Skyddad.

> It means “protected” in Swedish.

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

All mails are encrypted by using **Stream Cipher Algorithm (CFB)** [golang.org/pkg/crypto/cipher/#Stream]

Installation

> This project needs to Go (At least 1.13) to compile.
> Download from **here** [golang.org/dl]

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,
    Date: 2020-02-28 16:31:44.348294522 +0300 +03 m=+0.097153476,
    Body: [ Encrypted ] 7e332fd3b2f52103da2b45f50271d290885fabb747947643b66dcca0212c79d5dc113b
```

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,
    Date: 2020-02-28 16:32:00.319808639 +0300 +03 m=+0.110649554,
    Body: [ Encrypted ] 0ef9f4a3a82446e445bf8c3e687d30b7b9cb5afa55c0c34a6b789787d4587159455ff3892b64cf5339d
```

Showing e-mails.

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

Excepted result.

```
To: testing-user-2
    From: testing-user-1,
    Date: 2020-02-28 16:32:00.319809 +0300 +03,
    Body: [ Decrypted ] Top secret message by using custom message.
    ----------
    From: testing-user-1,
    Date: 2020-02-28 16:31:44.348295 +0300 +03,
    Body: [ Decrypted ] Top secret message.
```

To-Do

- [x] Add end-to-end encryption between users.
- [x] Add custom key usage. (–key)
- [ ] Add encryption for user passwords.