Skyddad.

> It means "protected" in Swedish.

This program was written for Cryptology lesson that's given at Pamukkale University.

Features.

- All mails are encrypted by using **Stream Cipher Algorithm (CFB)**.
- You can simply see if mails are changed. Mail hashes are calculated by using SHA-256 algorithm **crypto/sha256**.

Installation

> This project needs to Go (At least 1.14) to compile.
> Download from **here**.

Get the repo.

```
go get github.com/boratanrikulu/skyddad
```

Set your DB.

This project needs Postgresql DB.
You need to create a database named **skyddad**.

Set your env file.

You need to set database information to env file.
Set `.env` file to wherever you use the skyddad command or `${HOME}/.config/skyddad/.env`

There is a env sample: **here**.

Usage

```
NAME:
   Skyddad - A mail client that keep you safe.

USAGE:
   skyddad [global options] command [command options] [arguments...]

COMMANDS:
   mails      Show all mails that is sent by the user.
   send-mail  Send mail to the user.
   sign-up    Sign up to use the mail mail service.
   help, h    Shows a list of commands or help for one command

GLOBAL OPTIONS:
   --help, -h  show help (default: false)
```

Testing

Creating users.

```
skyddad sign-up --username "testing-user-1" --password "user-1-pass"
```

Excepted result.

```
(✓) User was created.
  Username: testing-user-1,
  Password: user-1-pass,
```

Sending mails.

```
skyddad send-mail --username "testing-user-1" --password "user-1-pass" \
                  --to-user "testing-user-2" \
                  --body "Top secret message."
```

Excepted result.

> Body section would be different.

```
------------------
(✓) Mail was sent.
    ---------
    From: testing-user-1,
    To: testing-user-2
    Date: 2020-03-13 17:12:15.378794251 +0300 +03 m=+0.121973922,
    Hash: f1b8a5f9377b8b77a21eb61234383d5c071aca09cdd20bacbd88dafeef6bf3a4
    Body: [ Encrypted ] 5551f78abe3b48328930b2ab8b99fcab1e0907e2bae90552b73ddd0b5dee6680eb2d8f
------------------
(✓) A mail was sent to "testing-user-1" from "testing-user-2".
```

Sending mail by using custom key.

```
skyddad send-mail --username "testing-user-1" --password "user-1-pass" \
                  --to-user "testing-user-2" \
                  --body "Top secret message by using custom message." \
                  --key "11011001100010101100101001010101"
```

Excepted result.

> Body section would be different.

```
------------------
(✓) Mail was sent.
    ---------
    From: testing-user-1,
    To: testing-user-2
    Date: 2020-03-13 17:12:30.962514735 +0300 +03 m=+0.121759609,
    Hash: 222797e57a004862a373f407b0f74509410b9e141faae0ce80232c9a08c199ca
    Body: [ Encrypted ] b7e32c6a8adf5d633884c6f678b12e13e9176f1d3e28a3e159902cdbdc7c6df1ca98793741ef630a8e6
------------------
(✓) A mail was sent to "testing-user-1" from "testing-user-2".
```

Showing e-mails.

```
skyddad mails --username "testing-user-2" --password "user-2-pass"
```

Excepted result.

```
------------------
To: testing-user-2
    ---------
    (✓) Message is not changed.
    From: testing-user-1,
    To: testing-user-2
    Date: 2020-03-13 17:12:30.962515 +0300 +03,
    Hash: 222797e57a004862a373f407b0f74509410b9e141faae0ce80232c9a08c199ca
    Body: [ Decrypted ] Top secret message by using custom message.
    ---------
    (✓) Message is not changed.
    From: testing-user-1,
    To: testing-user-2
    Date: 2020-03-13 17:12:15.378794 +0300 +03,
    Hash: f1b8a5f9377b8b77a21eb61234383d5c071aca09cdd20bacbd88dafeef6bf3a4
    Body: [ Decrypted ] Top secret message.
------------------
(✓) "2" mails are listed for "testing-user-2" user.
```

Spam attack to the user.

```
skyddad spam-attack --username "testing-user-1" --password "user-1-pass" \
                    --to-user "testing-user-2" \
                    --number-of-mails "5"
```

Excepted result.

```
------------------
(✓) Mail was sent.
    ---------
    From: testing-user-1,
    To: testing-user-2
    Date: 2020-03-13 17:22:46.303585394 +0300 +03 m=+0.125540346,
    Hash: 01bd1caf93137d3d3cb62dc6fdfcbbf807e275619c47ce6e18215b5082c67088
    Body: [ Encrypted ] 68f14fd87497c7caeb3aa2a332e3544ded671037fe306bf9251b44a68546fec4de48ba0a5853177719
    Body Text: luck I mistakenly You, lies. unregistered trust—I visit, I settings original You, trust—I of
------------------
(✓) Mail was sent.
    ---------
    From: testing-user-1,
    To: testing-user-2
    Date: 2020-03-13 17:22:46.309430942 +0300 +03 m=+0.131393907,
    Hash: babcc1aebe05777eb67f4793dd9531d076ad35e61d23fd1d531453807f7816e
    Body: [ Encrypted ] 92be326d6d259c1f9b9c777d2badb7d047f49608a08a61e538a74d54d32c42583952064346616dcbeb
    Body Text: connection became corrupted to to system, Consider when settings disconnected. mistakenly do
------------------
(✓) Mail was sent.
    ---------
    From: testing-user-1,
    To: testing-user-2
    Date: 2020-03-13 17:22:46.313874077 +0300 +03 m=+0.135837041,
    Hash: 37ed96896234a4a69c14258145cb5d7dd7c17fdcbfaa21b92d0f2dcb00af2c78
    Body: [ Encrypted ] 2f4cf58a4971111ab1802d94db57dae2f44e15e772a616aed7b28a629037c6aadb73e993496ecc50b70
    Body Text: process, else's years to been original trusted I You, trust—I now before not I way did a lif
------------------
(✓) Mail was sent.
    ---------
    From: testing-user-1,
    To: testing-user-2
    Date: 2020-03-13 17:22:46.318787882 +0300 +03 m=+0.140750864,
    Hash: 68f395c3c87fe75ec4edc4cfaffcd5f825fe97a7ad7a7ee6115bff2c5975ef40
    Body: [ Encrypted ] ddd377fbe1a2141e286ab5a3d8913cc9c85beb8819b4ffeee5517e08433890630acb2a3b7c7347b89d7
    Body Text: had your You I ago Our way task to wish been initially Our have files. reset broken corrupte
------------------
(✓) Mail was sent.
    ---------
    From: testing-user-1,
    To: testing-user-2
    Date: 2020-03-13 17:22:46.32349206 +0300 +03 m=+0.145455035,
    Hash: d7295f53590754432b67288d13fe66f8126a44a541896d7daec9f5072926f84d
    Body: [ Encrypted ] 28c72233952df7b38e27a16cc64df7122bbf36926a8f053585a3fc179dc1dbc376da6ba72785a1d6057
    Body Text: it. Our before had your link detect. You, else's been became not broken before to ended. to
------------------
(✓) Spam attack has been completed. "5" mails was sent to "testing-user-2".
```

To-Do

- [x] Add end-to-end encryption between users.
- [x] Add custom key feature. (–key)
- [x] Add spam attack feature. (–spam-attack)
- [x] Add hash control feature for checking if message is changed.
- [ ] Add encryption for user passwords.