КРИПТОГРАФИЯ

ВО ВСЕХ ЕЁ ПРОЯВЛЕНИЯХ

ЭЦП
VPN
ЭДО
TLS
...

ШИФР - ЭТО МЕТОД ПРЕОБРАЗОВАНИЯ ДАННЫХ ТАКИМ ОБРАЗОМ, ЧТОБЫ ОНИ БЫЛИ НЕЧИТАЕМЫМИ ДЛЯ ВСЕХ, КРОМЕ ТЕХ, КТО ИМЕЕТ КЛЮЧ ДЛЯ ИХ ДЕШИФРОВАНИЯ.

АЛГОРИТМ ШИФРОВАНИЯ - ЭТО МАТЕМАТИЧЕСКИЙ МЕТОД, КОТОРЫЙ ИСПОЛЬЗУЕТСЯ ДЛЯ РЕАЛИЗАЦИИ ШИФРА.

КЛЮЧ - ЭТО СЕКРЕТНАЯ ИНФОРМАЦИЯ, ИСПОЛЬЗУЕМАЯ ДЛЯ ШИФРОВАНИЯ И ДЕШИФРОВАНИЯ ДАННЫХ.

АЛФАВИТ - ЭТО НАБОР СИМВОЛОВ, ИСПОЛЬЗУЕМЫХ ДЛЯ ПРЕДСТАВЛЕНИЯ ДАННЫХ.

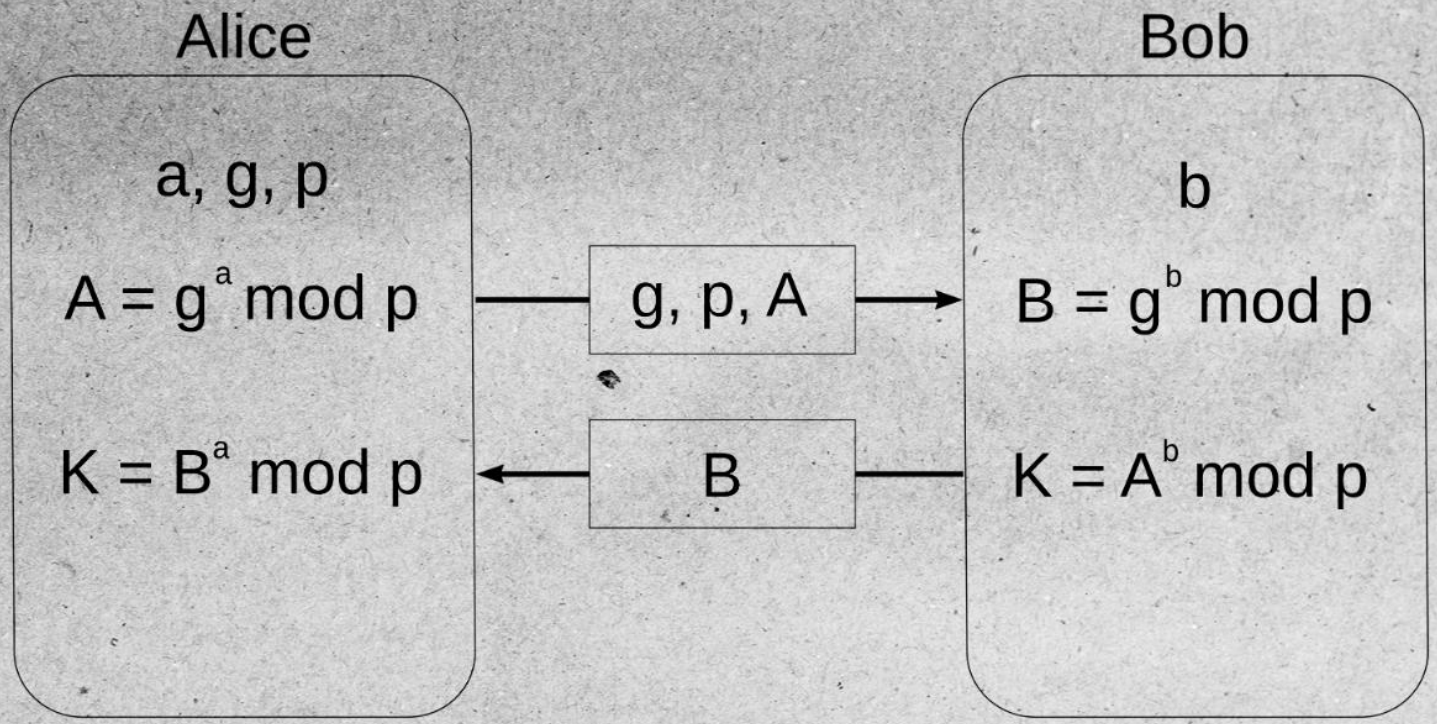
КРИПТОСТОЙКОСТЬ - ЭТО СПОСОБНОСТЬ ШИФРА ПРОТИВОСТОЯТЬ АТАКАМ, НАПРАВЛЕННЫМ НА ЕГО ВЗЛОМ.

АТБАШ

ШИФР ЦЕЗАРЯ

Подробное описание

ПРОТОКОЛ ДИФФИ – ХЕЛЛМАНА



$$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$$

Алгоритм Diffie-Hellman

DX

Alice

$y = \alpha^x \bmod p$ p - простое $p > 2^{1024}$

Bob

1. A,B выбирают числа p - простое, $\alpha < p$ - целое
2. A: $K_A < p$ - целое - private key Alice
3. A: $K_A^{\vee} = \alpha^{K_A} \bmod p$ - public key Alice
4. A $\rightarrow$ B $K_A^{\vee}, p, \alpha$
5. B: $K_B < p$ - целое число private key Bob
6. B: $K_B^{\vee} = \alpha^{K_B} \bmod p$ - public key Bob
7. B $\rightarrow$ A $K_B^{\vee}$
8. A: $K_{AB} = (K_B^{\vee})^{K_A} \bmod p$
9. B: $K_{BA} = (K_A^{\vee})^{K_B} \bmod p$

$K_{AB} = K_{BA} = K$ - общий секретный ключ

$K_{AB} = (\alpha^{K_B})^{K_A} \bmod p = \alpha^{K_B \cdot K_A} \bmod p$

$K_{BA} = (\alpha^{K_A})^{K_B} \bmod p =$

$= \alpha^{K_A \cdot K_B} \bmod p$

ЭВОЛЮЦИЯ ШИФРОВАНИЯ

* * * * *

ВНЕДРЕНИЕ ТЕХ.СРЕДСТВ

ПОЛИАЛФАВИТНЫЕ ШИФРЫ

РАЗВИТИЕ МАТЕМАТИЧЕСКИХ АЛГОРИТМОВ

НАЧАЛО ПЕРЕХОДА К МАТЕМАТИЧЕСКОЙ КРИПТОГРАФИИ


ШИФРЫ
СИММЕТРИЧНЫЕ
АССИМЕТРИЧНЫЕ
БЛОЧНЫЕ
ПОТОЧНЫЕ

Симметричное шифрование

ﻀ² ¼¼ﻄĞﻈ² Ş¾ﻄﻄ!ş ² ğ ﻄﻈÞﻄ¾ ﻄ!ﻈﻄýﻈĞﻄﻄĞĞﻄ³ ;

- ﻇĞċ!–ﻄ³¾¾Čﻄ!³ ﻈĞﻈﻈČﻄ!³⁄ﻋ× ¾ﻈ!¹ ﻄş ² ğ ﻄﻈÞﻄĞċ/!
- ﻇĞċ!³ ½¯ Ş!ş ² ğ ﻄﻈÞﻄ¾ · /!ﻀ!ﻄþﻈ!Fﻈ¼ﻈĆ č¯ !–ﻄ³¾¾Čﻄ!
  ş ² ğ ﻈﻋ¯ Ğﻈ· !Fﻈ!³ ﻄ³ ﻈ¼ﻋ. Ğﻈ!ﻄ½þﻈﻈ² Ğ¼ﻋ/
- ﻄﻈĞ!³ Ğﻈ!ﻈý½ﻄ–ﻄﻄĞ³ ½¯ Şﻈ¼!² !¹ ¾ﻄﻄĞﻄ½þﻈﻈ² Ğ¼!¼ﻈ× ﻄĞ
  ﻄﻈﻈş ² ğ ﻄﻈÞﻄĞċ!ﻈﻈﻈýĆ ﻄ¾ ﻄ
- ﻇ½ !¾ﻄ!¹ ¾ﻄĞċ!³ ½¯ Şﻄ!Ğﻈ!ﻈﻈﻈş ² ğ ﻄﻈÞﻄĞċ!–ﻄ³¾¾Čﻄ!FﻈŞĞ !
  ¾ﻄÞﻈ¹ ¼ﻈ× ¾ﻈ/

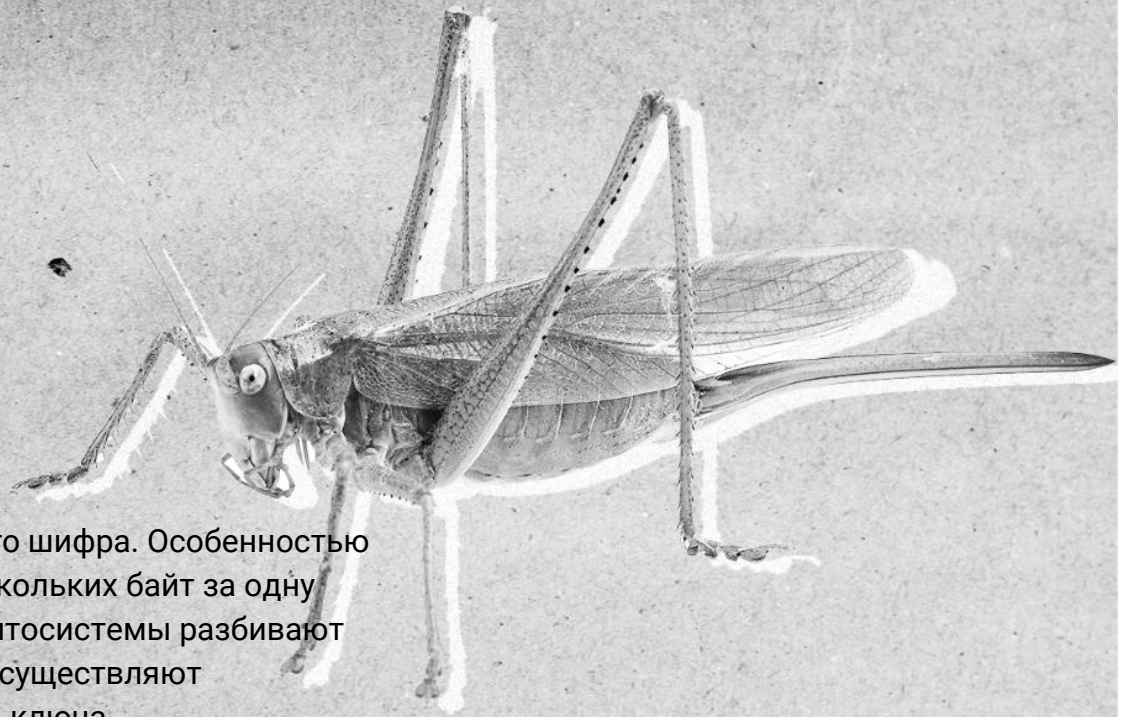
СИММЕТРИЧНЫЕ БЛОЧНЫЕ ШИФРЫ РФ И РБ

Боль и страдания по ГОСТу

Магма Описание

Кузнечик Описание

BelT Описание



Блочный шифр — разновидность симметричного шифра. Особенностью блочного шифра является обработка блока нескольких байт за одну итерацию (как правило 8 или 16). Блочные криптосистемы разбивают текст сообщения на отдельные блоки и затем осуществляют преобразование этих блоков с использованием ключа

СИММЕТРИЧНЫЕ ПОТОЧНЫЕ ШИФРЫ

Описание

RC4
RC5
ChaCha20
Salsa20
AES-CTR

Поточные шифры характерны тем, что шифруют информацию по одному биту за такт шифрования. Учитывая, что среди операций с битами существуют только две обратимые – сумма по модулю 2 и логическое отрицание, то выбор принципа шифрования очевиден – биты открытого текста должны складываться с битами ключевой последовательности с помощью операции

АССИМЕТРИЧНЫЕ ШИФРЫ

+ Высокая безопасность
+ Удобство использования

- Медленная скорость
- Большой размер ключей

Асимметричное шифрование

مثل² ¼¼ьĞь² Ş¾ьblş ² ğ ьььÞь¾ ьlььь¾ьÞь¾ь!¾ь!Fььььع!Ş² ььb½!ص¾ь!² ¹ !đĞ² ع!Ş² ььb¼♀!ьĞ³ ьČĞČь!³ ½¯ Ş!³ ьĞььČь!–ььbĞ₹Fь¾¼Þььb¼/!ص!Fь½ьĆč¯ !đĞьþь!Ş² ь½ь!³ Ğь!ɛþь–¾ь!¼ь× ьĞ¹ ьş ² ğ ьььÞьĞč!ьььbýĆь¾ ь/!صь! ьььbş ² ğ ьььÞьĞč!ьþь!ь!Fь½ьĆč¯ !đĞьþь!× ь!Ş² ь½ь!¾ь!Fь½₹Ş² Ğь· /

˘ ½ !ьььbş ² ğ ьььÞ³ ² !ýььɛĞÞĞbbbbь!Ş² ь½ь!♀!¹ ь³ ьČĞČь!³ ½¯ Ş/!ص¾–ь½× ь¾ýČĞč!ьь³ ььĞ¾Č¼/ ĐĞь!¾ь!¼ьþɛĞýČĞč!–Þь!ь½₹Şььb¾Čع!³ ½¯ Şь/!ص³ ьČĞČь!² !¹ ь³ ьČĞČь!³ ½¯ Ş!Þbbþ–ь!ьÞ· ¹ ь³Č!¼ь× –ع! ььbýььь!ь¼þььb² Ğ¼ь¼!³ ьĞььČь!² ع!ÞČ–ьɛĞ!صČь½Þ!Ğь¼!ŞĞь!Þ¾₹Ğь² !đĞьþь!ь½þььb² Ğ¼ь!ььbĞč!Ğььbč-! Ğь× ь!ььb³ ььĞ¾ьь!Ş² ь½ь-!³ ьĞbbbbь!ьÞ· ¹ ь¾ь!ь!ьýь² ¼² !³ ½¯ Şь¼² /

ضط¼Čь!FbbbbĞbb!ь₹bbbýع!ɛьĞь³¾ьÞ² Ğč!Ğь³ ع¯ !ьÞ· ¹ č!♀!Þ¹ · Ğč!–Þь!ýь½₹ş ² ع!FbbbbĞČع!Ş² ь½ь!² ! ₹ььbь¼¾ь× ² Ğč!² ع/!صČ!Fь½₹Ş² ¼!ьĆء!ýь½₹ş bbь!Ş² ь½ь-!³ ьĞbbbbь!² !ýع–ьĞ¼½ь× ьĞč!Þ!bb³¾Þь!¾ьş ьþь! ь¼þььb² Ğ¼ь/!ش!Þ¾₹Ğь² !đĞьþь!ь¼þььb² Ğ¼ь!ýع–ьĞĞь³ ь· !¼ьĞь¼ьĞ³ ³ ь-!³ ьĞbbbь· !¹ ьÞ² ь² ĞьĞbb¹ ½ь× ь¾ · ! Ş² bb½¾ь!¼¾ь× ² Ğь½ /!ظ½ !¼Č!¾ь!¹ ¾bb¼!¾ !ь–¾ь!² ¹ !Fbbьþь³ьŞь½₹¾Čع!FbbbbĞČع!Ş² bb½!Ğь!bb¹ ½ь× ² Ğč! ¾ь!¼¾ь× ² Ğь½ !Ğь³ bb!ьþbb¼¾ьb!Ş² ь½ь!ýع–ьĞьŞь¾₹č!ь½ь× ¾ьbb!¹ ь–ьŞbb/

Хеширование используется для создания уникального идентификатора для данных.
Шифрование используется для защиты данных от несанкционированного доступа.

Хеширование является необратимым процессом.
Шифрование является обратимым процессом.

Хеш-коды обычно имеют фиксированную длину, независимо от длины исходных данных.
Шифрованный текст может иметь любую длину, в зависимости от длины исходных данных и используемого алгоритма шифрования.

Хеширование обычно является быстрым процессом.
Шифрование может быть более медленным процессом, чем хеширование.

ГЛАВНЫЕ ХЕШ-ПРОТОКОЛЫ

MD5
SHA-1
SHA-256
SHA-512

Онлайн хеширование

Семейство SHA

SHA (Алгоритмы безопасного хеширования) – это семейство криптографических хеш-функций, способных принимать сообщения произвольной длины и вычислять уникальный хеш-код фиксированной длины. Хеш-код SHA может быть использован для проверки целостности сообщения, а также для генерации цифровой подписи сообщения.

подробное описание

DES

DES - Стандарт шифрования данных (DES) - это алгоритм блочного шифрования, который принимает простой текст блоками по 64 бита и преобразует их в зашифрованный текст с использованием ключей из 48 бит.

Это алгоритм с симметричным ключом, что означает, что для шифрования и дешифрования данных используется один и тот же ключ.

Алгоритм DES (стандарт шифрования данных) является наиболее широко используемым алгоритмом шифрования в мире.

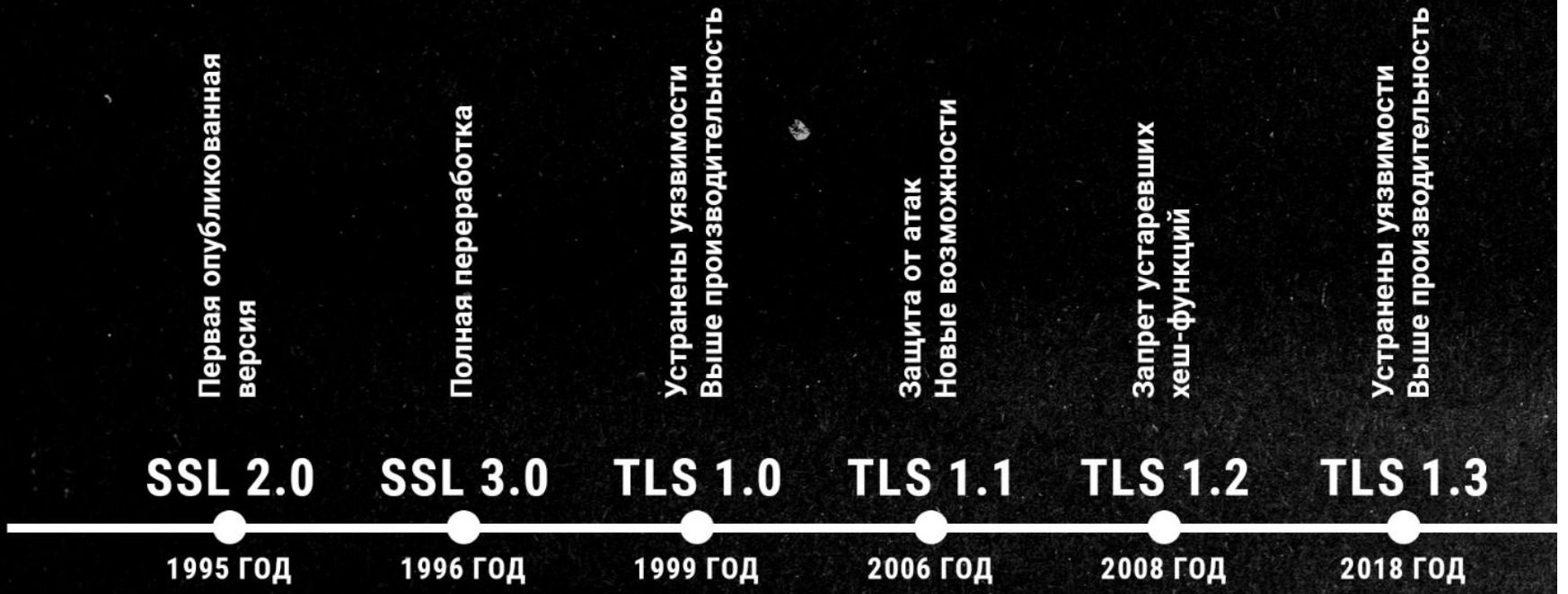
На протяжении многих лет и среди многих людей «создание секретного кода» и DES были синонимами.

Что такое сертификат SSL/TLS?

Сертификат SSL/TLS — это цифровой объект, который позволяет системам проверять личность и впоследствии устанавливать зашифрованное сетевое соединение с другой системой с использованием протокола Secure Sockets Layer/Transport Layer Security (SSL/TLS). Сертификаты используются в рамках криптографической системы, известной как инфраструктура открытого ключа (PKI). PKI дает одной стороне возможность устанавливать подлинность другой стороны с помощью сертификатов (при условии, что обе стороны доверяют третьей стороне, известной как центр сертификации). Таким образом, сертификаты SSL/TLS действуют как цифровые удостоверения личности для защиты сетевых подключений и установления подлинности веб-сайтов в Интернете, а также ресурсов в частных сетях.

подробное описание

ЭВОЛЮЦИЯ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ



ش!Şط¼!ظط¹ ¾ İ ط!Ғظظ Ğظ³ ظ½ظÞ!I UUQ!² !I UUQT

Визуально различие очевидно: оно в букве S, которая означает «Secure» — безопасность. Это небольшое, но ключевое отличие может сохранить компьютер от заражения вирусами, а бизнес — от потери денег и клиентов. Рассмотрим подробнее, что такое протоколы HTTP и HTTPS и как они отличаются друг от друга.

Подробное описание

Создание самоподписанного сертификата

ГЛАВНЫЕ VPN ПРОТОКОЛЫ

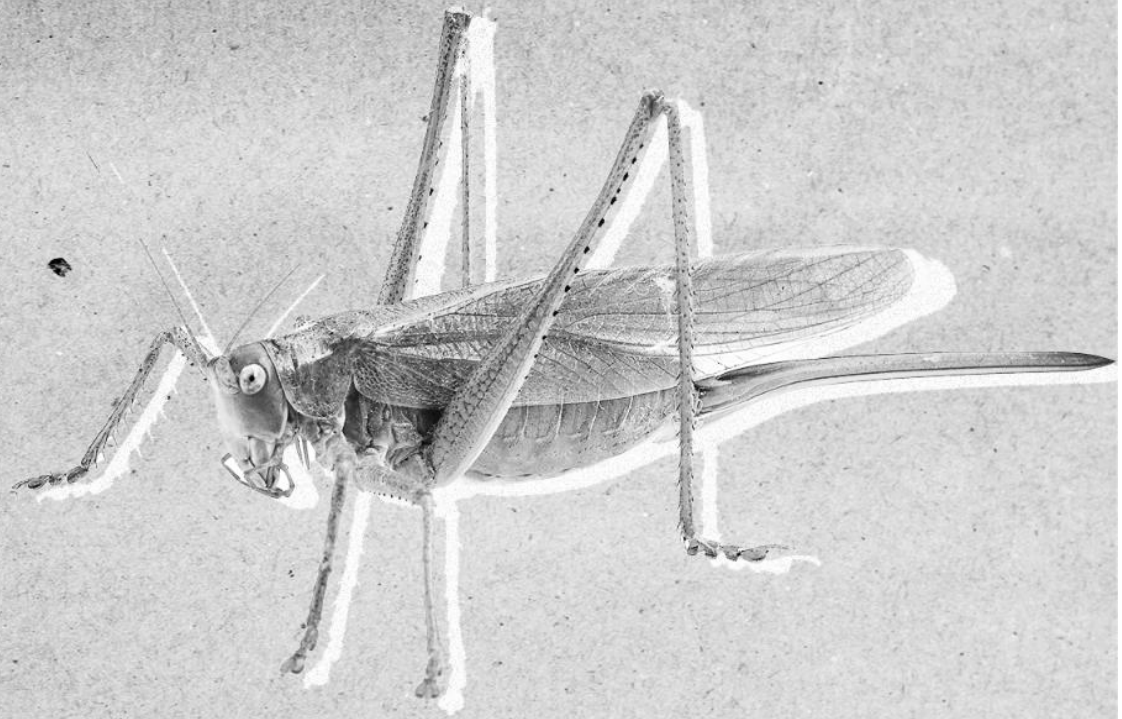
OPENVPN
IKEV2/IPSEC
L2TP/IPSEC
WIREGUARD

подробное описание

ГОСТОВЫЕ VPN РФ И РБ

Континент
ViPNet
C-Teppa
Diamond
Dionis
...

Обзор устройств



УДОСТОВЕРЯЮЩИЕ ЦЕНТРЫ

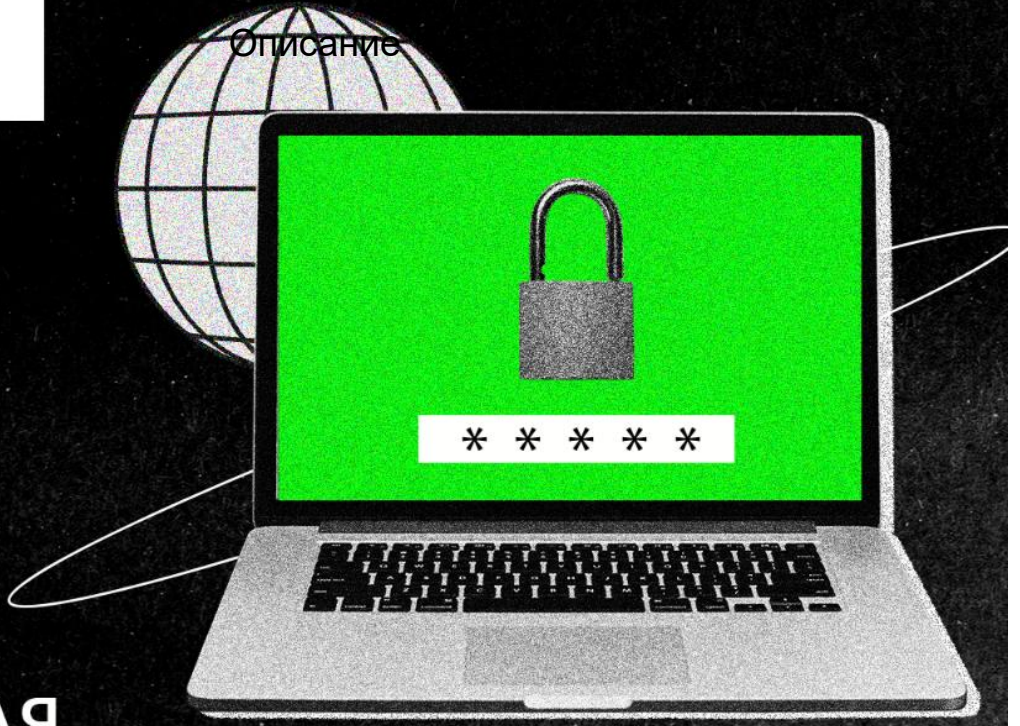
Удостоверяющий центр — это компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей.

Описание

Локальные

ВИДЫ ЭЛЕКТРОННОЙ ПОДПИСИ

Описание



ПРОСТАЯ

УСИЛЕННАЯ

УСИЛЕННАЯ КВАЛИФИЦИРОВАННАЯ

Описание

Программы для работы с ЭЦП

КОМПРОМЕТАЦИЯ КЛЮЧА

ХРАНЕНИЕ КЛЮЧЕЙ ШИФРОВАНИЯ В БЕЗОПАСНОМ МЕСТЕ.

ИСПОЛЬЗОВАНИЕ НАДЕЖНЫХ ПАРОЛЕЙ ДЛЯ ЗАЩИТЫ КЛЮЧЕЙ ШИФРОВАНИЯ.

РЕГУЛЯРНОЕ ОБНОВЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СИСТЕМНЫХ КОМПОНЕНТОВ.

ИСПОЛЬЗОВАНИЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ.

ПРАКТИКА

1. Настрйока 2FA.
2. Создание открытого и закрытого ключа SSH, подключение к серверу по ключу. (описание для всех ОС)
   - ssh-keygen
   - ssh-copy-id root@123.123.123.123

Домашнее задание

1. Создать пару ключей SSH на Kali Linux, экспортировать открытый ключ на сервер Ubuntu Server. Настроить конфиг SSH для аутентификации по ключам.
2. Сделать подключение SSH по ключу(прислать скрин)
3. Удалить пару ключей на Kali и публичный ключ на Ubuntu.
4. Установить 2FA с TOTP токеном на Ubuntu Server, провести конфигурацию и выдачу токена пользователю.
5. Подключиться с Kali на Ubuntu и использованием TOTP(прислать скрин)
6. На сервере Ubuntu(серверная), развернуть ftp сервер(vsftpd) и провести базовую настройку(загуглите, если не найдёте, пишите мне).
7. Подключиться к FTP серверу с Kali и отправить туда любой файл. Прислать скрин об успешной отправке файла.
8. В PfSense настроить блокирующее правило(Floating) по src.ip=kali, dst.ip=ubuntu, dst.port=20,21, protocol=tcp. Настроить логирование этого правила и прислать скрин блокировки(в логах).