Sprint 1

Segurança de Aplicações e Dados

Rúben Medeiros (1201679)

Docentes:

Marelo Santos

Vladir Vicente

Data: 25/11/2022

Índice

[Introdução 3](#_Toc120288076)

[Carregar Plugboard 4](#_Toc120288077)

[Substituir as Letras da Plugboard 5](#_Toc120288078)

[Salt para Testes de KAT 6](#_Toc120288079)

[Salt para realizar o Brute Force 7](#_Toc120288080)

[Cifra de Ceaser 8](#_Toc120288081)

[Execução dos Testes KAT 9](#_Toc120288082)

[Ler o Ficheiro da Wordlist 10](#_Toc120288083)

[SHA-512 11](#_Toc120288084)

[Brute Force 12](#_Toc120288085)

[Password Final 13](#_Toc120288086)

[Conclusão 14](#_Toc120288087)

# Introdução

Foi proposta pelos docentes Marcelo e Vladir a realização de uma cifra chamada “Cifra de Ceaser”.

Cifra de Ceaser é um dos métodos mais antigos e mais conhecidos da criptografia. Esta cifra baseia-se numa substituição do alfabeto. Com isto quero dizer que a mensagem de input chega a um *plugboard*, onde este é diferente de aluno para aluno, passando de seguida por rotores e volta novamente ao *plugboard* para mostrar a mensagem alterada.

Este trabalho teve a ajuda de dois colegas meus: “Diogo Sousa e André Padilha” que se disponibilizaram para me ajudar durante toda a realização do projeto.

# Carregar Plugboard

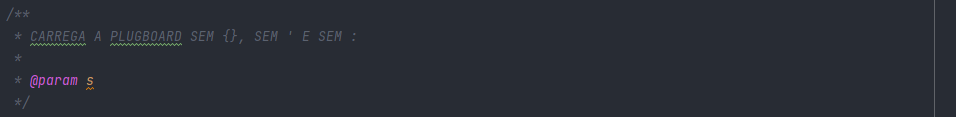
Inicialemente comecei por carregar a plugboard e com isso utilizei uma variável estática e final, no qual tem a minha plugboard que os professores forneceram no enunciado.

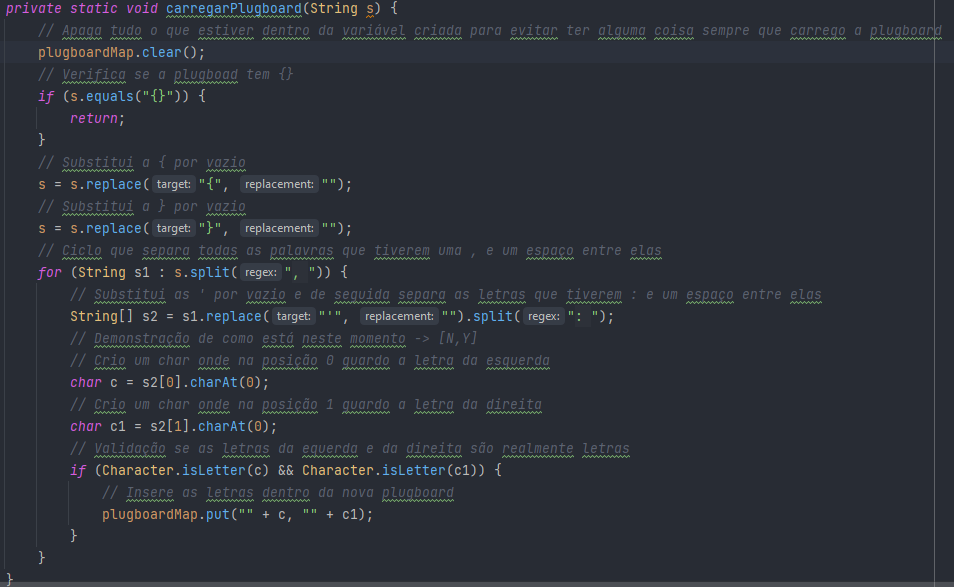


De seguida, criei outra variável onde vai conter a minha plugboard com apenas as letras.



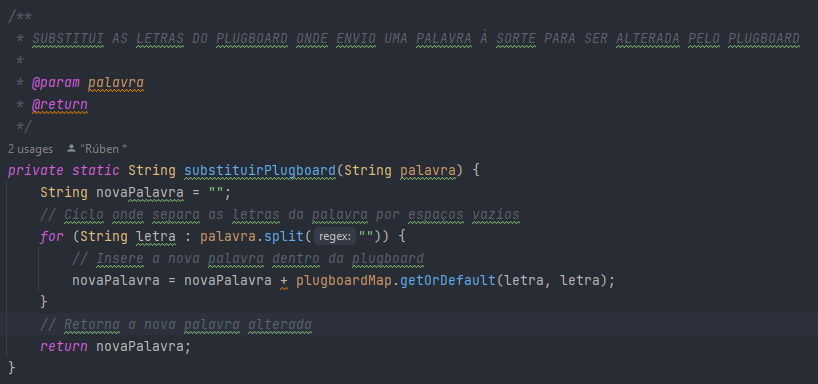
Finalmente criei o método para carregar a plugboard.





# Substituir as Letras da Plugboard

Para ver se a plugboard estava a funcionar, devidi criar um método onde inseria uma palavra a meu gosto e verificava através do plugboard se as letras da palavra tinham sido alteradas.



# Salt para Testes de KAT

Para realizar todos os testes KAT tive que inicialmente criar uma variável com todas as letras do alfabeto.



Depois disso, criei o método para fazer o salt, tanto à esquerda do alfabeto, tanto à direita.

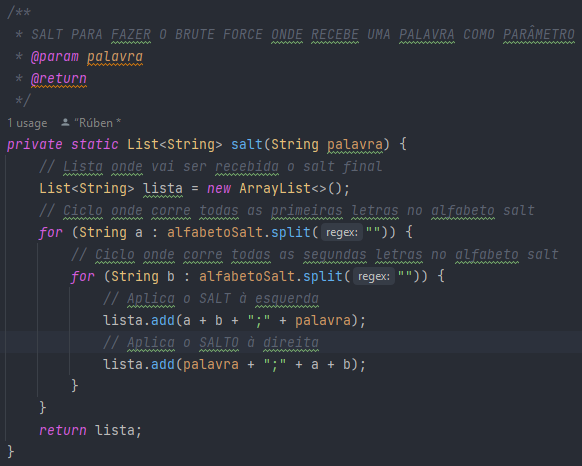


# Salt para realizar o Brute Force

Depois de ter criado o primeiro salt fiz exatamente a mesma coisa que fiz no método anterior, sendo que a única diferença é que não utilizei o alfabeto normal, mas sim o dado pelo enunciado. Para isso tive que criar uma variável nova com o novo alfabeto.

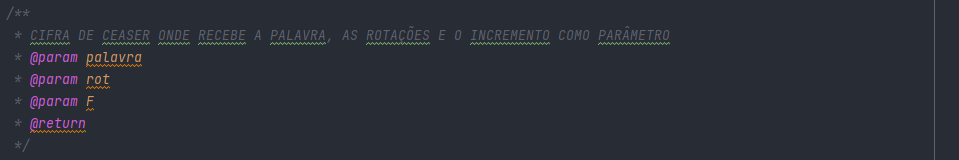


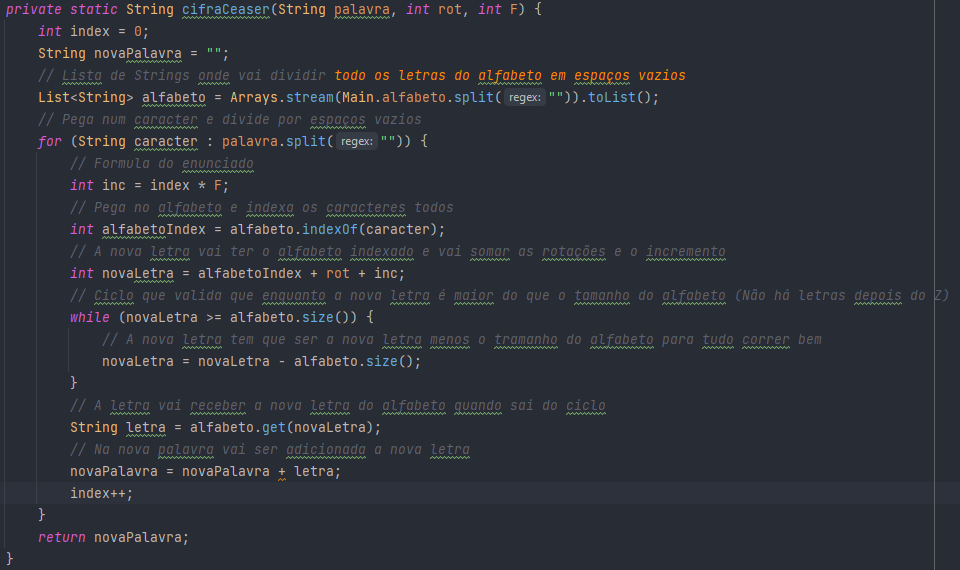
Logo a seguir criei o método para fazer o Salt.



# Cifra de Ceaser

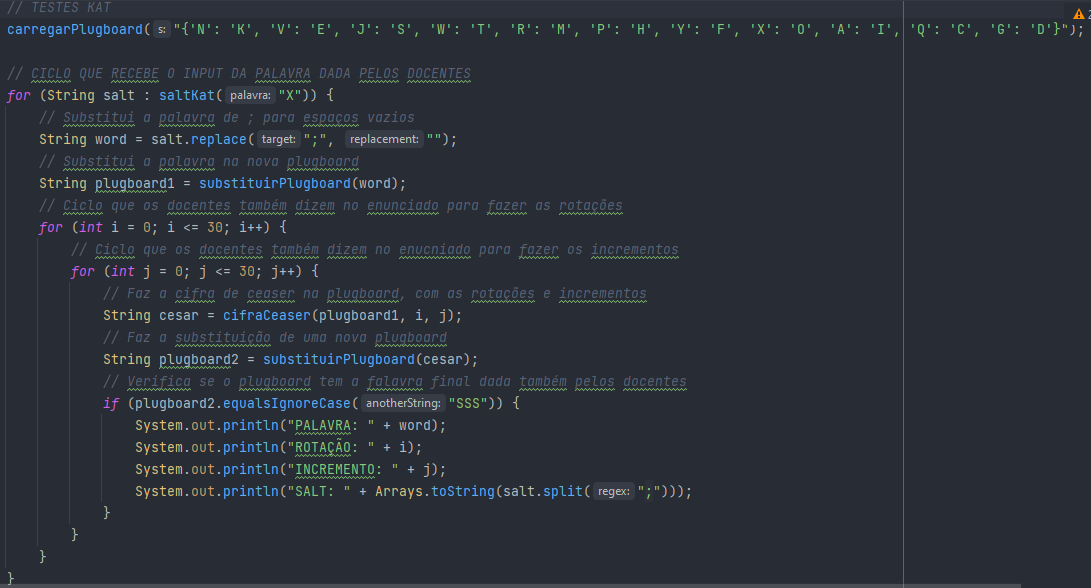
Logo a seguir ao método anterior, resolvi fazer o método para calcular a cifra de ceaser.





# Execução dos Testes KAT

Depois de ter feito o método da cifra de ceaser decidi começar com a realização de todos os testes KAT o que felizmente foram todos bem sucedidos.



# Ler o Ficheiro da Wordlist

Para começar resolvi por criar uma String onde tinha o caminho da wordlist.



De seguida, criei um método simples para ler e guardar o conteúdo do ficheiro numa lista de Strings.



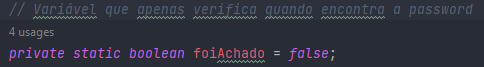
# SHA-512

Nesta parte decidi ir à internet ver métodos para o SHA-512. Confesso que tive bastante dificuldades e a ajuda dos meus colegas neste método foi crucial.



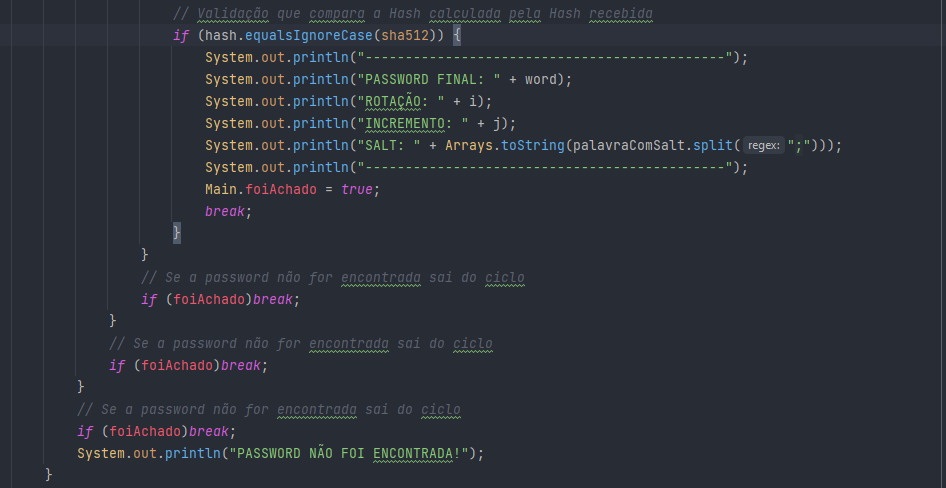
# Brute Force

O meu brute force foi feito dentro do método Main. Com isto, comecei por criar uma variável chamada foiAchado que verifica se encontrou ou não a password.



De seguida foi feito vários ciclos para fazer o Brute Force.





# Password Final

Depois de 5 horas à espera de resultados, o output do brute force foi o seguinte:

Password: JRCFYCI

ROTAÇÃO: 11

INCREMENTO: 8

PALAVRA + SALT: JRCRYF + CI

# Conclusão

Este projeto no sprint 1 não foi de acordo com as minhas espectativas, porque nunca estive com tantas dificuldades como estive com este projeto. Quero desde já agradecer aos meus colegas pelo tempo perdido comigo e pela sua disponibilidade. Neste sprint consegui aprender algumas coisas sobre criptografia e o quanto dificil é para alguém que domina e não domina a área.