CENTRO UNIVERSITÁRIO FEEVALE

FÁBIO BRAMBILLA

ANÁLISE E MODELAGEM DE UMA FERRAMENTA PARA APOIO AO ENSINO DA CRIPTOGRAFIA

Novo Hamburgo, Junho de 2009.

FÁBIO BRAMBILLA

ANÁLISE E MODELAGEM DE UMA FERRAMENTA PARA APOIO AO ENSINO DA CRIPTOGRAFIA

Centro Universitário Feevale
Instituto de Ciências Exatas e Tecnológicas
Curso de Bacharelado em Sistemas de Informação
Trabalho de Conclusão de Curso

Professor orientador: Ricardo Ferreira de Oliveira

Novo Hamburgo, Junho de 2009.

AGRADECIMENTOS

Gostaria de agradecer a todos os que, de alguma maneira, contribuíram para a realização deste trabalho de conclusão, em especial:

A minha mãe que desde o princípio me apoiou e incentivou a procurar nos estudos o futuro promissor.

À Aline que me apoiou quando foi necessário.

A meu pai, que mesmo não estando neste mundo, tenho certeza de que torce por mim.

A todos meus amigos que compreenderam os momentos em que não pude estar presente.

Ao professor Ricardo pelas orientações deste trabalho.

E finalmente, os meus colegas de trabalho que me apoiaram para que o trabalho pudesse ser realizado.

RESUMO

Desde os tempos primórdios existe a necessidade de enviar informações entre indivíduos. Em muitos casos, como por exemplo, durante períodos de guerras e revoluções, é importante que, caso o mensageiro seja interceptado, a mensagem não seja entendida pelo interceptador. Na área de negócios, tal situação também ocorre com freqüência. Comunicações entre funcionários de uma empresa podem conter dados sigilosos evidenciando a necessidade de alguma forma de proteção contra interceptação. Na área da informática esta preocupação não poderia ser diferente. Devido ao constante acesso indevido a informações sigilosas, as empresas estão cada vez mais percebendo a importância de elevar o seu nível de segurança, pois o roubo de informações acaba prejudicando seus negócios. A criptografia é uma técnica bastante utilizada para proteger os dados de empresas, garantindo, dessa forma, o sigilo das informações de seus clientes, informações de faturamento e seus planejamentos estratégicos para a conquista de novos clientes. Para os profissionais da área de informática é muito importante conhecer esta técnica para que possam sugerir a seus gestores formas de aplicação da mesma, garantindo a segurança da informação em seus ambientes. Desta forma, este trabalho tem como objetivo a analise e modelagem de uma ferramenta capaz de demonstrar aos alunos dos cursos relacionados à informática, os aspectos e técnicas disponíveis na área de criptografia, a importância de se utilizar esta criptografia para proteção dos dados armazenados, bem como incentivá-los a pesquisar mais sobre o assunto, aumentando seu conhecimento com relação à segurança e proteção de informações.

Palavras chave: Criptografia de dados. Segurança da Informação. Ferramenta de aprendizado.

ABSTRACT

Since the early days there is a need to send information among people. In many cases, such as during periods of wars and revolutions, it is important that if the messenger is intercepted, the message can not be understood by the interceptor. In the area of business, this also occurs frequently. Communications between employees of a company may contain confidential data showing the need for some form of protection against interception. In computer science this concern could not be different. Due to constant not permitted access to confidential information, companies are realizing more and more, the importance of raising the level of security, since the capture of information leads to loss of business profits. The cryptography is a technique widely used to protect data of companies, ensuring thus the secrecy of the information of its customers, billing information and its strategic plans for the conquest of new customers. For professionals in the area of information technology is very important to know this technique, so they can make suggestions to their managers how to implement it, ensuring information security in their environments. Thus, this work aims at analyzing and modeling of a tool capable of demonstrating to students in courses related to computers, the aspects and techniques available in the area of cryptography, the importance of using this encryption to protect stored data and encourage them to find more about it by increasing their knowledge regarding the safety and security of information.

Keywords: Data cryptography. Information Security. Tools for learning.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

Crypt	Criptografia
MD	*Message Digest*
SHA	*Secure Hash Algorithm*
NSA	*National Security Agency*
DES	*Data Encryption Standard*
AES	*Advanced Encryption Standard*
IDEA	*International Data Encryption Algorithm*
PGP	*Pretty Good Privacy*
RSA	*Rivest Shamir Adleman*
Eclipse RCP	*Eclipse Rich Client Platform*
MSDE	*Microsoft SQLServer Desktop Engine*

SUMÁRIO

INTRODUÇÃO

A tecnologia de segurança em informática deve ser exercida por todos os profissionais (usuários e de informática) da organização e terá sua coordenação exercida por "analista de segurança em informática", que estabelecerá práticas, para efeito de consubstanciar a atividade de segurança em informática (GIL, 1998).

De acordo com GIL, entende-se que todos os usuários de informática são responsáveis pela segurança de suas informações, tanto os que utilizam seus computadores para armazenar as informações, quanto os administradores de rede, que são os responsáveis por adotar as melhores práticas de segurança para o ambiente corporativo.

O usuário que deixa sua estação desbloqueada está, mesmo que inconscientemente, deixando abertura para que outros usuários do sistema tenham acesso às suas informações, podendo, dessa forma, ter acesso a dados sigilosos, como números de contas, folha de pagamentos, planejamentos estratégicos, planejamento de marketing e, até mesmo, códigos fontes de produtos.

Esta política de segurança deve ser adotada pelo administrador de rede e os usuários devem estar cientes de que qualquer envio de informação que partir de sua senha de acesso será de sua responsabilidade.

O simples fato de bloquear a estação é apenas uma forma de proteger as informações da empresa, porém, existem problemas de acessos externos, onde usuários mal-intencionados acessam as informações da empresa através de falhas de segurança do sistema, roubando informações importantes para o negócio da empresa.

Segundo Cronkhite (2001), CD *Universe*, uma loja de música on-line, experimentou uma brecha devastadora em sua segurança de dados. Em janeiro de 1999, um hacker russo, Maxxus, roubou milhares de números de cartão de crédito de seus clientes. Depois ele tentou chantagear a empresa, pedindo dinheiro. Quando a empresa decidiu não pagar o resgate, ele

postou 25.000 dos números na Internet. Esse incidente minou a confiança do cliente, não apenas para essa empresa, mas também para outras empresas on-line.

Segurança sempre foi um assunto importante em desenvolvimento de sistemas, mas atualmente duas novas tecnologias trouxeram a segurança para o foco: a Internet e os sistemas ERP (*Enterprise Resource Planning*). No primeiro caso, a vantagem da interconexão entre computadores de todos os tamanhos e tipos traz enormes ganhos, mas exige segurança muito maior, pois facilita o acesso do hacker. No segundo, um número crescente de empresas vem informatizando toda sua área produtiva, aumentando o valor das informações e o prejuízo ao perdê-las (ALBUQUERQUE, 2002).

Criptografia é o processo pelo qual uma informação ou um texto é embaralhado de forma que só seja possível a obtenção do texto original aplicando-se uma operação baseada em uma chave de acesso. Para obter o dado original, é necessário, portanto, saber qual a operação para decriptografia (o algoritmo) e a chave de acesso (ALBUQUERQUE, 2002).

Algoritmos criptográficos basicamente objetivam “esconder” informações sigilosas de qualquer pessoa desautorizada a lê-las, isto é, de qualquer pessoa que não conheça a chamada chave secreta de criptografia (TERADA, 2000).

Com base no cenário citado acima, foi encontrada a necessidade de criação de uma ferramenta que possa auxiliar os alunos dos cursos relacionados à informática, a importância da utilização da técnica de criptografia.

Este trabalho teve como objetivo, propor a análise e modelagem de uma ferramenta que seja capaz de mostrar a estes alunos os conceitos relacionados à criptografia e que eles possam entender os motivos pelos quais se deve utilizar esta técnica, além de poder simular na própria ferramenta os conceitos estudados.

Este estudo pode ampliar a visão dos alunos com relação à importância de manter os dados e comunicação protegidos, garantindo que suas informações estratégicas não sejam acessadas por pessoas indevidas.

Para alcançar este objetivo, foi efetuada a revisão bibliográfica da história da criptografia, especificando os pontos mais relevantes e que proporcionaram o surgimento de novas técnicas. Além deste histórico, foi efetuado o levantamento dos métodos utilizados atualmente e criados simuladores onde o aluno pode interagir com a ferramenta, aplicando na prática o conteúdo estudado. Além deste referencial teórico, foi analisada uma ferramenta para simulação de criptografia de forma geral, pois não foram encontradas ferramentas

direcionadas especificamente ao ensino da criptografia, mas sim simuladores que não possuem foco especificamente na questão didática. Com base na análise deste simulador, foram identificadas as possíveis melhorias a serem implementadas na ferramenta proposta.

Este trabalho está dividido em quatro capítulos. O primeiro capítulo contém a descrição dos termos relacionados à criptografia, bem como a história da mesma para que seja possível explicar as técnicas de criptografia destacadas para este trabalho. O segundo capítulo apresenta as especificações técnicas dos métodos de criptografia visando adquirir conhecimento e requisitos para a modelagem da ferramenta. O terceiro capítulo contém a modelagem da ferramenta proposta, onde podem ser vistos os requisitos funcionais e não-funcionais, casos de uso, diagrama de classes, diagramas de atividades e diagramas de seqüência. Finalmente, o quarto capítulo contém informações sobre o protótipo criado, onde foram validados os requisitos levantados.

1. CRIPTOGRAFIA

Para que o aluno possa entender o que é a criptografia, a ferramenta modelada deverá possuir recursos que demonstrem ao aluno o histórico da criptografia, como surgiu a criptografia, quais os tipos de criptografia, quais os conceitos relacionados à criptografia, e outras informações que estaremos relacionando no decorrer deste capítulo.

1.1 Histórico da Criptografia

Já é de conhecimento dos estudiosos que a criptografia é um assunto que não teve seu surgimento e constante crescimento devido à popularização da internet. A criptografia é utilizada antes mesmo do surgimento dos sistemas computacionais.

Segundo Trigo (2007), o uso da criptografia é bastante antigo. Um dos primeiros registros de confiabilidade dos dados aparece no tempo dos reis, em que um rei selava a carta com o seu anel de cera. Quando a carta chegava para outro rei, ele sabia que ninguém havia lido aquela mensagem porque continuava selada. O formato dos anéis era particular a cada rei.

Já segundo LOIDREAU, a origem da criptografia, provavelmente, remonta aos princípios da existência humana, logo que as pessoas tenham tentado aprender a se comunicar, conseqüentemente, tiveram de encontrar meios para garantir a confidencialidade de parte das suas comunicações. Contudo o primeiro uso deliberado de métodos técnicos para criptografar mensagens pode ser atribuído aos antigos Gregos, em meados do século VI A.C. uma vara, chamada "*Scytale*" ou Licurgo foi utilizado. O emissor enrolaria um pedaço de papel ou tira de couro à volta da vara e escreveria a sua mensagem longitudinalmente nela. Depois abria o papel ou tira de couro, o qual era enviado para o endereço respectivo. A decriptação da mensagem sem o conhecimento do comprimento das varas – atuando aqui como uma chave secreta – era considerada impossível. Mais tarde os romanos utilizaram o código cifrado de César para comunicar (uma terceira letra do alfabeto).

SMITH confirma a teoria de Loidreau que diz ser a *Scytale* a forma de cifragem mais antiga existente. SMITH cita ainda que nos tempos antigos a comunicação entre os membros da Grécia era feita através de tatuagens no couro cabeludo do escravo mais confiável. Após o crescimento do cabelo, o escravo era enviado para o destino. Quando o mensageiro chegava ao destino, ele era instruído a falar a seguinte frase: “Corte meu cabelo e veja o que tem debaixo”. Dessa forma o cabelo do mensageiro era raspado e dessa forma a mensagem era lida pelo receptor.

Segundo o site Escriba Café, o surgimento da criptografia ocorreu durante a Segunda Guerra Mundial, onde enquanto ocorria à guerra armada, os criptógrafos procuravam algoritmos para decifrar mensagens enviadas pelos adversários e simultaneamente, criavam novos códigos em busca de sigilo nas informações enviadas.

No entanto, os alemães tiveram posse da máquina chamada Enigma, a qual gerava códigos tão complexos que os alemães acreditavam ser impossíveis de decifrar. Não poderia ser impossível de decifrar, porém, quase impossível. Este fato é comprovado com o fato de que, uma mensagem enviada pelo capitão de um dos submarinos de guerra interceptada, pôde ser decifrada apenas em março de 2006 com a ajuda de mais de 5000 computadores trabalhando em conjunto.

Para tanto, iremos dividir o estudo da História da Criptografia em três épocas, sendo elas, a História Antiga, História Medieval e História Moderna.

1.1.1 História Antiga

Couto explica que cerca de 1900 a.C, todas as construções precisavam estar documentadas através de entalhes em blocos de argila. Por se tratar de uma documentação, estes blocos eram bastante grandes e não poderiam ser dobrados para ter seu tamanho reduzido. Acredita-se, desde então, que os entalhadores (escribas) que trabalhavam para os faraós tiveram a idéia de substituir palavras ou trechos de texto a serem entalhados com o objetivo de diminuir o tamanho dos blocos de argila, além de manter em segredo a informação de onde estariam guardados os tesouros do faraó.

Já em 1500 a.C na Mesopotâmia os primeiros registros de uso da criptografia encontrados em fórmulas para fazer esmaltes de cerâmica. Esta fórmula estava entalhada em tabletes de argila e foi encontrada às margens do Rio Tigre. Neste mesmo período podem ser encontrados os primeiros sinais de utilização da esteganografia, que é a arte da “escrita

escondida". Enquanto a criptografia trata de esconder o sentido das mensagens, a esteganografia trata de esconder a existência dessas mensagens.

300 a.C o filósofo e geômetra grego de nome Erastóstenes que ficou conhecido por calcular com precisão o diâmetro da Terra, cria um método para identificação dos números primos, o qual foi batizado de Crivo de Erastóstenes.

50 a.C ocorreu o surgimento da Cifra de Cesar, a qual consistia em substituir as letras de uma mensagem pela letra correspondente ao deslocamento do alfabeto em três posições. A letra "A" era substituída pela letra "D", a letra "B", substituída pela letra "E" e assim por diante.

1.1.2 História Medieval

Foram encontrados indícios de códigos muito interessantes do período da história medieval, mesmo tendo sido considerada esta a "Idade das Trevas". O período de História Medieval ou História Média iniciou em 476, com a queda do Império Romano e se estendeu até 1453, com a queda da Constantinopla.

Por volta de 79 d.C., antecedente à Idade Média, foi utilizado a Fórmula Sator ou quadrado latino, encontrados em um amuleto de bronze e uma coluna na cidade de Pompéia, encontrados na Ásia e datados do século V a.C. Nestes dois objetos foi encontrado o Palíndromo "*rotas arepo tenet opera sator*", que é o anagrama mais famoso da história.

Em 200 d.C surgiu o trabalho que mostrava detalhadamente como misturar poções especiais, chamado de Papiro de Leiden. Nos momentos mais importantes da confecção das poções, era possível encontrar textos cifrados. Uma das receitas acredita-se, que era o filtro do amor.

No ano de 400 d.C pode ser encontrada a criptografia no livro Kama-Sutra de Vatsayana como partes integrantes das 64 artes que as pessoas devem conhecer e praticar. A arte de saber escrever em cifras e escrever palavras de forma peculiar, além de falar mudando as formas das palavras, conhecido como criptofonia.

Entre os anos 718 e 786 teve surgimento o livro Kitab al Mu'amma do árabe Al-Khalil, escrito em grego contendo assuntos sobre a criptografia. A obra foi escrita originalmente para o Imperador Bizantino. O autor ficou famoso por decifrar um criptograma que baseado no início do texto original, o qual foi supostamente a frase "Em nome de Deus".

Este método é conhecido como Método da Palavra Provável, o qual passou a ser utilizado como padrão para decifrar as mensagens Enigma no período da Segunda Guerra Mundial.

Por volta de 1187 a 1229 foi apresentado pela primeira vez na história, o livro Explicações Claras Para a Solução de Mensagens Secretas, escrito pelo árabe Ibn Dunainir explicando as Cifras Algébricas, que consiste em substituir letras por números através de cálculos aritméticos.

1.1.3 História Moderna

Couto explica que no ano de 1518 Johannes Trithemius escreve o primeiro livro impresso sobre criptologia. Trithemius é o criador da cifra esteganográfica, onde cada letra é representada como uma palavra obtida a partir de uma sucessão de colunas.

No ano de 1533 o alemão Heinrich Cornelius Agrippa Von Nettelsheim descreve sua cifra de substituição monoalfabética, conhecida hoje como Cifra de Pig Pen, que significa "Porco no chiqueiro", onde cada letra é associada a um porco e alocada em sua "casa", que seria o chiqueiro.

No ano de 1550 Girolamo Cardono, inventor do primeiro procedimento com autochave, publicou sua obra chamada De Subtilitate libri XXI, que consiste em uma folha de material rígido contendo aberturas retangulares, onde são escritas as mensagens. Escrita a mensagem, basta retirar a folha e preencher os espaços com outros caracteres.

Para que o receptor possa ler o conteúdo da mensagem, basta utilizar o mesmo tipo de folha, com as mesmas aberturas retangulares.

No ano de 1551 o matemático e astrólogo inglês John Dee foi reconhecido por seu trabalho com o chamado Alfabeto Enoquiano também conhecido como Linguagem angelical e também por suas idéias.

Em 1585 Blaise de Vigenère apresenta os primeiros sistemas autênticos de texto puro e texto cifrado com autochave em seu livro sobre cifras.

1.2 Conceitos

Agora que apresentamos um pouco da história da criptografia, vamos explanar os termos envolvidos com esta técnica, permitindo ao aluno entender o conteúdo que estará disponível na ferramenta.

Schneier (1996) descreve os termos relacionados à técnica de criptografia da seguinte forma: uma mensagem de texto puro é denominada *plaintext* ou *cleartext*. O processo de transformar a mensagem de texto puro em uma mensagem com texto de conteúdo oculto é chamado de Encriptar ou Cifrar. A mensagem encriptada é denominada *ciphertext* ou Criptografada. O processo de tornar a mensagem encriptada em texto puro novamente é denominado Decriptografar ou Decifrar. A figura 1.1 ilustra o processo de envio de uma mensagem até o destinatário, descrevendo cada etapa citada acima.

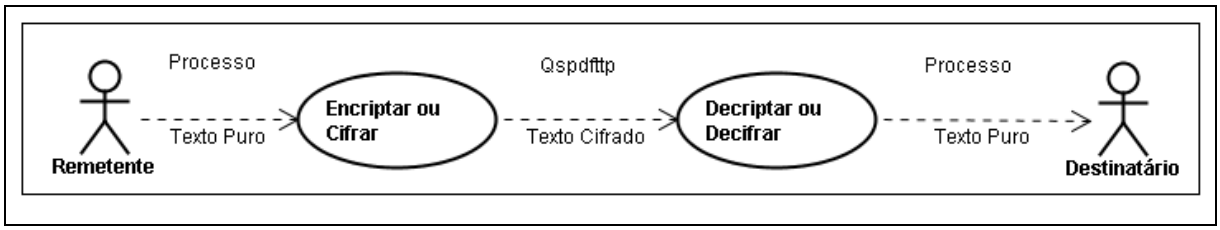

Figura 1.1: Terminologias.
Fonte: O autor.

1.2.1 Invasor

O invasor é o indivíduo que tenta roubar informações dos usuários que possuem seus sistemas desprotegidos, utilizando várias técnicas de invasão.

Além de roubar informações, os invasores podem fazer-se passar por outras pessoas, desativar sites que estão em pleno funcionamento, deixar sistemas lentos e até mesmo impedir a compra de produtos através de sites de compras on-line.

Cheswick explica que o objetivo real de um invasor é recuperar o texto puro, ou então, pelo menos recuperar a chave que foi utilizada para efetuar a criptografia, tendo acesso dessa forma à mensagem original. Explica ainda que seja admissível que o método de criptografia seja facilmente conhecido através da engenharia reversa, porém, o grande segredo está na chave utilizada, e esta é que deverá estar muito bem protegida.

1.2.2 Criptoanálise

O conceito Análise Criptográfica é designado para o estudo sobre a quebra de sistemas criptográficos.

O termo Criptoanálise, segundo Dover, é utilizado para definir a análise e solução das cifras, sem considerar o código utilizado para criptografar tal informação.

Já Dubois (2001) destaca que Criptoanálise é o estudo das cifras cujo código é desconhecido.

Ao contrário, Haykin (2004) define Criptoanálise como todo o processo necessário para encontrar a chave secreta, conhecendo-se o criptograma (texto cifrado) e probabilidades de vários textos normais e chaves.

Titel afirma que Criptoanálise é o termo utilizado para a quebra dos códigos de criptografia aplicados às mensagens.

Geus (2007) apóia a teoria de que o termo Criptoanálise é a ciência de recuperar a informação cifrada, sem que se tenha acesso à chave de criptografia, de forma a obter a mensagem original, ou a própria chave de criptografia.

1.2.3 Criptanalista

O termo Criptanalista é bastante semelhante ao invasor, pois este se refere ao indivíduo que procura as fraquezas dos algoritmos.

O Criptanalista utiliza seu conhecimento, além de outras ferramentas, para quebrar algoritmos mais rapidamente, pois, todos podem ser quebrados de alguma forma. Os melhores algoritmos são simplesmente os que demoram mais tempo para serem quebrados.

1.2.4 Criptógrafo

O termo Criptógrafo é utilizado para identificar o indivíduo que desenvolve sistemas de criptografia. O Criptógrafo deve conhecer as falhas de seu sistema, pois os invasores ao descobrirem tais falhas, não revelarão de forma fácil, visto que é uma porta de entrada garantida para roubo de informações.

Segundo Chomsky (2006), a Teoria das Representações Semânticas Inatas defende, além da teoria de que existem representações semânticas na mente/cérebro, defende a teoria de que a mente é um Criptógrafo:

> "'a mente pensa seus pensamentos em mentalês, codifica-os no local da linguagem natural e, então, transmite-os' a um ouvinte que 'tem um Criptógrafo em sua cabeça também, é claro, que logo após continua a decodificar a mensagem' (CHOMSKY)"

1.2.5 Criptografia

Segundo Menezes (1997), Criptografia é o estudo de técnicas matemáticas relacionadas aos aspectos de segurança da informação, como confiabilidade, integridade dos dados, autenticação de entidade e autenticação de origem.

O termo Criptografia possui origem grega, onde *Kriptós* quer dizer escondido e *Graphos* quer dizer escrita. Dessa forma, podemos definir a palavra criptografia como escrita

escondida ou escrita oculta. Criptografia é então a arte de escrever em cifras ou em códigos de forma a permitir que apenas o destinatário a compreenda.

Titel explica criptografia como sendo um método que impede que as pessoas não autorizadas tenham acesso às informações que estão sendo repassadas para outros usuários. Utilizando-se *hashing* para a codificação das mensagens é possível ocultar estas informações.

Coulouris (2007) define criptografia como a ciência de manter as informações em sigilo.

Clementino (2007) afirma que na era dos Computadores, criptografia e intimidade estão extremamente relacionadas, pois criptografia trata-se de um conjunto de funções que visam garantir o sigilo das informações, utilizando um padrão de normas especiais de uma cifra ou código.

Carmona (2005) define criptografia como encapsulamento de dados considerados sensíveis em arquivos, onde apenas quem possui o código ou chave de acesso corretos, poderá estar efetuando a abertura dos mesmos.

1.2.6 Criptovirus

Segundo Young (2004), Criptovirus é o termo utilizado para os vírus de computadores que utilizam chaves públicas em suas execuções nos comutadores das vítimas. O grande diferencial do Criptovirus é que ao se instalar no computador da vítima, o mesmo criptografa os arquivos do usuário com a criptografia padrão RSA e a chave pública é repassada ao usuário apenas mediante pagamento de um valor determinado pelo criador do vírus. Caso a vítima não tenha *backup* de suas informações e precise dos arquivos, ele deverá efetuar o pagamento para poder ter acesso às informações.

Dessa forma, o criador do vírus pode distribuir livremente a chave pública, pois a chave privada permanece somente sob seu conhecimento.

1.2.7 Criptovirologia

Criptovirologia, segundo Young, é o termo utilizado para definir a análise e utilização dos criptovirus. Esse estudo busca, através da chave pública, encontrar as diferenças entre o arquivo original e o arquivo escrito por ele mesmo.

1.2.8 Chave de Criptografia

Segundo Carvalho, a chave é uma informação que serve de código para que as informações sejam criptografadas e decriptografadas. O processo de criptografia deve ser executado de forma fácil para quem possui o conhecimento da chave utilizada e deve ser considerado impossível de descobrir por quem não conhece esta chave.

O conceito de Chave para o mundo da tecnologia consiste em definir que, apenas quem possui o conhecimento de tal chave poderá decifrar dados criptografados com a mesma.

Utilizando analogias para explicar, é como se fosse a chave da porta de casa, onde apenas quem possui acesso à chave conseguirá abrir a porta. Caso não possua, a porta não pode ser aberta.

Na área de Tecnologia, o conceito utilizado é o mesmo. Somente aquele que possuir o conhecimento da chave correta para decriptografar informações é que poderá fazê-lo.

Segundo Tittel, o nível de segurança na criptografia baseado em Chave dependerá do comprimento da chave utilizada. Caso sejam utilizados apenas números decimais, uma chave com dois dígitos terá apenas 100 combinações possíveis para que seu conteúdo seja descoberto. Aumentando para três dígitos, serão necessárias 1000 combinações para que o conteúdo seja descoberto.

Da mesma forma que existem as chaves, existe técnicas para aplicação da criptografia, onde, por exemplo, dados que foram criptografados utilizando o algoritmo *Triple* DES não poderão ser decriptografados utilizando-se o algoritmo *Advanced Encryption Standard* (AES), mesmo que a chave utilizada seja conhecida pelo invasor.

As chaves podem ser denominadas como Chave Pública, Chave Privada, Chave Simétrica e Chave Assimétrica.

1.2.8.1 Chave Pública

Para Chave Publica pode ser atribuído o conceito de uma chave de livre distribuição, a qual pode ser enviada para qualquer indivíduo. De nada adianta ter uma chave pública se não é conhecida a chave privada. A composição de ambas as chaves é que possibilita o descobrimento da mensagem oculta.

Tittel explica que quando o remetente estiver pronto para enviar uma mensagem ao destinatário, o mesmo criptografa os pacotes utilizando uma chave privada, na qual somente ele possui acesso. A mensagem é transmitida através do canal de comunicação existente. Esta forma de criptografia gera dois pares de chaves, das quais, apenas uma é conhecida pelos

elementos envolvidos. O mesmo cálculo matemático efetuado para a criação da chave do remetente é aplicado no lado do destinatário ao receber a mensagem, sendo necessária a combinação das duas chaves envolvidas para que a mensagem possa ser efetivamente convertida para texto puro. Sem o conhecimento das duas chaves, não é possível descobrir qual está faltando para fazer a composição completa da formula.

Este esquema criado por Diffie e Hellman não procura proteger o meio de comunicação, mas sim, os dados que são trafegados, tornando os mesmos ilegíveis para os possíveis interceptadores da mensagem.

1.2.8.2 Chave Privada

A chave privada é o ponto mais importante da criptografia, pois esta chave privada é a responsável por garantir o completo sigilo das informações. Sem a chave privada, não é possível decriptografar a mensagem.

1.2.8.3 Chave Simétrica

A Criptografia de Chave Simétrica é caracterizada pelo fato de que a mesma chave utilizada para criptografar uma mensagem será utilizada para decriptografar. Desta forma, caso a mensagem seja interceptada durante o envio, o interceptador poderá facilmente obter o acesso ao conteúdo da mensagem.

Geus destaca como características do algoritmo de chave simétrica a velocidade de execução do algoritmo, porém, não se faz possível a aplicação de certificados e assinaturas digitais. Além disso, deve ser distribuída através de um meio de comunicação seguro, a chave gerada para o usuário.

Cheswick (2005) afirma que na Criptografia de Chave Simétrica, também conhecida como Criptografia de Chave Secreta existe apenas uma chave para a operação de encriptação e decriptação.

1.2.8.4 Chave Assimétrica

Segundo Stallings (2006), Diffie e Hellman foram os pioneiros da Criptografia Assimétrica. Eles desenvolveram um algoritmo onde é possível utilizar uma chave pública e uma chave privada. Não é possível efetuar a leitura da mensagem criptografada sem o conhecimento da chave privada, dessa forma uma mensagem ao ser interceptada estará menos volátil à quebra de sua criptografia.

A Criptografia Assimétrica consiste em utilizar duas chaves distintas para efetuar a criptografia e decriptografia das informações.

No final da década de 70 foi desenvolvido o método da criptografia assimétrica e a tecnologia de chaves pública e privada. Você encriptava com a chave pública do destinatário e somente ele poderia desencriptar utilizando a sua chave privada, e também haveria como saber com certeza absoluta se a pessoa que mandou a mensagem era realmente quem dizia ser (ASSUNÇÃO, 2002).

Este método consiste em gerar uma chave privada que é conhecida apenas por um indivíduo específico e uma chave pública que pode ser amplamente distribuída. Ao enviar a chave pública, as aplicações podem efetuar a criptografia dos dados utilizando esta chave, a qual pode ser decriptografada apenas com o conhecimento da chave privada. O transporte destas informações ocorre por meio de certificados. Este certificado garante que a mensagem recebida foi realmente enviada pelo usuário que afirma tê-la enviado.

1.2.9 Tabelas *Hash*

Goodrich explica que um dicionário de dados é semelhante a um dicionário de palavras, onde os mesmos são utilizados para encontrar e organizar as palavras. O dicionário de dados é utilizado para associar chaves a elementos, onde se torna possível efetuar a inclusão e remoção de registros deste dicionário, além de efetuar a consulta dos itens alocados neste dicionário através de suas chaves.

As tabelas *Hash* são compostas por dois elementos, sendo um deles denominado *Bucket* e outro elemento as funções de *Hash*.

O elemento *Bucket* pode ser considerado com um repositório de chaves e elementos. Para uma tabela *Hash*, armazena um arranjo A de tamanho N, onde A é o próprio *Bucket* e N é a capacidade do arranjo.

Já o elemento Funções *Hash* mapeia cada chave em um inteiro, criando dessa forma o código *Hash*. Este código *Hash* então é o endereçamento dos elementos contidos no *bucket*.

Carmona define *Hash* como um método cuja característica principal é não permitir a duplicidade de dados, além de transformar os dados de tal forma que o resultado será sempre exclusivo, sendo impossível retorná-lo ao formato original.

1.2.10 Esteganografia

Johnson define esteganografia como uma forma de proteger informações, assim como na criptografia, pois além de criptografar uma mensagem, a mesma é “camuflada”, sendo acrescentada em meios de transmissão aparentemente puros.

A mensagem criptografada pode ser transferida através de meios, como por exemplo, fotos de jornal onde são posteriormente escaneadas e seu conteúdo revelado, ou então, através do meio digital como em correio eletrônico, arquivos de áudio, vídeo, espaços disponíveis em disco, partições e também imagens.

O método da esteganografia consiste em esconder a mensagem criptografada em *bits* não utilizados de imagens, arquivos texto, arquivos de áudio e vídeo, além de poder adicionar em partições do disco rígido, adicionada a pacotes a serem transferidos pela rede e códigos fonte de *softwares*.

No caso de inserção de mensagens em imagens, pode ser utilizado o *bit* menos significante da imagem para efetuar o armazenamento dos dados. Dessa forma, a imagem será normalmente visualizada a olhos nus, sendo necessária uma ferramenta de análise da imagem para detectar a alteração dos *bits*.

Depois de identificado o conteúdo nesta imagem, a mensagem deverá ser ainda decriptografada, demandando maior tempo para decifrar a mensagem.

1.2.11 Enigma

Segundo Pacitti (2003), a máquina Enigma teve seu surgimento no período da Segunda Guerra Mundial, onde os alemães criptografavam suas mensagens utilizando esta máquina e transmitiam através do rádio. O que os alemães não sabiam, era que a Inglaterra já estava utilizando a máquina denominada Colossus para decifrar suas mensagens.

Couto explica que a máquina cifradora Enigma era muito semelhante a uma máquina de escrever, onde ao digitar as letras engrenagens de latão se movimentavam e transformavam o texto puro em texto completamente sem sentido. Apenas quem possuísse a máquina enigma com a mesma calibragem é que poderia estar decifrando a mensagem enviada.

Segundo ele, a máquina Enigma teve seu inicio de utilização comercialmente em 1920, não somente por parte dos nazistas, mas também, por vários outros governos. Nesta época existiam vários modelos da Máquina Cifradora Enigma, sendo o modelo conhecido como Wehrmacht Enigma o mais discutido por ter sido usado pelos aliados para decifrar as

mensagens interceptadas, antecipando, segundo os historiadores, o fim da Guerra em pelo menos um ano.

Assim como outros sistemas rotores, a Enigma combinava sistemas mecânicos e elétricos, onde a parte mecânica consistia em um teclado em conjunto com discos rotativos, chamados rotores, dispostos em fila e que avançam ao pressionar uma tecla e o circuito elétrico é responsável pela geração da luz com a letra correspondente à letra pressionada após a cifragem.

Ao ser pressionado, o teclado aciona as conexões para câmbio de codificação, que por sua vez aciona os rotores, o rotor espelho, os rotores pela ordem inversa e finalmente a placa de luzes, ativando ao final a luz com a letra codificada.

A máquina cifradora Enigma era composta por um teclado com 26 letras, um quadro com 26 lâmpadas, um dispositivo chamado *scrambler* composto por três rotores e um quadro com cavilhas denominado *steckerboard*.

A partir de 1941 a marinha alemã passou a utilizar a máquina Enigma com quatro rotores (M4), sendo ainda mais complexa do que a conhecida com três rotores (M3).

Na figura 1.2 pode ser visualizada a Máquina Cifradora Enigma.

Figura 1.2: Máquina Cifradora Enigma.
Fonte: Wikipédia (http://pt.wikipedia.org/wiki/Ficheiro:Enigma.jpg)

A figura 1.3 ilustra os três rotores contidos na Máquina Cifradora Enigma.

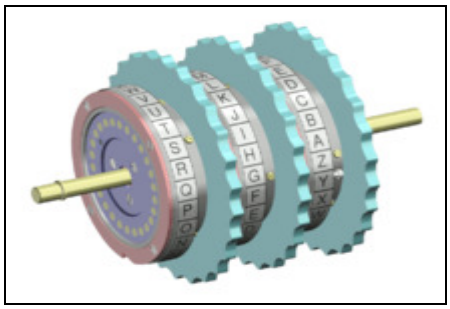

Figura 1.3: Rotores da Máquina Cifradora Enigma.
Fonte: Wikipédia (http://pt.wikipedia.org/wiki/Ficheiro:Enigma_rotor_set.png)

1.2.12 Assinaturas Digitais

Titel define Assinatura Digital como uma técnica para informar ao destinatário que realmente quem enviou a mensagem foi o remetente que se diz ser. Exemplificando melhor, poderia ser enviada uma carta com assinatura do "Papai Noel", porém, quem iria garantir que realmente veio dele?

Titel explica então que no caso das assinaturas digitais, a mensagem é criptografada utilizando-se a chave privada e apenas o destinatário que possui a chave pública poderá efetuar a decriptação da mensagem, confirmando dessa forma que o remetente é realmente quem ele diz ser.

Um protocolo muito utilizado para a autenticação de assinaturas digitais é o Kerberos, cujo nome vem da mitologia grega para um cachorro com três cabeças que ficava guardando a entrada do Hades.

1.3 Métodos e Aplicações da Criptografia

Neste item serão relacionados alguns métodos e aplicações da criptografia, relacionados aos conteúdos pesquisados nos tópicos anteriores.

1.3.1 Criptografia Simétrica

Agora que conhecemos o conceito de Criptografia Simétrica, vamos explanar algumas técnicas de utilização desta criptografia.

1.3.1.1 Substituição

> "As escritas cifradas simples, com substituição de letras em um único passo, predominaram na criptologia européia desde a era romana até o século XV. E então surgiu rapidamente na Europa uma série de avanços que não só transformaram a criptologia, mas lançaram as bases para o desenvolvimento da estatística e dos computadores. Todos esses avanços fundamentaram-se no súbito aparecimento do "disco cifrador" atribuído ao primeiro dos grandes "homens da Renascença", Leon Battista Alberti (1404-1472), conhecido por esse motivo como "o pai da criptologia". "Com essa invenção", escreve Kahn, "o Ocidente, que até este ponto

> tinha igualado, mas nunca superado o Oriente na criptologia, tomou uma dianteira que nunca mais perderia.” (SATINOVER, 1997)

Alberti criou dois discos de placas de cobre, onde a circunferência de um dos discos era maior do que a circunferência do outro. Dessa forma, no disco maior Alberti escreveu de forma circular de 24 letras e números diferentes, possibilitando assim a combinação dos discos de 24 maneiras distintas.

Bastava apenas Alberti enviar a informação das letras que deveriam ser combinadas para que a mensagem fosse decodificada e transformada em texto puro novamente.

Mesmo com esta “invenção”, o método de criptografia permanecia como substituição, porém, ao escrever algumas palavras Alberti girava novamente o disco, podendo, dessa forma, uma mesma palavra estar escrita de várias formas, tornando um eficiente método de substituição polialfabética.

A figura 1.4 ilustra o disco de Alberti.

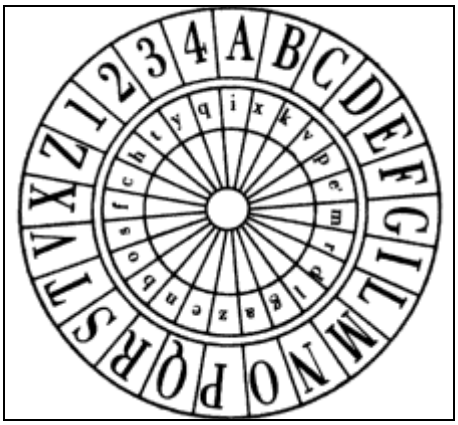

Figura 1.4: Disco cifrador criado por Alberti
Fonte: A verdade por trás do código da bíblia. Página 109

Segundo SMITH (1955), a maioria dos criptogramas científicos foi originada pelos Gregos, os quais utilizavam freqüentemente figuras geométricas para suas aplicações.

Um dos métodos conhecidos de substituição é a criação de um quadrado contendo as letras do alfabeto. Para cada letra escolhida, era representada através do número referente à linha e do número referente à coluna.

Por exemplo, a letra C era representada por 31. A letra H era representada por 32. A letra I representava ao mesmo tempo seu valor e também a letra J.

Tabela 1.1: Tabela de substituição

	2	3	5	4	1
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Fonte: *Cryptography. The Science of Secret Writing*. Pagina 65.

Já segundo SCHNEIER, o método mais simples de criptografia por substituição é o método onde cada caractere do texto puro é substituído por outro caractere, o qual terá como resultado a palavra criptografada. Para decriptografar a mensagem, basta substituir novamente as letras alteradas pelas letras originais, obtendo acesso, dessa forma, à mensagem original.

Podem ser utilizados três métodos para efetuar a criptografia por substituição:

Substituição Simples ou Substituição Monoalfabética, onde cada caractere é substituído por uma letra correspondente na mensagem cifrada.

Substituição Polialfabética quando mais de um caractere é substituído por outros caracteres.

Substituição Poligrâmica, onde blocos de caracteres são substituídos por outros blocos de caracteres.

1.3.1.2 Cifra de César

"Discutivelmente, o esquema de criptografia mais antigo é a Cifra de Cesar, que recebeu esse nome em homenagem a Júlio Cesar, que usou este esquema para proteger importantes mensagens militares (todas as mensagens de César eram escritas em Latim, naturalmente, o que as tornava incompreensíveis para a maioria das pessoas). A Cifra de Cesar é uma maneira simples de confundir uma mensagem escrita em linguagem que forma palavras a partir de um alfabeto. (GOODRICH, 1899. Pag. 112)"

A Cifra de Cesar consiste em deslocar as letras do alfabeto em três posições. Ou seja, substituir a letra 'A' pela letra 'D', a letra 'B' pela letra 'E'. Ao chegar à letra 'X', a letra a substituir volta para o início do alfabeto, sendo utilizada então, a letra 'A'. A letra 'Y' é substituída pela letra 'B' e finalmente, a letra 'Z' substituída pela letra 'C', concluindo a rotação em todo o alfabeto.

Tabela 1.2: Posição de letras para Cifra de César.

1ª Linha	A	B	C	D	E	F	G	H	I	J	K	L	M
Encriptado	D	E	F	G	H	I	J	K	L	M	N	O	P

Fonte: O autor.

Tabela 1.3: Continuação posição de letras para Cifra de Cesar.

1ª Linha	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Encriptado	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fonte: O autor.

Utilizando esta tabela como base e aplicando a Cifra de César, a palavra BRAMBILLA criptografada ficaria EUDPELOOD.

A linha referente à 1ª linha é a palavra que deseja criptografar. Basta substituí-la pela letra referente à linha Encriptado e será gerada a nova palavra. A segunda linha, nada mais é do que o alfabeto com algumas posições deslocadas. Este deslocamento, obviamente, deve ser previamente combinado entre ambas as partes através de um meio seguro.

Neste exemplo, o deslocamento é de 3 posições, sendo, conseqüentemente, a chave de criptografia igual a 3.

1.3.1.3 Cifra de Vigenère

Em 1586, o francês Blaise de Vigenère baseado em Alberti e Trithemius lançou seu livro de criptologia descrevendo detalhadamente sua cifra de substituição polialfabética utilizando palavras chaves, o que ficou conhecido como Carreiras de Vigenère.

Segundo Salomon (2005), Vigenère criou a mais importante extensão do algoritmo criado por Trithemius para a Substituição Polialfabética de mensagens, onde o mesmo utilizando-se do mesmo método aplicou o conceito de chave.

A tabela 1.4 representa um exemplo das carreiras de Vigenère ilustrando a forma como os caracteres eram distribuídos no quadro.

Tabela 1.4: Carreiras de Vigenère.

Texto Puro	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: *Cryptography. The Science of Secret Writing*. Página 71.

Utilizando as Carreiras de Vigenère, após um período longo de trabalho acabava tornando-se comum a existência de erros devido à dificuldade de visualização das letras.

Na coluna superior horizontal estão disponíveis as letras do texto puro. Através de uma chave a ser utilizada, encontra-se a primeira letra da chave na coluna vertical esquerda e a letra desta intersecção é a letra correspondente, criptografada.

Vamos exemplificar criptografando a palavra “cifra” utilizando a chave “texto”.

Ao encontrar a letra “c” (primeira letra a ser cifrada) na coluna superior, busque a letra “t” (primeira letra da chave) e a intersecção das mesmas será a letra criptografada, que neste caso, é a letra “v”. A letra “i” deve ser encontrada na coluna superior e na coluna esquerda vertical a letra “e”, resultando na letra “m”, e assim por diante. O resultado da palavra cifra após aplicar as Carreiras de Vigenère é “vmcko”.

Utilizando as tabelas encontradas como “modelos” para as Carreiras de Vigenère, foi criada a tabela 1.5 para demonstrar o exemplo:

Tabela 1.5: Exemplo de aplicação da Carreira de Vigenère.

Texto puro	C	I	F	R	A
Chave	T	E	X	T	O
Deslocamento	19	4	23	19	14
Resultado	V	M	C	K	O

Fonte: O autor.

Salomon explica que a Cifra de Vigenère é fácil de ser quebrada devido ao fato de que, as letras do texto puro, ficam na parte superior da tabela, sendo possível efetuar as combinações necessárias para decriptografar a mensagem utilizando-se apenas 26 linhas com as possíveis combinações.

1.3.1.4 Régua de Saint-Cyr

Situada na cidade de Saint-Cyr, a academia militar francesa, entre 1880 e início do século XX deu origem a este instrumento que se destinava a instruir os estudantes de criptologia. Auguste Kerckhoff, holandês reconhecido no mundo no mundo da criptologia foi quem batizou esta régua com o nome da cidade.

A régua permite a substituição monoalfabética de letras apenas colocando uma tira com dois alfabetos seguidos deslizando sobre uma tira mais larga, contendo apenas um alfabeto ordenado e utilizando-se a palavra chave como ponto para deslocamento da régua.

A figura 1.5 demonstra a régua de Saint-Cyr.

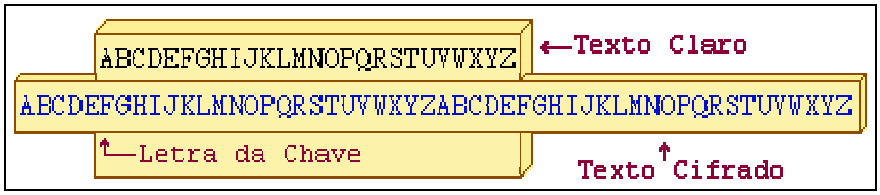

Figura 1.5: Régua de Saint-Cyr
Fonte: Criptografia NumaBoa

1.3.1.5 Transposição

Diferentemente da Cifra de Substituição que altera as letras originais da mensagem por outras letras, a Cifra de Transposição mantém os mesmos caracteres originais, porém, alterando a sua ordem de apresentação.

Para que isto seja possível, deve ser escolhida uma palavra chave com caracteres não repetitivos e disposta esta palavra em colunas de uma grade de dados. Supondo que a palavra chave escolhida seja “cesar”, a tabela ficaria da seguinte forma.

A tabela 1.6 distribui em uma grade a chave que será utilizada para criptografar a palavra.

Tabela 1.6: Chave para cifra de Transposição.

C	E	S	A	R

Fonte: O autor.

Depois de adicionada a palavra chave na grade, colocam-se números seqüenciais, seguindo a ordem alfabética de cada letra, conforme tabela 1.7:

Tabela 1.7: Ordenação da chave seguindo ordem alfabética.

C	E	S	A	R
2	3	5	1	4

Fonte: O autor.

Utilizando a chave “cesar” e seguindo a ordem alfabética, ficaria “acers”:

O próximo passo então é a distribuição da mensagem que desejamos aplicar a transposição nas linhas abaixo da numeração, respeitando o limite de colunas disponíveis.

Como exemplo, vamos efetuar a transposição da mensagem “fomosdescobertos”.

Tabela 1.8: Tabela com a mensagem a ser transposta.

C	E	S	A	R
2	3	5	1	4
F	O	M	O	S
D	E	S	C	O
B	E	R	T	O
S	X	P	Q	T

Fonte: O autor.

Após a distribuição da mensagem nas devidas colunas, complementamos as colunas restantes com letras aleatórias para confundir o interceptador.

O próximo passo é utilizar todas as letras das colunas, seguindo a numeração em ordem crescente e adicioná-las em uma linha apenas. Após aplicarmos o método de transposição, o resultado da mensagem seria “OCTQFDBSOEEXSOOTMSRP”.

Para efetuar a quebra deste tipo de criptografia, o interceptador deverá conhecer a palavra chave para definição da quantidade de colunas e também da ordem da distribuição das letras, dificultando o entendimento da mensagem capturada. (Redes de computadores, P. 219)

Outra forma de aplicar a transposição é sem a utilização da palavra chave, distribuindo a mensagem em colunas. Sempre que for atingido um determinado número de linhas, a mensagem é continuada na próxima coluna. Seguindo o exemplo da mensagem "Fomos descobertos" e o número máximo de 3 linhas, teríamos a tabela 1.9:

Tabela 1.9: Tabela de Transposição sem palavra chave.

F	O	E	O	R	S
O	S	S	B	T	X
M	D	C	E	O	E

Fonte: O autor.

Os últimos caracteres do quadro não fazem parte da mensagem, porém, foram adicionados aleatoriamente para complementar o quadro e confundir o interceptador. A mensagem criptografada então poderá ser lida a cada linha, ficando da seguinte forma:

"FOEORSOSSBTXMDCEOE".

Após a aplicação deste método e destas transposições, temos a mensagem cifrada, pronta para ser enviada ao destinatário com o mesmo risco de interceptação das demais, porém, com um menor risco de visualização do conteúdo.

1.3.1.6 Data Encryption Standard (DES)

Segundo Terada (2000), o algoritmo DES é o mais utilizado internacionalmente ainda hoje, e foi um avanço cientifico significativo no sentido de ter sido o primeiro algoritmo de criptografia cujo conhecimento do código se tornou publico: até então todos os algoritmos eram secretos. Ou seja, a segurança do DES não se baseia no conhecimento do algoritmo, mas no conhecimento da chave secreta. Foi projetado pela IBM e publicado pelo National Bureau of Standards – NBS – em 1977 para ser adotado como padrão nos EUA para informações comerciais.

Tendo seu inicio de desenvolvimento na década de 1960 por Horst Feistel, o algoritmo denominado LUCIFER foi o projeto que teve seu desenvolvimento concluído em 1971. O projeto Lucifer possuia criptografia com blocos de 64-bits utilizando uma chave de 128 bits. Com base neste projeto, foi iniciado um projeto para desenvolvimento de uma cifra com blocos de 64-bits, porém utilizando uma chave de 56-bits, tornando-se o padrão DES.

> "O Padrão de Criptografia de Dados (DES – *Data Encryption Standard*) foi uma cifra desenvolvida pela IBM que foi adotada pelo governo dos Estados Unidos em janeiro de 1977, para as informações não-classificadas. Esse padrão também foi bastante usado por empresas e organizações públicas e governamentais. O conceito contido no DES é que o texto original é criptografado por substituição em blocos de 64 bits e é parametrizado por uma chave de 64 bits, dos quais apenas 56 são realmente utilizados na chave."

Com o passar do tempo, este padrão de criptografia deixou de ser seguro, sendo necessário melhorar o método implementado. Dessa forma foi criado o Encadeamento DES, onde o mesmo adiciona um bloco do texto original na seqüencia de dados criptografados. Após efetuar esta adição, é aplicada a criptografia sobre a mensagem por completo.

1.3.1.7 *Advanced Encryption Standard* (AES)

O *Advanced Encryption Standard* que chamaremos de AES, é, segundo Cheswick, o sucessor do DES. Embora o DES não seja mais considerado como suficientemente forte, seus métodos são amplamente utilizados e recomendados. O AES surgiu em 2002 quando Daemen e Jijmen adicionaram o modo contador, que foi aprovado para o AES.

O AES mapeia blocos de texto puro em blocos de texto cifrado e blocos de texto cifrado em texto puro, sendo conhecida como cifra de bloco. O que é alterado no padrão AES é que pode utilizar blocos de diferentes tamanhos, podendo ser de 128, 196 e 256 *bits*, sendo considerado como bloco padrão o de 128 *bits*.

As chaves a serem utilizadas também podem variar de acordo com esses tamanhos de blocos.

No AES, a criptografia é realizada mediante a transformação da mensagem de texto puro com 10, 12 ou 14 etapas via substituição e transformação, podendo variar a quantidade de etapas de acordo com o tamanho da chave.

Para cada etapa, são aplicadas quatro operações, onde, a primeira consiste em uma caixa de substituição (*S-Box*) de tamanho 8 X 8 em cada *byte*, a segunda e terceira operações para deslocamento de linhas e substituição de colunas em *array* e a quarta operação, onde os *bits* da chave são combinados com os dados. Após essas quatro operações, os dados são enviados para serem embaralhados.

O processo de decifragem da mensagem é o mesmo que o de cifragem, alterando apenas as tabelas e polinômios utilizados.

1.3.1.8 IDEA

O algoritmo IDEA (*International Data Encryption Algorithm*) foi criado em 1991 por Xuejia Lai e James Massey com o nome IPES. Atualmente este algoritmo é usado em sistemas de criptografia, como por exemplo, o PGP (*Pretty Good Privacy*), que é bastante utilizado para segurança de dados trafegados na internet e e-mails.

O IDEA utiliza blocos de 64-bits como o DES, no entanto, cada bloco é dividido internamente em 4 blocos de 16-bits utilizando-se uma chave de 128 bits.

1.3.2 Criptografia Assimétrica

Segundo Tittel (2003), assim como outros algoritmos de chave assimétrica, o RSA (*Rivest Shamir Adleman*) é indiscutivelmente mais lento do que algoritmos de chave simétrica. Isso se deve ao fato de que o tamanho das chaves utilizadas pode variar entre 512, 768, 1024 bits ou mais, elevando o período de processamento de encriptação e decriptação das mensagens. O processo de encriptação da mensagem ocorre da seguinte forma:

- O algoritmo gera uma chave aleatória para a sessão;

- Utilizando-se um método simétrico, a carga útil *payload* é criptografada;

- A chave de sessão é criptografada com o método RSA;

- A carga útil e a chave de sessão são enviadas ao receptor.

1.3.3 Funções HASH

Explicado o conceito de Tabelas Hash, vamos aos exemplos de aplicação das funções de *hash* em algoritmos como MD5 e SHA.

1.3.3.1 Message Digest 5

Segundo Salomon, *Message Digest* 5 (abreviada por MD5) é uma função desenvolvida por Ronald Rivest em 1992 com o objetivo de ser rápido (em especial em computadores de 32-bits) e com alto nível de segurança nas assinaturas digitais das aplicações. O MD5 recebe uma mensagem de qualquer tamanho e aplica um *hash* de 128-bits. Por se tratar de uma criptografia mais segura, a mesma possui velocidade de processamento inferior ao MD4.

MD5: A vedete do mundo do software livre, o MD5 é um algoritmo para obter *hash* de mensagens e foi desenvolvido por Ron Rivest no MIT. O algoritmo aceita como entrada

uma mensagem de tamanho arbitrário e produz como saída 128 bits (4 palavras de 32 bits) que representam seu valor de *hash* (CARMONA, 2005).

1.3.3.2 Secure Hash Algorithm (SHA)

Secure Hash Algorithm, uma Função de Espalhamento Unidirecional inventada pela NSA. Gera um valor *hash* de 160 *bits*, a partir de um tamanho arbitrário de mensagem. O funcionamento interno do SHA-1 é muito parecido com o observado no MD4, indicando que os estudiosos da NSA se basearam no MD4 e fizeram melhorias em sua segurança. De fato, a fraqueza existente em parte no MD5, citada anteriormente, descoberta após o SHA-1 ter sido proposto, não ocorre nele. Atualmente, não há nenhum ataque de criptoanálise conhecido contra o SHA-1. Mesmo o ataque da força bruta torna-se impraticável, devido ao seu valor *hash* de 160 bits. Porém, não há provas de que, no futuro, alguém não possa descobrir como quebrar o SHA-1 (GOMES, 2004).

1.3.4 Esteganografia

Conforme visto no conceito de Esteganografia, ela pode ser adicionada a vários tipos de arquivos e dentre eles, imagens.

No caso de aplicação de mensagens em imagens, pode ser feito de várias formas, porém, serão citadas duas delas. Uma das formas é através da utilização do bit menos significativo para o armazenamento da imagem, onde apenas a aparência da imagem fica mais escura, sem que seja possível visualizar a olho nu a alteração. A segunda forma é através da adição do conteúdo da mensagem no final do arquivo de imagem, utilizando-se um caractere identificador, como, por exemplo, ‘®’. Para efetuar a leitura da mensagem contida na imagem, basta carregar o mesmo para edição e encontrar o caractere separador, buscando a seqüência posterior ao identificador.

2. Simuladores e Trabalhos Correlatos na Área de Ensino da Criptografia

2.1 Ferramentas encontradas

Foram encontrados vários simuladores para os métodos de criptografia citados neste trabalho, no entanto, apenas uma ferramenta direcionada ao estudo desta técnica e esta ferramenta está dividida em dois projetos, denominados Cryptool e JCriptool.

Cryptool é uma ferramenta de *e-learning*, fruto de um projeto Open Source que visa disponibilizar um ambiente em que se possam verificar os resultados gerados quando utilizadas as técnicas de criptografia implementadas na mesma.

Esta ferramenta possui dois projetos em desenvolvimento, onde o primeiro está sendo desenvolvido em C#, utilizando-se o ambiente Visual Studio 2008 e tendo sido denominado Criptool. O segundo projeto está sendo desenvolvido na plataforma Java, utilizando o ambiente Eclipse RCP (*Eclipse Rich client Platform*) e tendo sido denominado JCryptool.

2.2 Funcionalidades existentes

Na versão 1.4.30 Beta 3 da Cryptool é possível encontrar simuladores para criptografar e Decriptografar utilizando chaves simétricas, assimétricas e híbridas.

A ferramenta permite que sejam visualizados e acompanhados os passos necessários para a completa aplicação do método escolhido.

A ferramenta disponibiliza conteúdo para a teoria dos números.

É possível, através da ferramenta, encontrar um jogo educativo denominado *Number Shark*, o qual visa ensinar crianças de até 10 anos a utilização de fatoração de números.

2.3 Tipo de licenciamento

O licenciamento da ferramenta Cryptool é Open Source, onde qualquer desenvolvedor com conhecimentos nas linguagens Java ou C# pode baixar através do site o

código fonte e efetuar as devidas modificações. Enviando novamente pelo site as alterações poderão ser disponibilizadas em novas versões da ferramenta.

2.4 Desenvolvimento de novas funcionalidades

Por se tratar de uma ferramenta Open Source, a Cryptool pode ser amplamente atualizada e é totalmente permitida a adição de funcionalidades à ferramenta, sendo necessário apenas o desenvolvedor efetuar o download dos códigos fonte disponíveis no site e criar as funcionalidades de sua escolha.

No decorrer da análise da ferramenta, foram implementadas diversas funcionalidades e disponibilizadas nas versões, porém, nenhuma relacionada à tradução para o idioma Português.

2.5 Interatividade com o aluno

A ferramenta possui interatividade total com o aluno, pois o mesmo pode fornecer todas as informações necessárias para a simulação do ambiente. O aluno pode visualizar através da própria ferramenta todos os passos necessários para a completa encriptação das informações.

2.6 Obter mais informações sobre a ferramenta

A ferramenta pode ser baixada em http://www.cryptool.de, onde estarão disponíveis, além da própria ferramenta, os códigos fonte da aplicação. De posse do código fonte é possível alterar a ferramenta de forma que seja adicionado conteúdo ao atual, aumentando dessa forma a abrangência da ferramenta.

2.7 Interface

Na figura 2.1 pode ser visualizada a interface da ferramenta Cryptool.

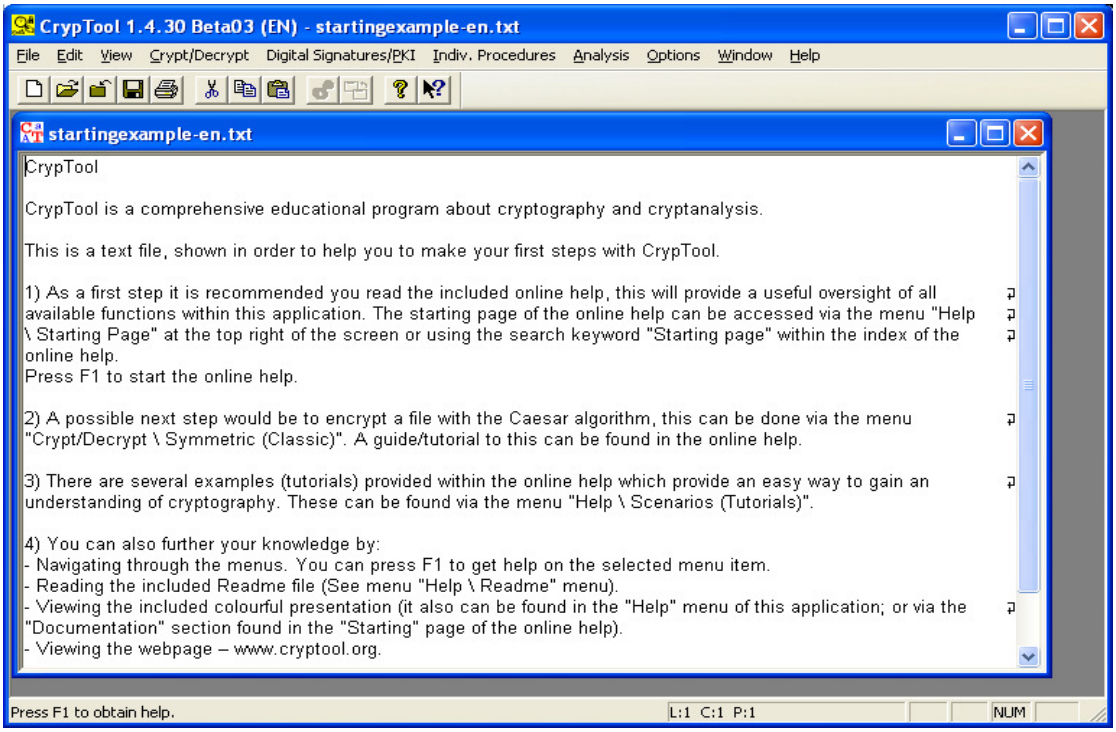

Figura 2.1: Interface da ferramenta Cryptool
Fonte: Retirado *printscreen* da própria ferramenta em execução.

3. Modelagem da Ferramenta

Para que um projeto possa ser implementado e ter sucesso na sua realização durante o desenvolvimento, se faz necessária a modelagem da ferramenta, onde será possível visualizar todas as características que o projeto terá. Para que a modelagem possa ser realizada, o primeiro passo é a definição dos requisitos do sistema.

Neste capítulo serão descritos os requisitos funcionais e não-funcionais da ferramenta, além dos Casos de Uso, Diagrama de atividades, Diagrama de Estados e Diagrama de Seqüencia.

3.1 Requisitos

Segundo Bezerra, a etapa de Levantamento de Requisitos, também conhecida como elicitação de requisitos, é a etapa onde serão mapeados todos os problemas que deverão ser resolvidos com a implementação da ferramenta proposta. Este é o ponto em que desenvolvedor e cliente definem o que será ou não atendido pela ferramenta.

3.1.1 Funcionais

Nos requisitos funcionais deverão estar contidas todas as funcionalidades que o sistema estará proporcionando ao utilizador.

Com base na análise efetuada sobre o conteúdo a ser ministrado e nas simulações a serem criadas, foram identificados os seguintes requisitos funcionais:

- A ferramenta deverá ensinar o que é criptografia;

- A ferramenta deverá demonstrar ao aluno a história da criptografia;

- A ferramenta deverá dispor de exercícios teóricos e práticos para preenchimento;

- A ferramenta deverá dispor de exemplos para os conteúdos;

- A ferramenta deverá armazenar o histórico de preenchimento dos exercícios e permitir ao professor visualizar as estatísticas dos alunos;

- A ferramenta deverá possuir manutenção de usuários;

- A ferramenta deverá permitir que os usuários sejam desativados;

- A ferramenta deverá possuir conteúdo teórico para esteganografia;

- A ferramenta deverá possuir recursos para aplicação de esteganografia de mensagens em imagens;

- A ferramenta deverá possuir conteúdo teórico para criptografia 3DES;

- A ferramenta deverá permitir a simulação de criptografia 3DES;

- A ferramenta deverá armazenar as informações em banco de dados MSDE;

- A ferramenta deverá possuir conteúdo teórico para Cifra de Cesar;

- A ferramenta deverá possuir simulador para a Cifra de César;

- A ferramenta deverá possuir conteúdo teórico para Chave Pública, Chave Privada, Chave Simétrica e Chave Assimétrica;

- A ferramenta deverá possuir conteúdo teórico para Criptovirologia, invasor, criptanalista e criptanálise;

- O aluno deverá efetuar *login* na ferramenta para sua própria identificação;

- A ferramenta deverá possuir um cadastro para usuários, contendo número de matrícula, senha, informação sobre o *status* do usuário (informando se está ativo ou não), nome completo e tipo de usuário, podendo ser administrador, professor ou aluno;

- A ferramenta deverá possuir recursos para efetuar a impressão de material.

3.1.2 Não-funcionais

Bezerra define os requisitos não-funcionais como sendo os requisitos que são desejáveis no sistema, sem interferir no funcionamento do mesmo.

Com base na análise efetuada, foram definidos os seguintes requisitos não-funcionais:

- A ferramenta deverá possuir uma tela de boas vindas para o usuário com a opção de não mostrar novamente;

- Após a tela de boas vindas deverá ser apresentada uma seqüencia de atividades a serem realizadas para a correta simulação dos métodos propostos;

- A ferramenta deverá possuir imagens ilustrativas para os conceitos e exemplos apresentados;

3.2 Diagrama de Classes

Segundo Guedes (2008), o diagrama de classes é o diagrama mais importante, pois é a partir dele que os demais serão gerados. Nele estarão contidos os atributos e métodos de cada classe, visualizando de forma estruturada todas as classes envolvidas na ferramenta modelada, além de apresentar a forma como as classes se relacionam e trocam informações.

Com base na teoria de Guedes, foi desenvolvido o diagrama de classes para o sistema, ilustrado na figura 3.1.

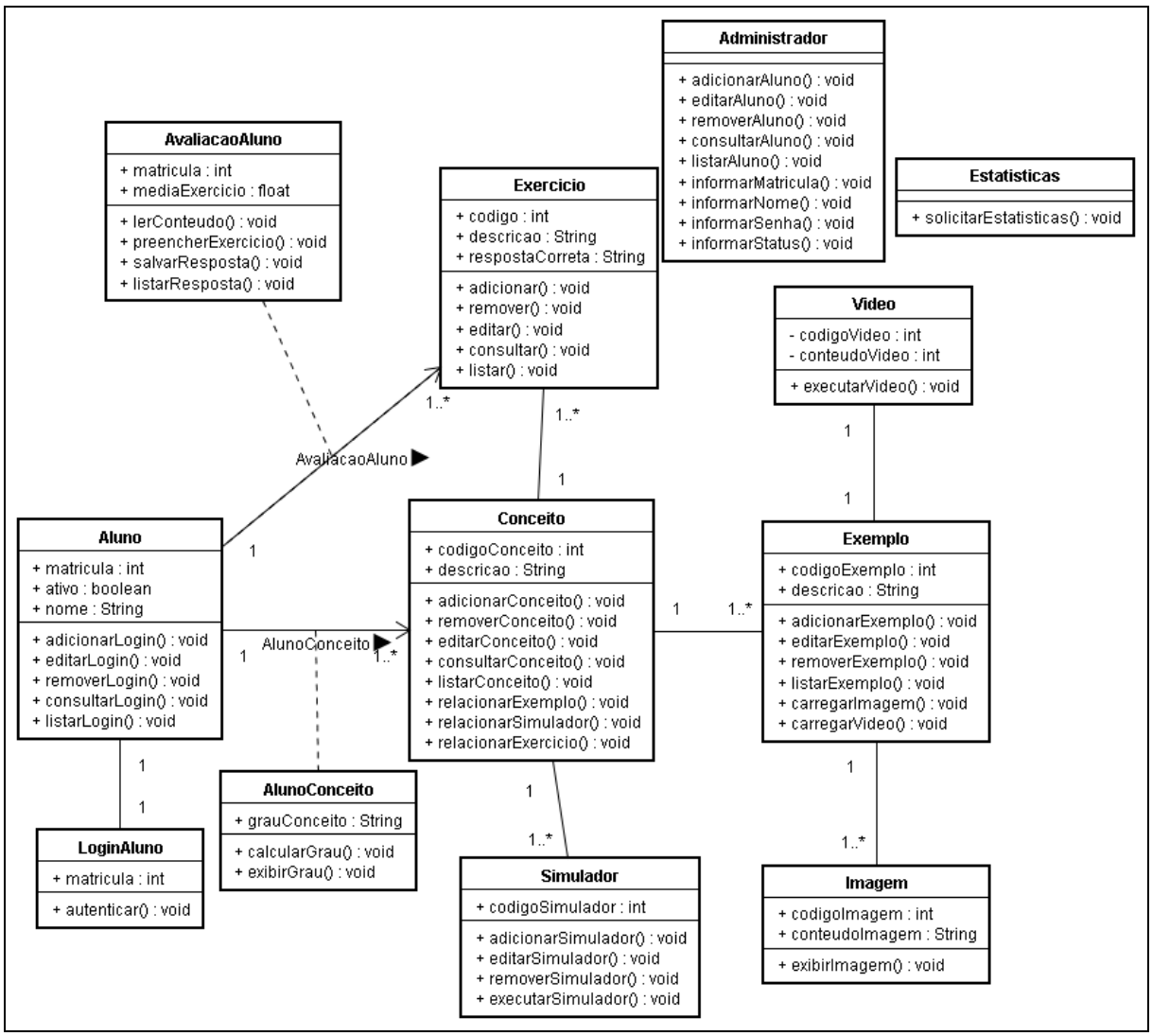

Figura 3.1: Diagrama de Classes da ferramenta
Fonte: O autor.

3.3 Diagrama de Caso de Uso

Conforme Guedes (2008), o Diagrama de Casos de Uso procura, através de uma linguagem simples, permitir a compreensão do comportamento externo do sistema. Através de uma perspectiva do usuário, tenta representar o comportamento de forma a ser entendido por qualquer pessoa. Dentre os diagramas da UML, é considerado o mais abstrato, se tornando dessa forma o mais flexível. O Diagrama de Casos de Uso é utilizado, sobretudo, para as etapas de levantamento de requisitos, podendo ser alterado durante o processo de engenharia e servindo como base para a modelagem dos demais diagramas.

Seguindo a definição de Guedes, foram definidos os Casos de Uso listados e explicados abaixo:

3.3.1 Caso de Uso Estudo de Conceito

No Caso de Uso de Estudo de Conceito, o aluno deverá efetuar a leitura do conteúdo disponibilizado na ferramenta.

Descrição

Aluno efetuará o estudo dos conceitos disponibilizados na ferramenta.

Pré-condição

- O aluno deverá estar autenticado no sistema.

Ator

Aluno

Fluxo principal

Ação do aluno	**Resposta do Sistema**
1 – Seleciona no sistema a opção desejada;	2 – Exibe ao aluno o conteúdo selecionado
3 – Efetua o estudo do conceito;	

3.3.1.1 Diagrama de Caso de Uso Estudo de Conceito

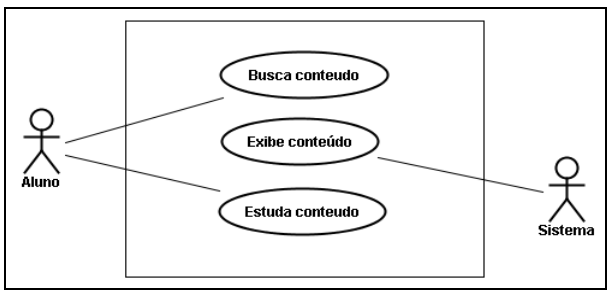

Figura 3.2: Diagrama de Caso de Uso Estudo de Conceito
Fonte: O autor.

3.3.1.2 Diagrama de Seqüência de Estudo de Conceito

O diagrama de seqüência de Estudo de Conceito foi criado para ilustrar a troca de mensagens entre as classes do sistema. A figura 3.3 apresenta essa troca de mensagens.

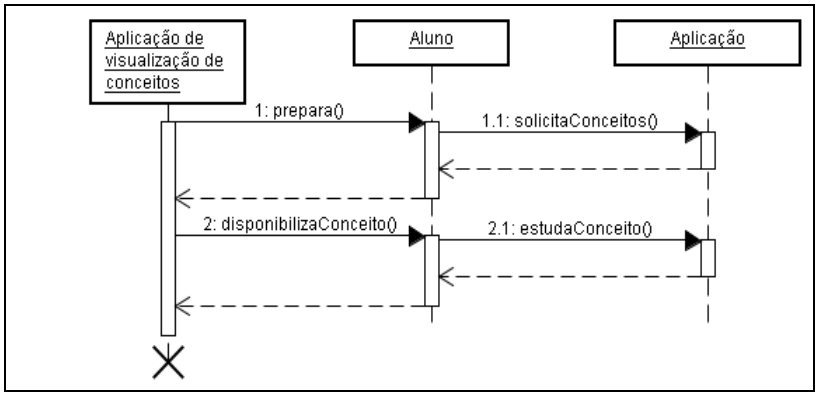

Figura 3.3: Diagrama de Seqüência de Estudo de Conceito
Fonte: O autor.

3.3.2 Caso de Uso Visualização de Exemplos

O Caso de Uso de Visualização de Exemplos se faz necessário para que o aluno possa, através da ferramenta, visualizar os exemplos disponibilizados para o conceito ilustrado.

Descrição

Aluno visualizará na ferramenta os exemplos relativos ao conteúdo lido.

Pré-condição

- O aluno deverá estar autenticado no sistema.
- O aluno deverá ter efetuado a leitura de todo o conteúdo relativo ao conceito escolhido.

Ator

Aluno

Fluxo principal

Ação do aluno	**Resposta do Sistema**
1 – Seleciona no sistema a opção desejada;	2 – Pesquisa na base de dados os exemplos da atividade solicitada;
	3 – Exibe ao aluno os exemplos relativos ao conteúdo selecionado;
4 – Visualiza os exemplos apresentados e efetua os questionamentos ao professor, caso existam.	

3.3.2.1 Diagrama de Caso de Uso Visualização de Exemplos

O Caso de Uso Visualização de Exemplos foi ilustrado na figura 3.4 de forma a representar a solicitação do aluno ao sistema os exemplos disponíveis, e estes, buscar os recursos de imagens, textos e/ou vídeos na base de dados, caso não estejam alocados na ferramenta.

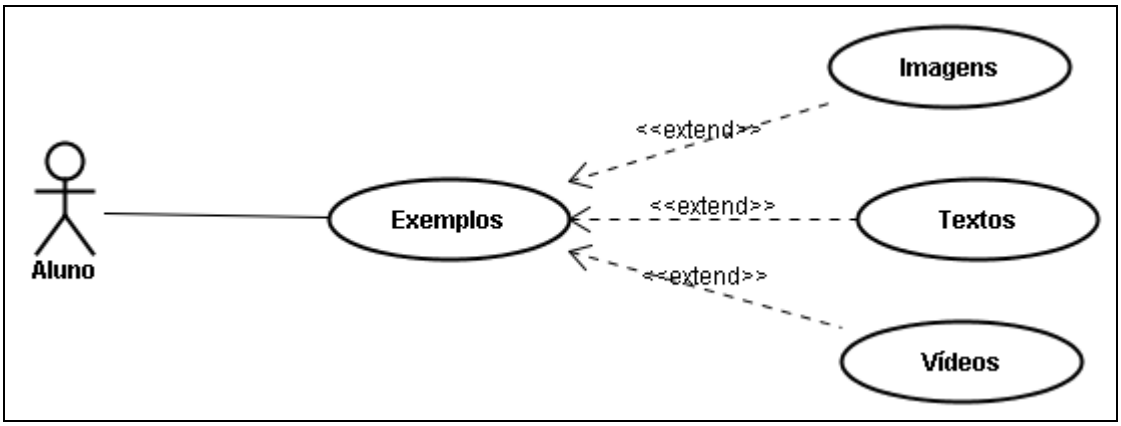

Figura 3.4: Diagrama de Caso de Uso Visualização de Exemplos
Fonte: O autor.

3.3.2.2 Diagrama de Seqüencia de Visualização de Exemplos

Abaixo está o diagrama de seqüência desenvolvido para a visualização dos exemplos na ferramenta.

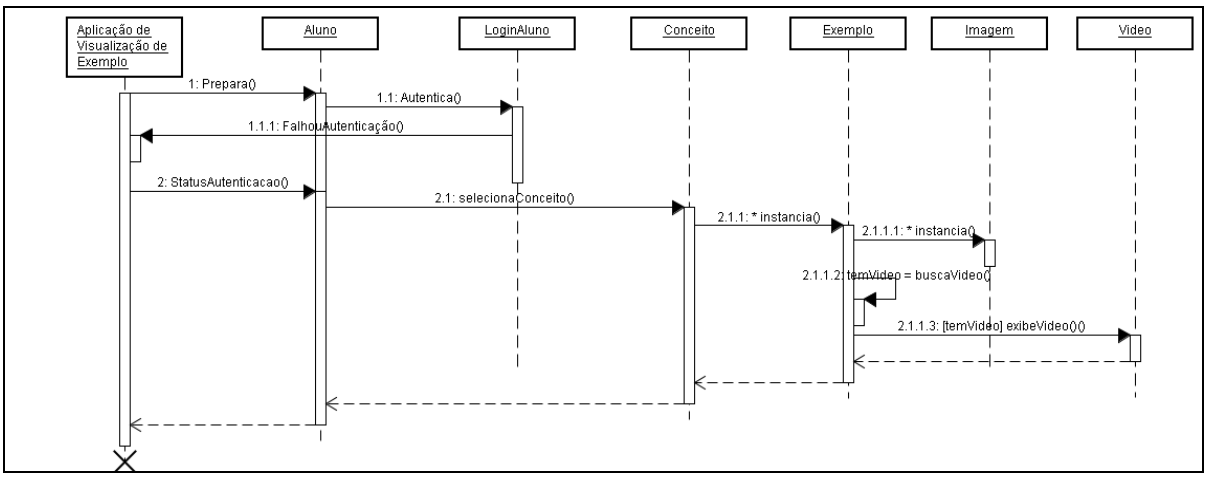

Figura 3.5: Diagrama de Seqüência de Visualização de Exemplos
Fonte: O autor.

3.3.3 Caso de Uso Execução Simulador

O Caso de Uso para Execução do Simulador foi desenvolvido para que o aluno possa interagir com o sistema executando as simulações necessárias para o entendimento das técnicas aplicadas.

Descrição

Aluno executará o simulador relativo ao conteúdo estudado.

Pré-condição

- O aluno deverá estar autenticado no sistema.
- O aluno deverá ter efetuado a leitura de todo o conteúdo relativo ao conceito escolhido.
- O aluno deverá ter visualizado os exemplos.

Ator

Aluno

Fluxo principal

Ação do aluno	Resposta do Sistema
1 – Seleciona no sistema o simulador do conteúdo estudado;	2 – Exibe ao aluno o simulador solicitado;
3 – Interage com o simulador;	

3.3.3.1 Diagrama de Caso de Uso Execução Simulador

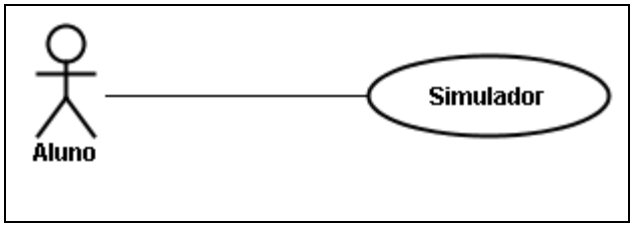

Figura 3.6: Diagrama de Caso de Uso de Execução Simulador
Fonte: O autor.

3.3.3.2 Diagrama de Seqüencia de Execução do Simulador

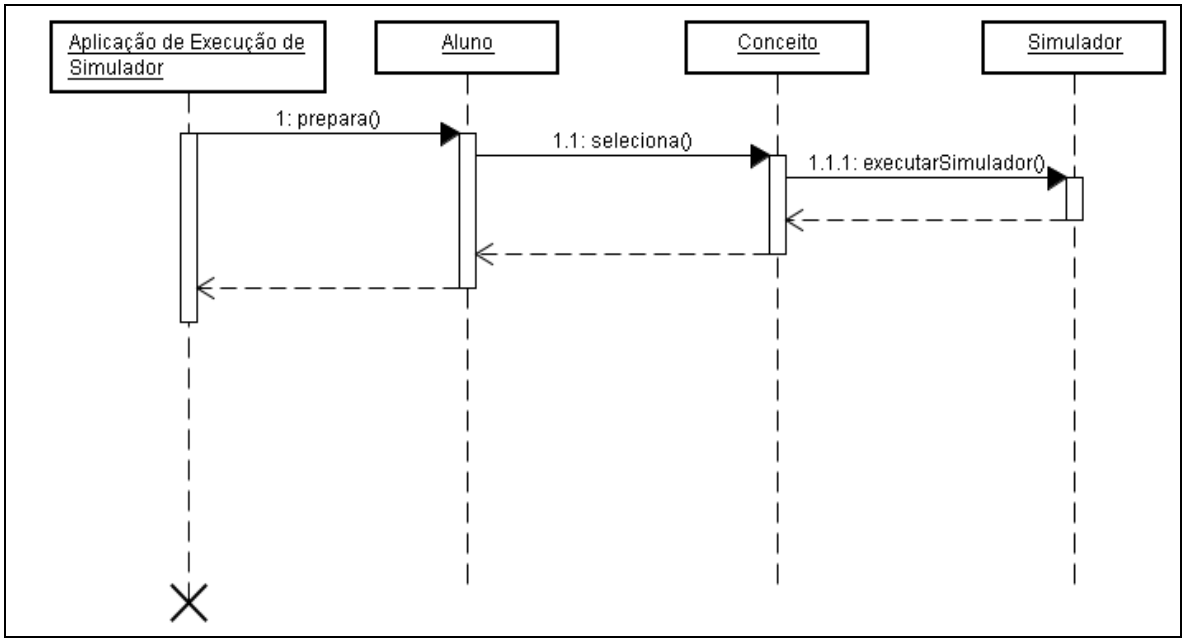

Figura 3.7: Diagrama de Seqüência de Execução Simulador
Fonte: O autor.

3.3.4 Caso de Uso Resolução Exercício

O Caso de Uso de Resolução Exercício se fez necessário para que o aluno possa preencher os exercícios propostos para o conceito estudado.

Descrição

Aluno solicitará ao sistema os exercícios do conteúdo estudado.

Pré-condição

- O aluno deverá estar autenticado no sistema;
- O aluno deverá ter efetuado a leitura de todo o conteúdo relativo ao conceito escolhido;
- O aluno deverá ter visualizado os exemplos e executado o simulador;

Ator

Aluno

Fluxo principal

Ação do aluno	**Resposta do Sistema**
1 – Seleciona no sistema os exercícios relativos ao conteúdo estudado;	2 – Exibe ao aluno os exercícios relativos ao conteúdo;
3 – Preenche no sistema os exercícios	4 – Grava na base de dados as respostas do

apresentados; aluno;

3.3.4.1 Diagrama de Caso de Uso Resolução Exercício

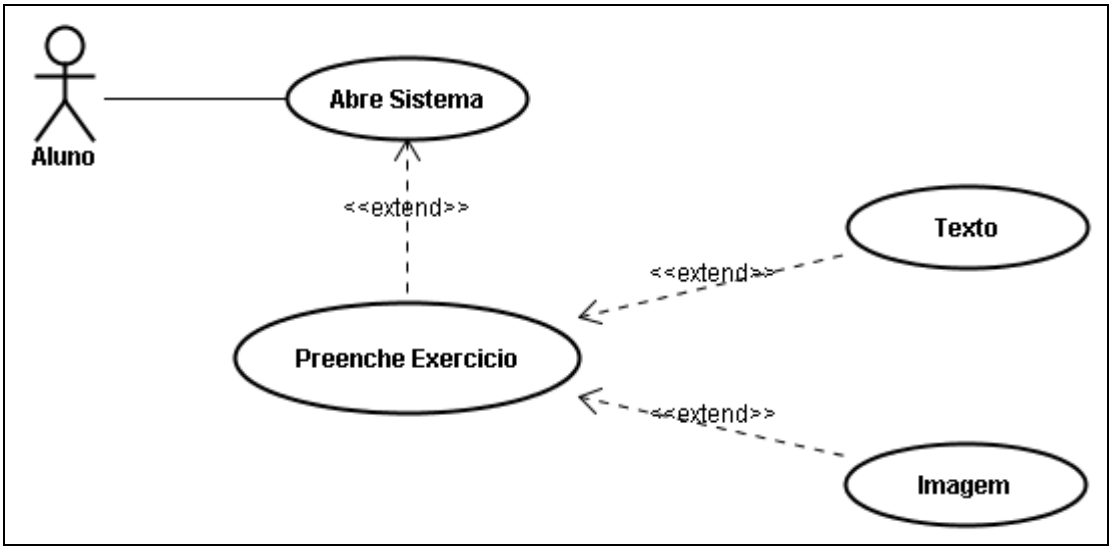

Figura 3.8: Diagrama de Caso de Uso de Resolução de Exercício
Fonte: O autor.

3.3.4.2 Diagrama de Seqüencia de Resolução do Exercício

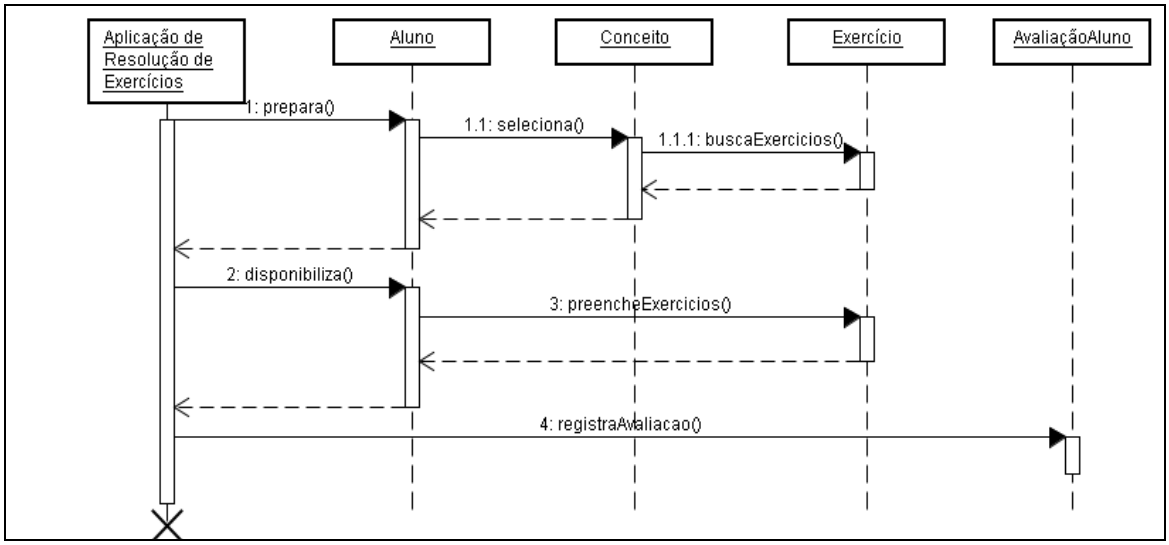

Figura 3.9: Diagrama de Seqüência de Resolução de Exercício
Fonte: O autor.

3.3.5 Caso de Uso Cadastro Aluno

Durante a modelagem foi percebida a necessidade de Cadastro do Aluno, onde deverá ser possível adicioná-lo ao sistema para que sejam disponibilizados os devidos conteúdos ao mesmo.

Descrição

O administrador do sistema cadastra no sistema o aluno

Pré-condição

- O administrador deverá estar autenticado no sistema

Ator

Administrador

Fluxo principal

Ação do Administrador	Resposta do Sistema
1 – Aciona no sistema a manutenção de alunos;	2 – Exibe ao administrador a interface da manutenção de alunos;
3 – Informa a matricula do aluno;	
4 – Informa o nome do aluno;	
5 – Informa uma senha padrão;	
6 – Marca opção de usuário ativo;	
7 - Aciona o botão de gravação das informações;	8 – Salva informações na base de dados; 9 – Retorna ao administrador a mensagem de sucesso.

3.3.5.1 Diagrama de Caso de Uso Cadastro Aluno

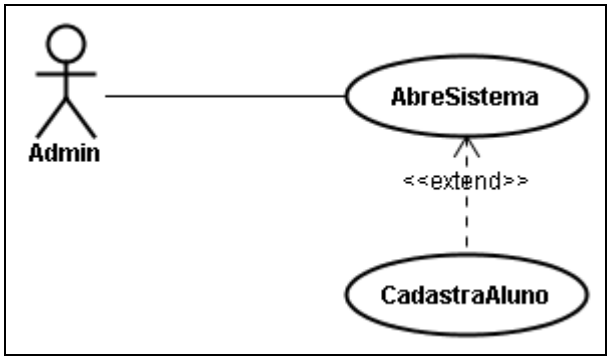

Figura 3.10: Diagrama de Caso de Uso de Cadastrar aluno
Fonte: O autor.

3.3.5.2 Diagrama de Seqüencia de Cadastro Aluno

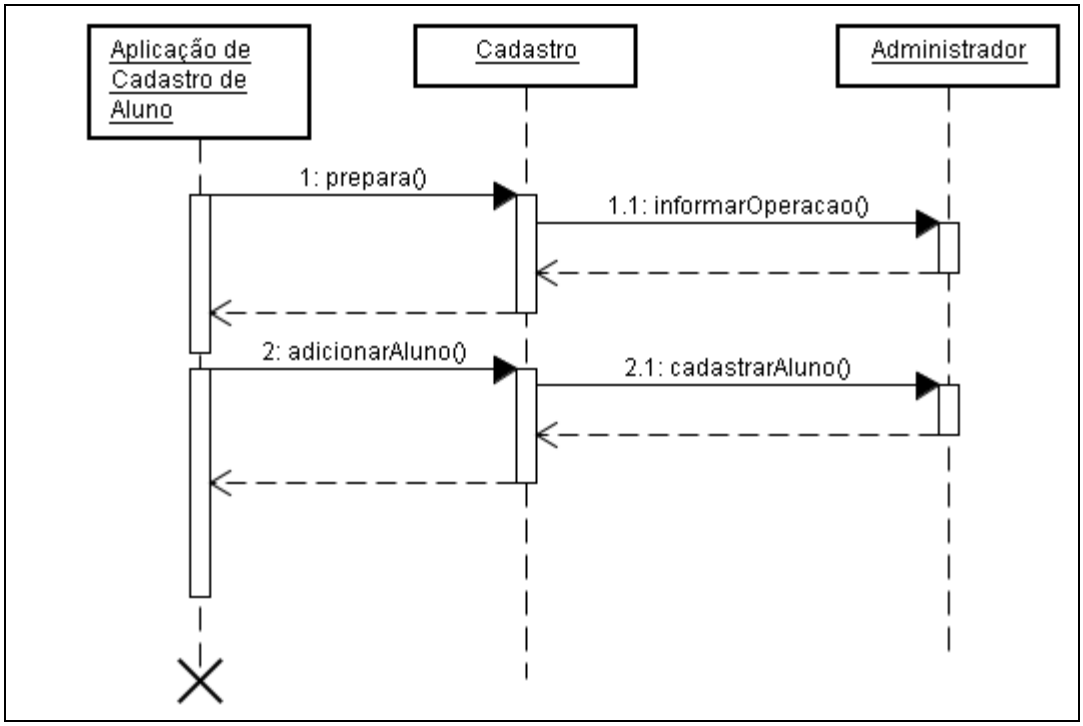

Figura 3.11: Diagrama de Seqüência de Cadastrar Aluno
Fonte: O autor.

3.3.6 Caso de Uso Obtenção de Estatísticas

Dentre os requisitos funcionais, foi identificada a necessidade de Obtenção de Estatísticas dos exercícios preenchidos pelos alunos. Para este requisito, foi desenvolvido o Caso de Uso de Obtenção de Estatísticas.

Descrição

O professor poderá visualizar as estatísticas de resolução dos exercícios dos alunos.

Pré-condição

- O professor deverá estar autenticado no sistema;
- O aluno deverá ter preenchido os exercícios.

Ator

Professor

Fluxo principal

Ação do Professor **Resposta do Sistema**

1 – Aciona no sistema de visualização de estatísticas;

2 – Exibe ao professor a interface da visualização das estatísticas;

3 – Informa o nome do aluno;

4 – Seleciona a lição a ser visualizada;

5 – Exibe na tela as estatísticas.

3.3.6.1 Diagrama de Caso de Uso Obtenção de Estatísticas

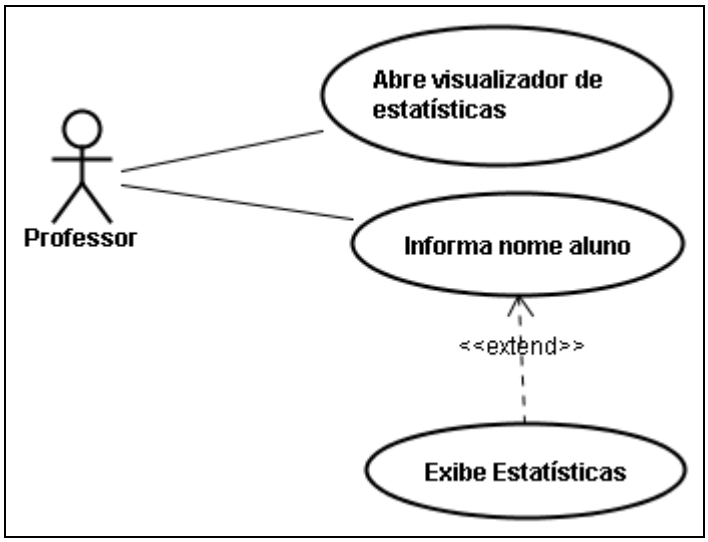

Figura 3.12: Diagrama de Caso de Uso de Obtenção de Estatísticas
Fonte: O autor.

3.3.6.2 Diagrama de Seqüencia Obtenção de Estatísticas

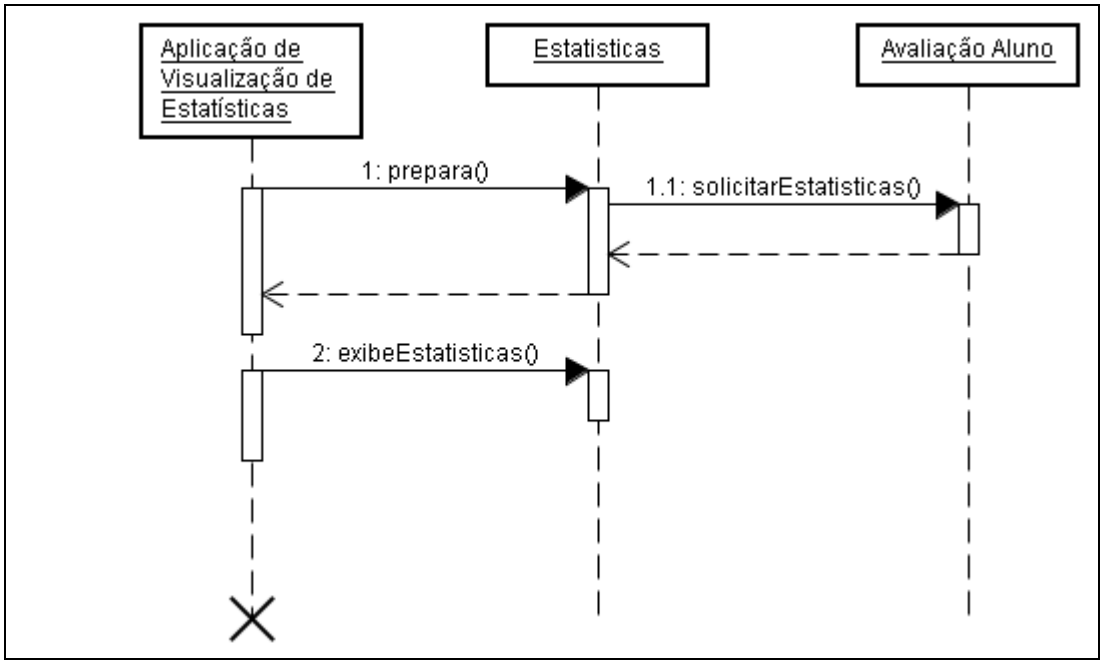

Figura 3.13: Diagrama de Seqüência de Obtenção de Estatísticas
Fonte: O autor.

3.3.6.3 Diagrama de Estado

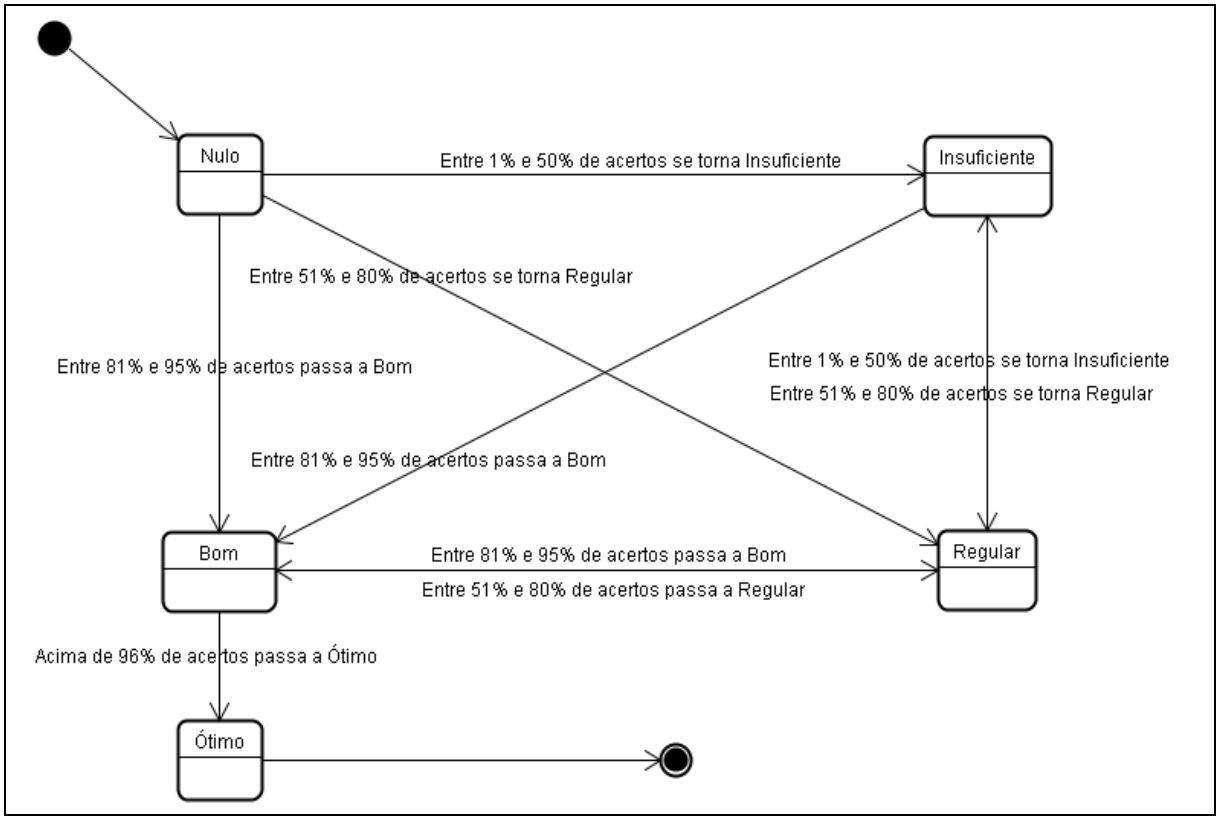

Figura 3.14: Diagrama de Estado de Estatísticas do Aluno
Fonte: O autor.

3.3.7 Caso de Uso Impressão de Material

Dentre os requisitos funcionais identificados, está contida a necessidade de impressão de material que foi apresentada na ferramenta, para tanto, foi desenvolvido o Caso de Uso de Impressão de Material.

Descrição

O aluno poderá imprimir o material sobre os conceitos e a listagem de exercícios.

Pré-condição

- O aluno deverá estar autenticado no sistema;
- O aluno deverá escolher o material a ser impresso;
- O material deverá estar disponível para impressão.

Ator

Aluno

Fluxo principal

Ação do Aluno	Resposta do Sistema
1 – Aciona no sistema de visualização de impressão de material;	2 – Exibe ao aluno os materiais disponíveis para impressão;
3 – Seleciona o material a ser impresso;	
4 – Aciona o botão de impressão;	5 – Envia para a impressora o material escolhido.

3.3.7.1 Diagrama de Caso de Uso Impressão de Material

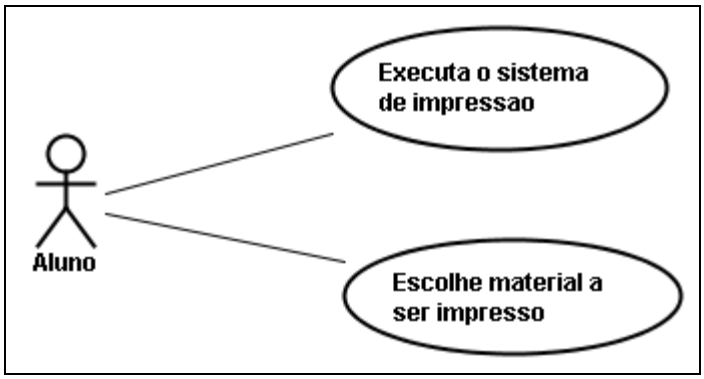

Figura 3.15: Diagrama de Caso de Uso de Impressão de Material
Fonte: O autor.

3.3.7.2 Diagrama de Seqüencia Impressão de Material

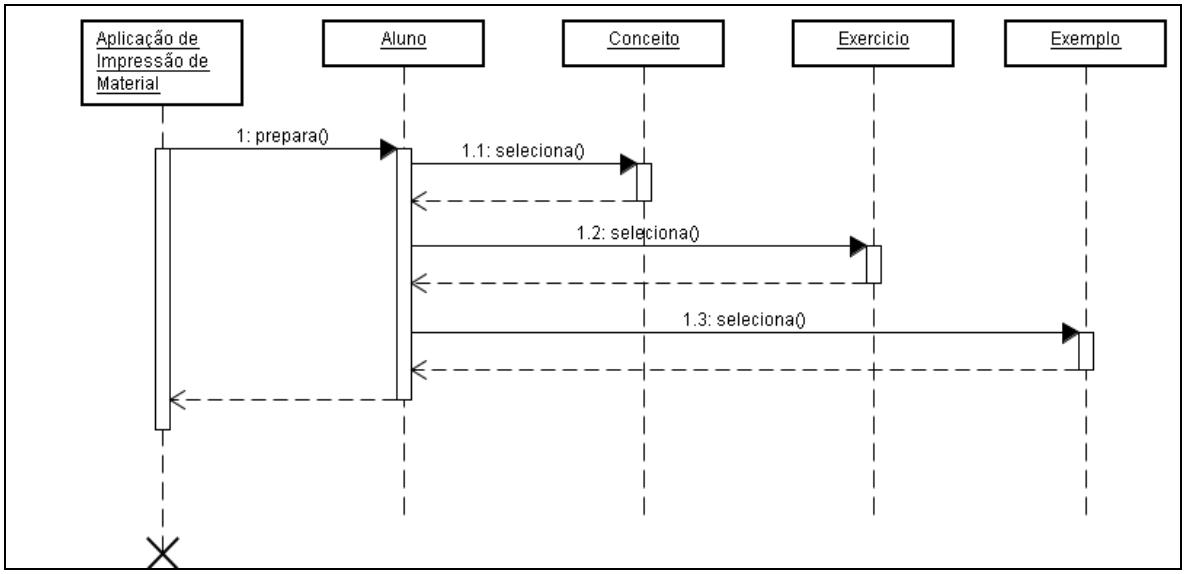

Figura 3.16: Diagrama de Seqüência de Impressão de Material
Fonte: O autor.

3.4 Diagrama de Atividades

Segundo Ramos (2006), um diagrama de atividades é um caso particular do diagrama de estados, onde todos, ou a maioria dos estados são tratados de atividades e todas, ou a maioria, das transições são desencadeadas pela conclusão das atividades dos estados anteriores.

Com base nesta definição, foi desenvolvido o diagrama de atividades ilustrado abaixo:

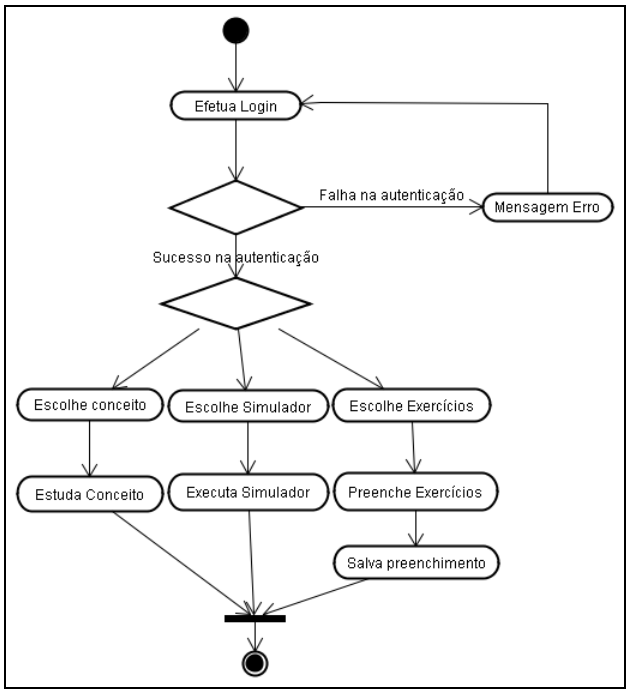

Figura 3.17: Diagrama de Atividades do aluno
Fonte: O autor.

4. Aspectos de Projeto do Protótipo

4.1 Recursos utilizados

Para a criação do protótipo foi utilizada a linguagem Object Pascal no ambiente de desenvolvimento Delphi 7 por se tratar de uma ferramenta de fácil e rápida utilização.

Foi utilizado o padrão UML para a modelagem com o objetivo de que a ferramenta possa ser implementada em outras linguagens de programação;

Para a criação dos Casos de uso foram utilizadas as Descrições Particionadas, onde foi representada nas tabelas, a coluna com ações do usuário e em outra coluna as respostas do sistema.

O Grau de Abstração do Caso de Uso foi do tipo essencial, o qual não faz menção à tecnologia utilizada.

O banco de dados utilizado para o armazenamento de estatísticas e usuários foi o MSDE (*Microsoft SQLServer Desktop Engine*).

Para a criação do ER foi utilizada a ferramenta DBDesigner da versão 4.0.5.6 Beta, o qual pode ser visualizado no item 4.3 deste trabalho.

4.2 Interface

Como o objetivo principal deste trabalho foi a análise e modelagem de uma ferramenta para apoio ao ensino da criptografia, foi desenvolvido um protótipo, onde foram identificadas melhorias a serem implementadas no sistema, alterando de forma significativa o diagrama de classes inicial.

O nome escolhido para a ferramenta foi *Cryptroom*, o qual busca passar a idéia de uma sala de estudos de criptografia.

Abaixo apresentaremos algumas telas criadas para a modelagem proposta.

A figura representa a tela de *login* do sistema, onde o aluno definirá seu nome de usuário (matrícula) e a senha para que possa utilizar o sistema e atrelar ao seu usuário as métricas de utilização e preenchimento de exercícios.

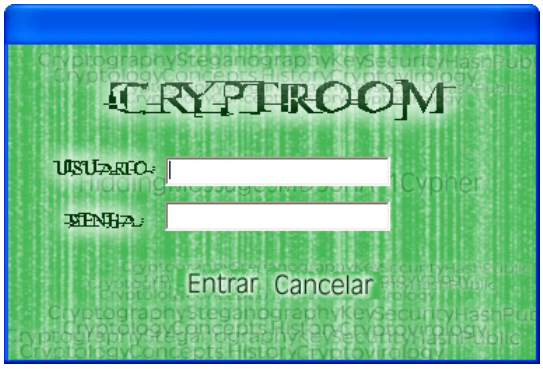

Figura 4.1: Tela de *login* do protótipo
Fonte: O autor.

Durante a modelagem, foi percebida a necessidade de criação de uma tela de manutenção de usuários, onde serão definidas as permissões dos mesmos, baseadas no tipo de usuário, podendo ser administrador (permissão total no sistema), professor (permissão para visualização de estatísticas dos alunos) e aluno (sem qualquer tipo de permissão administrativa).

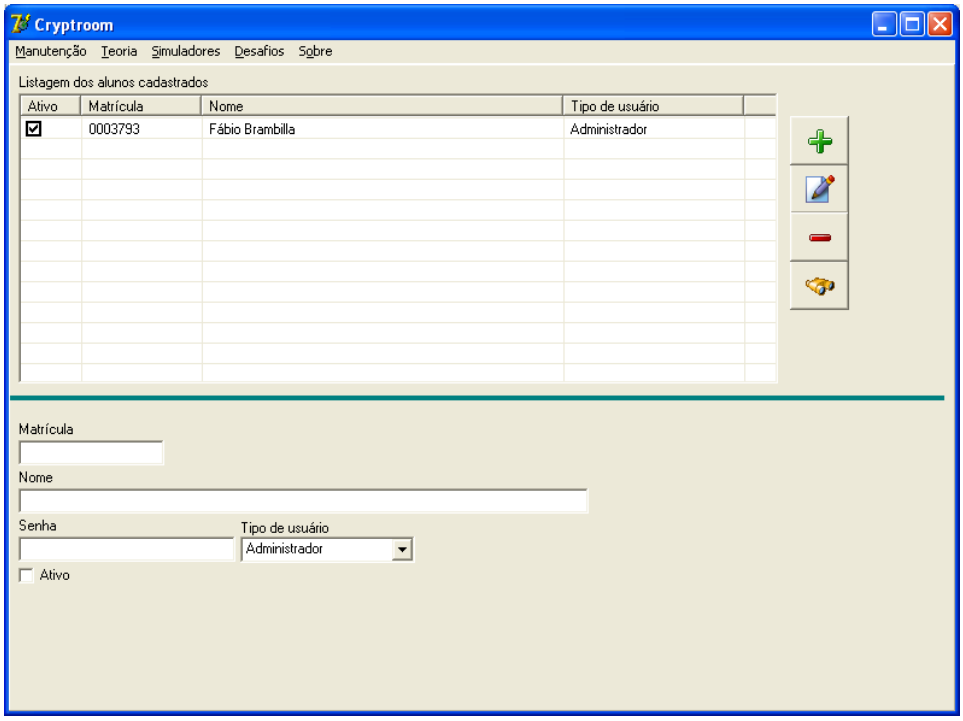

Figura 4.2: Tela de cadastro de usuários do protótipo criado
Fonte: O autor.

A história da Criptografia sendo ilustrada nos tempos antigos, medievais e modernos. Ao deslizar o cursor entre os anos apresentados, o conteúdo inferior é alterado, mostrando através da interface do aplicativo a descrição daquele período na história da criptografia.

Neste tipo de ilustração, podem ser acrescentadas imagens que demonstram ao aluno as técnicas de criptografia utilizadas naquele determinado período.

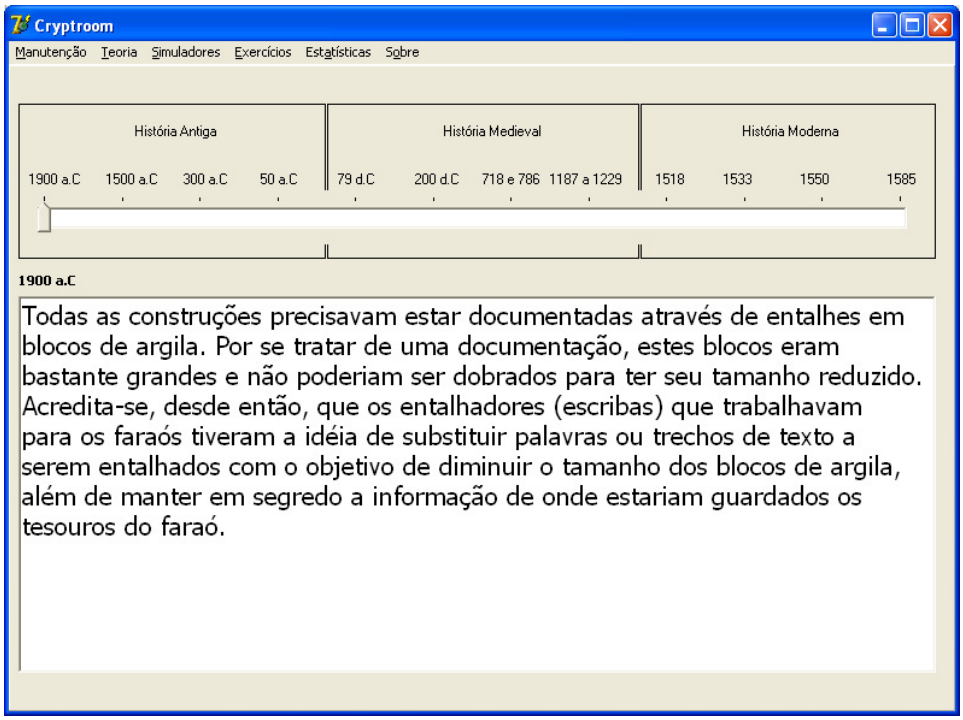

Figura 4.3: Tela com conteúdo da história da criptografia
Fonte: O autor.

Até este momento, apresentamos os conteúdos referentes aos conceitos disponibilizados na ferramenta. Além da implementação destes conceitos, foram criados simuladores, os quais permitem ao aluno interagir com o programa e buscar seus resultados.

A figura 4.4 ilustra a tela de simulação da Cifra de Cesar, onde se faz possível escolher o deslocamento, escolher a palavra a ser criptografada e ver na própria interface o resultado cifrado.

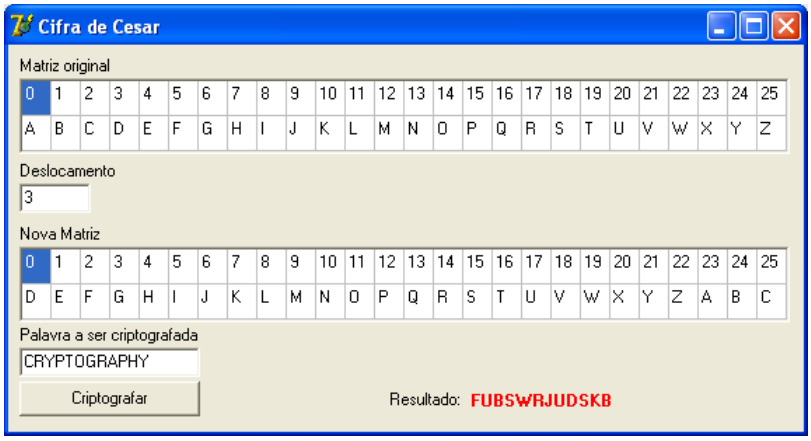

Figura 4.4: Tela de simulador da Cifra de Cesar
Fonte: O autor.

Além do simulador da Cifra de Cesar, foi implementado na ferramenta um simulador de esteganografia, o qual gera uma imagem com a mensagem adicionada, conforme figura 4.5. Dessa forma, o aluno pode visualizar o arquivo de saída comparando com o original em busca de indícios da existência da mensagem na imagem.

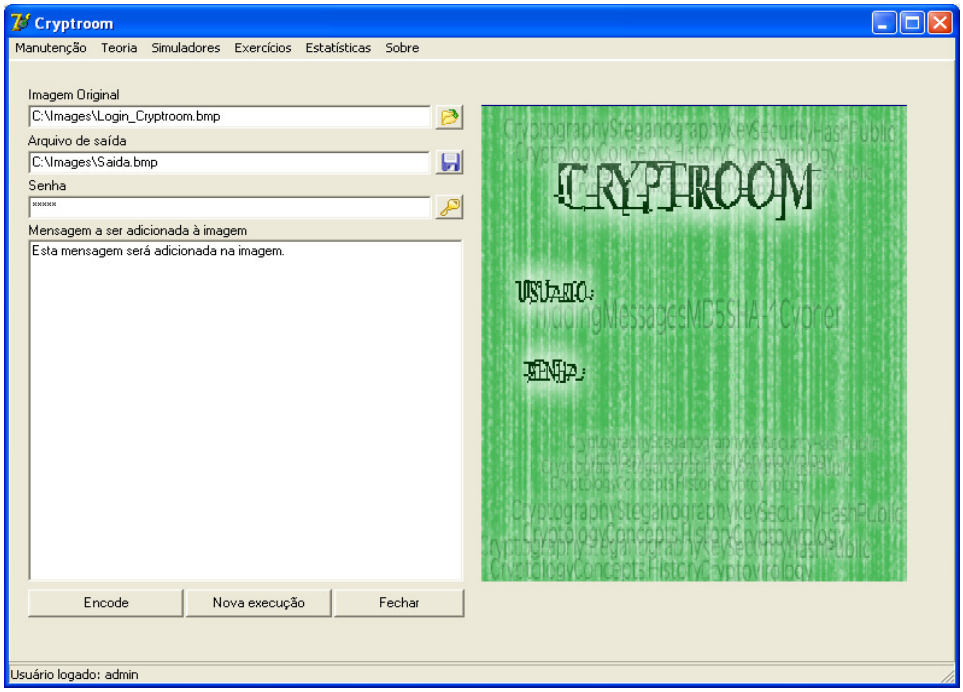

Figura 4.5: Tela de simulador de esteganografia
Fonte: O autor.

Foi desenvolvido, conforme imagem 4.6, um simulador para a criptografia *DES* e *Triple DES* (*3DES*), onde é informada a mensagem que será criptografada e recebendo como saída, a mensagem cifrada. Caso seja *DES*, utiliza chave de 64 *bits*. Caso seja 3DES, utiliza uma chave de 128 *bits*.

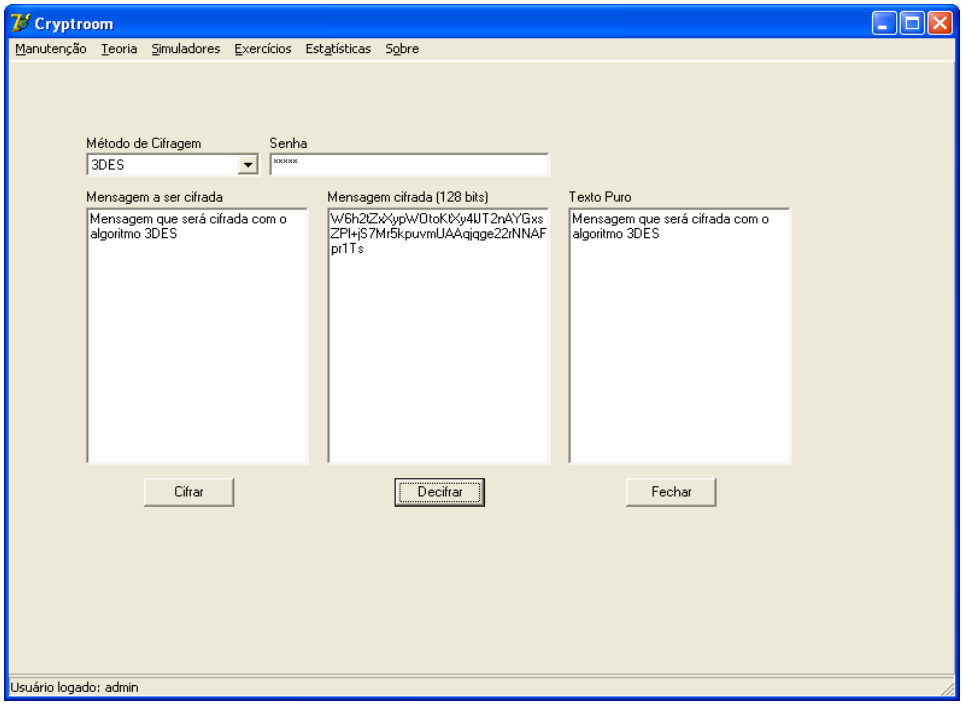

Figura 4.6: Tela do simulador DES e 3DES
Fonte: O autor.

Dentre os simuladores implementados, é possível visualizar o simulador dos algoritmos de *Hash* MD5 e SHA-1, visualizando na tela o conteúdo cifrado. Este simulador está destacado na figura 4.7.

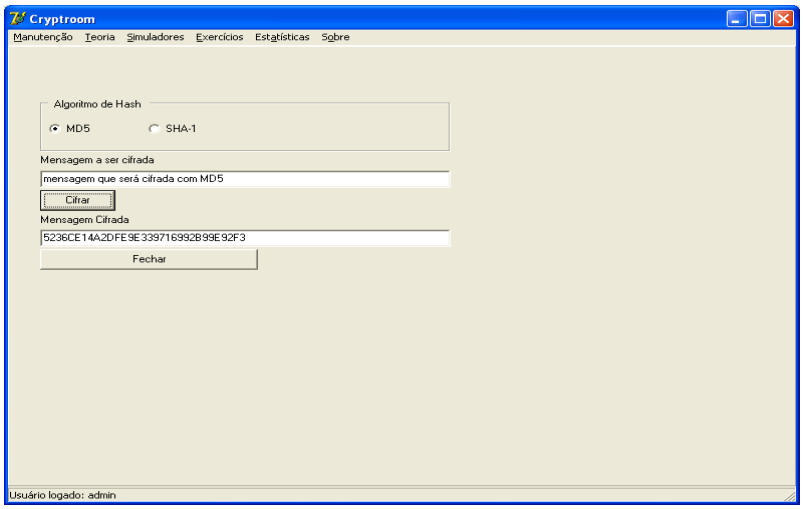

Figura 4.7: Tela do simulador de MD5 e SHA-1
Fonte: O autor.

4.2.1 Exercícios

Para que o aluno possa aplicar na prática os conceitos estudados, na modelagem da ferramenta foram adicionados recursos para que sejam apresentados exercícios ao aluno.

Estes exercícios deverão ser preenchidos e a partir dos resultados serão retiradas as métricas para a composição de sua nota referente ao conteúdo.

Os exercícios foram elaborados baseando-se nos conceitos e nas possibilidades de utilização dos próprios simuladores para a resolução destes, restando ao aluno saber exatamente qual o simulador correto para uso.

Os exercícios de múltipla escolha serão corrigidos no instante do preenchimento, permitindo dessa forma que o próprio aluno veja na ferramenta as questões erradas e procure no material o conteúdo correto. Além destes, o aluno deverá decifrar algumas mensagens utilizando as técnicas abordadas neste trabalho.

4.2.1.1 Exercícios sobre conceitos

Os exercícios sobre conceitos são teóricos, restando ao aluno apenas selecionar a opção correta ou descrever a sua resposta com relação ao conceito.

Dentre os exercícios teóricos, podemos citar 6 que foram adicionados ao protótipo:

Exercício 1. Qual a origem da palavra Criptografia?

a – Grega

b – Romana

c – Árabe

d – Japonesa

e – Inglesa

Exercício 2. Qual o termo utilizado para o processo de transformação de uma mensagem em texto puro para uma mensagem criptografada?

a – *Plaintext*

b – *Ciphertext*

c – Cifrar

d – Decifrar

e - Transformar

Exercício 3. Qual o significado da palavra Esteganografia?

a – Escrita Cifrada

b – Escrita Oculta

c – Escrita Invisível

d – Escrita Escondida

e – Escrita Embaralhada

Exercício 4. Explique a diferença entre a cifra de substituição e a cifra de transposição.

Exercício 5. Cite os tipos de chave de criptografia disponibilizados na ferramenta.

Exercício 6. Para cada tipo de chave de criptografia, faça uma breve explicação sobre o funcionamento.

Ainda, baseando-se na modelagem criada, foi possível adicionar uma tela ao protótipo que visa disponibilizar ao aluno os exercícios que deverão ser preenchidos pelo mesmo. Nesta mesma tela o aluno poderá saber se conteúdo está correto ou não, corrigindo eventuais falhas durante o processo de acompanhamento dos conceitos. Para os exercícios descritivos, o professor deverá possuir uma área onde faça as correções necessárias nos exercícios e o mesmo possa definir como resposta correta ou não do aluno.

A figura 4.8 apresenta os exercícios teóricos implementados no protótipo.

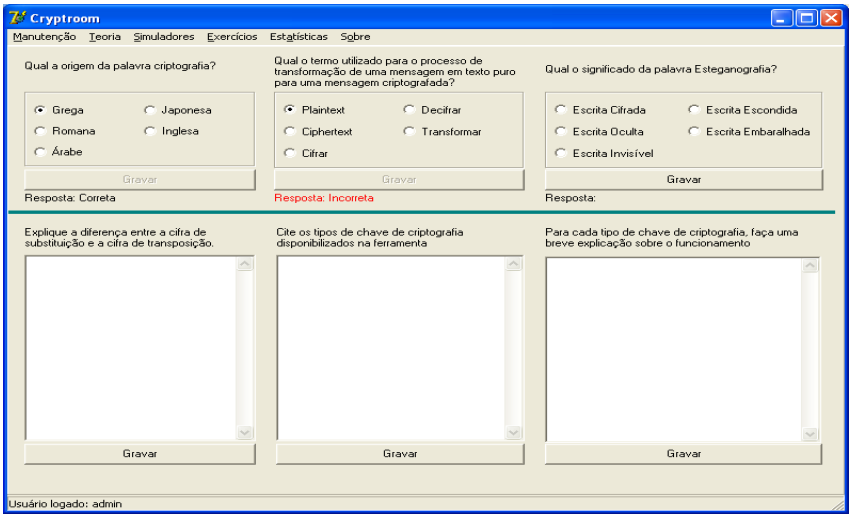

Figura 4.8: Tela de exercícios teóricos
Fonte: O autor.

4.2.1.2 Exercícios práticos

Para que o aluno possa exercitar o que está estudando com o objetivo de fixar melhor o conteúdo, foi incluído na modelagem da ferramenta recursos para suporte a exercícios práticos, onde destacamos abaixo três deles que foram adicionados ao protótipo.

Exercício 1. Cifra de César é um método de substituição onde aplicado um deslocamento de letras, é gerado um código cifrado. Utilizando um deslocamento de três posições, decifre a mensagem abaixo:

D SDODYUD FULSWRJUDILD VLJQLILFD HVFULWD RFXOWD

Exercício 2. Utilizando as Carreiras de Vigenère, encontre o texto puro e a chave utilizada:

Texto puro								
Chave								
Deslocamento	2	0	17	17	4	8	17	0
Resultado	X	I	X	V	R	M	I	E

Exercício 3. Utilizando o método de transposição, ordene a tabela abaixo e descreva o resultado da mensagem:

C R I P T O

C I F R A D

E T R A S P

O S I C A O

A P L I C A

D A

A figura 4.9 apresenta os exercícios práticos implementados no protótipo, onde o aluno efetua o preenchimento e envia para a base de dados para correção.

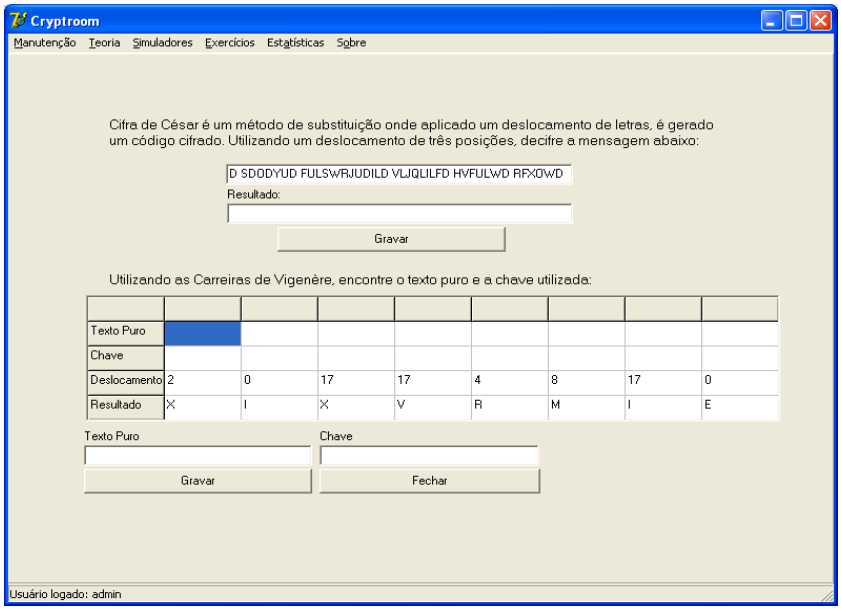

Figura 4.9: Tela de exercícios práticos
Fonte: O autor.

4.3 Modelo ER

Por se tratar de um sistema onde deverão ser armazenados apenas os usuários e os preenchimentos dos exercícios para que possam ser estabelecidas as devidas métricas, foi necessário criar 4 tabelas na base de dados para este armazenamento.

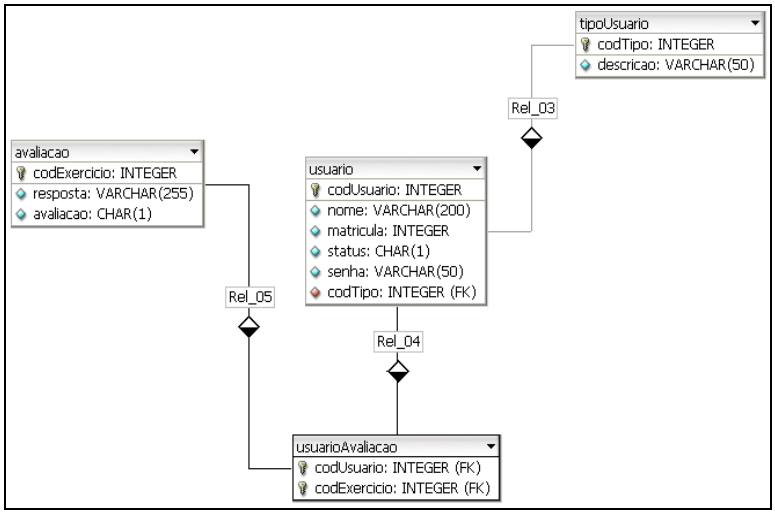

Figura 4.10: Diagrama Entidade Relacionamento
Fonte: O autor.

4.4 Recursos Futuros

A iVirtua Solutions, empresa situada na cidade de Montenegro, desenvolvedora de software para Gestão de TI demonstrou interesse em implementar a ferramenta para que os clientes que adquirirem o produto possam entender a importância da proteção de suas informações.

Para tanto, a ferramenta estará integrada ao módulo Forense, com previsão de lançamento em Setembro de 2009. Para esta primeira versão, a ferramenta deverá possuir recursos de simulação para Esteganografia em arquivos do disco, independente de serem imagens, arquivos de vídeo ou áudio.

Além deste simulador, surgiu a necessidade de acrescentar no projeto informações relativas ao produto fabricado pela iVirtua, denominado Trauma Zer0, onde seriam ministrados os treinamentos utilizando a estrutura do projeto modelado.

Ainda em tempo, está previsto a melhoria de exibição e acompanhamento da execução dos algoritmos de criptografia, abrangendo também alunos das cadeiras de programação.

Conclusão

A partir do momento em que foi delimitado o tema para estudo deste trabalho, era sabido que não seria um trabalho simples de ser executado. Analisar ferramentas existentes e com base nas funcionalidades existentes, modelar uma ferramenta que fosse capaz de auxiliar os alunos dos cursos relacionados à informática a necessidade de proteção de suas informações. Além desta "dificuldade", o fato de não ter cursado nenhuma cadeira do curso que contivesse o assunto criptografia, surgiram diversas dúvidas com relação ao conteúdo a ser adicionado na modelagem, mas que durante a execução do trabalho foram sendo sanadas com os conhecimentos adquiridos com a leitura e pesquisa.

A realização deste trabalho foi bastante motivadora, pois a cada conteúdo aprendido aumentava o interesse pelo assunto e a certeza de estar fazendo uma boa pesquisa. Durante a pesquisa e modelagem vislumbrei a possibilidade de posterior implementação da ferramenta com perspectivas de adaptação da mesma para contemplar recursos da empresa onde trabalho.

Como não possuía experiência tanto na área de criptografia, quanto na área de modelagem, foi efetuada a modelagem baseando-se nos simuladores encontrados durante as pesquisas.

Durante a pesquisa de conteúdo para elaboração deste Trabalho de Conclusão foi possível identificar a necessidade de material de apoio à criptografia devido a não encontrar ferramentas didáticas, direcionadas ao ensino da criptografia, e sim, simuladores que colocam na prática os conceitos existentes, independente de ser conhecido pelo aluno ou não. A necessidade de uma ferramenta para apoio aos estudantes no aprendizado sobre a criptografia também pôde ser considerada como uma necessidade real, pois a criptografia garante a proteção das informações e atualmente é um diferencial competitivo para as empresas.

De acordo com os estudos efetuados, a criptografia não se aplica apenas à informática, estando ela presente desde os tempos dos faraós, o que demonstra que de fato, não é uma técnica obsoleta, mesmo existindo padrões de criptografia definidos em 1977 que são amplamente utilizados.

A utilização de uma ferramenta para apoio ao ensino da criptografia proporcionará ao aluno a visualização de forma sucinta das técnicas envolvidas no assunto, bem como, agrupar em um único lugar os conceitos teóricos e práticos, através dos simuladores.

Como objetivo geral deste trabalho foi a modelagem de uma ferramenta para apoio ao ensino da criptografia e que através desta ferramenta fosse possível identificar a necessidade de utilização destas técnicas no ambiente corporativo, com base nos fatos históricos ficou comprovada a necessidade de utilização desta técnica, independente do ramo de atividade ou da época em que se está vivendo.

Dos objetivos específicos definidos para o projeto, foi possível alcançar todos, sendo adicionados ainda outros itens que não estavam previstos no projeto inicial. Estes demais itens se mostraram necessários no decorrer dos estudos.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBUQUERQUE, Ricardo. RIBEIRO, Bruno. **Segurança no desenvolvimento de Software**. Rio de Janeiro: Editora Campus, 2002.

ASSUNÇÃO, Marcos Flávio. **Guia do Hacker Brasileiro**. Editora Visual Books, 2002.

BAUER, Friedrich L. **Decrypted secrets: methods and maxims of cryptology.** Editora Springer, 2007.

BUCHMANN, Johannes A.. **Introdução à criptografia**. São Paulo: Editora Berkeley, 2002.

CARMONA, Tadeu. **Segredos da espionagem digital**. Editora Digerati, 2005.

CARVALHO, João A. **Informática para concursos**. Editora Elsevier, 3ª Edição.

CHESWICK, WILLIAM R. Et All. **Firewalls e segurança na internet: Repelindo o Hacker Ardiloso**. Bookman, 2005.

CHIRILLO, John. **Hack Attacks Encyclopedia: A Complete History of Hacks, Cracks, Phreaks, and Spies over Time**. New York: John Wiley and Sons, 2001.

CHOMSKY, Noam. **Novos Horizontes No Estudo Da Linguagem E Da Mente. Editora** UNESP, 2006.

CLEMENTINO, Edilberto **B. Processo judicial eletrônico: o uso da via eletrônica na comunicação de documentos processuais sob o enfoque histórico e principiológico, em conformidade com Lei 11.419.** Jurua Editora, 2007

COBB, Chey. **Cryptography for Dummies**. New York: For Dummies, 2004.

COULOURIS, George. Et All. **Sistemas distribuídos – Conceitos e Projeto.** Bookman.2007.

COUTO, Sérgio P. **Decifrando a fortaleza digital.** Universo dos livros Editora LTDA.2005.

CRIPTOGRAFIA NUMA BOA. A régua de Saint-Cyr. 2005. Disponível em: http://www.numaboa.com/criptografia/dispositivos/411-Saint-Cyr. Acesso em 20 maio 2009.

CrypTool Introduction. Disponível em: http://www.cryptool.de/. Acesso em 14 abril 2009.

CRONKHITE, Cathy. MCCULLOUGH, Jack. **Hackers: Acesso negado**. Rio de Janeiro: Editora Campus, 2001.

DUBOIS, Jean. Et All. **Dicionário de lingüística**. Editora Cultrix, 2001.

ESCRIBA CAFÉ. Transcrição: Criptografia. Disponível em: http://www.escribacafe.com/criptografia/. Acesso em 19/05/2009.

GAINES, Helen F. **Cryptanalysis. A Study of Ciphers and Their Solution**. London: Dover Publications, 1989.

GEUS, Paulo L., NAKAMURA, Emilio T. **Segurança de Redes em Ambientes Cooperativos - Fundamentos, Técnicas, Tecnologias, Estratégias.** Novatec Editora, 2007.

GIL, Antonio de L.. **Segurança em Informática**. São Paulo, Editora Atlas, 1998.

GOMES, Carlos F. S., Et All. **Gestão da Cadeia de Suprimentos**. Cengage Learning Editores, 2004.

GOODRICH, Michael T. TAMASSIA, Roberto. **Estruturas de dados e algoritmos em JAVA**.

GOODRICH, Michael T. TAMASSIA, **Roberto. Projeto de Algoritmos**.

GRAF, Jon C. **Cryptography and E-Commerce**. New York: Wiley, 2000.

GUEDES, Gilleanes T.A. **UML – Uma Abordagem Prática**. Editora Novatec. 2008.

HAYKIN, Simon. **Sistemas de comunicação analógicos e digitais**. Bookman, 2004.

HOOK, David. **Beginning Cryptography with Java**. New York: Wrox 2005.

KNUDSEN, Jonathan. **Java Cryptography**. New York: O´Reilly 1998.

LUBBE, Jan C.A. GEE, Steve. **Basic methods of cryptography.** Cambridge University Press, 1998.

MEL, H.X. BAKER, Doris. **Cryptography decrypted**. One Lake Street: Addison-Wesley, 2001.

PACITTI, Tércio. **Construindo o Futuro Através da Educação - Do Fortran à Internet.** Cengage Learning Editores, 2003.

PETERSON, Larry L., DAVIE, Bruce S. **Computer Networks: A Systems Approach.** Morgan Kaufmann, 2007.

SALOMON, David. **Coding for Data and Computer Communications**. Berlin: Springer 2005.

RAMOS, Ricardo A. **Treinamento Prático em UML**. Digerati Books.2006.

SATINOVER, Jeffrey. Et All. **A verdade por trás do código da bíblia**. Editora Pensamento, 1997.

SCHNEIER, Bruce. **Applied Cryptography: Protocols, Algorithms, and Source Code in C**. New York: John Wiley & Sons, 1996.

SMITH, Laurence D. **Cryptography: The Science of Secret Writing**. London: Dover Publications, 1955.

STALLINGS, William. **Cryptography and network security: principles and practice.** Prentice Hall, 2006.

TERADA, Routo. **Segurança de dados: Criptografia em Redes de Computador**. São Paulo: Editora Edgard Blüncher Ltda, 2000.

TITTEL, Ed. **Redes de Computadores.** Bookman, 2003.

TITTEL, Ed. **XML**. Editora Bookman. 2003.

TRIGO, Clodonil Honório. **OpenLDAP - Uma Abordagem Integrada**. Novatec, 2007.

WAYNER, PETER. **Disa Appearing Cryptography: Information Hiding: Steganography & Watermarking**. San Francisco: Morgan Kaufmann Publishers, 2002.

YOUNG, A., YUNG, M.. **Malicious Cryptography: Exposing Cryptovirology**. Wiley, 2004.