Universidade Regional de Blumenau
Centro de Ciências Exatas e Naturais

Bacharelado em Ciências da Computação
Trabalho de Conclusão de Curso

Protótipo de software para ocultar texto criptografado em imagens digitais.

Acadêmico: Fábio Luis Tavares Jascone
Orientador: Francisco Adell Péricas

Blumenau, novembro de 2003

Roteiro

- Introdução
- Segurança da Informação
- Criptografia
- Esteganografia
- Criptografia x Esteganografia
- Desenvolvimento do Protótipo
- Considerações finais

Introdução

- Necessidade de melhores mecanismos para garantir segurança das transações de informações confidenciais
- Utilização de criptografia
- Estudo e aplicação de esteganografia

- **Objetivo:**
  - Ocultar e extrair texto criptografado de imagens *bitmap*

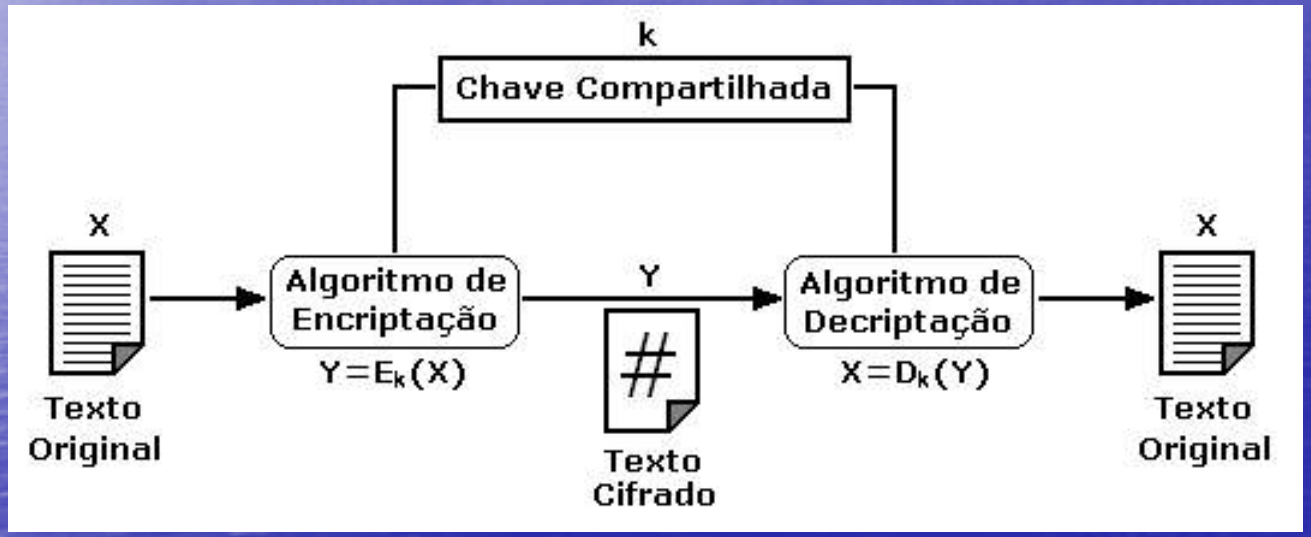
Segurança da Informação

- Conceito:
  - Controlar o acesso a informação
  - Informações de uso restrito não devem ser acessadas por pessoas não autorizadas
  - Codificação da informação
- Mecanismos de Segurança:
  - Criptografia, Assinatura Digital, Integridade dos Dados, Controle de Acesso, Firewall, ...
- Segurança na Internet:
  - Em nível de enlace
  - Entre origem e destino
  - Em nível de aplicativo

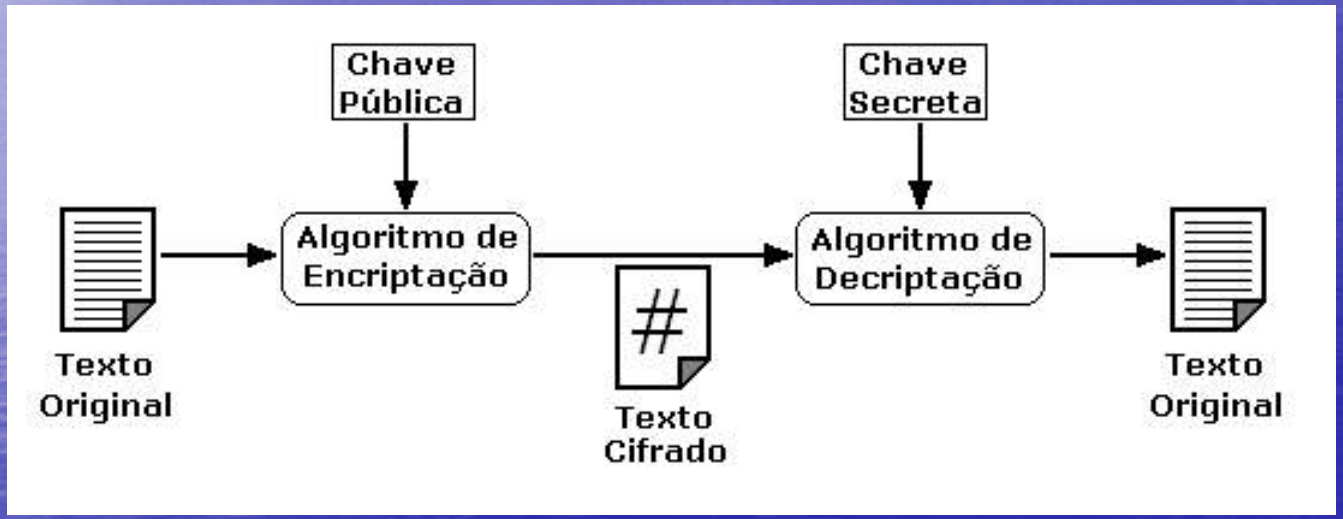
Criptografia

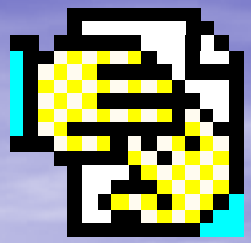
- Arte de escrever em código tornando uma mensagem incompreensível
- Surgiu da necessidade de se enviar informações sensíveis através de meios de comunicação não confiáveis
- Garantir Segurança:
  - Sigilo
  - Integridade
  - Autenticação (usuário, remetente, destinatário e atualidade)
- Algoritmos Criptográficos:
  - Simétrico ou de Chave Secreta (DES, AES)
  - Assimétrico ou de Chave Pública (RSA)

Algoritmo Simétrico



Algoritmo Assimétrico





Esteganografia

- Grego: *stegano* (oculto) e *graphy* (escrita)
- Literalmente significa "escrita encoberta"
- Arte de comunicar-se secretamente
- Oculta uma mensagem sigilosa dentro de uma informação sem importância
- Na computação utiliza áreas de dados pouco significativas ou não utilizadas dos arquivos

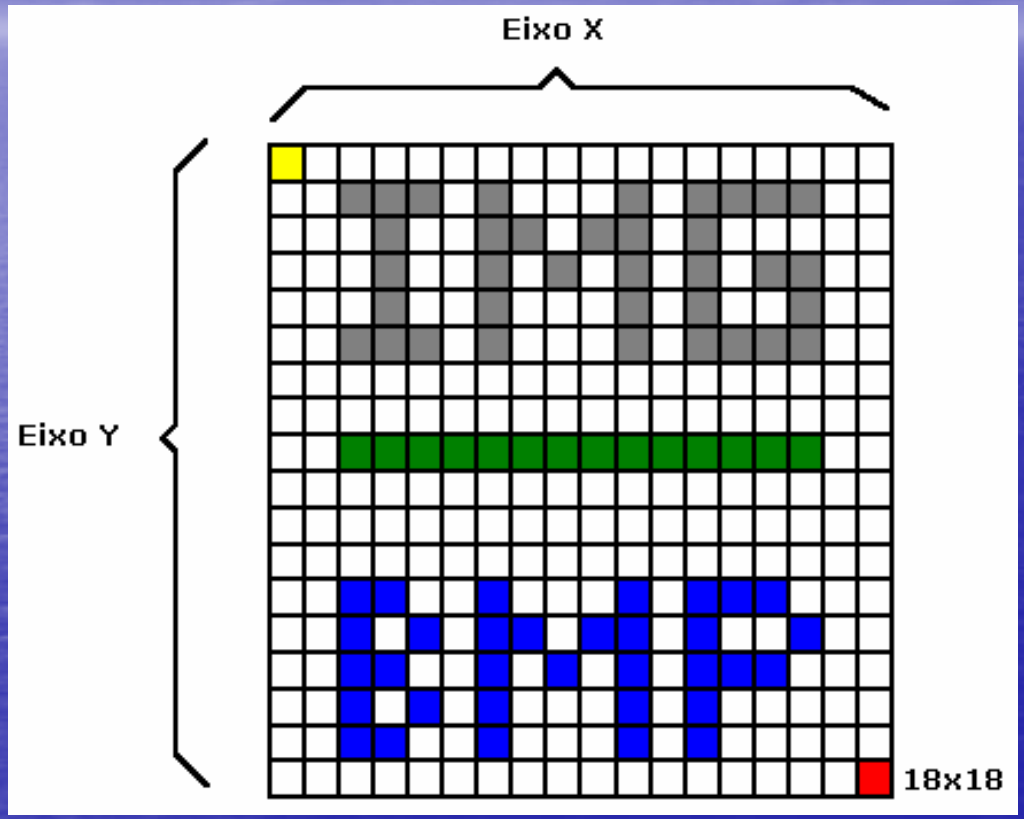
Criptografia x Esteganografia

- Criptografia:
  - Há presença de mensagem
  - Informação ilegível, mas certeza da existência
- Esteganografia:
  - Não há presença explícita de mensagem
  - Dificilmente é detectada

Esteganografia com Imagens

- Imagem: Matriz de números que representam intensidades de cores em vários pontos (*pixel*)
  - 1 *pixel* = 24 bits (16 milhões de cores)
  - *Bitmap* = matriz de *pixels* ou "mapa de bits"
- RGB (*Red*, *Green*, *Blue*): Sistema de cores
  - (0, 0, 0) = cor branco
  - (255, 255, 255) = cor preto
  - (255, 0, 0) = cor vermelho puro
  - (0, 255, 0) = cor verde puro
  - (0, 0, 255) = cor azul puro
- Método LSB: inserção no bit menos significativo

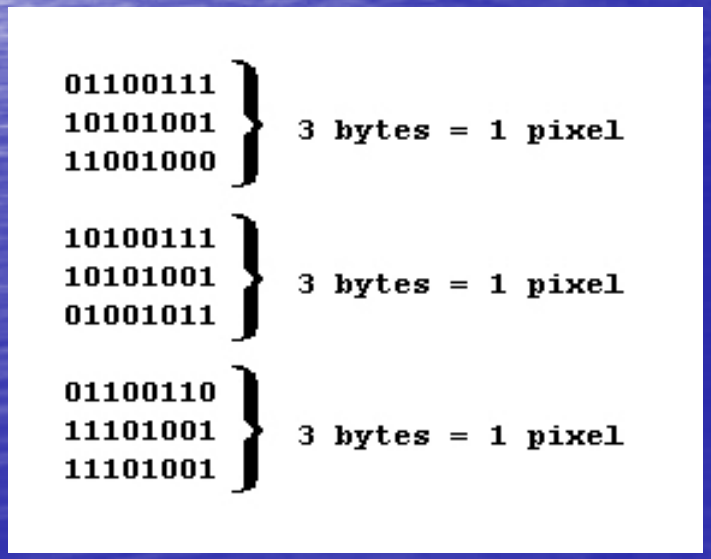
Imagem (*bitmap*)

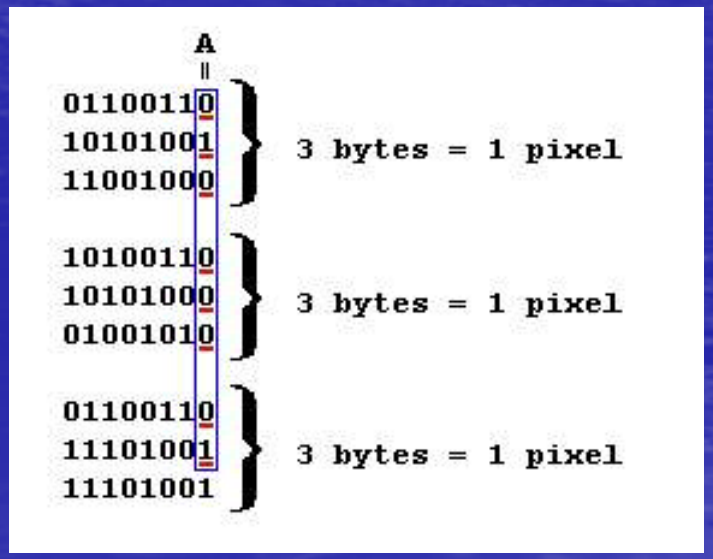


Método LSB

- Mais comum para armazenar informação em imagens
- Utiliza o(s) bit(s) menos significativo(s) de cada *pixel*
- Capacidade de armazenamento:
  - Ex.: Imagem de 24 bits com resolução 800 x 600 = 480.000 *pixels* = 1.440.000 bytes (1 *pixel* = 3 bytes) = 180.000 caracteres (8 bytes da imagem = 1 byte do texto)

Exemplo:





Áreas de Aplicação

- Comunicação Secreta
- Direitos Autorais
- Auxiliar pesquisas por imagens em uma base de dados
- Gravar informações como autor, título e data em arquivos de mídia

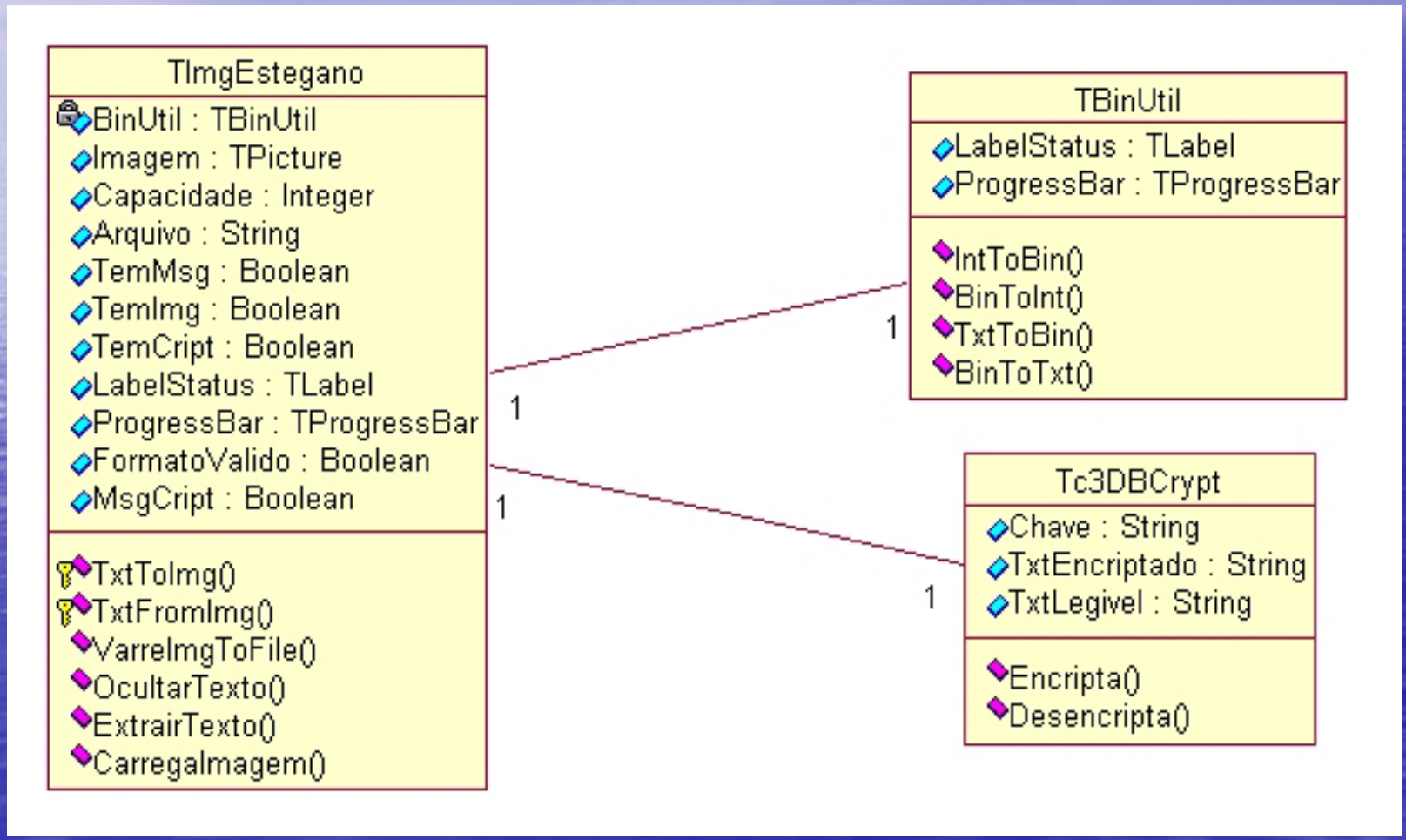
Desenvolvimento do Protótipo

Requisitos Principais do Problema a ser Trabalhado

- Criptografia: Algoritmo simétrico – AES (algoritmo *Rijndael*)
- Esteganografia: Método LSB
- Dois tipos de usuário:
  - Emissor
  - Receptor

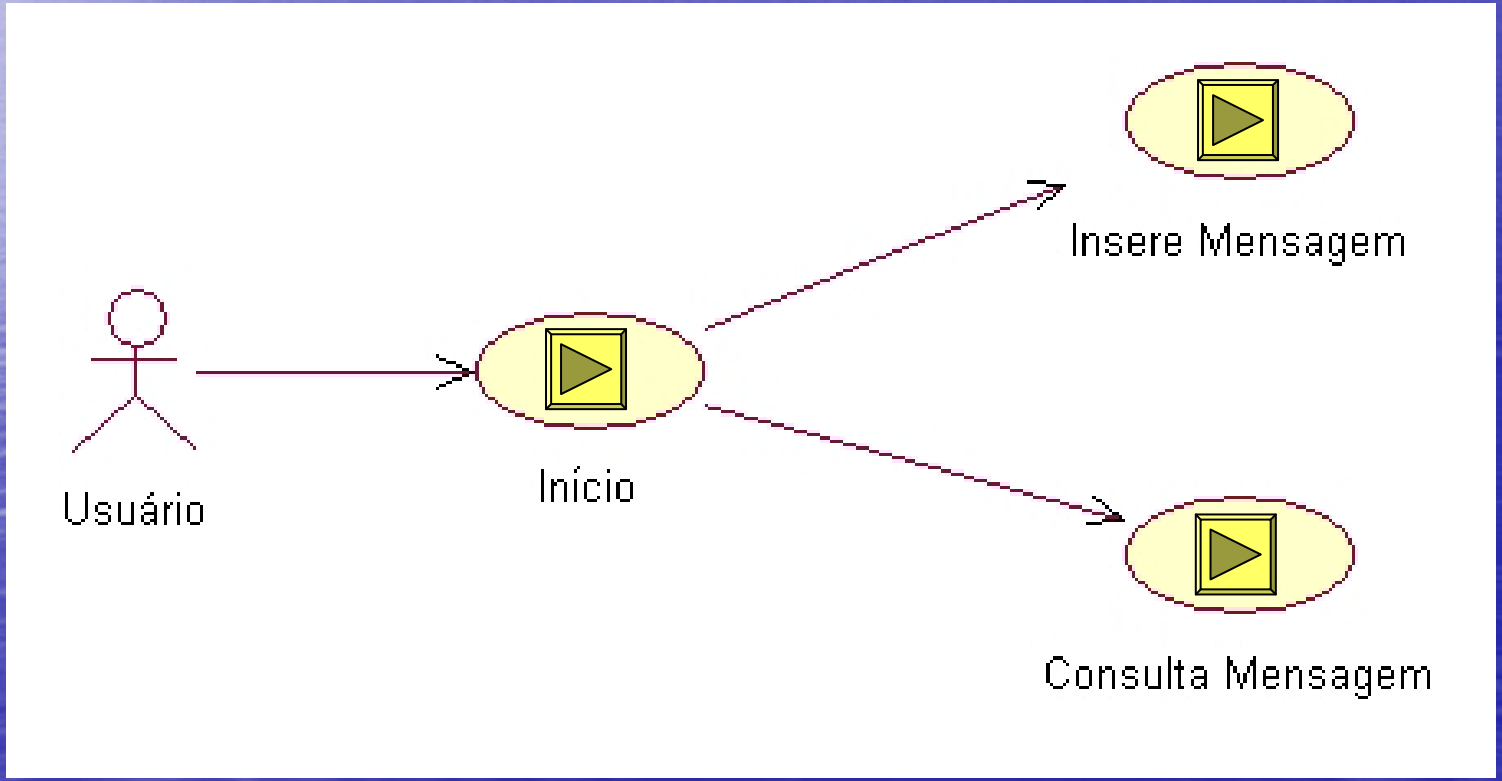
Especificação do Protótipo

- **Diagrama de classes:**



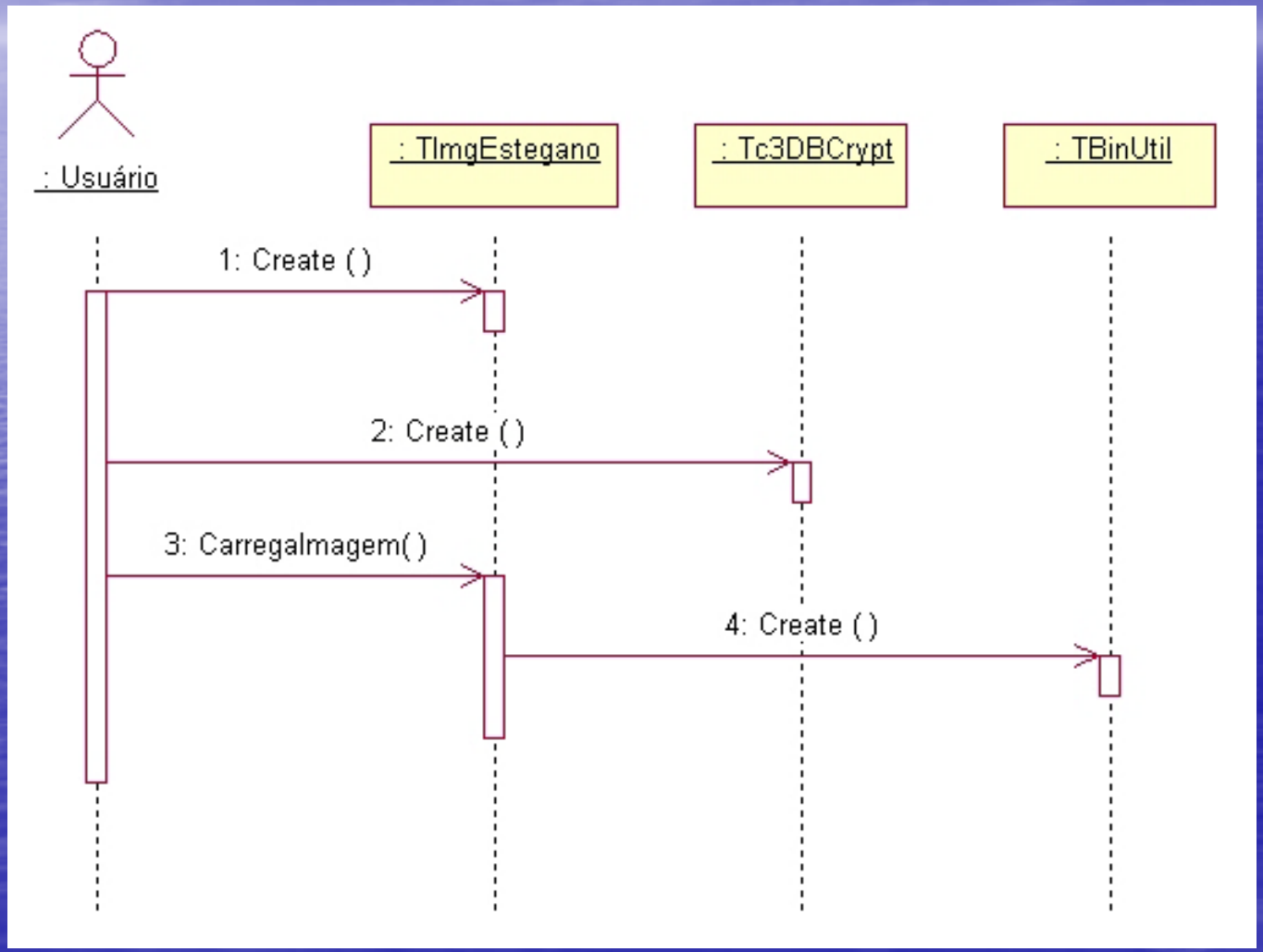
Especificação do Protótipo

- **Casos de uso:**



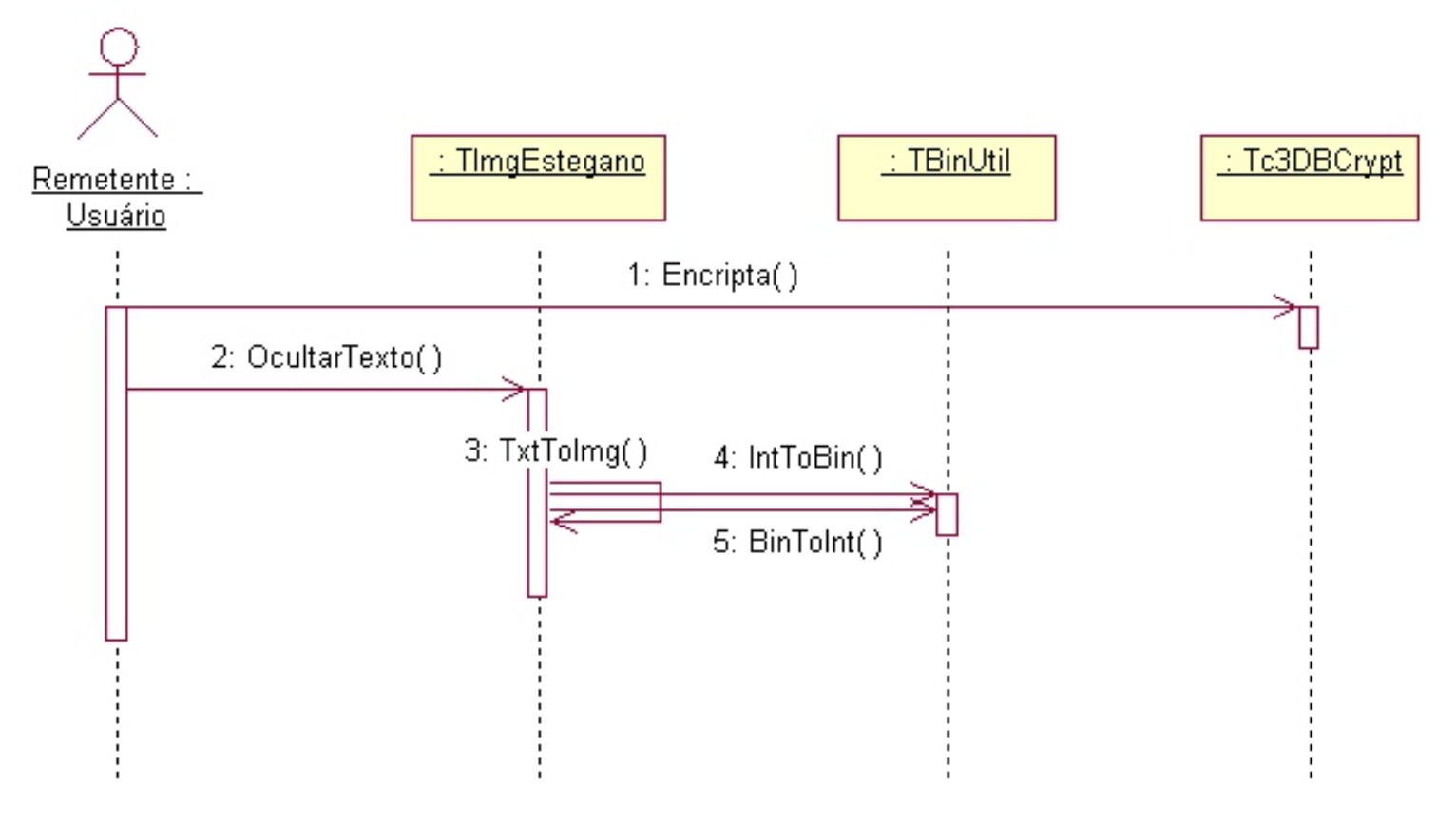
Diagramas de Seqüência

- Início:



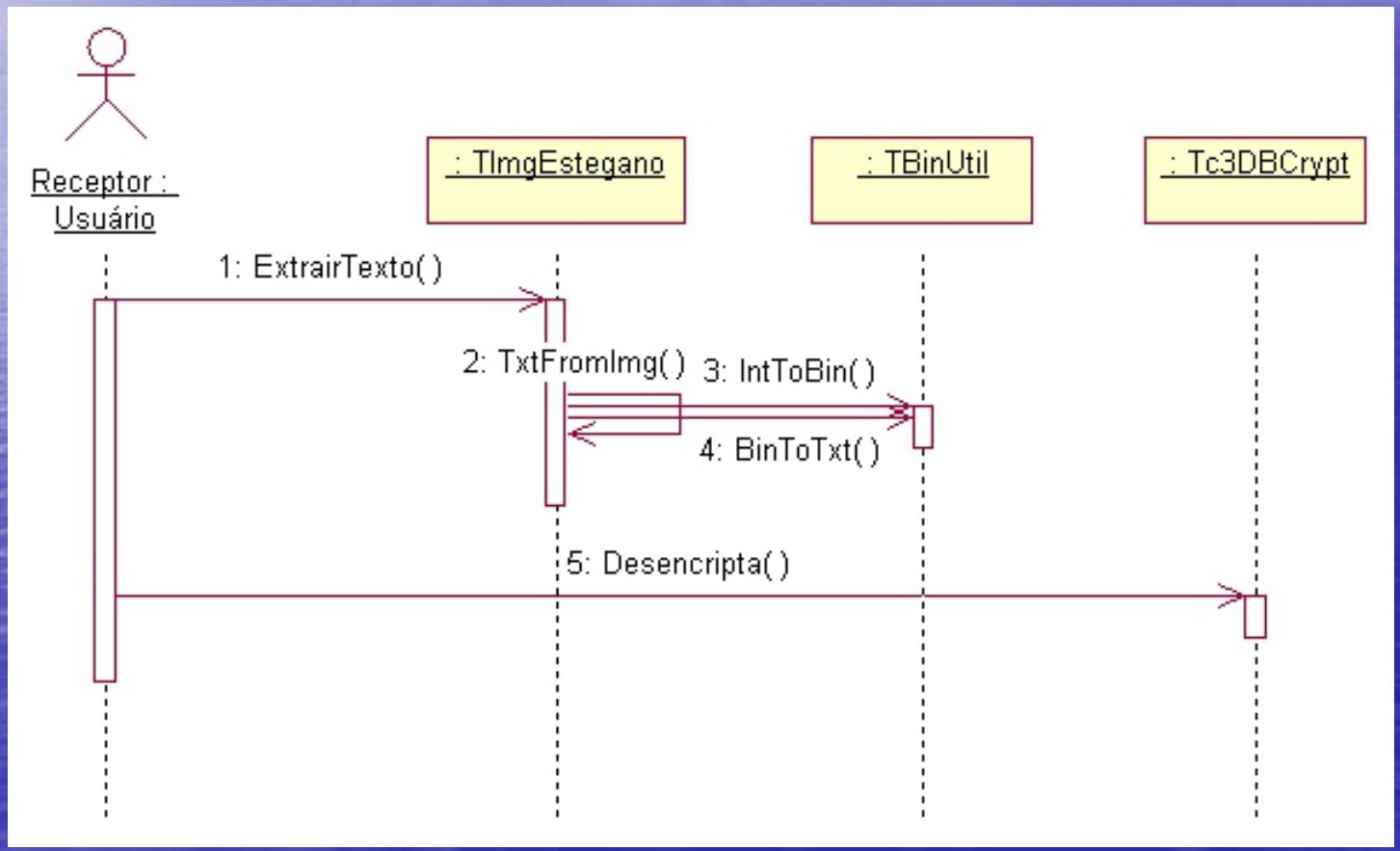
Diagramas de Seqüência

- **Insere Mensagem:**



Diagramas de Seqüência

- **Consulta Mensagem:**

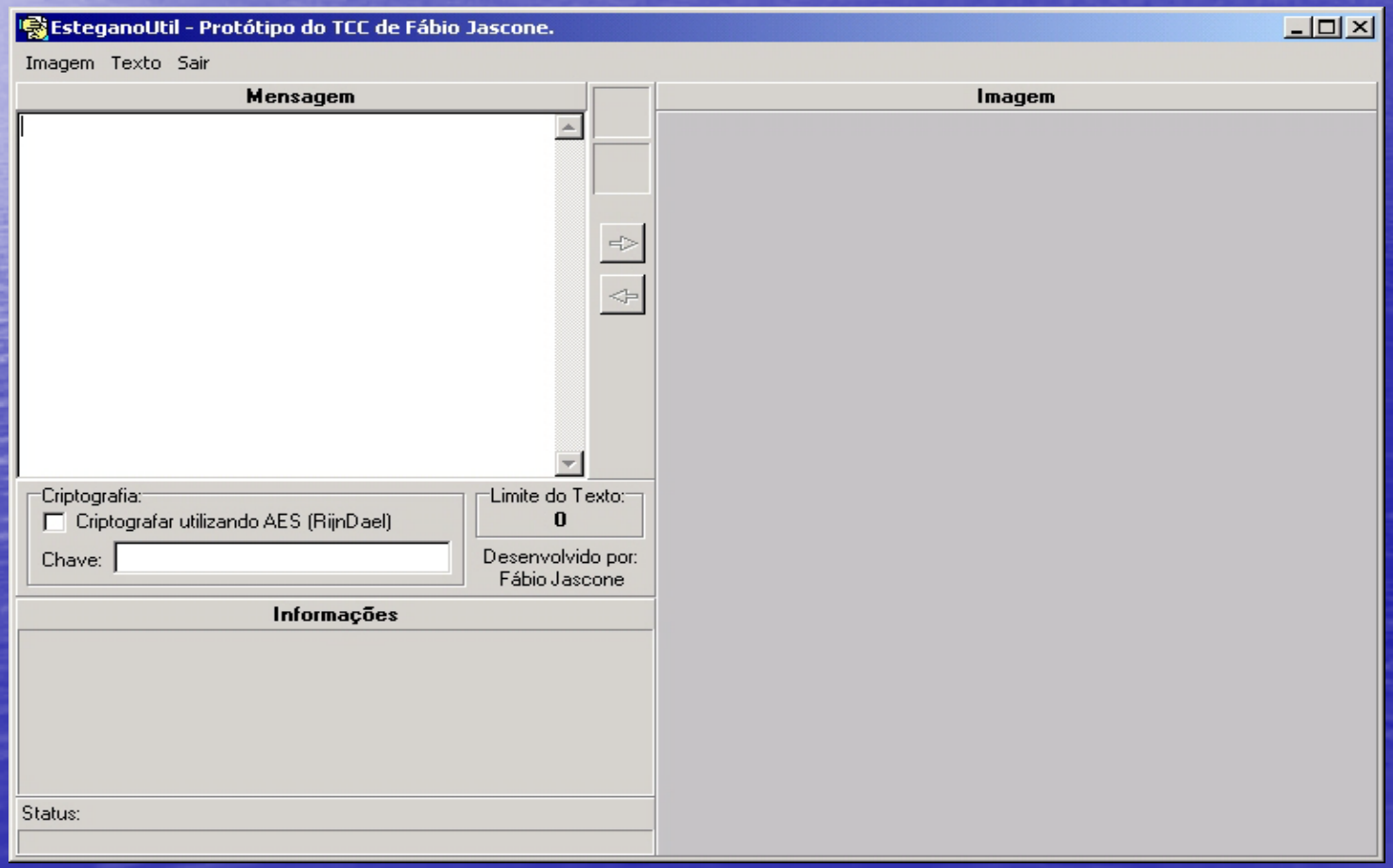


Implementação

- Técnicas e ferramentas utilizadas:
  - Criptografia:
    - Componente de terceiros
    - Mensagem + Chave = Mensagem Criptografada
    - Mensagem Criptografada + Chave = Mensagem
  - Esteganografia:
    - Sequencial (*pixel* a *pixel*)
    - Identificadores para delimitar o início (“#INI#” ou “#CRP#”) e o final (“#FIM#”) da mensagem
    - Informação + Imagem = Imagem Modificada
    - Imagem Modificada = Informação

Implementação

- **Opções do Menu:**
  - Imagem / Abrir – Salvar - Salvar Binário
  - Texto / Abrir – Salvar – Limpar
  - Sair



Considerações Finais

- **Conclusões**:
  - Objetivo atendido
  - Criptografia: novo padrão AES
  - Esteganografia: aplicação e técnicas
  - Limitação: utilizar apenas formato de imagem *bitmap*

Considerações Finais

- **Extensões**:
  - Outras técnicas de esteganografia
  - Esteganografia em outros arquivos de mídia (ex.: arquivos de áudio ou vídeo)
  - Implementar a compressão de Huffman
  - Utilização de outros algoritmos de criptografia

Apresentação do Protótipo

Muito Obrigado

Fábio Jascone - 27/11/2003