Nevezi-Strango Dávid, IA, Anul III

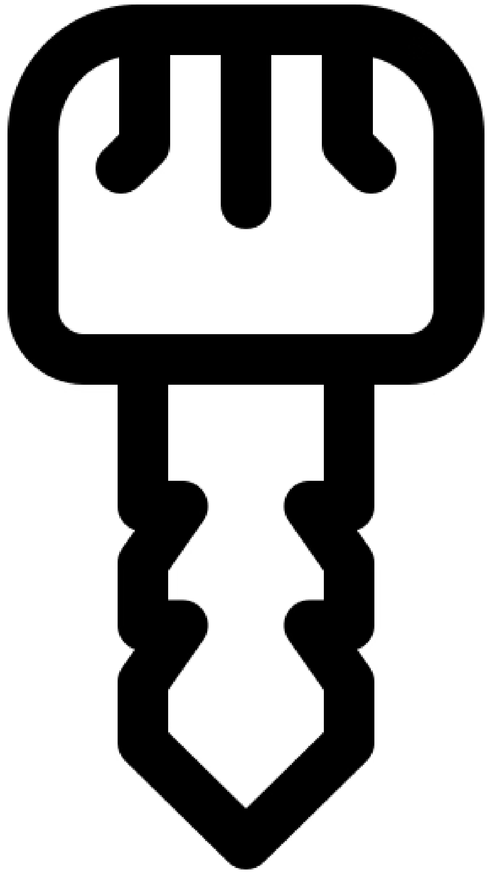
May 2023

CRYPTOOL

May 2023

Project summary

WHAT IS THE PROJECT?



A CLI-based tool for encryption, decryption, hash and cryptanalysis

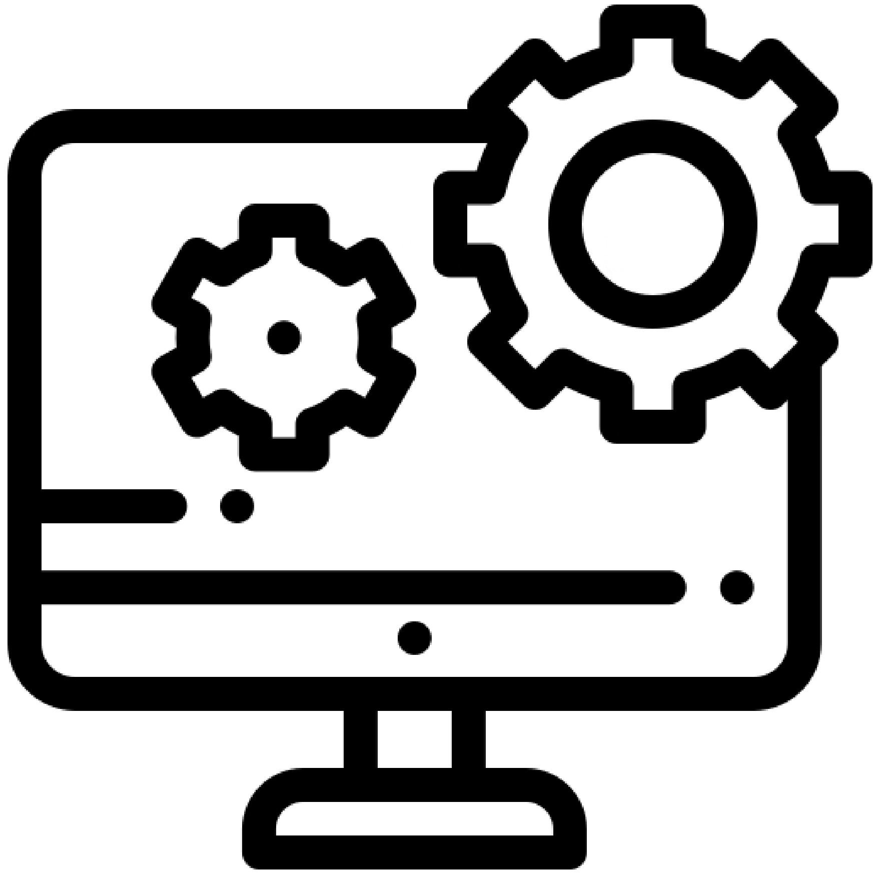
How do you launch it?

The very first thing you want to know

```
PS D:\User Stuff\Faculta\SC> python .\main.py -h
usage: main.py [-h] (-e | -d | -g | -ha | -a) (--rsa | --rc4 | -b | -p | -c | --sha256 | --des | --tdes) [-m MESSAGE|<MESSAGE_PATH>] [-k KEY|<KEY_PATH>] [-o <OUTPUT_PATH>] [-v]

options:
  -h, --help            show this help message and exit
  -e, --encrypt         Flag argument for encryption of supported chipers/algorithms
  -d, --decrypt         Flag argument for decryption of supported chipers/algorithms
  -g, --generate        Flag argument for generating keys for supported algorithms
  -ha, --hashing        Flag argument for supported hashing algorithms
  -a, --cryptanalysis   Flag argument for cryptanalysis of supported chipers/algorithms
  --rsa                 Flag argument for RSA
  --rc4                 Flag argument for RC4
  -b, --bifid           Flag argument for Bifid chiper
  -p, --polybius        Flag argument for Polybius chiper
  -c, --cesaer          Flag argument for Cesaer chiper
  --sha256              Flag argument for SHA-256
  --des                 Flag argument for DES (ECB)
  --tdes                Flag argument for TDES-EDE (ECB)
  -m MESSAGE|<MESSAGE_PATH>, --message MESSAGE|<MESSAGE_PATH>
                        message or path to message input file
  -k KEY|<KEY_PATH>, --key KEY|<KEY_PATH>
                        key or path to key input file (For RSA, have the two values separated by space or newline, last value has to be n)
  -o <OUTPUT_PATH>, --output_path <OUTPUT_PATH>
                        path to output file
  -v, --version         show program's version number and exit
```

Launch examples



```
PS D:\User Stuff\Faculta\SC> python .\main.py -d -p -m "44232443 2443 15332231244323"
THIS IS ENGLISH
```

```
PS D:\User Stuff\Faculta\SC> python .\main.py -e -p -m "this is english"
44232443 2443 15332231244323
```

```
PS D:\User Stuff\Faculta\SC> python .\main.py -ha --sha256 -m .\text.txt
d7430f79f34bd1b79efea4128fae3ca979aed9d28b489aae76679a6b2c5112d9
```

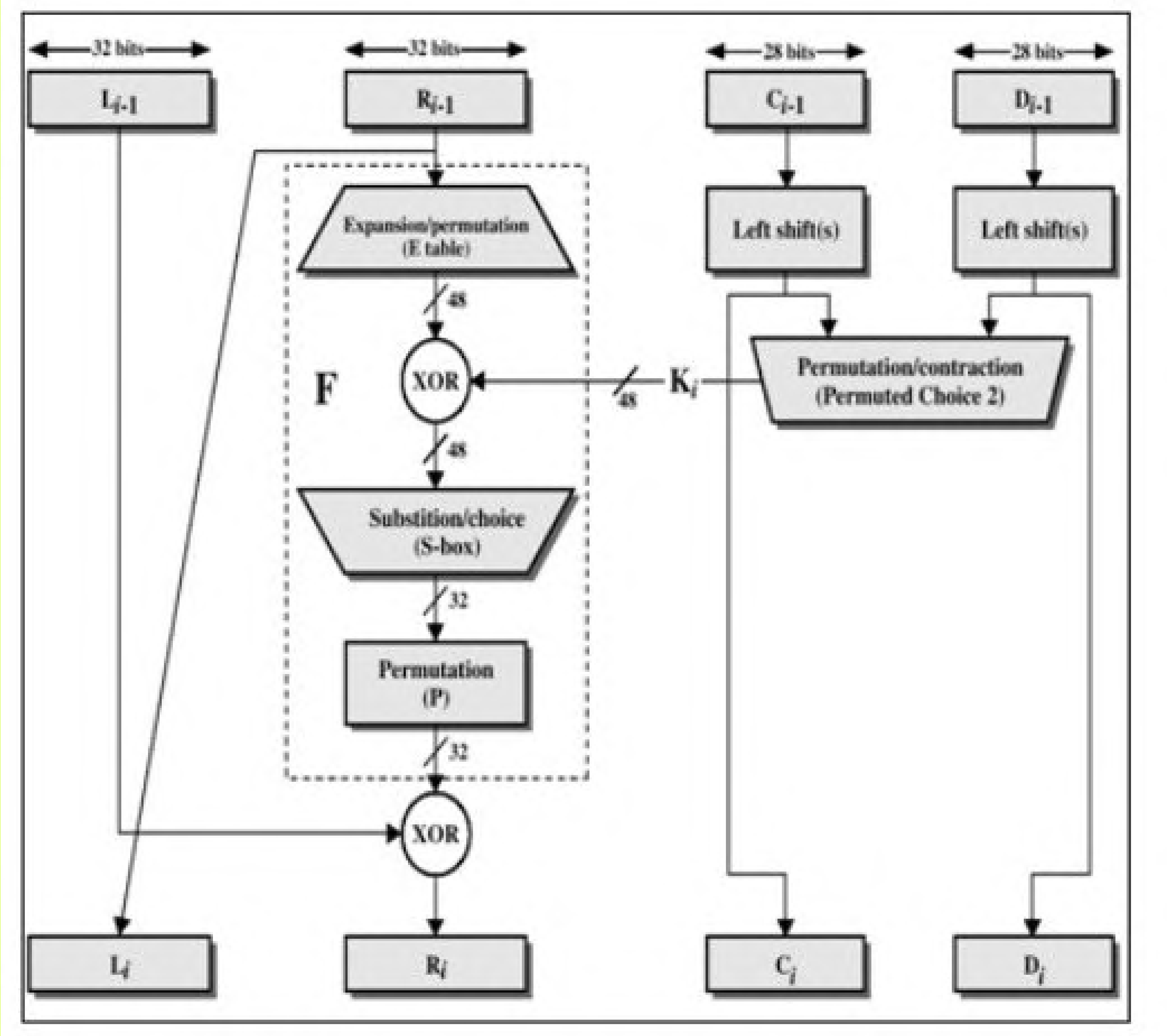
```
PS D:\User Stuff\Faculta\SC> python .\main.py -e --des -m 123456ABCD132536 -k AABB09182736CCDD
3201337c3a38828183b832bf31383339
PS D:\User Stuff\Faculta\SC> python .\main.py -d --des -m 3201337c3a38828183b832bf31383339 -k AABB09182736CCDD
123456ABCD132536
```

Examples are included in the archive

Algorithms

DES using bitarray

```
>>> a = bitarray('101110001')
>>> ~a  # invert
bitarray('010001110')
>>> b = bitarray('111001011')
>>> a ^ b
bitarray('010111010')
>>> a &= b
>>> a
bitarray('101000001')
>>> a <<= 2   # in-place left shift by 2
>>> a
bitarray('100000100')
>>> b >> 1
bitarray('011100101')
```



*3DES-EDE is also available

DES diagram: https://www.researchgate.net/figure/Depiction-of-One-Round-of-DES-212-3-DES-Algorithm-In-cryptography-techniques-Triple_fig2_306425963

bitarray library: https://pypi.org/project/bitarray/

Algorithms

RC4

KEY SCHEDULING

- j = 0
- for i = 0 to 255 do

    j = j + S[i] + K[i] mod 256

    swap S[i] and S[j]
- end for

PSEUDO- RANDOM GENERATION ALGORITHM

- set I and j back to 0
- for i = i + 1

    j = j + S[i] mod 256

    swap S[i] and S[j]

    t = S[i] + S[j] mod 256

    KeyStream = S[t]
- end for

Encryption and Decryption

- CT = PT xor KeyStream
- PT = CT xor KeyStream

RC4 pseudocode: https://www.youtube.com/watch?v=1UP56WM4ook&

Algorithms

RSA

RSA Key Generation

Output: public key: $k_{pub} = (n, e)$ and private key: $k_{pr} = (d)$

1. Choose two large primes p and q.
2. Compute $n = p \cdot q$.
3. Compute $\Phi(n) = (p-1)(q-1)$.
4. Select the public exponent $e \in \{1, 2, \ldots, \Phi(n) - 1\}$ such that

$$\gcd(e, \Phi(n)) = 1.$$

5. Compute the private key d such that

$$d \cdot e \equiv 1 \bmod \Phi(n)$$

For step 5, we're using the following formula:

$$d = (1 + k^* \Phi(n))/e$$

RSA Key Gen: https://samsclass.info/141/proj/pRSA2.htm

May 2023

CRYPTOOL

Live Demo

CRYPTOOL

THE END

NEVEZI-STRANGO DÁVID, IA, ANUL III

DAVID.NEVEZI00@E-UVT.RO