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**.
- Mails are signed by using **ED25519 Algorithm**. That is an automatic operation. When you signup to system, private and public keys are created. When you send a mail, the mail will be signed by using your private key. Users checks received email’s signatures by checking from-user’s public key.
- It support sending secret images (Steganography). It use **auyer/steganography** library.

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 keeps you safe.

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

COMMANDS:
   mails        Show all mails that were sent by the user.
   send-mail    Send mail to the user.
   sign-up      Sign up to the mail service.
   spam-attack  Attack to the user with spam mails.
   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: 2020-04-30 19:34:34.435383788 +0300 +03 m=+0.120306794,
    Hash: f1b8a5f9377b8b77a21eb61234383d5c071aca09cdd20bacbd88dafeef6bf3a4
    Signature: 4b1a105d60dfd23d56f80a0fa298452458e20b1ad3f75b77a6dd6d81f67a44057fce4c8ca8aa6b10af5381aa6429
    Body: [ Encrypted ] 5795eb9b062d86a1482aa6c378f5ef1c99e26d98fba30aea99e45ab8fda34ba93c8ca1
------------------
(✓) 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. Hash is same.
    (✓) Message is signed by testing-user-1. That's an real signature.
    From: testing-user-1,
    To: testing-user-2
    Date: 2020-04-30 19:34:34.435384 +0300 +03,
    Hash: f1b8a5f9377b8b77a21eb61234383d5c071aca09cdd20bacbd88dafeef6bf3a4
    Signature: 4b1a105d60dfd23d56f80a0fa298452458e20b1ad3f75b77a6dd6d81f67a44057fce4c8ca8aa6b10af5381aa6429
    Body: [ Decrypted ] Top secret message.
------------------
(✓) "1" mails are listed for "testing-user-2" user.
```

Sending mails that contains secret images.

```
skyddad send-mail --username "testing-user-1" --password "user-1-pass" \
                  --to-user "testing-user-2" \
                  --body "Top secret message." \
                  --secret-message "A message to encode to image." \
                  --image-path "/path/to/F.jpg"
```

Excepted result.

```
------------------
(✓) Mail was sent.
    ----------
    From: testing-user-1,
    To: testing-user-2
    Date: 2020-05-03 03:29:09.338050197 +0300 +03 m=+6.320650255,
    Hash: f1b8a5f9377b8b77a21eb61234383d5c071aca09cdd20bacbd88dafeef6bf3a4
    Signature: 0f3137f99bb5dee5964771cbc7e69173e7a287f2ecc6f0aa061988c0d669095a4299cd8cc8b90d4689ae20eab10d
    Body: [ Encrypted ] 57af225317b106c0af1c5e14799ad34162dbb24fba50ff0be60d83f07ae931da040011
    ----------
    Image: Secret image is attach to mail.
    Image has this secret message: "A message to encode to image."
    ----------
------------------
(✓) A mail was sent to "testing-user-1" from "testing-user-2".
```

Showing mails that contains secret images.

It is same with normal mails.
If image is attached to mail,
you will see the image address and the secret message.

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

Excepted result.

```
------------------
To: testing-user-2
------------------
    (✓) Message is not changed. Hash is same.
    (✓) Message is signed by testing-user-1. That's an real signature.
    From: testing-user-1,
    To: testing-user-2
    Date: 2020-05-03 03:32:37.894067 +0300 +03,
    Hash: f1b8a5f9377b8b77a21eb61234383d5c071aca09cdd20bacbd88dafeef6bf3a4
    Signature: 0f3137f99bb5dee5964771cbc7e69173e7a287f2ecc6f0aa061988c0d669095a4299cd8cc8b90d4689ae20eab10d
    Body: [ Decrypted ] Top secret message.
    ----------
    Image: It containes an secret image.
    Image saved at: "/path/to/secret489931897"
    Image contains a secret message,
    It says: "A message to encode to image."
    ----------
------------------
    (✓) Message is not changed. Hash is same.
    (✓) Message is signed by testing-user-1. That's an real signature.
    From: testing-user-1,
    To: testing-user-2
    Date: 2020-05-03 03:32:27.952383 +0300 +03,
    Hash: f1b8a5f9377b8b77a21eb61234383d5c071aca09cdd20bacbd88dafeef6bf3a4
    Signature: 0f3137f99bb5dee5964771cbc7e69173e7a287f2ecc6f0aa061988c0d669095a4299cd8cc8b90d4689ae20eab10d
    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: 2020-04-30 19:38:13.325474363 +0300 +03 m=+0.117518951,
    Hash: d0c8ac4f1ab67fa73201eef453d51520a72b028c7a23676c6dbeb974ddc14e96
    Signature: 07e0a7b9e57bbc91df760df2cb15ec000cb64cd2e7fb4c15b29698ef7f85b1409b737296f70ae01ef9da9b8955c2
    Body: [ Encrypted ] 15d0593106daf17ab7093356702ad26f8d939a21f97c7d9ff839d8299aec56945988419bcb156496f09
    Body Text: Consider Consider uninstallation Our good of a it. I before my original completed from So de
------------------
(✓) Mail was sent.
    ----------
    From: testing-user-1,
    To: testing-user-2
    Date: 2020-04-30 19:38:13.330720123 +0300 +03 m=+0.122764712,
    Hash: f70c90e43f6945eb422267ad03d95b5fc1123f2c595b2e50da15f2dd199293f1
    Signature: 6050cd086513f693d69f76b856911d3ecbbf1b4c52f1c00e3b4302ac5e731c482d96c2dd9b558817d03f3e8b7fac
    Body: [ Encrypted ] a794b5942125968dd57108849aea3a8ceab839f7c17865216b776762879902f4f161ae3f63976080355
    Body Text: the wish now original process, did You, my uninstallation Our found. luck Consider to years
------------------
(✓) Mail was sent.
    ----------
    From: testing-user-1,
    To: testing-user-2
    Date: 2020-04-30 19:38:13.335537344 +0300 +03 m=+0.127581931,
    Hash: 62201221fd8c5937288a4cbef185b1f1b4f1adb0b5174035a3301d5e610e1979
    Signature: 2cf85768d17647635fb94ed5a12502200536570d6647650d4aa3d00e29f4c4eb6e7c4aa7c454b2828d655ef3faea
    Body: [ Encrypted ] 38190a5e927e6c4d3ec391ae6aae54cfc41a9debe228e08444d21498b3b1f6e860e5aa1a53ac1df009a
    Body Text: now a its So completed unregistered Consider trusted from I task before back relationship, m
------------------
(✓) Mail was sent.
    ----------
    From: testing-user-1,
    To: testing-user-2
    Date: 2020-04-30 19:38:13.339615542 +0300 +03 m=+0.131660132,
    Hash: e55b243174be368b35231915f2ef37ed6812c47fb217df549c494ad54022b049
    Signature: c643a34a87c94b738796d767f36c6aaf8d95dc3a45d244d5005d1f0586aea47806d80d5a6ebd43378325d45e43ff
    Body: [ Encrypted ] c88593acb64e7f57173df8c480311c360d83c590bd997305cf852bb067cfce33b90122164ada90420ae
    Body Text: forbidden have now wish luck initially visit, ended. I your to You your have forbidden forbi
------------------
(✓) Mail was sent.
    ----------
    From: testing-user-1,
    To: testing-user-2
    Date: 2020-04-30 19:38:13.343571884 +0300 +03 m=+0.135616472,
    Hash: a5402043cd8b0d4cf772e18dd30c9bcb4637f28b80d28a28ef6ec34b8291bd42
    Signature: 3604a0f11094920356ee88308253852ec9b6d825a464931bff4ca0e2ace2e27835dab3013b58bcc494e8042e11e2
    Body: [ Encrypted ] 8f5804b26215c9af6841c4f7aba08b4029bf79b194e4c0cedb5449c1d13ccfdf3595f331fb69a530003
    Body Text: 404 Our before in had the its years have files. had five five download in a uninstallation h
------------------
(✓) 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 spam attack feature. (–spam-attack)
- [x] Add hash control feature for checking if message is changed.
- [x] Add electronic signatures for e-mails.
- [x] Add secret image option (Steganography).
- [ ] Add encryption for user passwords.