



# **Geração de Chaves Criptográficas Usando Um Algoritmo Bio Inspirado**

**Nicholas B. F. F. Hugueney**

Trabalho de Conclusão de Curso – 2014

Projeto Final I

Orientador: Prof. Dr. Carlos Miguel Tobar Toledo

Coorientador: Micael Cabrera Carvalho

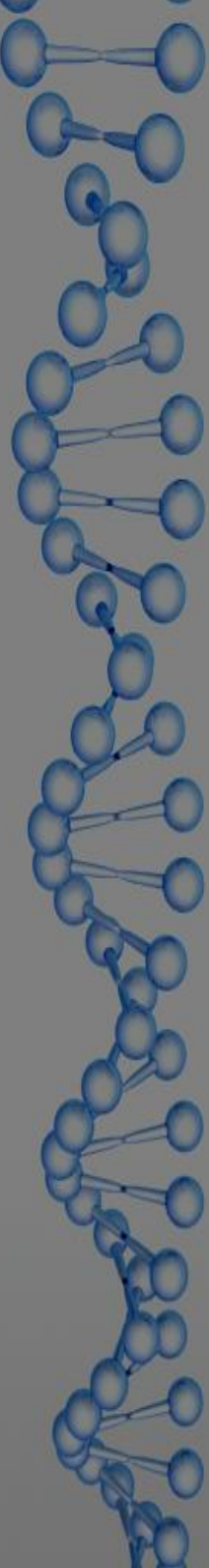


# Introdução

.Chaves criptográficas são usadas para cifrar dados sensíveis;

.PKC (*Public Key Cryptography*) é o modelo mais utilizado atualmente;

.Chaves são classificadas de acordo com sua robustez, característica que promove maior qualidade de segurança ao dado cifrado.



.Segurança por criptografia é refém do poder de processamento das máquinas;

.Cifras podem ser quebradas por força bruta;



# Problema

- .A escolha de uma chave criptográfica robusta não é uma tarefa simples;
- .Se existe uma solução, esta pode sempre ser encontrada por força bruta, basta tempo.
- .Tamanho grande de chave não é suficiente para segurança;
- .Ataques podem ser conduzidos de forma distribuída;



# Objetivo

.Gerar chaves criptográficas robustas.

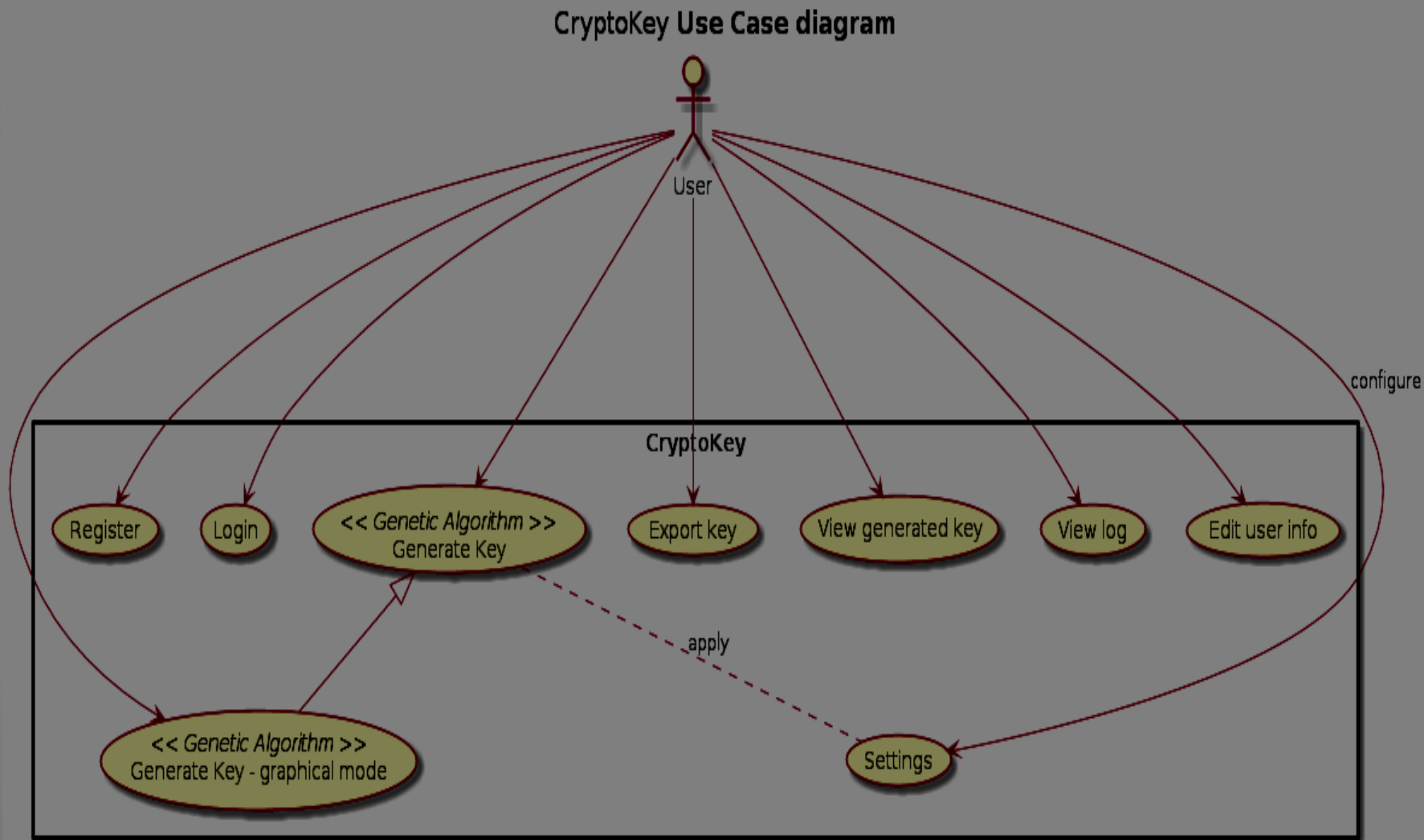


# Diagramas

.Use Case

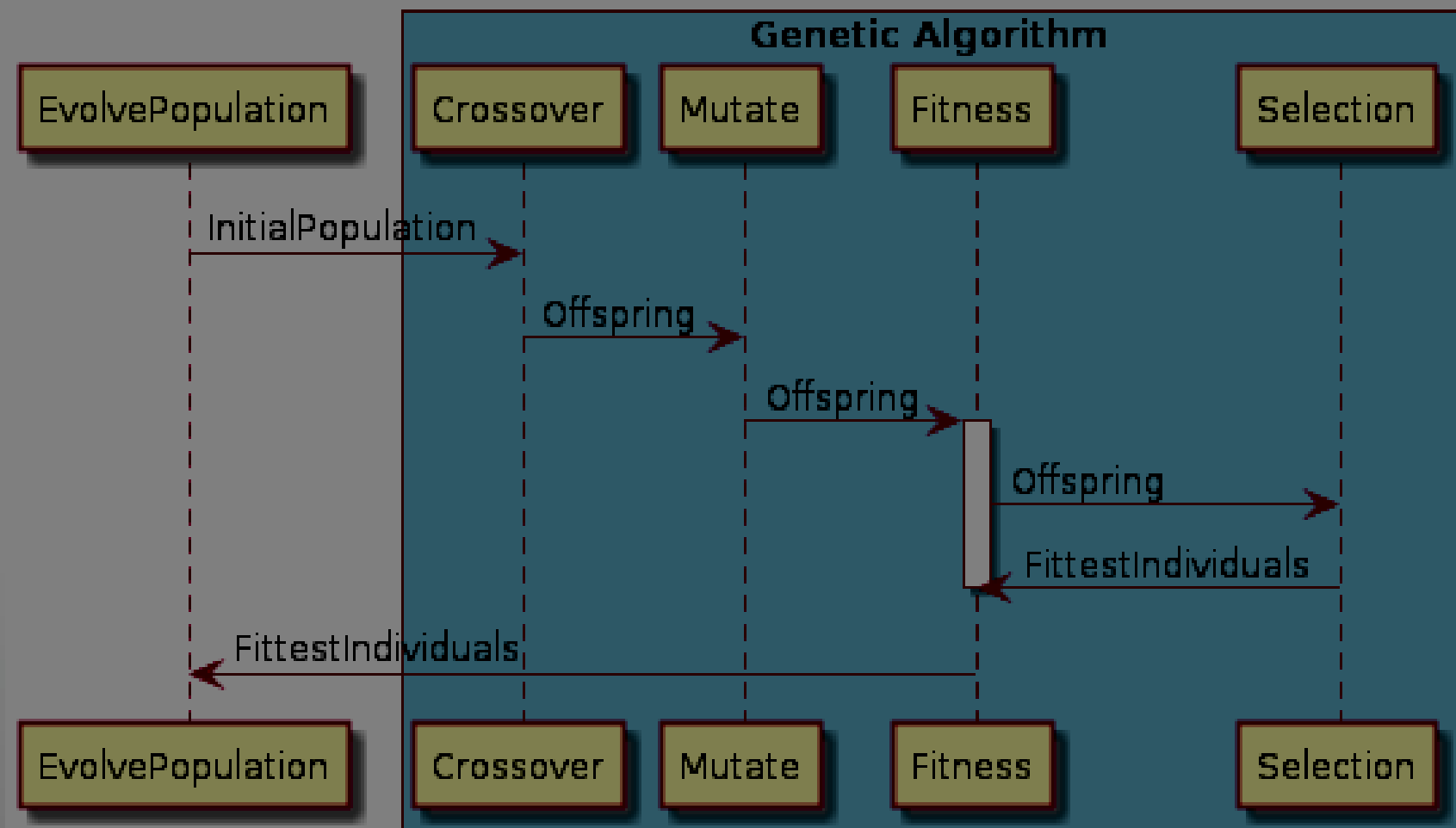
.Sequência (GA)

# Diagrama de Caso de Uso



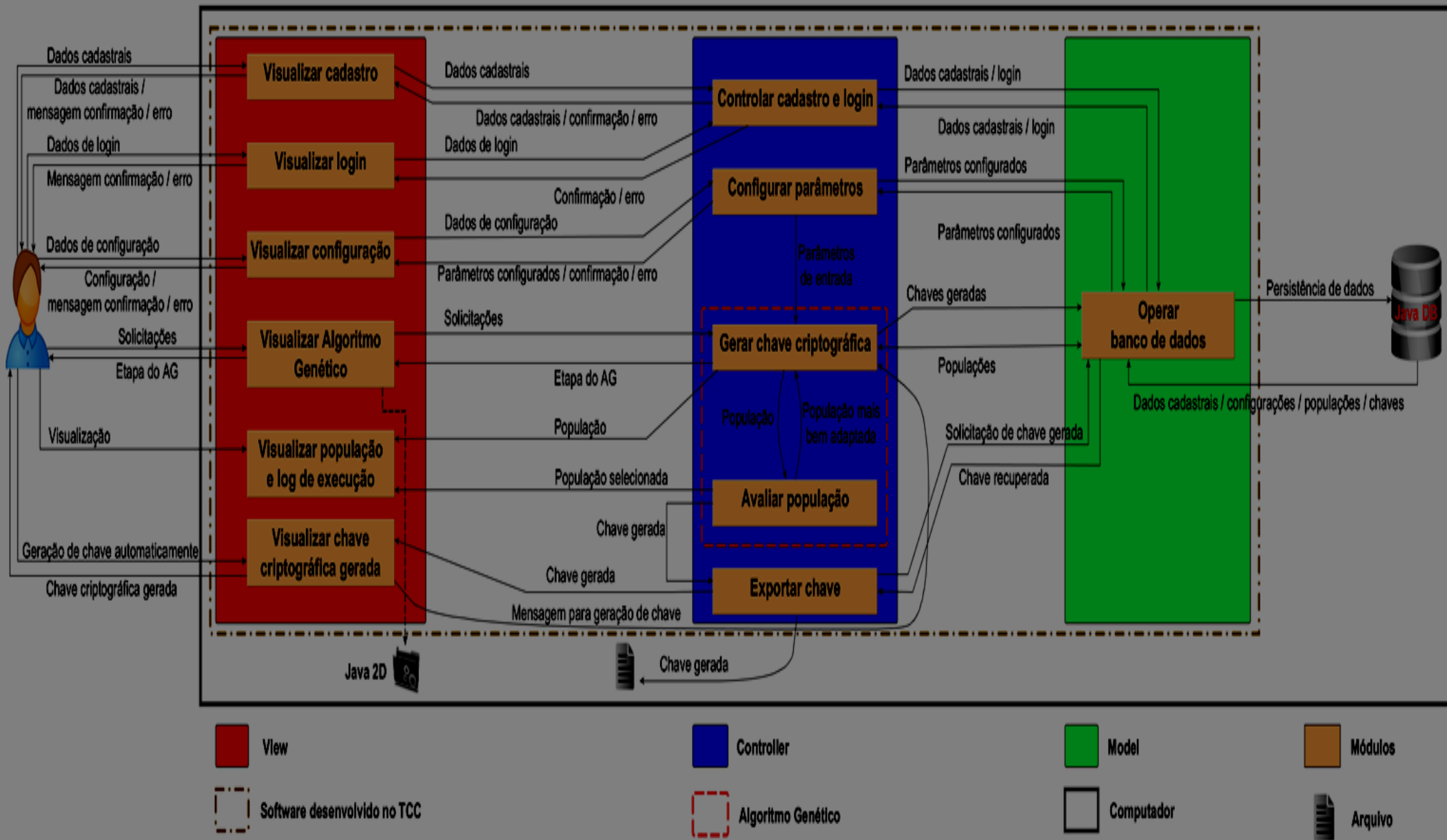
# Diagrama de Sequência (GA)

CryptoKey Genetic Algorithm Sequence diagram





# Diagrama de Arquitetura





# Dificuldades

.Chaves criptográficas;

.Algoritmo Genético (AG);

.Representação gráfica da execução do AG;

.Etapa de *fitness* do AG.



# Plano de Avaliação

.Chaves geradas serão avaliadas através de testes estatísticos:

- *Frequency test* (Pearson's *Chi-square*);
- *Gap test*,

.O sucesso do trabalho será determinado uma vez que os resultados dos testes mostrem que há aleatoriedade na geração de chaves.



## Horas trabalhadas

Durante o desenvolvimento do trabalho, o aluno percebeu que as estimativas de horas de trabalho não foram precisas, de tal forma que o cronograma precisou ser reajustado.

O cronograma, portanto, passou a contar com 7 *sprints* de 30 horas cada.

Essa atualização pode ser observada no plano de trabalho



# Horas trabalhadas

Sprint 1: 34 horas (terminada)

Sprint 2: 63 horas (terminada)

Total trabalhado: 97 horas

Total previsto: 210 horas

Progresso:  $97/210 = 46,19\%$