



Sources & Information

Подписывайтесь на телеграм канал https://t.me/fkb_ctfers

Ciphey/Ciphey

Translations DE FR HU ID IT NL PT-BR RU ZH
Documentation | Discord | Installation Guide Fully automated decryption/decoding/cracking tool using natural language processing & artificial

<https://github.com/Ciphey/Ciphey>



CyberChef

The Cyber Swiss Army Knife - a web app for encryption, encoding, compression and data analysis

<https://gchq.github.io/CyberChef/>



xaairy/mipt-ctf

Курс по подготовке к соревнованиям по компьютерной безопасности формата CTF. Занятия проходили в МФТИ в 2014-2015 и 2015-2016 учебных годах. Каждое занятие состоит из небольшой лекции и практики в виде решения задач на

<https://github.com/xaairy/mipt-ctf/>



Ganapati/RsaCtfTool

RSA attack tool (mainly for ctf) - retrieve private key from weak public key and/or uncipher data - Ganapati/RsaCtfTool

<https://github.com/Ganapati/RsaCtfTool/blob/master/RsaCtfTool.py>



Книга Брюса Шнайера Прикладная Криптография


<https://s3-us-west-2.amazonaws.com/secure.notion-static.com/e10a9a64-5080-4992-b1db-88a1a13f6dee/kripto.pdf>

Статьи и презентации

[Hash_functionshttps://docs.google.com/presentation/d/1804sbujluAIEJqSCZWh9t6liBI5Lbf_3-2IUcAN4GE/edit?usp=drivesdk](https://docs.google.com/presentation/d/1804sbujluAIEJqSCZWh9t6liBI5Lbf_3-2IUcAN4GE/edit?usp=drivesdk)

Гайд по криптографии: что такое электронная цифровая подпись и как она работает

Электронная цифровая подпись сейчас на слуху - многие современные компании потихоньку переходят на электронный документооборот. Да и в повседневной жизни ты наверняка сталкивался с этой штукой. Немного магии, и вуаля - все документы подписаны! Осталось

 <https://xakep.ru/2016/12/15/crypto-part5/>



Симметричные шифры

Симметричные шифры Оглавления Требования Общая схема Виды симметричных шифров Параметры алгоритмов
Симметричные шифр - способ шифрования, в котором для шифрования и расшифрования применяется один и тот же криптографический ключ. До изобретения схемы асимметричного шифрования единственным существовавшим способом

 <http://kriptografea.narod.ru/sim.html>