Защита данных

Н. Аскеров

Важность защиты данных

Защита данных важна, поскольку это защищает информацию организации от мошеннических действий, взлома, фишинга и кражи личных данных. Любая организация, которая хочет работать эффективно, должна обеспечить безопасность своей информации, внедрив план защиты данных.

Веб-приложения

Банкинг

Цифровые подписи

Чат-приложения

Электронная почта

Криптовалюта

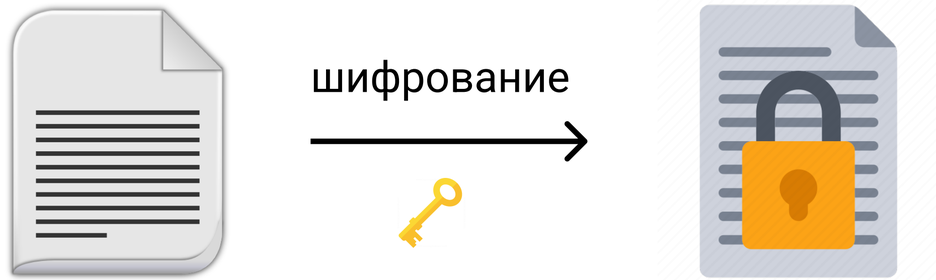
Криптография

Криптография - наука о методах обеспечения:

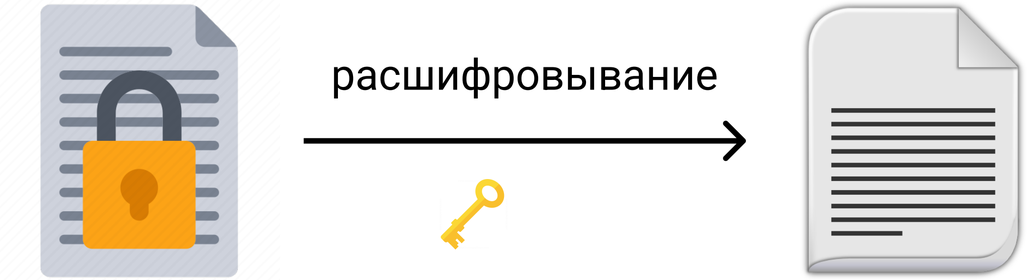
- конфиденциальности - невозможности прочтения информации посторонним
- целостности данных - невозможности незаметного изменения
- аутентификации - проверки подлинности авторства или других свойств объекта
- шифрования - кодировка данных

Шифрование данных

Шифрование - применения криптографического преобразования открытого текста на основе алгоритма и ключа в шифрованный текст.



Расшифровывание — процесс криптографического преобразования шифрованного текста в открытый.



Виды текста

Исходный текст	Секретный ключ
Привет мир!	???

Шифрованный (AES-256)

U2FsdGVkX18Z0auB4CewlkIHeS4M33Ingux/qZJRGfWktO1SxqWRgVLk/I6dv2BP

Шифр

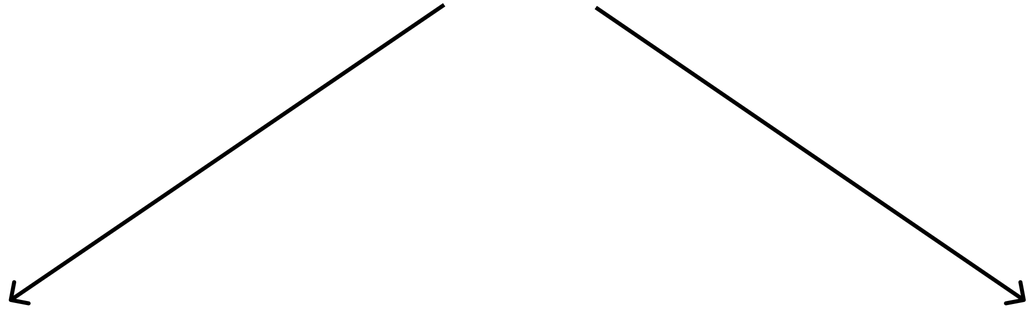
Шифр — совокупность криптографических преобразований

... _ _ _ ... <- Шифр Морзе (SOS)

А •–	И ••	Р •–•	Ш ––––
Б –•••	Й •–––	С •••	Щ ––•–
В •––	К –•–	Т –	Ъ •––•–•
Г ––•	Л •–••	У ••–	Ы –•––
Д –••	М ––	Ф ••–•	Ь –••–
Е •	Н –•	Х ••••	Э ••–••
Ж •••–	О –––	Ц –•–•	Ю ••––
З ––••	П •––•	Ч –––•	Я •–•–

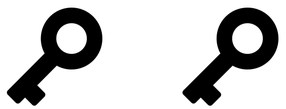
<- Азбука Мо́рзе

Шифрование



Симметричное

Ассимметричное



Симметричное шифрование

Twofish, Serpent, AES (Rijndael), Camellia, Salsa20, ChaCha20, Blowfish, CAST5, Kuznyechik, RC4, DES, 3DES, Skipjack, Safer, IDEA

Асимметричное шифрование

RSA, Diffie-Hellman, ECC, ECDSA, El Gamal, DSA

Спасибо за внимание

Пример симметричного шифрования на языке TypeScript