# Вибір та реалізація базових фреймворків та бібліотек

## Crypto++

### Key Generation

```
$ /usr/bin/time -v ./a.out 1
RSA keys generated and saved.
        Command being timed: "./a.out 1"
        User time (seconds): 0.00
        System time (seconds): 0.00
        Percent of CPU this job got: 50%
        Elapsed (wall clock) time (h:mm:ss or m:ss): 0:00.02
        Average shared text size (kbytes): 0
        Average unshared data size (kbytes): 0
        Average stack size (kbytes): 0
        Average total size (kbytes): 0
        Maximum resident set size (kbytes): 6784
        Average resident set size (kbytes): 0
        Major (requiring I/O) page faults: 40
        Minor (reclaiming a frame) page faults: 252
        Voluntary context switches: 32
        Involuntary context switches: 3
        Swaps: 0
        File system inputs: 7584
        File system outputs: 16
        Socket messages sent: 0
        Socket messages received: 0
        Signals delivered: 0
        Page size (bytes): 4096
        Exit status: 0
```

### Encryption

```
$ /usr/bin/time -v ./a.out 2 ./text3.txt ./out/enc_3.bin |tee -a logs.txt
wants to load
File encrypted and saved as ./out/enc_3.bin
```

```
        Command being timed: "./a.out 2 ./text3.txt ./out/enc_3.bin"
        User time (seconds): 0.00
        System time (seconds): 0.00
        Percent of CPU this job got: 66%
        Elapsed (wall clock) time (h:mm:ss or m:ss): 0:00.00
        Average shared text size (kbytes): 0
        Average unshared data size (kbytes): 0
        Average stack size (kbytes): 0
        Average total size (kbytes): 0
        Maximum resident set size (kbytes): 6912
        Average resident set size (kbytes): 0
        Major (requiring I/O) page faults: 1
        Minor (reclaiming a frame) page faults: 268
        Voluntary context switches: 3
        Involuntary context switches: 0
        Swaps: 0
        File system inputs: 208
        File system outputs: 8
        Socket messages sent: 0
        Socket messages received: 0
        Signals delivered: 0
        Page size (bytes): 4096
        Exit status: 0
```

## Decryption

```
$ /usr/bin/time -v ./a.out 3 ./out/enc_3.bin ./out/dec_3.bin |tee -a
logs.txt
File decrypted and saved as ./out/dec_3.bin
        Command being timed: "./a.out 3 ./out/enc_3.bin ./out/dec_3.bin"
        User time (seconds): 0.00
        System time (seconds): 0.00
        Percent of CPU this job got: 100%
        Elapsed (wall clock) time (h:mm:ss or m:ss): 0:00.00
        Average shared text size (kbytes): 0
        Average unshared data size (kbytes): 0
        Average stack size (kbytes): 0
        Average total size (kbytes): 0
        Maximum resident set size (kbytes): 7040
        Average resident set size (kbytes): 0
        Major (requiring I/O) page faults: 0
```

```
        Minor (reclaiming a frame) page faults: 272
        Voluntary context switches: 1
        Involuntary context switches: 0
        Swaps: 0
        File system inputs: 0
        File system outputs: 8
        Socket messages sent: 0
        Socket messages received: 0
        Signals delivered: 0
        Page size (bytes): 4096
        Exit status: 0

$ cat ./out/dec_3.bin
hello, crypto++
```

# PyCrypto

## Key Generation

```
$ /usr/bin/time -v python3 crypto_.py 1
RSA keypair generated and saved to private.txt and public.txt.
Elapsed time during the whole program in seconds: 0.26893354399999225
        Command being timed: "python3 crypto_.py 1"
        User time (seconds): 0.32
        System time (seconds): 0.03
        Percent of CPU this job got: 90%
        Elapsed (wall clock) time (h:mm:ss or m:ss): 0:00.39
        Average shared text size (kbytes): 0
        Average unshared data size (kbytes): 0
        Average stack size (kbytes): 0
        Average total size (kbytes): 0
        Maximum resident set size (kbytes): 18420
        Average resident set size (kbytes): 0
        Major (requiring I/O) page faults: 51
        Minor (reclaiming a frame) page faults: 3010
        Voluntary context switches: 174
        Involuntary context switches: 2
        Swaps: 0
        File system inputs: 8656
        File system outputs: 16
        Socket messages sent: 0
        Socket messages received: 0
```

```
        Signals delivered: 0
        Page size (bytes): 4096
        Exit status: 0
```

## Encryption

```
$ /usr/bin/time -v python3 crypto_.py 2 text.txt
File encrypted: text.txt.enc
Elapsed time during the whole program in seconds: 0.013989853999646584
        Command being timed: "python3 crypto_.py 2 text.txt"
        User time (seconds): 0.08
        System time (seconds): 0.01
        Percent of CPU this job got: 94%
        Elapsed (wall clock) time (h:mm:ss or m:ss): 0:00.10
        Average shared text size (kbytes): 0
        Average unshared data size (kbytes): 0
        Average stack size (kbytes): 0
        Average total size (kbytes): 0
        Maximum resident set size (kbytes): 18256
        Average resident set size (kbytes): 0
        Major (requiring I/O) page faults: 1
        Minor (reclaiming a frame) page faults: 3047
        Voluntary context switches: 40
        Involuntary context switches: 11
        Swaps: 0
        File system inputs: 8
        File system outputs: 8
        Socket messages sent: 0
        Socket messages received: 0
        Signals delivered: 0
        Page size (bytes): 4096
        Exit status: 0
```

## Decryption

```
$ /usr/bin/time -v python3 crypto_.py 3 text.txt.enc
File decrypted: text.txt.enc.dec
Elapsed time during the whole program in seconds: 0.031101351999950566
        Command being timed: "python3 crypto_.py 3 text.txt.enc"
```

```
        User time (seconds): 0.10
        System time (seconds): 0.02
        Percent of CPU this job got: 99%
        Elapsed (wall clock) time (h:mm:ss or m:ss): 0:00.12
        Average shared text size (kbytes): 0
        Average unshared data size (kbytes): 0
        Average stack size (kbytes): 0
        Average total size (kbytes): 0
        Maximum resident set size (kbytes): 18512
        Average resident set size (kbytes): 0
        Major (requiring I/O) page faults: 0
        Minor (reclaiming a frame) page faults: 3053
        Voluntary context switches: 41
        Involuntary context switches: 6
        Swaps: 0
        File system inputs: 0
        File system outputs: 8
        Socket messages sent: 0
        Socket messages received: 0
        Signals delivered: 0
        Page size (bytes): 4096
        Exit status: 0

$ cat text.txt.enc.dec
Some text
```

# OpenSSL

## Key Generation

```
$ /usr/bin/time -v ./a.out 1
        Command being timed: "./a.out 1"
        User time (seconds): 0.19
        System time (seconds): 0.00
        Percent of CPU this job got: 100%
        Elapsed (wall clock) time (h:mm:ss or m:ss): 0:00.19
        Average shared text size (kbytes): 0
        Average unshared data size (kbytes): 0
        Average stack size (kbytes): 0
        Average total size (kbytes): 0
        Maximum resident set size (kbytes): 5632
        Average resident set size (kbytes): 0
```

```
        Major (requiring I/O) page faults: 1
        Minor (reclaiming a frame) page faults: 419
        Voluntary context switches: 1
        Involuntary context switches: 4
        Swaps: 0
        File system inputs: 232
        File system outputs: 16
        Socket messages sent: 0
        Socket messages received: 0
        Signals delivered: 0
        Page size (bytes): 4096
        Exit status: 0
```

## Encryption

```
$ /usr/bin/time -v ./a.out 2 ../text.txt
Encrypting

0000 - 61 16 74 1d aa f2 ea e0-67 94 9c ec b2 be af 75   a.t.....g......u
0010 - 6c 97 9f b7 39 b1 1b 11-d2 6e 39 ab 1f 56 06 eb   l...9....n9..V..
0020 - 9d 77 33 18 00 a9 06 81-e3 7e 84 81 f7 cd a7 23   .w3......~.....#
0030 - 72 6a b9 d2 14 f0 6b ae-ee d5 e9 3c 15 1c c9 e9   rj....k....<....
0040 - d8 b2 35 d0 a7 1c 5a b4-28 e1 a8 aa 3e e0 dc 81   ..5...Z.(...>...
0050 - 6f 26 42 97 08 bb df 61-07 46 f2 59 d3 7d 49 cf   o&B....a.F.Y.}I.
0060 - 15 42 05 a3 64 28 12 48-ce 52 2c 84 6c 98 2c d8   .B..d(.H.R,.l.,.
0070 - 28 b4 4e df 16 60 14 43-c2 9d 93 fe e3 b7 f8 9e   (.N..`.C........
0080 - ad 14 b9 f3 73 bf 84 7d-ff 1d 85 e4 12 30 8f ae   ....s..}.....0..
0090 - 45 82 31 5d 7b fe f7 58-9a e6 21 b4 b9 a2 3c 24   E.1]{..X..!...<$
00a0 - a9 78 3b 5a 1c d4 1f 2d-58 9f 4b 01 02 93 76 06   .x;Z...-X.K...v.
00b0 - 45 0d 7f b9 4c 76 87 4c-02 66 ee bf 19 41 07 81   E...Lv.L.f...A..
00c0 - dd f6 8c 12 07 32 5f 76-0d b8 9b 81 ce ac ab f5   .....2_v........
00d0 - ae 5d 8f 74 48 ec 01 08-8c 2a 64 a3 f9 74 bb 0c   .].tH....*d..t..
00e0 - be a7 09 bd cd 38 1b b3-90 21 cb 9c ef 85 36 1a   .....8...!....6.
00f0 - 36 87 3f 1c e4 0b ee 54-be d0 ab 88 73 ee 9e 7b   6.?....T....s..{
len: 10, len2: 256
        Command being timed: "./a.out 2 ../text.txt"
        User time (seconds): 0.00
        System time (seconds): 0.00
        Percent of CPU this job got: 88%
        Elapsed (wall clock) time (h:mm:ss or m:ss): 0:00.00
        Average shared text size (kbytes): 0
```

```
        Average unshared data size (kbytes): 0
        Average stack size (kbytes): 0
        Average total size (kbytes): 0
        Maximum resident set size (kbytes): 5760
        Average resident set size (kbytes): 0
        Major (requiring I/O) page faults: 0
        Minor (reclaiming a frame) page faults: 410
        Voluntary context switches: 1
        Involuntary context switches: 0
        Swaps: 0
        File system inputs: 0
        File system outputs: 8
        Socket messages sent: 0
        Socket messages received: 0
        Signals delivered: 0
        Page size (bytes): 4096
        Exit status: 0
```

## Decryption

```
$ /usr/bin/time -v ./a.out 3 ./out/enc.bin
decrypting
0000 - 53 6f 6d 65 20 74 65 78-74 0a                      Some text.
len: 256, outl: 10
Some text
        Command being timed: "./a.out 3 ./out/enc.bin"
        User time (seconds): 0.01
        System time (seconds): 0.00
        Percent of CPU this job got: 95%
        Elapsed (wall clock) time (h:mm:ss or m:ss): 0:00.02
        Average shared text size (kbytes): 0
        Average unshared data size (kbytes): 0
        Average stack size (kbytes): 0
        Average total size (kbytes): 0
        Maximum resident set size (kbytes): 5888
        Average resident set size (kbytes): 0
        Major (requiring I/O) page faults: 0
        Minor (reclaiming a frame) page faults: 413
        Voluntary context switches: 0
        Involuntary context switches: 0
        Swaps: 0
```

```
        File system inputs: 0
        File system outputs: 8
        Socket messages sent: 0
        Socket messages received: 0
        Signals delivered: 0
        Page size (bytes): 4096
        Exit status: 0
```

## Results:

| Library | Key Gen | Encryption | Decryption |
|---|---|---|---|
| Crypto++ | 0:00.02 | 0:00.00 | 0:00.00 |
| PyCrypto | 0:00.27 | 0:00.01 | 0:00.03 |
| OpenSSL | 0:00.19 | 0:00.00 | 0:00.02 |