Projeto: Criptografia

Segurança Informática e nas Organizações

Gonçalo Almeida nº 79994

Hugo Oliveira nº 76322

Alterações Principais relativamente ao projeto inicial:

Como alterações chave na nossa implementação:

1 - Abandonámos a realização manual do algoritmo DH e passámos a gerar um a partilhar do módulo disponibilizado em cryptography.io. Desta forma também, passámos a criar um par de chaves assimétricas a partir da chave partilhada (anteriormente apenas passámos o segredo partilhado por uma função de síntese, garantindo assim maior segurança na comunicação.

2 - Passámos a garantir a integridade das mensagens com controlo por MAC de forma seguindo a norma Encrypt-then-MAC

3 - Conseguimos implementar a rotação de chaves que anteriormente não tinha ficado bem demonstrada por falhas na nossa solução desenvolvida

Introdução

Este trabalho tem como objetivo avaliar competências adquiridas nas aulas em criptografia.

Para isso, foi-nos apresentado um trabalho que consiste na criação de um canal seguro entre um cliente e um servidor tornando a comunicação entre eles segura através do envio de informação cifrada.

Protocolo

A comunicação entre o servidor e o cliente começa através de uma troca de chaves de **Diffie-Hellman** que permite que duas partes que não possuem conhecimento a priori de cada uma, compartilhem uma chave secreta sob um canal de comunicação inseguro. Tal chave pode ser usada para encriptar mensagens posteriores usando um esquema de cifra de chave simétrica.

Depois passamos para a negociação de algoritmos. Para tal usamos os seguintes:

Cifras Simétricas:

AES

ChaCha20

3DES

Modos de Cifra:

GCM

CBC

Algoritmos de Síntese:

SHA256

SHA384

SHA512

O cliente envia para o servidor todas estas opções, que irá escolher aleatoriamente uma opção para cada algoritmo. Apos isto irão ser criadas as respetivas chaves.

Neste momento a comunicação pode começar.

O cliente envia o nome do ficheiro para o servidor e este cria um ficheiro na pasta files onde será guardado o conteúdo do ficheiro do cliente.

O servidor responde com uma mensagem OK e o cliente começa a enviar o conteúdo do ficheiro para o servidor em mensagens tipo DATA.

Dentro destas mensagens o conteúdo vai encriptado.

Uma vez no servidor, o conteúdo da mensagem é desencriptado e guardado no ficheiro previamente criado pelo servidor.

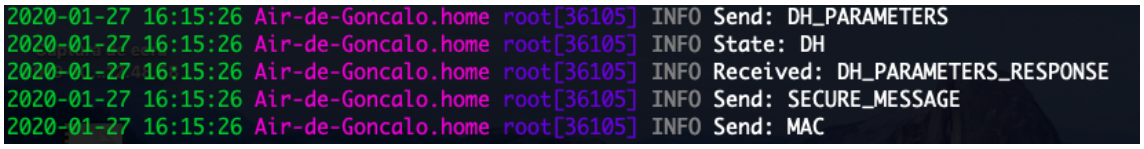
Por medidas de segurança, irá ocorrer uma rotação das chaves sempre que o cliente enviar um novo ficheiro.

Capturas de ecrã

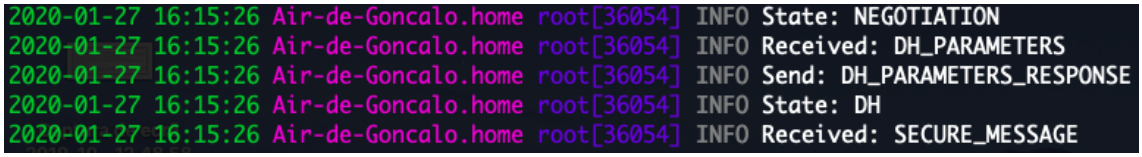
Negociação e chaves:

Diffie-Hellman

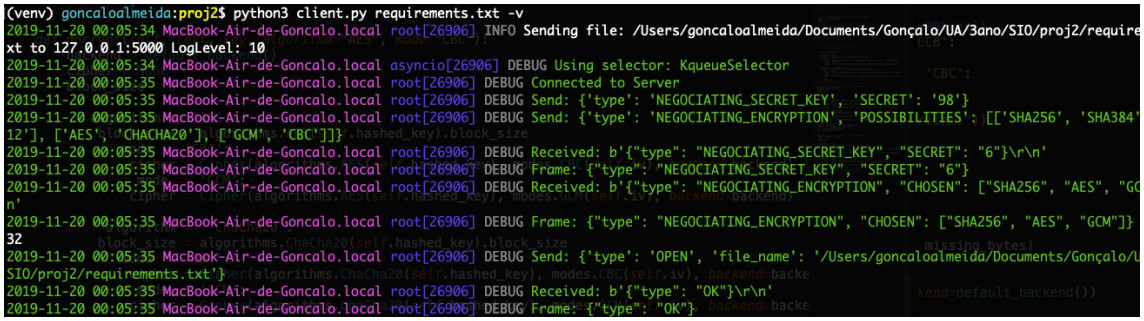
Cliente

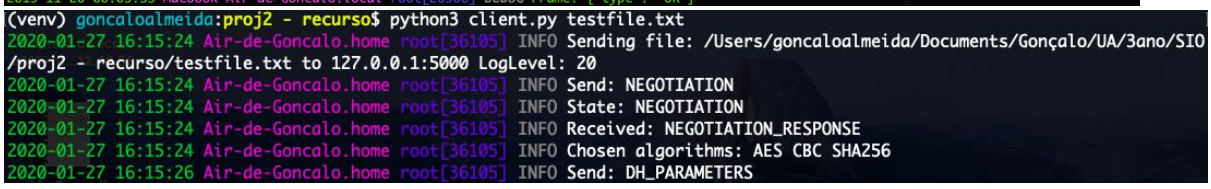


Servidor

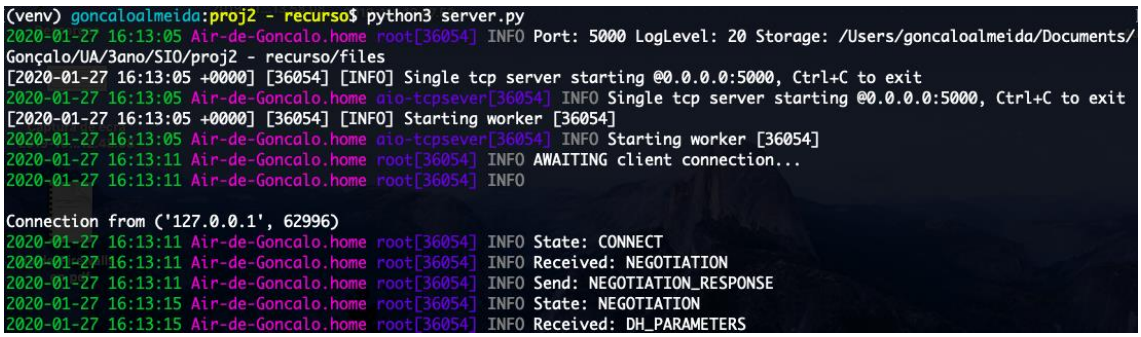


Cliente:



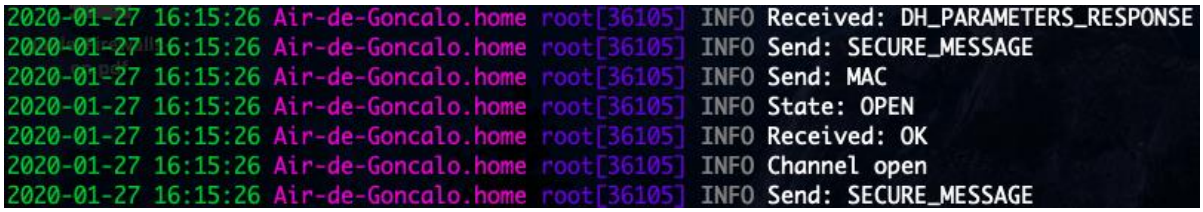


Servidor:

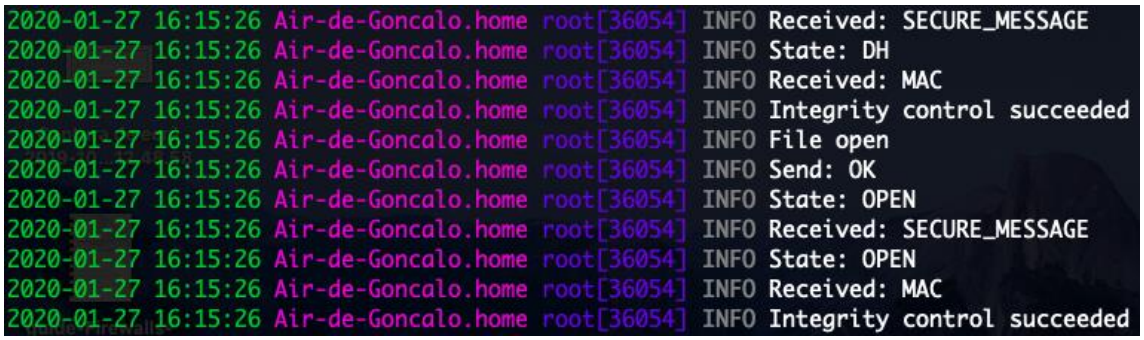


Abrir conexão:

Cliente:

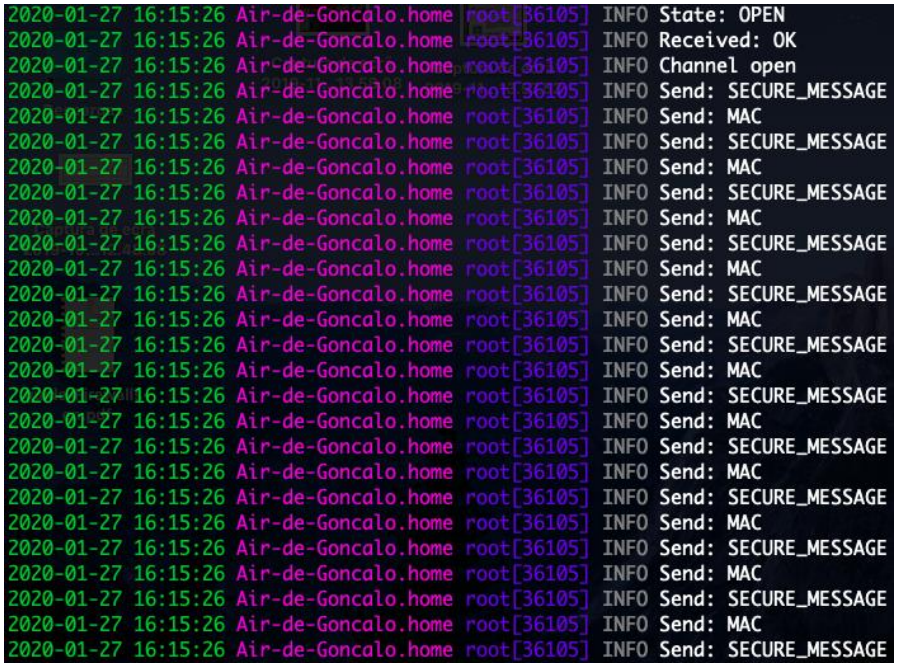


Servidor:



Processamento de Dados:

Cliente:



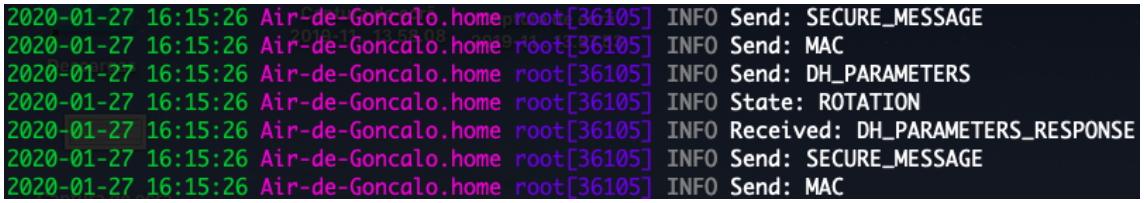
```
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO State: OPEN
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Received: OK
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Channel open
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: SECURE_MESSAGE
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: MAC
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: SECURE_MESSAGE
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: MAC
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: SECURE_MESSAGE
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: MAC
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: SECURE_MESSAGE
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: MAC
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: SECURE_MESSAGE
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: MAC
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: SECURE_MESSAGE
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: MAC
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: SECURE_MESSAGE
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: MAC
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: SECURE_MESSAGE
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: MAC
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: SECURE_MESSAGE
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: MAC
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: SECURE_MESSAGE
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: MAC
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: SECURE_MESSAGE
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: MAC
2020-01-27 16:15:26 Air-de-Goncalo.home root[36105] INFO Send: SECURE_MESSAGE
```

Servidor:

```
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO State: OPEN
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO Received: SECURE_MESSAGE
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO State: OPEN
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO Received: MAC
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO Integrity control succeeded
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO State: DATA
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO Received: SECURE_MESSAGE
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO State: DATA
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO Received: MAC
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO Integrity control succeeded
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO State: DATA
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO Received: SECURE_MESSAGE
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO State: DATA
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO Received: MAC
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO Integrity control succeeded
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO State: DATA
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO Received: SECURE_MESSAGE
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO State: DATA
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO Received: MAC
2020-01-27 16:15:26 Air-de-Goncalo.home root[36054] INFO Integrity control succeeded
```

Rotação de chaves:

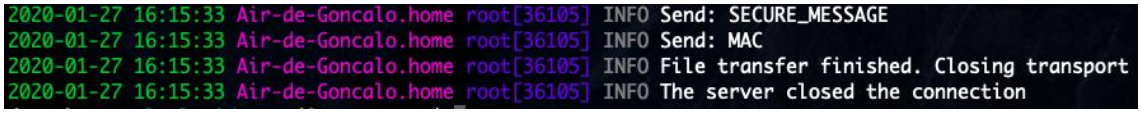
Cliente



Servidor

Término do processo

Após o envio de todos os blocos que constituem o ficheiro, o cliente envia uma mensagem do tipo CLOSE através do método Confidencialidade e termina sua conexão com o servidor:



Conclusão

Com a realização deste trabalho, sentimos que conseguimos alcançar as metas estipuladas para o desenvolvimento do mesmo. Assim, conseguimos também colocar em prática e ainda descobrir um pouco mais do que o que aprendemos sobre comunicações seguras no que concerne os mecanismos para garantir o nível segurança minimamente exigido para tal.