UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
INSTITUTO METRÓPOLE DIGITAL
BACHARELADO EM TECNOLOGIA DA INFORMAÇÃO

RELATÓRIO: **implementação de Chat Seguro**

ACSA LAIANE ARCANJO AUGUSTO
GABRIEL MARTINS SPÍNOLA

NATAL, RN
2019

ACSA LAIANE ARCANJO AUGUSTO
GABRIEL MARTINS SPÍNOLA

RELATÓRIO: **implementação de Chat Seguro**

Relatório apresentado como requisito para obtenção de aprovação na disciplina Segurança de Redes, no Curso de Bacharelado em Tecnologia da Informação , na Universidade do Rio Grande do Norte.
Prof. Dr. Silvio Costa Sampaio

NATAL, RN
2019

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

O projeto trata-se de uma aplicação para troca de mensagens de texto (estilo chat) de maneira que seja possível a troca entre pares utilizando criptografias específicas.

O objetivo em si é executar os algoritmos de criptografias Simple DES (S-DES), Rivest Cipher 4 (RC4) e o de troca de chaves Diffie-Hellman, e usá-los na implementação do Chat com sistema interno de criptografia de mensagem, usando uma porta 5354, com socket TCP. No qual, ambos os pares geram chave de segurança (com o Diffie-Hellman) e essa poderá ser modificada pelo usuário em tempo de execução da aplicação, bem como o algoritmo de criptografia utilizado (S-DES ou RC4).

Esse trabalho foi implementado nas linguagens de Python e em C++, sendo dividido em quatro partes. Dentre elas, a implementação de cada algoritmo de criptografia para cifrar e decifrar, tal como o S-DES em python e o RC4 em C++, com leitura do arquivo que contém a mensagem e decodificando também em um arquivo. E os demais em python, como o algoritmo de troca de chaves Diffie-Hellman e o do próprio Chat que faz uso dos códigos (adaptados a classes em python) anteriormente citados.

2. COMO EXECUTAR

Para mudar a criptografia para o modelo SDES, utiliza-se o comando ‘\crypt sdes’ .

Certifique-se de que já existe outro usuário conectado para usar os comandos de alteração de criptografia.

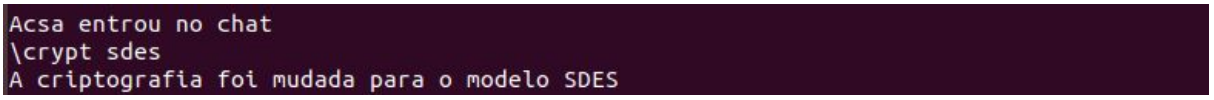


Figura 1 - mudando criptografia para SDES

Para mudar a criptografia para o modelo RC4, utiliza-se o comando ‘\crypt rc4’.

Figura 2 - mudando criptografia para RC4

Para desabilitar a criptografia e enviar as mensagens do jeito que foi enviado de um cliente para o outro, utiliza-se o comando ‘\crypt none’.

Figura 3 - Desabilitando criptografia

O comando ‘\commands’ imprime todos os comandos disponíveis no cliente.

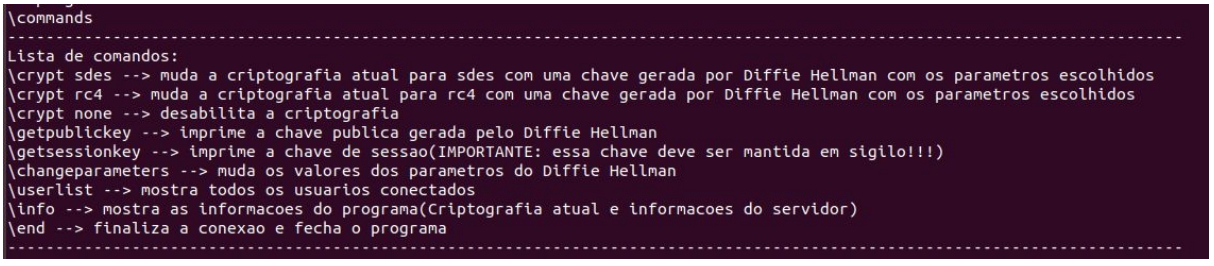


Figura 4 - mostrando todos os comandos do programa

O comando ‘\getpublickey’ imprime a chave pública do cliente que foi gerado a partir dos parâmetros que foram inicializados na abertura do programa.

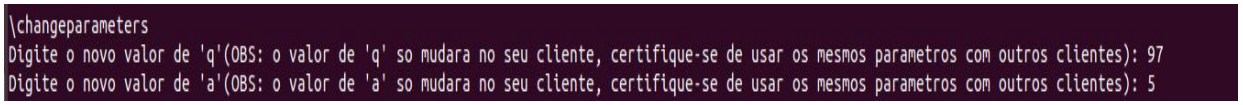
Figura 5 - imprimindo chave pública

O comando ‘\getsessionkey’ imprime a chave de sessão. IMPORTANTE: essa chave deve ser mantida em sigilo.

Figura 6 - imprimindo chave de sessão

O comando ‘\changeparameters’ muda os parâmetros utilizados para gerar a chave pública pelo algoritmo Diffie Hellman.

Figura 7 - alterando parâmetros



O comando ‘\userlist’ imprime os usuários conectados ao chat.

Figura 8 - imprimindo usuários conectados

O comando ‘\info’ imprime as informações sobre a criptografia que está sendo utilizada no momento, a qual servidor está conectado e os parâmetros sendo utilizados pelo algoritmo Diffie Hellman.

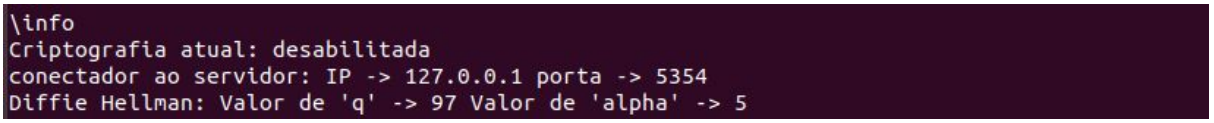


Figura 9 - imprimindo informações

O comando ‘\end’ finaliza o cliente.

Figura 10 - finalizando cliente chat seguro

3. SAÍDA DO PROGRAMA

Figura 11 - Saída do terminal, algoritmo para criptografia RC4 feito no c++

Para inicializar o servidor utilize a linha de comando ‘python servidorChat.py IPdoServidor’.

Figura 12 - Saída do terminal, servidor chat seguro

Para inicializar o cliente utilize a linha de comando ‘python clienteChat.py IPdoServidor ‘SeuNick’ ‘parametro Diffie Hellman q’ ‘parametro Diffie Hellman alpha’.

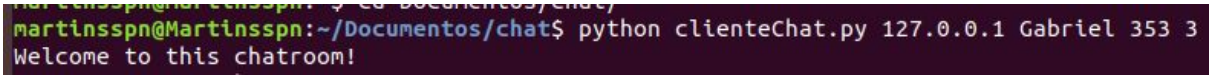


Figura 13 - Saída do terminal, cliente chat seguro

4. CONSIDERAÇÕES FINAIS

Este trabalho apresentou a implementação dos algoritmos criptográficos S-DES, RC4, e o de troca de chaves Diffie-Hellman. Esses utilizados na implementação do Chat Seguro, com sistema interno de escolha de cifra das mensagens, fazendo uso do código do Diffie-Hellman para gerar a chave inicial.

Além disso, com o objetivo de visualizar o funcionamento das criptografias especificadas e observá-las em uma aplicação simples, tal como o Chat, usando uma porta particularizada, com socket TCP, constatando um dos pilares para ajudar a delimitar e incrementar o nível de segurança da aplicação. Também podendo avaliar o nível de eficiência e praticidade oferecido por cada uma.

5. REFERÊNCIAS

GeeksforGeeks A computer science portal for geeks. Simple Chat Room using Python. Disponível em <https://www.geeksforgeeks.org/simple-chat-room-using-python>. Acesso em 05 de setembro de 2019.