# INTRODUCTION TO CRYPTOGRAPHY

**INTRO TO CRYPTOGRAPHY AND CAREER CHOICES IN CRYPTOGRAPHY**

# Introduction to Cryptography

Cryptography is the science of keeping information safe.

- Confidentiality
- Integrity
- Authentication

# Types of Cryptography

Cryptography is broadly classified into three types: symmetric cryptography with each type serves different purposes, from securing communication and verifying identity to ensuring data has not been tampered with.

## Symmetric Encryption

Same key for encryption
and for decryption

## Asymmetric Encryption

One public key for encryption and another private key for decryption

## Hash Functions

Functions that turns any data into a irreversible fixed-length digital fingerprint.

## Digital Signatures

Sender signs, receiver verifies, ensures authenticity and integrity.

# HANDS - ON 1

## Hash functions

# Symmetric Cryptography

## AES - Advanced Encryption Standard

AES is very fast and widely used to secure web traffic, virtual private networks, and encrypted storage.

## RC4 - Rivest Cipher

Once a popular stream cipher for its speed. It encrypts data one byte at a time, which is different from block ciphers like AES.

## ChaCha20

Fast, secure stream cipher used for encryption in modern applications

# HANDS - ON 2

## in python

# Asymmetric Cryptography

## RSA Encryption

Asymmetric algorithm for encryption, decryption, and digital signatures securely.

Encrypts data itself

## Diffie Hellman

Algorithm for securely exchanging cryptographic keys over untrusted channels.

Give secure key exchange for sharing data

# HANDS - ON 3

## in python

# Digital Signature Signing using RSA

- The sender creates a hash of the message.
- The hash is encrypted with sender’s private RSA key to generate signature.
- The recipient uses the sender’s public RSA key to decrypt the signature.
- The recipient compares the decrypted hash with the message hash to verify integrity.

# Leveraging OpenSSL

## for cryptography - what is it?

Open-source cryptography toolkit for SSL/TLS and general-purpose crypto
Provides commands for

- Generating keys (RSA, etc)
- Creating CSRs (Certificate Signing Requests)
- Generating and verifying digital certificates
- Hashing (SHA, MD5, etc.)

# HANDS - ON 4

## in real time in kali

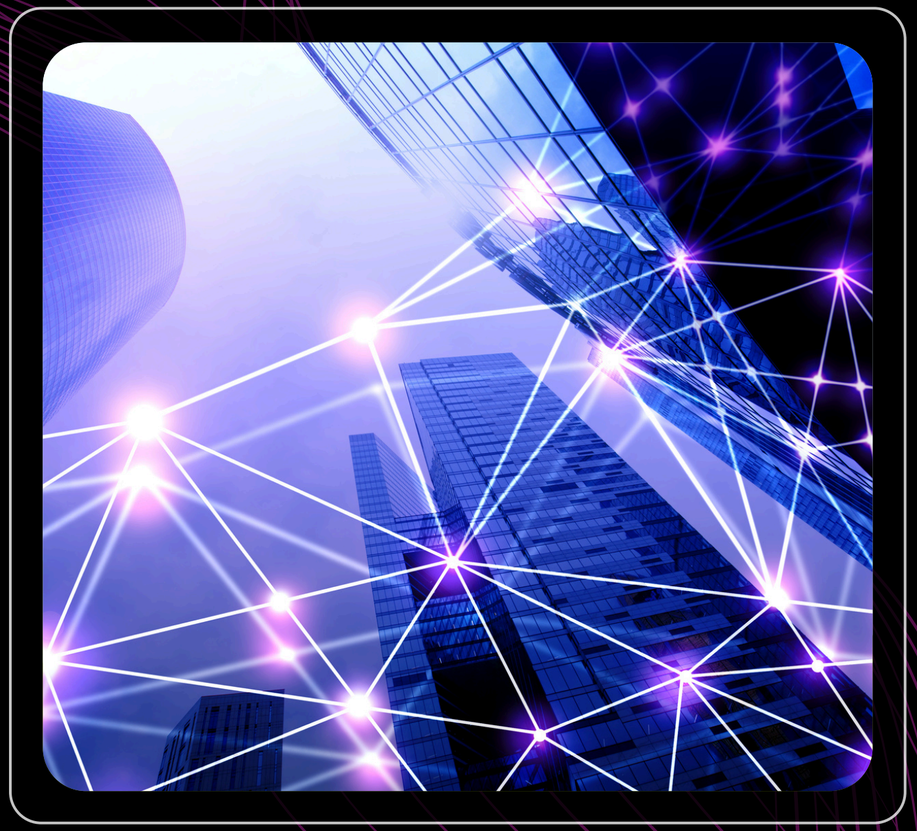
# Ciphers - Fun Part of Cryptography

https://medium.com/aardvark-infinity/100-different-ciphers-aa3d0f183735

Ciphers are algorithms that transform plaintext into unreadable text to secure data.

YOU KNOW WHAT! YOU CAN EVEN CREATE YOUR OWN CIPHER!
LIKE EVEN WITH OBJECTS !!

# CyberChef - To know about it



## Overview about Cyber Chef

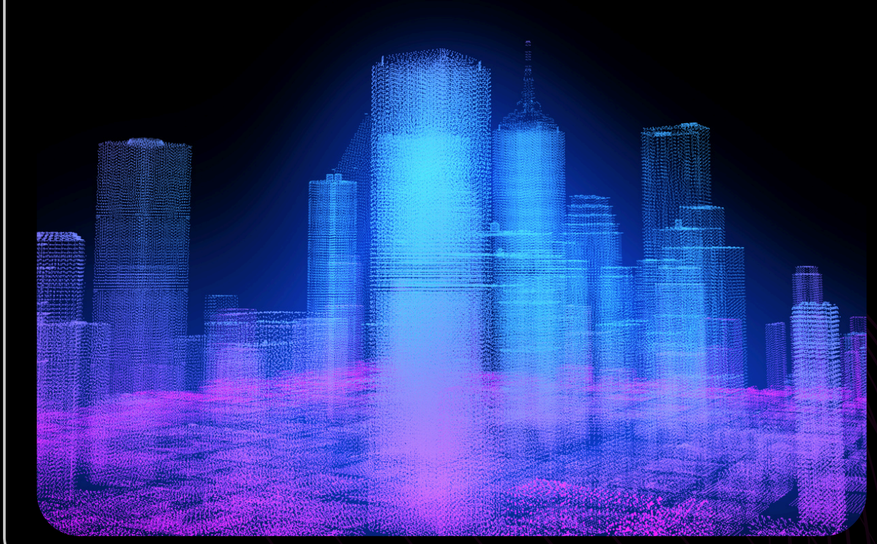
CyberChef is a web-based tool that lets you encode, decode, encrypt, decrypt, and transform data with a simple drag-drop interface.

# HANDS - ON 5

## in chrome/firefox in kali

# True Crypt

TrueCrypt is an open-source encryption software used to create encrypted volumes, full disk encryption, and hidden containers to protect sensitive data.



01

**Encrypted containers**

02

**Full Disk Encryption**

03

**Drives, Folders**

04

**Flexibility in security**

# What you ALL DO AND PRACTICE

SPEND TIME ON
THE INTERNET

CAN PRACTICE
CRYPTOGRAPHY CTF
PRACTICE


READ MANUALS ON THE TOOLS
RELATED TO CRYPTO

CREATE YOUR OWN
CIPHERS AND HAVE FUN

# Career & Scope IN CRYPTO

### Blockchain / Cryptocurrency Developer

Focus on smart contracts, digital signatures, and algorithms.

### Defense Cryptographer

Develop and break ciphers for national security, intelligence, or military applications.

### Cryptanalysis Specialist

Test and audit encryption systems, certificates, and secure communications.

# SUMMARY!

# AND QUESTIONS?

# Thank You!