Michel Henrique da Silva Nascimento

CRIPTOGRAFIA EM BANCO DE DADOS

Recife

26 de Março de 2017

Michel Henrique da Silva Nascimento

CRIPTOGRAFIA EM BANCO DE DADOS

Trabalho de pesquisa sobre criptografia em banco de dados apresentado ao professor Luis Leite para disciplina de Banco de dados II do curso de tecnologia em análise e desenvolvimento de sistemas do IFPE-Recife

Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco

Tecnologia em Análise e Desenvolvimento de Sistemas

Recife

26 de Março de 2017

Resumo

Este trabalho pretende através de pesquisas realizadas em alguns livros e sites na internet, abordar um pouco o tema da criptografia em banco de dados, de uma forma mais geral, passando pela sua história, abordando um pouco aspectos relativos a sua definição, entendendo brevemente resquícios de técnicas de fato para sua execução e mostrando um pouco da sua aplicabilidade nos dias de hoje na segurança da informação, assim como sua importância a respeito da necessidade do conhecimento sobre o assunto, tendo em vista o tempo e o mundo informatizado em que se vive hoje.

Palavras-chaves: Criptografia. Segurança da Informação.

Lista de ilustrações

Sumário

Introdução

Nas últimas décadas, a palavra criptografia tem ganhado muito destaque, principalmente no meio tecnológico onde é diretamente associada a proteção dos dados pessoais ou de empresas em computadores e na internet. Apesar disso, a criptografia se inicia em tempos muito mais antigos do que essas poucas décadas de grande destaque, isso reflete a importância do estudo sobre essa questão e o impacto social, econômico ou político que esse assunto despende. Nos próximos capítulos serão abordadas questões referentes a esse assunto, a partir de revisões bibliográficas para ser apresentado na disciplina de banco de dados II, será discutido um pouco o assunto da criptografia de forma mais centralizada, ressaltando a sua história e desenvolvimento, assim como sua própria definição mais formal no capítulo 1 de forma bastante breve, algumas técnicas de criptografia serão explicadas e exemplificadas no capítulo 2 para que se fique mais claro tal propósito, e será mostrando também um pouco da sua aplicabilidade no capítulo 3 ressaltando sua importância e a força da sua presença no mundo hoje.

1 Conceitos de Criptografia

1.1 Criptografia

A criptografia é a ciência e o estudo da escrita secreta (DENNING, 1945). De uma forma mais geral a criptografia pode ser entendida como uma ferramenta ou método utilizado para que se possa esconder alguma mensagem. Esse método pode ser tido como base no quesito de segurança computacional. Segundo (HOUAISS, 2007) a criptografia é o conjunto de técnicas e princípios para cifrar a escrita e assim torná-la ininteligível para os que não tem acesso às convenções combinadas. A câmara Brasileira de Comércio Eletrônico considera como criptografia, a aplicação de um secreto para substituição dos caracteres, de modo que a mensagem se torna ininteligível para quem não conhece o padrão criptográfico utilizado. Por sua vez a legislação brasileira considera a criptografia[1] como "Disciplina que trata dos princípios, meios e métodos para a transformação de dados, de forma a proteger a informação contra acesso não autorizado a seu conteúdo". Tendo em vista as considerações acima, fica claro o objetivo básico da criptografia, seja para cifrar ou decifrar coisas, pode-se observar melhor na figura abaixo:

Figura 1: Esquema generalizado para a cifragem de um texto

Fonte: (MORENO, 2005)

O processo de transformação de um texto normal em um texto cifrado é conhecido como encriptação, assim como o processo reverso, ou seja, que transforma um texto cifrado em texto comum é tido como decriptação e ambos são controlado por uma ou mais chaves criptográficas.

Outro termo tem ocorrência bastante comum quando se fala em criptografia, a criptoanálise que se refere à ciência e estudo dos métodos para se quebrar as cifras. Uma cifra pode ser dita como quebrável se for possível determinar o texto simples ou a chave para o texto cifrado.

[1] Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d3587.htm> Acesso em 26 de março de 2017

A título de terminologia, tem-se a palavra criptografia como derivada de cripto, do grego kruptós("oculto", "obscuro", "ininteligível") mais grafia do grego graphía("escrever", "escrita") dando consistência assim a definição já abordada.

1.2 História da criptografia

Apesar da criptografia parecer um termo bastante atual pela sua importância e uso nos sistemas informatizados que se mostram nos dias atuais, ela é tão antiga quanto a própria escrita tendo em vista que já estava presente nos hieróglifos egípcios, enquanto que a ideia geral da criptografia surgiu ainda antes disso. Segundo (REIS, 1989), o primeiro vestígio de criptografia conhecido data de 1900 A.C. e a primeira descrição de um sistema de criptografia militar de que se tem notícia foi feita pelos gregos no quinto século antes de Cristo e também que a criptanálise surgiu com os árabes em torno dos anos 600.

Em 50 a.C, Júlio César usou sua famosa cifra de substituição para cifrar (criptografar) comunicações governamentais. Para compor seu texto cifrado, César alterou letras desviando-as em três posições; A se tornava D, B se tornava E etc. Às vezes, César reforçava seu método de criptografar mensagens substituindo letras latinas por gregas. O código de César é o único da Antigüidade que é usado até hoje. Atualmente qualquer cifra baseada na substituição cíclica do alfabeto denomina-se código de César. Apesar da sua simplicidade (ou exatamente por causa dela), essa cifra foi utilizada pelos oficiais sulistas na Guerra de Secessão americana e pelo exército russo em 1915(MORENO, 2005).

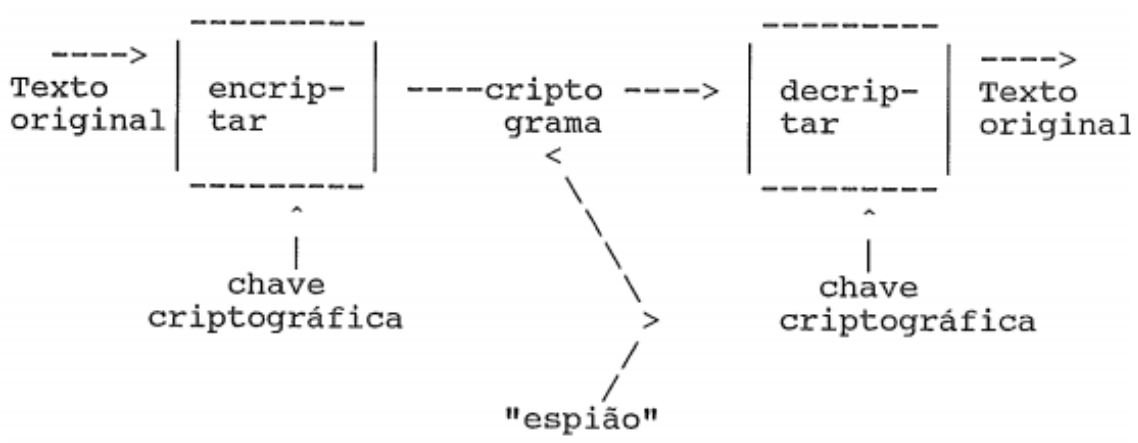
Algumas invenções tecnológicas de extrema relevância usaram-se desse princípio como o telégrafo e o rádio, que também ajudaram a desenvolver de forma significativa o estudo da criptografia na sua completude, o que remete inevitavelmente a guerras, a criptologia e toda sua complexidade entra nesse terreno de forma muito elevada, se tornando uma necessidade entre países em guerras devido a sua funcionalidade e as próprias características inerentes aos conflitos.

Um dos pontos mais importantes da história da humanidade em que pode-se perceber a inserção da criptografia se encontra na entre 1933 e 1945 em tempos da segunda guerra mundial, onde a Alemanha nazista possuía uma máquina chamada 'enigma' que continha um forte código de encriptação para aquela época e que chegou a ser desvendado contribuindo de forma bastante relevante para o fim da guerra.

2 Algoritmos e Técnicas de Criptografia

Sabendo-se que a criptografia em si consiste em mascarar a mensagem a ser transmitida por algum meio de forma que só o destinatário pode entender. Esse fator essencial para que haja o entendimento entre o emissor e o destinatário é a chave. Um sistema simples de criptografia pode ser entendido melhor pela imagem abaixo:

Figura 2: Criptossistema



Fonte: (REIS, 1989)

Na figura 2 pode-se perceber um organograma pouco detalhado sobre um sistema bastante simples de criptografia, mostrando desde a entrada do texto original em um movimento unidirecional, sendo recepcionado por um processo de encriptação através de uma chave criptográfica, passando por um meio criptograma até a decriptação com o uso também da chave e em seguida a sua saída com o texto original reconstruído.

Segundo (CRUZ, 2009), tecnicamente, a criptografia divide-se em dois ramos: transposição e substituição, também conhecidos como cifra simétrica e cifra assimétrica respectivamente. Na simétrica cada letra mantém a sua identidade, mas muda de posição. Diferentemente da assimétrica onde o processo é inverso, isto é, cada letra muda de identidade, mas mantém sua posição. Historicamente conhecidos como Cifras Clássicas, esses sistemas de criptografar eram implementados manualmente ou com o emprego de dispositivos mecânicos simples.

2.1 Criptografa de Chave Simétrica(Transposição)

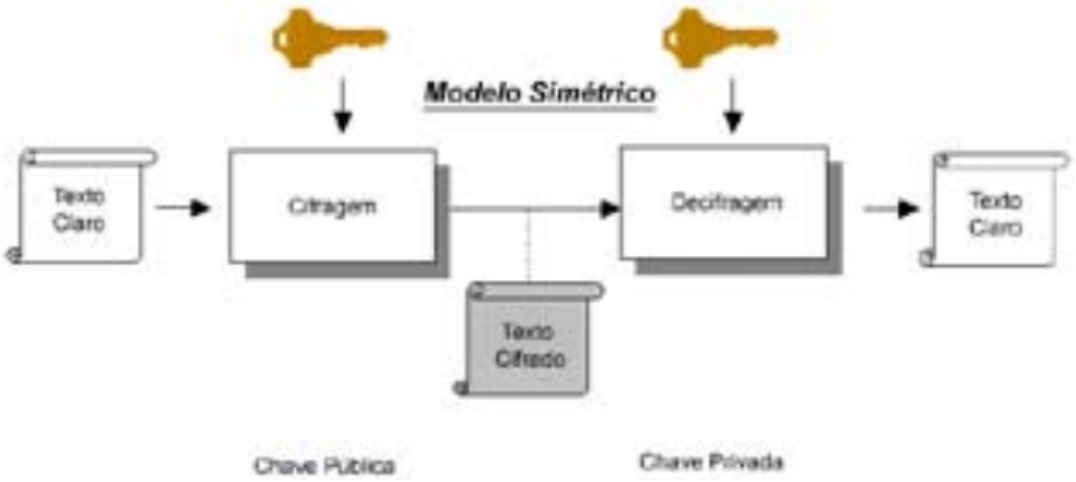
Segundo (MORENO, 2005) na criptografia de chave simétrica, os processos de cifragem e de decifragem são feitos com uma única chave, ou seja, tanto o remetente quanto

o destinatário usam a mesma chave. Esse tipo de criptografia consiste basicamente em um rearranjo de letras no texto da mensagem, o que pode ser entendido como um anagrama.

"O exemplo mais difundido de cifrador computacional de chave única é o DES (Data Encryption Standard), desenvolvido pela IBM e adotado como padãoo nos EUA em 1977. O DES cifra blocos de 64 bits (8 caracteres) usando uma chave de 56 bits mais 8 bits de paridade (o que soma 64 bits).O algoritmo inicia realizando uma transposição inicial sobre os 64 bits da mensagem, seguida de 16 passos de ciftagem e conclui realizando uma transposição final, que é a inversa da transposição inicial.Para os 16 passos de cifragem usam-se 16 sub-chaves, todas derivadas da chave original através de deslocamentos e transposições"(PISTELLI, 2001).

A criptografia de chave simétrica é usada por muito tempo e seguindo o histórico da criptografia já mencionado, ela acompanha esse uso desde os primórdios da humanidade. A intenção final do uso desse tipo de criptografia pode ser considerada a obtenção em si do sigilo dos dados de forma que a sua segurança fique amplificada e evitando assim que pessoas não autorizadas possam chegar a ter acesso às informações em questão.

Figura 3: Modelo de criptografia simétrica



Fonte: (MORENO, 2005)

Na figura 3 encontra-se um modelo gráfico referente ao sistema de criptografia simétrica, exibindo os pontos importantes e como interagem entre si.

2.1.1 Desvantagens da Criptografia simétrica

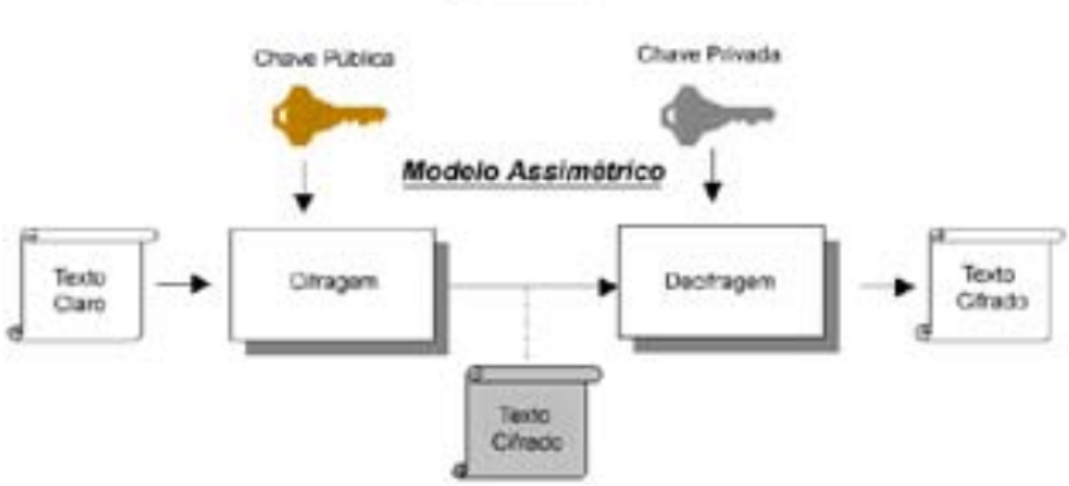
No geral o método de criptografia assimétrica tem algumas desvantagens, a principal delas se encontra no fato de que as partes que a usam e precisam usá-la devem ter acesso a mesma chave, então só a partir de algum tipo de prioridade elas podem se relacionar e assim realizar a cifragem e decifragem dos dados. Desse modo os problemas causados giram em torno de alguns problemas de segurança que decorrem do gerenciamento das

chaves. O fato do segredo da chave estar em pleno conhecimento por várias pessoas pode acabar causando um grande prejuízo tendo em vista que acontecendo algum problema com um deles independente da forma, tal situação vai sobrar para todos os outros. Um outro problema pode decorrer do próprio gerenciamento da distribuição da chave em si, sendo que a cada vez que uma nova pessoa fosse admitida ao grupo este necessitaria receber tal chave no citado processo de envio. Atualmente esse tipo de criptografia ainda é utilizado através do DES (Digital Encryption Standard) e do IDEA(International Data EncryptionAlgorithm).

2.2 Criptografia de Chave Assimétrica(Substituição)

Segundo (CRUZ, 2009) a substituição é a técnica criptográfica alternativa à transposição. Nesta, cada letra mantém sua identidade, mas muda de posição; naquela, a letra muda de identidade, mas mantém sua posição. Nesse tipo de criptografia a chave de ciframento é pública ou tornada acessível aos usuários, sem que haja quebra na segurança. Nesse ponto comparada com a chave de criptografia simétrica, esta possui certa vantagem, pois contorna o problema da distribuição de chaves mediante o uso de chaves públicas. Tanto que atualmente dentre os mecanismos de busca mais utilizados está o de assinatura digital que engloba esse tipo de criptografia assimétrica. A figura 4 mostra um modelo de

Figura 4: Modelo de criptografia assimétrica



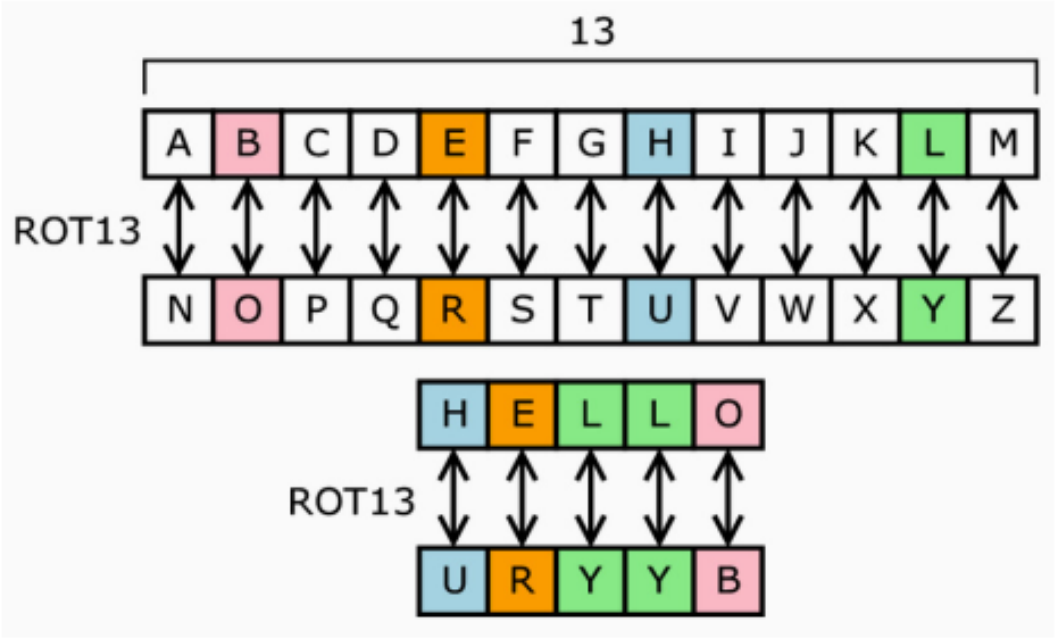
Fonte: (MORENO, 2005)

criptografia assimétrica com seus elementos compondo toda a esquemática que dão base ao funcionamento deste.

2.2.1 Cifra monoalfabética

Um exemplo do uso de criptografia assimétrica reside no fato de realizar apenas um emparelhamento entre as letras do alfabeto de uma forma randômica e assim, logo após substituir cada letra da mensagem original por sua correspondente, este tipo tem um problema de que pode ser facilmente quebrada por ataques simples.

Figura 5: Cifra monoalfabética



Fonte: (CRUZ, 2009)

A figura 5 representa uma organização do exemplo citado, mostrando de forma gráfica como acontece uma cifra monoalfabética, também conhecida como cifra de césar.

2.2.2 Cifra polialfabética

Este tipo de criptografia, diferentemente da monoalfabética possui um sistema polialfabético que se utiliza de algumas substituições em tempos distintos na mensagem, assim são usados vários alfabetos. Um exemplo de uso desse tipo foi conhecido primeiramente através da Cifra de Vigenère.

2.2.3 Criptografia Assimétrica Com Função de Sigilo

Nesse tipo de criptografia a função desejada para a chave pública seria a de sempre efetuar tal cifragem no tempo em que sua correspondente chave primária deveria ser usada para executar a decifragem.

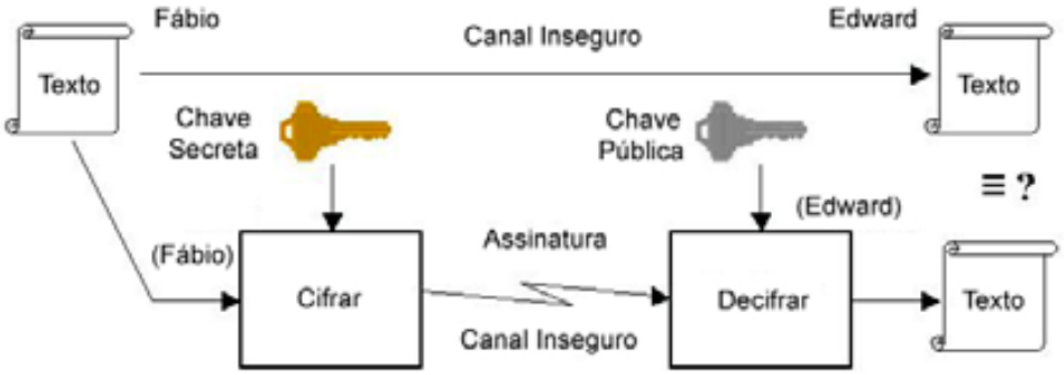
"O funcionamento do processo de cifragem e decifragem é simples. Suponha-se que Lucas desejasse enviar um texto qualquer para Bruno, querendo precaver-se quanto à possibilidade de que qualquer outra pessoa, que não o próprio Bruno, fosse capaz de lê-lo. Para isso, bastaria que Lucas utilizasse a chave pública de Bruno (por ser pública, deverá ser do conhecimento de Lucas e de todos) para cifrar a mensagem a ser enviada. Em decorrência, somente a chave privada de Bruno, e nenhuma outra, seria capaz de decifrar a mensagem enviada por Lucas. Como só Bruno é que deveria ter acesso à sua chave, somente ele conseguiria ler o conteúdo da mensagem recebida. Em resumo, pode-se dizer que a técnica de criptografia assimétrica foi concebida, inicialmente, para que um número ilimitado de pessoas pudessem enviar dados cifrados, com função de sigilo, para serem lidos por uma só pessoa (aquela que possuísse a chave privada que faz par com a chave pública utilizada para cifragem)"(GUIMARAES, 2001).

Desse modo se elimina as necessidades da distribuição e do gerenciamento das chaves secretas.

2.2.4 Criptografia Assimétrica com Função de Assinatura

Segundo (GUIMARAES, 2001) essa técnica de criptografia assimétrica permite que um emissor possa enviar dados assinados para um número ilimitado de pessoas. Onde nesse caso tem a assinatura oriunda de uma dedução, embasada na maneira como se produzem os dados cifrados e na maneira como se decifram tais dados. Como resultado da cifragem feita dessa forma, nada mais então se tem do que dados em estado normal vertidos para dados em estado cifrado. A possibilidade de verificar a existência da "assinatura"reside exclusivamente da necessidade de uso de uma chave pública de alguém, para fazer-se a decifragem de uma mensagem recebida.

Figura 6: Geração de assinatura digital de um documento



Fonte: (MORENO, 2005)

3 Importância e Aplicabilidade da Criptografia em banco de dados

3.1 Importância

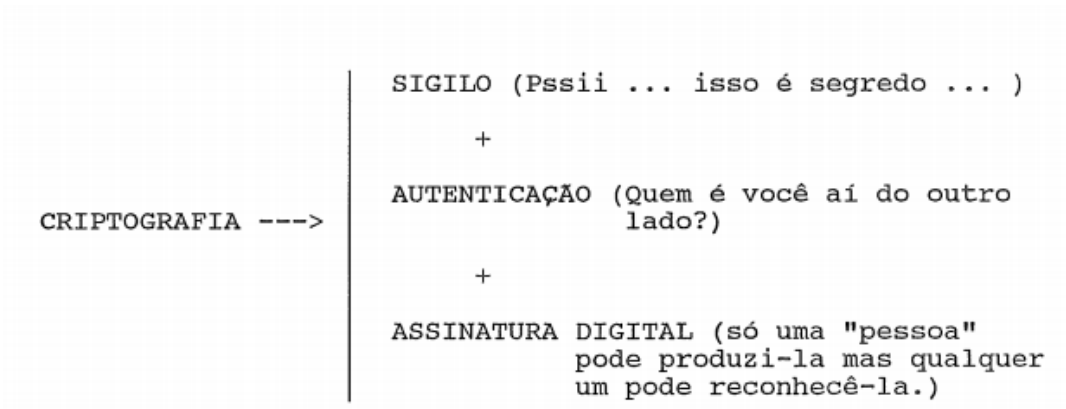
Desde sua invenção até a atualidade a criptografia desempenha um papel de extrema importância e foi criada em uma concepção primordialmente para atender as necessidades de sigilo, ou seja, evitar de alguma forma que outras pessoas que não deveram ou não poderiam ler certas mensagens o fizessem, tendo em vista o impacto disso em todos os aspectos no mundo diversas formas de sigilo tiverem que ser implementadas na medida em que outras diversas formas de quebrar tais sigilos eram desvendadas.

O uso dessa criptografia para outros recursos como o de formalizar uma certa autenticação do emissor da mensagem também se provou de extrema importância no decorrer dos tempos e da informatização das coisas, principalmente quando o mundo estava inserido no âmbito de guerras e a partir de tais evoluções o sigilo e a autenticação passaram a se desenvolver juntos, garantindo suprir as mais diversas necessidades de privacidade e segurança que o mundo exige das pessoas nessa era.

3.2 Aplicações

Existe uma série de aplicações nos tempos atuais que fazem uso de diversos tipos e métodos de criptografia, alguns mais impactantes que os outros e por isso merecem maiores destaques assim como maior esforço em sua elaboração. Esses tipos de aplicações podem estar contidos em três grandes grupos conforme mostra a figura 7:

Figura 7: Principais aplicações da criptografia



Fonte: (REIS, 1989)

Dentro dessa esquemática pode-se citar várias aplicações em que esses métodos estão inseridos.

3.2.1 Passwords

Segundo (REIS, 1989) passwords são a aplicação mais utilizada de criptografia nos meios computacionais. Um dos mais conhecidos e utilizados pelos usuários de computadores nos dias de hoje, são simplesmente as senhas que se digita para ter acesso a alguma funcionalidade de sistema e que se usa constantemente. Lógicamente essas senhas precisam estar bem protegidas, pois em sua maioria guardam informações importantes e até sigilosas.

3.2.2 Proteção de Software

Também é uma aplicação bastante comum o uso criptográfico nesses casos, aqui tem-se a finalidade de evitar modificações no próprio software ou que seja realizado algum tipo de cópia não autorizada, etc.

3.2.3 Informações Armazenadas

Certas informações que se deseja armazenar precisam estar ao acesso de certos usuários e ao mesmo tempo precisam ser seguras e não permitir que os mesmos a modifiquem, restringir o acesso de terceiros a esses tipos de informações se torna essencial e requer mais trabalho justamente pelo fato da necessidade de se ter os dados amostra e ao mesmo tempo resguardá-los.

3.2.4 Jogos

Os jogos hoje movimento uma indústria gigantesca e por esse motivo também precisam de um cuidado bastante forte na relação empresa/usuário. Diversos jogos compartilham de informações pessoais e até financeiras de seus jogadores, além de que um jogo hoje para se consolidar precisa ter sistemas anti-hackers bastante fortes. esse tipo de proteção é imprescindível hoje para uma empresa de jogos e reflete toda a sua importância nesse âmbito.

3.2.5 Satélites

Os satélites regem hoje os sistemas mais importantes de comunicação no mundo, são extremamente caros e carregam e transmitem informações muito valiosas, por esses e outros motivos inerentes a tal sistema de grande porte pode-se inferir uma importância vital em todo seu sistema de transporte de informações.

Conclusão

A partir dessa pesquisa foi possível perceber a importância gigantesca e o valor que se atribui hoje aos sistemas de criptografia em banco de dados, tendo em vista todo o seu ramo de aplicações dentro dos mais variados ambientes. Todos seus métodos de execução possuem uma forma de abordagem bem interessante que evoluiu bastante com o tempo e continua a evoluir a medida em que os sistemas que necessitam cada vez mais disso crescem.

O histórico do surgimento desses sistemas até os dias atuais mostra como é essencial o uso do mesmo, e por esse motivo a criptografia chega a se confundir com o princípio da humanidade e permanece de forma unida e quase inerente à existência dela, a segurança é e sempre foi um quesito fundamental nas estratégias e no modo de vida de todos, por isso ainda tais técnicas permanecem e permanecerão essenciais no intuito de suprir certas necessidades principalmente no que tange a informatização das coisas.

Referências

CRUZ, E. F. A criptografia e seu papel na segurança da informçÃo e das comunicações (sic) – retrospectiva, atualidade e perspectiva. *Universidade de Brasília*, 2009. Citado 3 vezes nas páginas 8, 10 e 11.

DENNING, D. E. R. Cryptography and 13ata security. *PURDUE UNIVERSITY*, 1945. Citado na página 6.

GUIMARAES, C. R. Criptografia para segurança de dados. *Centro Universitário do Triângulo*, 2001. Citado na página 12.

HOUAISS, A. Sdicionário eletrônico houaiss da língua portuguesa. 2. ed. *São Paulo: Ed. Objetiva*, 2007. Citado na página 6.

MORENO, e. a. Criptografia em software e hardware. *Novatec Editora*, 2005. Citado 6 vezes nas páginas 6, 7, 8, 9, 10 e 12.

PISTELLI, D. Criptografia. 2001. Citado na página 9.

REIS, V. L. M. Criptografia, segurança de dados e privacidade - até que ponto pode-se confiar na discrição dos computadores? *UNIVERSIDADE FEDERAL DO RIO DE JANEIRO*, 1989. Citado 4 vezes nas páginas 7, 8, 13 e 14.