CRYPTO

...

Crypto

Что запоминать?

- Старые виды шифрования (цезарь, виженера, морзе и тд)
- XOR, Base16, Bas32, Base64, Base85, Binary, Hex, ASCII таблицу.

Кодировать и декодировать вы можете на Кубершефе. Крайне полезный сайт и советую добавить его в закладку. Есть и подобные ему, но вспомним про “ручки, гугл, голова” и .. найдём сами по мере необходимости.

Задания в CTF с выше написанными видами кодирования и шифрования, считаются крайне легкими задачами, но для начала достаточно!

Что-то сложнее в крипте?

- RSA
- AES
- ECC

И другие асимметричные и симметричные криптосистемы. Их алгоритмы советую смотреть на вики. Так же много реализаций их уже описаны на многих языках, но опять же советую посмотреть на питон.

Питон один из математических языков, соответственно он и имеет много библиотек в этом направлении, которые существенно упрощают жизнь во время решения задач на крипту.

Итоги

В данной презентации не было примеров как решать, был очень краткий обзор на инструменты и советы.

Всё узнается с практикой и только с ней!