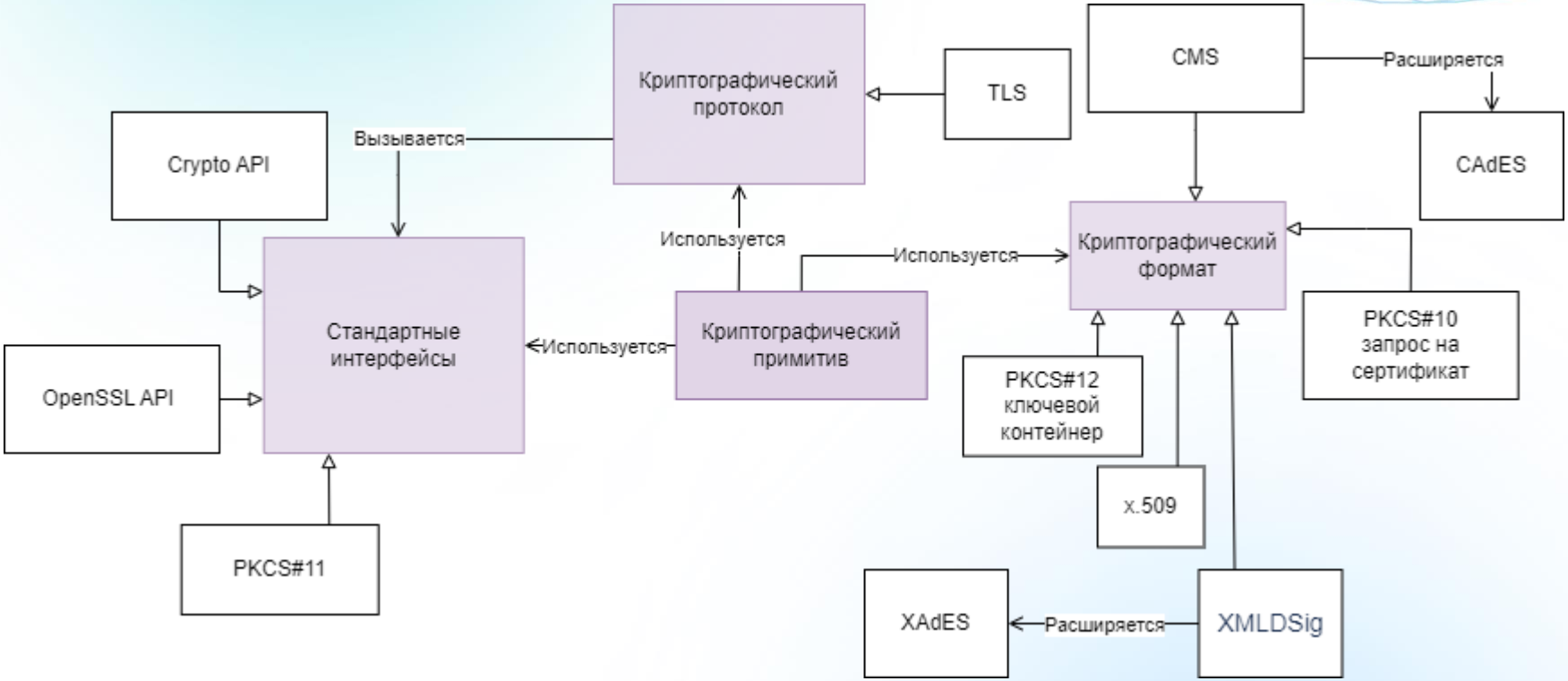


Comparison of cryptography libraries

Как всё взаимосвязано



Где это всё используется



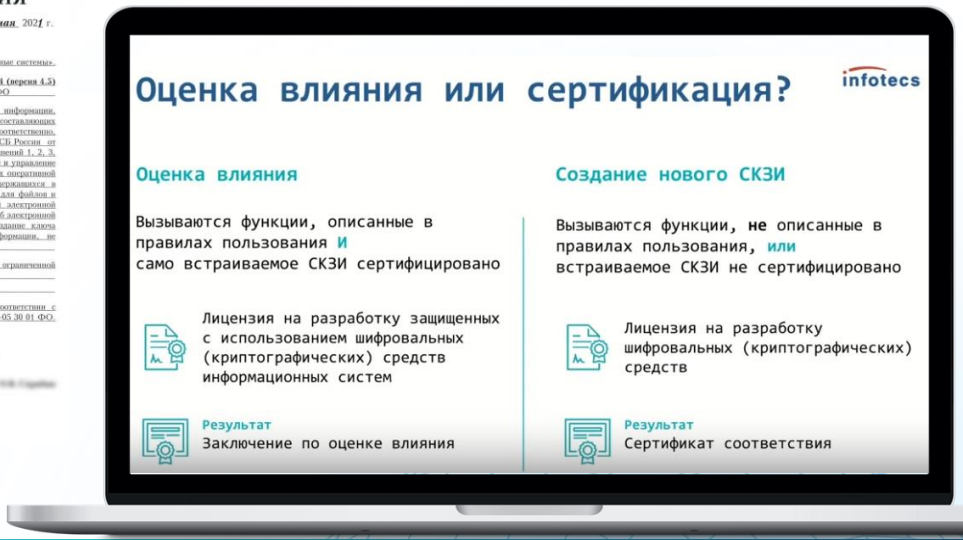
Резюме – контрольная точка

Криптографические методы защиты информации		Базовые криптографические алгоритмы	Виды ключей	Ц	К	А	Н
Шифрование	Симметричное шифрование	•“Кузнечик” и “Магма” (ГОСТ Р 34.12--2015) •AES	Секретный ключ.		+		
	Асимметричное шифрование	•RSA	Закрытый ключ (ключ расшифрования), открытый ключ (ключ зашифрования).				
Электронная подпись (асимметричные схемы)		•ГОСТ Р 34.10--2012 •RSA •ECDSA •EdDSA	Закрытый ключ (ключ ЭП), открытый ключ (ключ проверки ЭП).	+		+	+
Хэширование		•“Стрибог” (ГОСТ Р 34.11--2012) •SHA-2 •SHA-3	Бесключевой криптографический механизм.	+			
Имитовставка		Те же, что и для симметричного шифрования и хэширования.	Ключ аутентичности.	+		+	

А если ещё и сертифицировать надо..?

Сертификация криптографии в РФ

Как разрабатывать ПО с криптографией внутри



Криптография в мире

NIST Special Publication 800-108

Recommendation for Key Derivation Using Pseudorandom Functions

(Revised)

Lily Chen

Computer Security Division
Information Technology Laboratory

COMPUTER SECURITY

October 2009

U.S. Department of Commerce
Gary Locke, Secretary
National Institute of Standards and Technology
Patrick Gallagher, Deputy Director

Номер RFC	Тема
RFC 768 (англ.) RFC 768 (рус.)	UDP
RFC 791 (англ.) RFC 791 (рус.)	IP
RFC 792 (англ.) RFC 792 Архивная копия от 7 ноября 2011 на Wayback Machine (рус.)	ICMP
RFC 793 (англ.) RFC 793 (рус.)	TCP

Как проверить себя?

01. Используемые алгоритмы

02. Хранение секретов

03. Передача секретов

04. Случайные величины

[OWASP Developer Guide | Principles of Cryptography | OWASP Foundation]

Чеклист: используемые алгоритмы

- ❑ Не использую нестандартизированные механизмы
- ❑ Не использую устаревшие алгоритмы
- ❑ Проверил актуальность алгоритма и не нашёл лучше
- ❑ Проверил все требования заказчика
- ❑ Размер ключей и выхода хэш-функции соответствует рекомендациям
- ❑ Считаю имитовставку, потом зашифровываю

Encrypt-then-Sign или Sign-then-Encrypt, вот в чем вопрос

- ❑ Разрабатываемый продукт сохраняет необходимые (ожидаемые) функциональные характеристики при использовании криптографии

Чеклист: хранение секретов

Предусловие: выполнен чеклист 1

- ❑ Ключи **НЕ** хранятся в коде
- ❑ Ключи хранятся в защищённом виде:
  - ❑ На защищённом СКЗИ
  - ❑ На защищённом отчуждаемом ключевом носителе
  - ❑ В защищённом виде на диске
- ❑ У всех ключевых файлов R/O
- ❑ Изменения ключей регистрируются
- ❑ Хранилища ключей защищены с выполнением парольной политики

Чеклист: передача секретов

Предусловие: выполнены чеклисты 1 и 2

- ❑ Приватные ключи **НЕ** передаются в открытом виде
- ❑ Я обоснованно использую уровень модели OSI при использовании криптографии
- ❑ Защита реализована близко к данным
- ❑ Ключи удаляются вовремя
- ❑ Временные файлы безопасны

и

- приложение
- протокол
- сеть

или

- после использования
- после закрытия сессии
- после истечения срока действия

или

- не сохраняю ли я где-то открытый текст?
- не переношу ли я куда-то ключи в открытом виде?

Чеклист: случайные величины

Предусловие: отсутствует

- ❑ Пользуюсь рекомендованными функциями для генерации ключей

UUIDGEN
API UuidCreate()

- ❑ Использую UUID из специальных программ
- ❑ Генерирую новые UUID для каждой новой сущности

Language	Unsafe Functions	Cryptographically Secure Functions
C	`random()`, `rand()`	getrandom(2)
Java	`Math.random()`,,,, `StrictMath.random()` `java.util.Random` `java.util.SplittableRandom` `java.util.concurrent.ThreadLocalRandom`	java.security.SecureRandom, java.util.UUID.randomUUID()
PHP	`array_rand()`,,,, `lcg_value()` `mt_rand()` `rand()` `uniqid()`	random_bytes(), Random\Engine\Secure in PHP 8, random_int() in PHP 7, openssl_random_pseudo_bytes() in PHP 5
.NET/C#	`Random()`	RandomNumberGenerator

Cryptographic Storage - OWASP Cheat Sheet Series

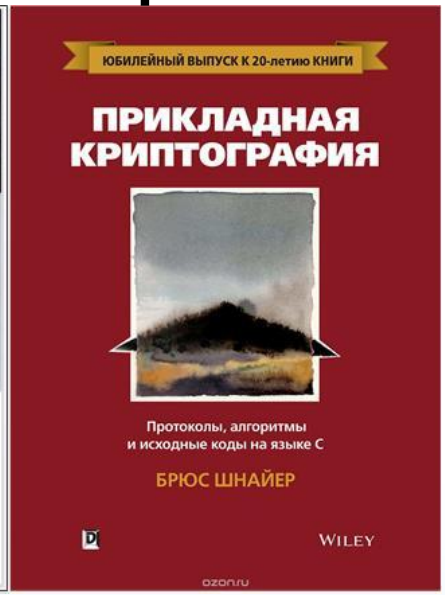
Выводы

не нужно её бояться!!

1. Криптография – это матрёшка
2. Отталкивайтесь от задач и уровня абстракции
3. Читайте и уточняйте тз!!
4. Проверяйте себя по пунктам чек-листа

нормально делай
нормально будет

Полезные материалы



Владимир Иванов «Криптография, шифрование»

Н. Смарт «Криптография»

Б. Шнайер «Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си»

Если хотите посмотреть на науку

[Квантовые технологии для защиты информации (quantum-crypto.ru)]

Квантовые технологии ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Справочная: квантовая криптография на пальцах

База знаний. Постквантовая криптография

Ответы на вопросы

infotecs

Спасибо за внимание!

infotecs.ru

Карьера

infotecs.team