Information Security HW 1 Instruction

0856622 余家宏

- Github Link (https://github.com/yamiefun/Information-Security-HW1)
- It’s recommended to read this instruction on hackmd for a better reading experience. Links are provided in Github above.

Environment

Python package requirement:

1. pycryptodome 3.9.9 (https://pycryptodome.readthedocs.io/en/latest/src/installation.html)
2. base64 (https://docs.python.org/3/library/base64.html#module-base64)
3. matplotlib (https://matplotlib.org/3.3.2/users/installing.html)
4. numpy (https://numpy.org/install/)

How to Run

Task 1~4

Usage

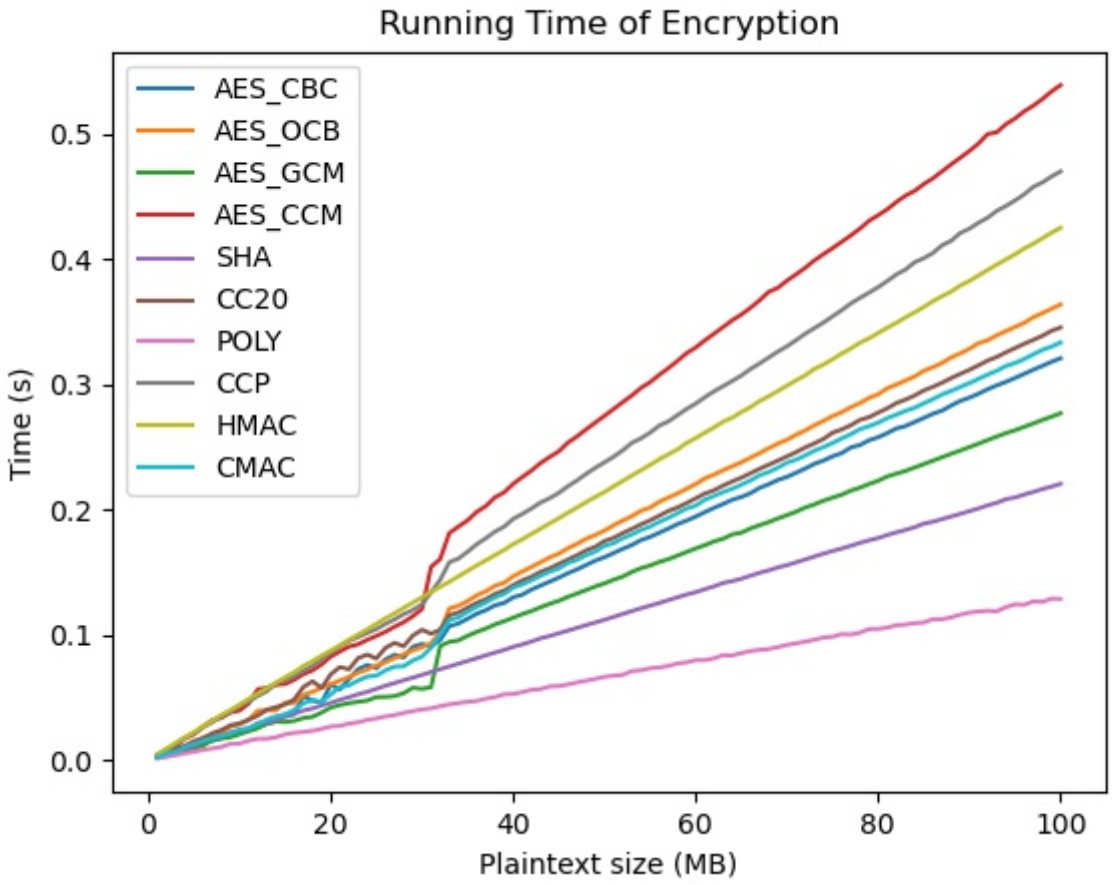
```
$ python3 task4.py
```

Parameters

- `--runs` : This code will run for n runs for averaging the running time. The default value is `1`.
- `--max_file` : This code will generate random files with size from `1` MB to `max_file` MB. The default value is `30`.
- `--rsa` : Use `--rsa` to enable RSA. Since the speed of RSA is extremely slow, please use small runs and max_file with rsa properly.

Output

Output will be a chart of running time of every encryption methods with different size of plaintext, and saved as `time.jpg`.
For example,



Task 5

Usage:

```
$ python3 task5.py
```

Parameters

None.

Output

Output will be printed in terminal directly.
For example,

```
Original key: XxDJmwBW+7AGtUJYHVXiug==
Guessed key:  XxDJmwBW+7AGtUJYHVXiug==
Guessed key is correct.
```