EIT TRAINING

TRAINING PLAN

- INTRODUCTION TO LINUX
- **FORENSICS AND OSINT**
- CRYPTOGRAPHY
- WEB EXPLOITATION
- REVERSE ENGINEERING
- BINARY EXPLOITATION

Cryptography

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

Terminology

- Plaintext: The message that we want to encrypt.
- Ciphertext: The result of encrypting a plaintext.
- Cipher: A method of encrypting or decrypting data.
- Key: Secret information needed to correctly decrypt ciphertext and obtain plaintext.
- Cryptoanalysis: Attacking ciphertext by finding a flaws in the underlying algorithm.

Terminology

- Encoding
- Encryption → Symmetric / Asymmetric
- Hashing

Terminology

- Encoding is not a form of cryptography, but a form of data representation. Immediately reversible, i.e. no key is used.

- Encryption is a reversible function. Used for maintaining data confidentiality and requires the use of a key (kept secret) in order to return to plaintext.

- Hashing is a one way function. Mainly used for validating the integrity of content and storing sensitive information.

Encoding

Encoding

ASCII

[99, 105, 116, 95, 121, 97, 95, 55, 97, 98, 105, 98, 105]

Binary (Base 2)

01100011 01101001 01110100 01011111 01111001
01100001 01011111 00110111 01100001 01100010
01101001 01100010 01101001

Hex (Base 16) bytes.fromhex()

63 69 74 5f 79 61 5f 37 61 62 69 62 69

Encoding

Base32

32-printable characters (A-Z2-7=)

MNUXIX3ZMFPTOYLCNFRGS===

Base64

There are 64 characters used to encode binary data. Character set: A-Za-z0-9+/=

Y2l0X3lhXzdhYmliaQ==

Base58

Character set: A-Za-z0-9

9HFgWyVKv7NURMvEu6

Encoding

Morse Code

-.-. .. - ..--.- -.-- .- ..--.- --... .- -... .. -... ..

Brainfuck

```
++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>>>-.+++++++.++++++++++.-----------
--------.++++++++++++++++++++++++++.------------------------.--.<-------------
-.>++.+.+++++++.-------.+++++++.
```

Ook!

```
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook. Ook? Ook. Ook. Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook. Ook? Ook. Ook? Ook. Ook? Ook. Ook! Ook! Ook? Ook! Ook. Ook? Ook. Ook? Ook. Ook? Ook. Ook? Ook! Ook!
Ook! Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook.
Ook! Ook! Ook! Ook! Ook! Ook. Ook? Ook. Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook. Ook. Ook? Ook. Ook. Ook. Ook.
Ook! Ook. Ook. Ook. Ook. Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook! Ook.
```

Encoding

Morse Code

-.-. .. - ..--.- -.-- .- ..--.- --... .- -... .. -... ..

Brainfuck

```
++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>>>-.+++++++.++++++++++.-----------
--------.++++++++++++++++++++++++++.-----------------------.--.<-------------
-.>++.+.+++++++.-------.+++++++.
```

Ook!

```
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook. Ook? Ook. Ook. Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook. Ook? Ook. Ook? Ook. Ook? Ook. Ook! Ook! Ook? Ook! Ook. Ook? Ook. Ook? Ook. Ook? Ook. Ook? Ook! Ook!
Ook! Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook.
Ook! Ook! Ook! Ook! Ook! Ook. Ook? Ook. Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook. Ook. Ook? Ook. Ook. Ook. Ook.
Ook! Ook. Ook. Ook. Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook! Ook.
```

Challenges!

pika pi?

pi pi pi pi pi pi pi pi pi pi pika pipi pi pipi pi pi pi pipi
pi pi pi pi pi pi pi pipi pi pi pi pi pi pi pi pi pi pi pi pichu
pichu pichu pichu ka chu pipi pipi pipi pipi ka pikachu
pi pi pi pi pi pi pikachu pi pi pi pi pi pi pi pi pi pi pi
pikachu pichu pichu pi pi pikachu pipi pipi pi pi pi pi pi
pikachu ka ka ka ka ka ka ka ka ka ka ka ka ka ka ka
ka ka ka ka ka ka ka ka ka pikachu pichu pichu
pikachu pipi pipi pi pi pi pikachu ka ka ka pikachu pi
pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi
pikachu ka ka ka ka ka ka ka ka ka ka ka pikachu ka
ka ka ka ka ka ka ka ka ka ka pikachu

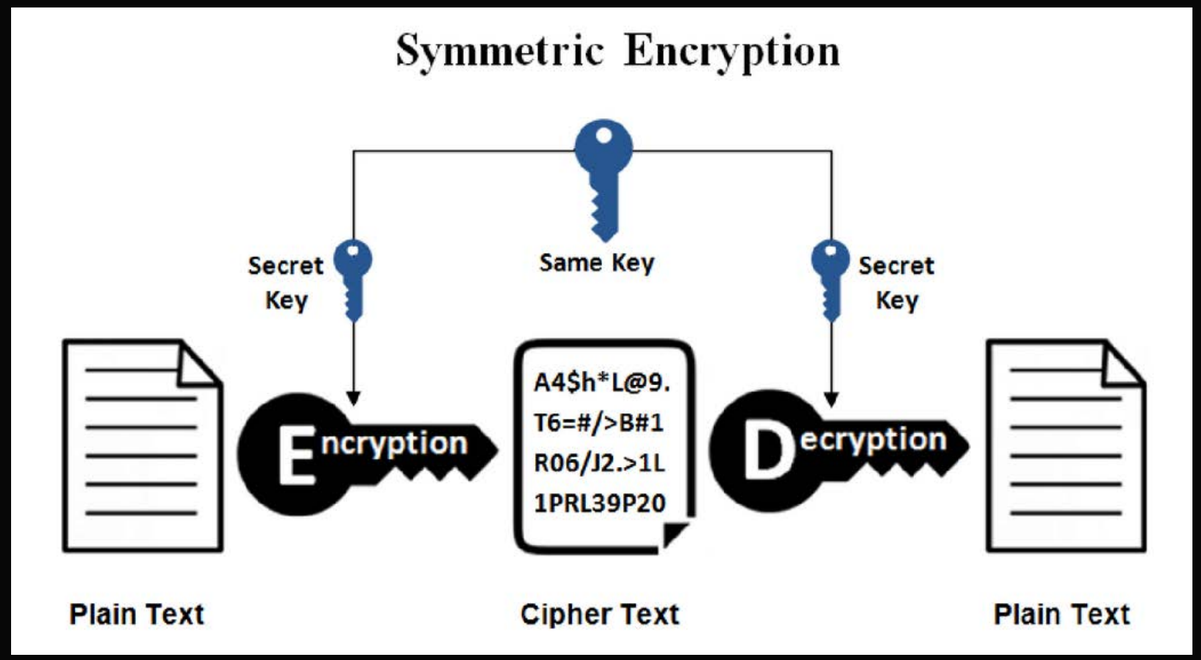
american breakfast

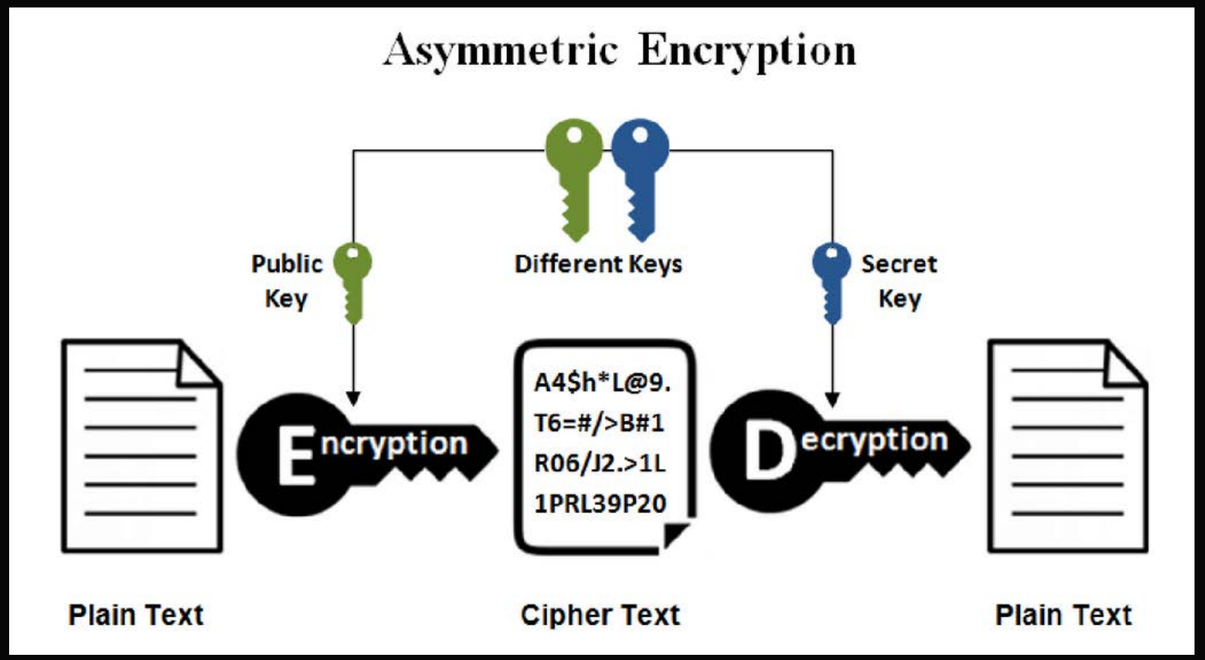
ABAAAAAABBAABAAAABBBABAAABAA
ABAAABAABBABABABBABAAAABBAAA
ABBABAAABABBABABBABABBAA

against the flow of time

n5WasxWYjBSZyFGlzNWaw1Wes9Gl0BXb

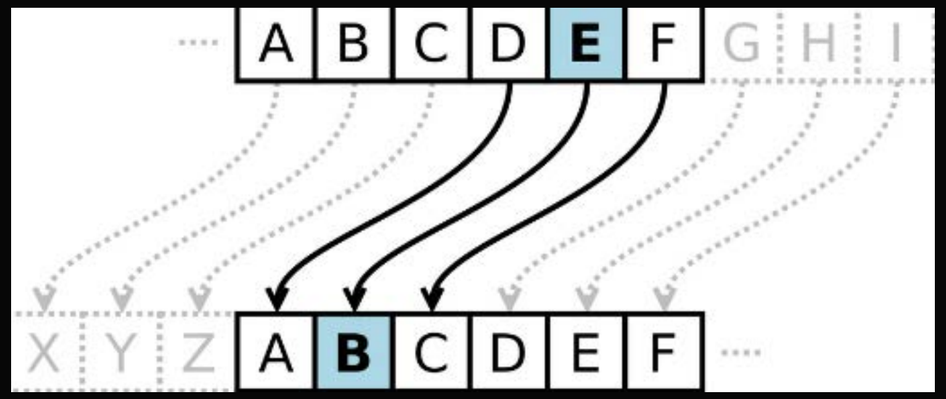
Encryption


Symmetric Encryption
Secret Key
Same Key
Secret Key
Encryption
A4$h*L@9.
T6=#/>B#1
R06/J2.>1L
1PRL39P20
Decryption
Plain Text
Cipher Text
Plain Text


Asymmetric Encryption
Public Key
Different Keys
Secret Key
Encryption
A4$h*L@9.
T6=#/>B#1
R06/J2.>1L
1PRL39P20
Decryption
Plain Text
Cipher Text
Plain Text

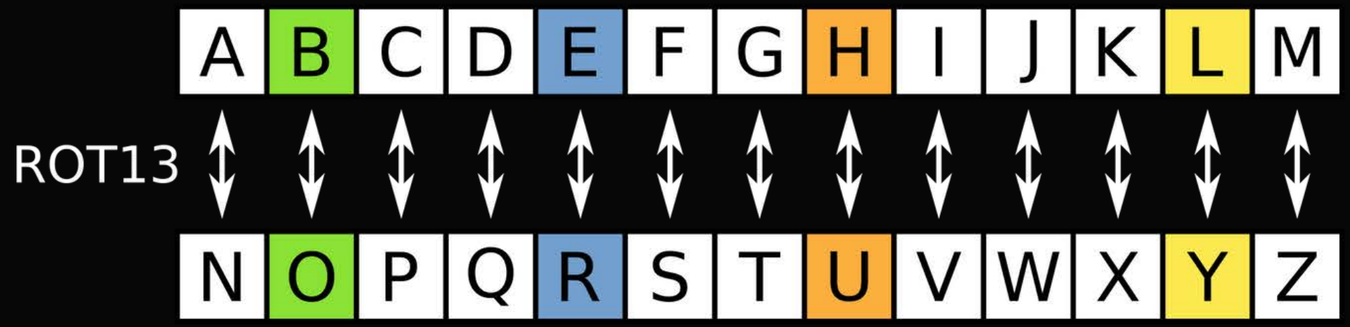
Symmetric Encryption (classic algorithms)

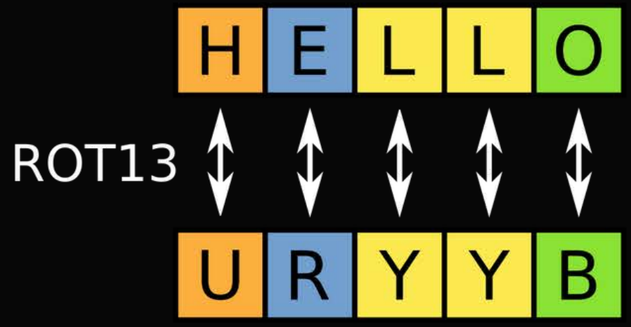
Caesar Cipher (ROT)



ROT23

Substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet





Symmetric Encryption (classic algorithms)

Vigenere Cipher

msg = hello world

key = test

ciphertext = msg + key % 26

H	E	L	L	O	W	O	R	L	D
7	4	11	11	14	22	14	17	11	3
T	E	S	T	T	E	S	T	T	E
19	4	18	19	19	4	18	19	19	4
0	8	3	4	7	0	6	10	4	7
A	I	D	E	H	A	G	K	E	H

Modern Encryption

```
message: HELLO
ascii bytes: [72, 69, 76, 76, 79]
hex bytes: [0x48, 0x45, 0x4c, 0x4c, 0x4f]
base-16: 0x48454c4c4f
base-10: 310400273487
```

Representation in base 10:

N = ord('O') * 256**0 + ord('L') * 256**1 + + ord('L') * 256**2 +
+ ord('E') * 256**3 + + ord('H') * 256**4

Symmetric Encryption

XOR

	C	c	s	c
msg =	01000011	01100011	01110011	01100011
	C	I	T	C
key =	01000011	01001001	01010100	01000011
	00	2A	27	20
ciphertext =	00000000	00101010	00100111	00100000

Symmetric Encryption

Useful Python Packages

- PyCryptodome
- gmpy2
- pwntools

```
chr() #converts an integer to its unicode character and returns it
ord() #returns an integer representing the Unicode character
bytes.fromhex() #converts hex to bytes
.hex() #gets hex representation of byte string
bytes_to_long() #convert "string" to base-10
long_to_bytes() #convert base-10 to "string"
```

Challenge!

first xor

Decrypt this: ,=$1'"6/""*,- c,-s:,6!c%*!07c+,1c0+"/?

key = CCSC