# SafeBox
# Partilha criptográfica de ficheiros
# Parte 1

Miguel Vicente 63832
Joel Pinheiro 65151

# 1 - Objectivos

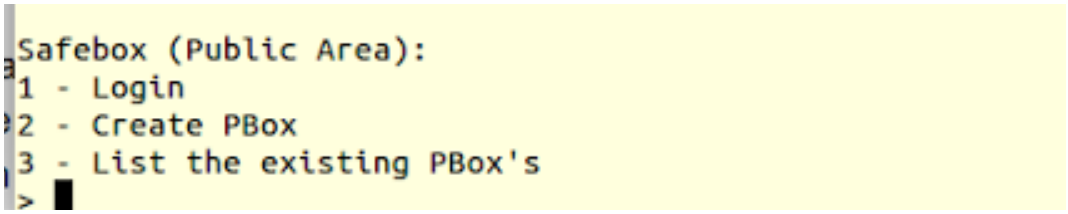
O objectivo da SafeBox é proporcionar ao utilizador um serviço de partilha de ficheiros seguro, independente do servidor, aplicando conteúdos leccionados na cadeira de Segurança.

# 2 - Abordagem

A SafeBox é uma aplicação de consola desenvolvida em Python, que faz uso de um servidor Cherrypy e de uma base de dados relacional desenvolvida em SQLite3. A comunicação entre os dois é feita através de pedidos HTTP.

# 3 - Funcionalidades

3.1 - Área Pública




Este é o menu inicial da SafeBox. Nesta altura o utilizador não possui uma sessão iniciada na SafeBox, assim sendo são lhe apresentadas as seguintes opções:

### 3.1.1 - Login

```
Safebox (Public Area):
1 - Login
2 - Create PBox
3 - List the existing PBox's
> 1
What's your username?
> client
What's your password?
>
```

Caso o utilizador já possua uma conta SafeBox, pode efectuar login na aplicação escolhendo a opção 1 e após inserir as suas credenciais e estas verificadas terá acessos às restantes funcionalidades da SafeBox.

### 3.1.2 - Create PBox

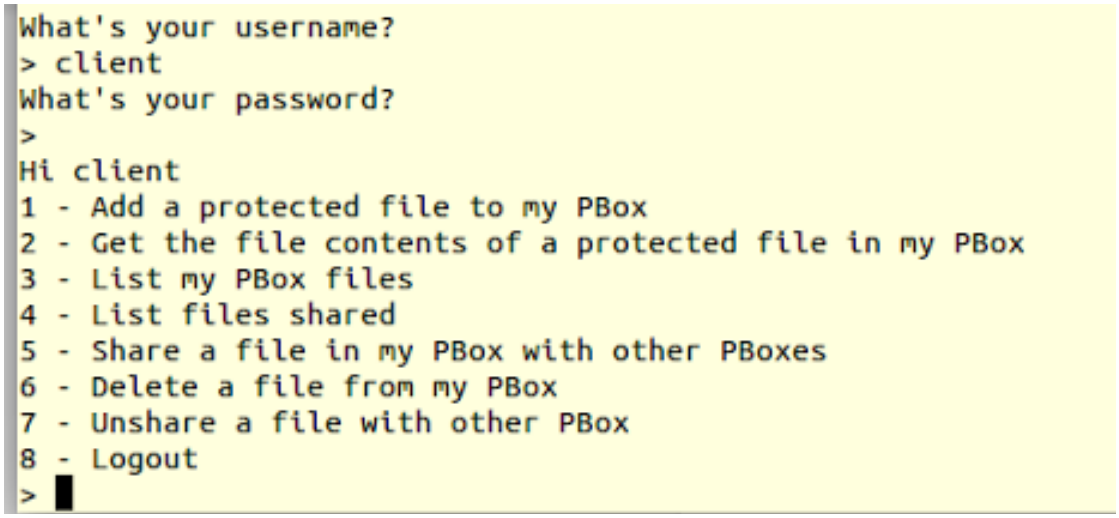
```
Safebox (Public Area):
1 - Login
2 - Create PBox
3 - List the existing PBox's
> 2
Username?
> user1
Password?
>
```

Esta opção permite a um novo utilizador criar uma PBox. Nesta fase da criação de utilizador, são geradas as suas chaves RSA pública e privada para futura cifragem e decifragem de ficheiros.
A chave privada ficará guardada no directório da aplicação de cliente e todos os restantes dados do utilizador são guardados a nível da base de dados. A sua password passa por um processo de hashing com a biblioteca bcrypt e ficará com esse formato na base de dados.

### 3.1.3 Logout

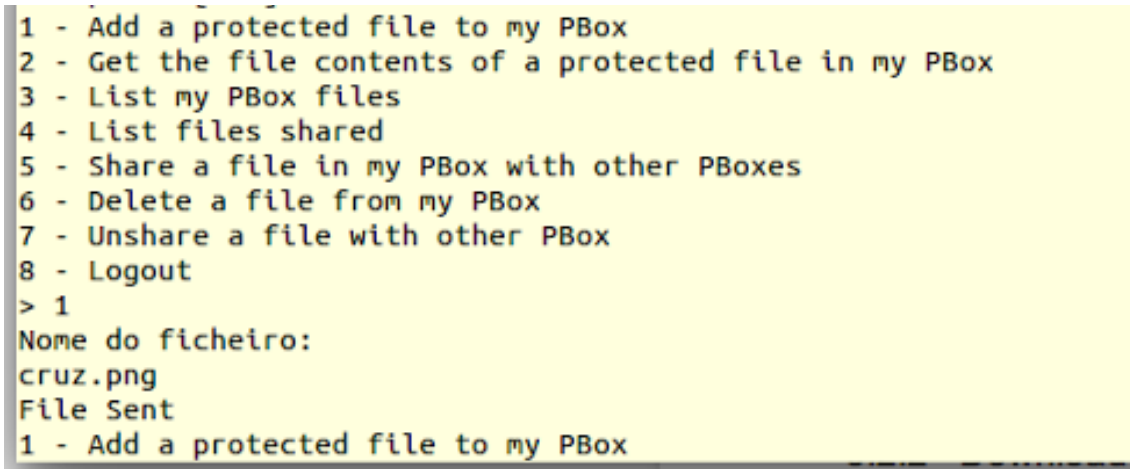
Termina a sessão na aplicação

## 3.2 - Área Restrita




Funcionalidades disponíveis para utilizadores logados na sua PBox.

### 3.2.1 - Upload de ficheiro



A opção de *upload* possibilita ao utilizador enviar um ficheiro para a sua Pbox. Caso o utilizador tente enviar um ficheiro com o mesmo nome de um ficheiro já existente na sua Pbox é lhe perguntado se deseja esmagar o ficheiro já existente. Se aceitar, o ficheiro e todos a meta-informação relativa a este é reescrita. No *upload* do ficheiro é gerada a chave da cifragem simétrica *AES*. Gerado o IV e *Access* e guardado na base de dados. É também adicionada uma entrada na tabela *file* e *sharing* (como *owner*).

3.2.2 - Download de ficheiro

Na opção *download* é imprimida uma lista de ficheiros cuja Pbox tem acesso. De seguida o utilizador seleciona qual o ficheiro que pretende descarregar. É validado se o ficheiro que o utilizador quer existe. O ficheiro cifrado é descarregado aos *chunks*. É decifrado o IV e Access com a chave privada do cliente que está guardada localmente e temos a cifra do AES. Com a cifra de AES deciframos o ficheiro cifrado e gravamos o ficheiro no cliente na mesma pasta onde o cliente está a correr o programa.

3.2.3 - Listagem de ficheiros na PBox do utilizador

É apresentada ao utilizador uma lista de ficheiros a que ele tem acesso na sua PBox, originais ou partilhados.

```
1 - Add a protected file to my PBox
2 - Get the file contents of a protected file in my PBox
3 - List my PBox files
4 - List files shared
5 - Share a file in my PBox with other PBoxes
6 - Delete a file from my PBox
7 - Unshare a file with other PBox
8 - Logout
> 3
7 cruz.png
```

3.2.4 - Listagem de ficheiros partilhados com outros utilizadores

```
Type username to share file with: client
File was shared
None
1 - Add a protected file to my PBox
2 - Get the file contents of a protected file in my PBox
3 - List my PBox files
4 - List files shared
5 - Share a file in my PBox with other PBoxes
6 - Delete a file from my PBox
7 - Unshare a file with other PBox
8 - Logout
> 4
7 cruz.png client
```

É apresentada ao utilizador uma lista com os ficheiros que o utilizador partilhou com outros utilizadores e o respectivo nome de utlizador.

3.2.5 - Partilhar um ficheiro com outro utilizador

```
Hi client2
1 - Add a protected file to my PBox
2 - Get the file contents of a protected file in my PBox
3 - List my PBox files
4 - List files shared
5 - Share a file in my PBox with other PBoxes
6 - Delete a file from my PBox
7 - Unshare a file with other PBox
8 - Logout
> 5
Select file to share
ID | Path
7 cruz.png

ID: 7
Type username to share file with: client
File was shared
```

Permite ao utilizador partilhar um ficheiro com outro utilizador. É apresentada ao utilizador a sua lista de ficheiros, da qual ele deve escolher o que quer partilhar e de seguida inserir o nome de utilizador com quem pretende partilhar.
A lógica de partilha segura do ficheiro passa por obter do servidor a chave pública do utilizador ao qual se vai dar acesso e a chave *AES* e o vector de inicialização (cifrados) do respectivo ficheiro.
No aplicação de cliente é decifrada a chave AES e o vector de inicialização com a chave privada do utilizador e recifrados com a chave pública do novo utilizador que irá ter acesso ao ficheiro.
É adicionado um novo registo na base dados na tabela de *sharings*, com a identificação do ficheiro, a recifra dos dados de acesso ao ficheiro, a identificação do utilizador que obteve acesso ao ficheiro e a identificação do utilizador que lhe deu acesso ao ficheiro.

3.2.6 - Apagar um ficheiro da minha PBox
Na opção apagar um ficheiro é imprimido uma lista de ficheiros que aquele utilizador é *owner*. É validado se o utilizador selecionou um dos ficheiros da lista. Se sim, são eliminadas todas as entradas da tabela sharing que estejam associadas aquele ficheiro e também a entrada na tabela file do ficheiro que se está a remover. No final, o ficheiro é efectivamente removido da safebox para sempre.

# 4 - Limitações

Existem alguma limitações de utilização da SafeBox nesta fase.

-Na criação de uma SafeBox, o cliente deverá correr num directório que não possua nenhuma chave privada, pois a criação de uma PBox irá

gerar uma chave privada nesse mesmo directório, podendo-se perder a chave original

-O upload de um ficheiro, requer que o ficheiro esteja no directório onde a aplicação de cliente está a correr.

-O download de um ficheiro não irá funcionar correctamente caso já exista um ficheiro com o mesmo nome nesse directório.

-O controlo de integridade de ficheiros não obtém um resultado correcto no download de um ficheiro partilhado, pois a aplicação não obtém correctamente a chave HMAC relativa a esse ficheiro.

-O retirar acesso de um ficheiro foi pensado com uma função recursiva que remove os sharings às pbox's que esta deu acesso e por aí diante recursivamente, no entanto, o algoritmo não funciona para todos os casos.

HOWTO

Para correr a aplicação cliente/servidor usamos uma ferramenta chamada VirtualEnv que tem todas as dependências necessárias à execução da aplicação não sendo assim necessário instalar nenhum módulo.
Para correr a aplicação cliente:

- Ir para o diretório do Client:
- Executar o comando: veclient/bin/python client.py

Para correr a aplicação do Server:

- Ir para o diretório do Server:
- Executar o comando: veserver/bin/python SafeBox.py