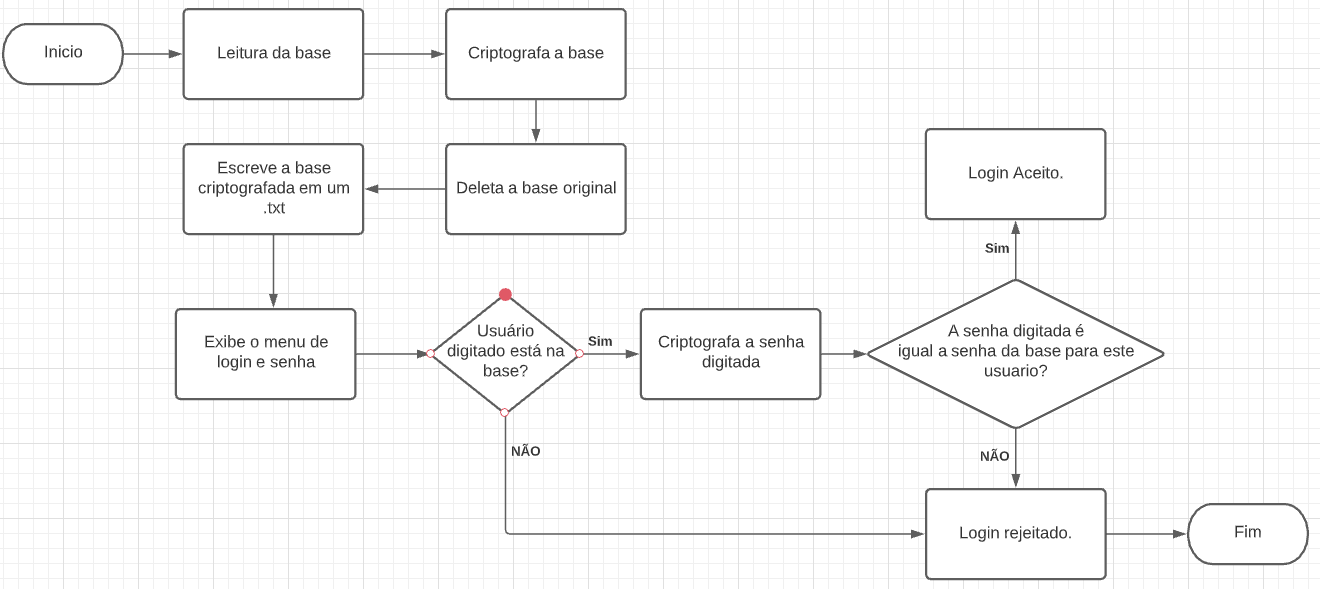
**Projeto 4 – Segurança da Informação**

**Nome:** Guilherme Henrique Moreira. **R.A:** 22117039-2

**Nome:** Victor Antônio de Queiroga. **R.A:** 22117054-1

**Logica do Código.**

O código desenvolvido segue a logica descrita no fluxograma abaixo:



**Logica da Criptografia.**

O método de criptografia funciona da seguinte forma:

Dada uma senha X, colocamos o sulfixo “BANGLAD” caso X[0] for uma letra entre A até G. Caso X[0] for uma letra de G até Z, colocamos o sulfixo “GUIZITH”. Após a função de sulfixo, adicionamos o nome de usuario atrelado a essa senha. Por fim, utilizamos a tecnica de Cifra de César seguindo o alfabeto abaixo:



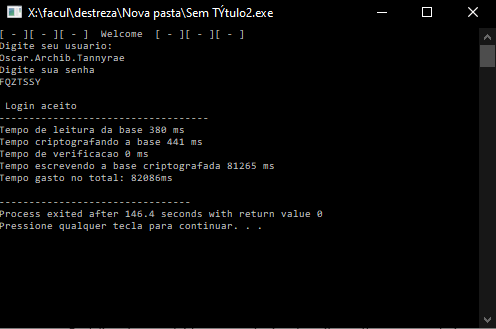
Ou seja, a função de criptografia pode ser dada por:

F(x,y) = ( y + Sulfixo(y) + x )

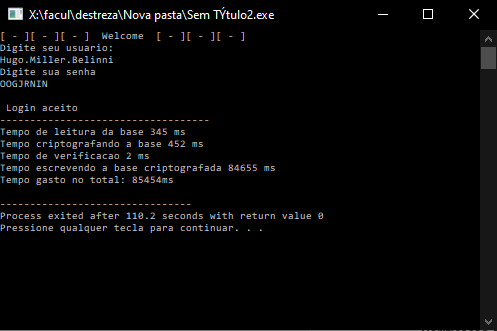
, onde x é o usuário e y é a senha.

**Tempos em validações aceitas.**

Validação do primeiro usuário da base

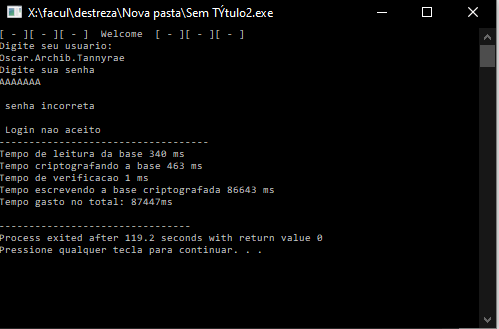


Validação do último usuário da base

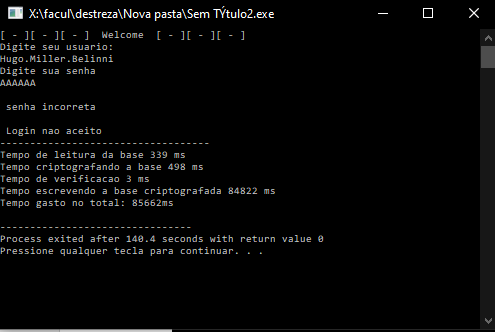


**Tempos em validações rejeitadas.**

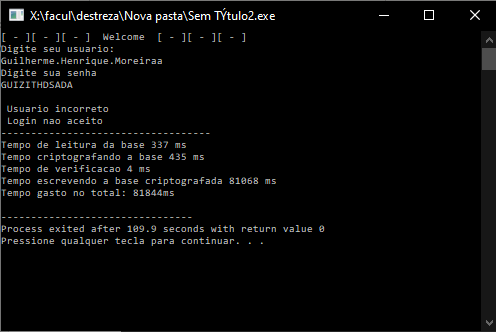
Validação do primeiro usuário da base



Validação do último usuário da base



Validação de usuário não cadastrado.



Podemos observar que o tempo de verificação é bem próximo em todos os casos. Isso se deve a forma como foi feita a validação:

1 - Verificando se o usuário existe (0-4 ms),

2 - Criptografando a senha digitada (0ms)

3 - Verificando se a senha digitada bate com o usuário encontrado (0 ms)

Com isso, temos que o tempo de verificação varia de 0 a 4 milissegundos, com uma média de 2 milissegundos.

**Link do projeto:** <https://github.com/Guizith/SecProj4>