Proteção de Procedimentos Armazenados em Banco de Dados SQL SERVER 2008 Utilizando Criptografia

Altair Alexandre Paula de Souza
Faculdade de Tecnologia da Zona Leste – SP – Brasil
altairaps@gmail.com

Carolina Luiza Chamas
Faculdade de Tecnologia da Zona Leste – SP – Brasil
carolchamas@hotmail.com

Leandro Colevati dos Santos
Faculdade de Tecnologia da Zona Leste – SP – Brasil
leandro.santos@fatec.sp.gov.br

Resumo - É comum a utilização de mecanismos de segurança para proteger dados em trânsito na internet ou na rede local tais como HTTPS ou VPNs, porém em determinados sistemas, os requisitos de segurança exigem medidas que garantam a segurança das informações mesmo que alguém mal intencionado consiga ter acesso direto ao banco de dados. Este trabalho pretende examinar meios para proteger informações no banco de dados, visando à confidencialidade das informações armazenadas no banco de dados. Para tanto, utiliza-se uma pesquisa bibliográfica levantando os principais aspectos da criptografia e um estudo de caso demonstrando a aplicação da criptografia em um ambiente de banco de dados.

Palavras-chave: Banco de Dados, Criptografia, SQL Server 2008, Stored Procedures.

Introdução

Segundo (KENAN, 2006) muitas organizações se apoiam no controle de acessos para proteção do banco de dados, o controle de acesso é um componente essencial, porém sua aplicação usual possui alguns pontos fracos com relação à garantia da confidencialidade como contas de usuário com permissão de 'somente leitura' utilizadas para manutenção em ambiente produtivo cuja utilização não é exclusiva, ambientes não produtivos para atividades de teste ou desenvolvimento, criados a partir de cópias da base de dados de produção, cópias de segurança da base de dados de produção e o nível de acesso dos próprios administradores do banco de dados cuja permissão de leitura é normalmente irrestrita.

Este artigo visa apresentar uma maneira garantir a confidencialidade de informações armazenadas em bases de dados, utilizando os conceitos que serão apresentados na fundamentação teórica, visando aumentar a segurança de dados sigilosos.

Com base neste cenário, pretendemos oferecer uma resposta ao problema a seguir: como garantir a confidencialidade de informações sigilosas mesmo que o intruso tenha conseguido acesso ao banco de dados?

A fim de encontrar uma solução para o problema levantou-se a seguinte hipótese: utilização de criptografia para proteger os dados confidenciais armazenados no banco de dados. A metodologia utilizada no trabalho foi estudo de caso apoiado em pesquisa

bibliográfica, o trabalho omite dados confidenciais e, em todo o estudo de caso, são apresentadas massas de dados fictícias.

Fundamentação Teórica

Banco de Dados

“Um banco de dados é uma coleção de dados relacionados. Os dados são fatos que podem ser gravados e que possuem um significado implícito.” (ELMASRI e NAVATHE, 2005 p 04).

Segundo (MULLINS, 2002), um banco de dados é um conjunto estruturado de dados persistentes sendo que um banco de dados simples pode ser um único arquivo contendo muitas linhas onde cada uma destas contém o mesmo conjunto de dados e cada campo tem um tipo de dados e comprimento específico.

Sistema Gerenciador de Banco de Dados (SGBD)

Para (SUMATHI e ESAKKIRAJAN, 2007), um Sistema Gerenciador de Banco de Dados (SGBD) é uma coleção de dados inter-relacionados (o banco de dados) mais um conjunto de programas para acessar e manter estes dados (o software gerenciador), o sistema não é direcionado a uma aplicação específica, o mesmo SGBD pode integrar um sistema voltado para diferentes aplicações atendendo a diferentes necessidades.

Um SGBD se encarrega do armazenamento e controle do acesso aos dados deixando para a aplicação que o utiliza apenas as tarefas especificas e inerentes a esta.

De acordo com (RODRIGUEZ e FERRANTE, 2000) o conceito dos sistemas gerenciadores de banco de dados começou a ser utilizado no início dos anos 60 sendo que no começo os dados eram armazenados de forma sequencial evoluindo para sistemas mais eficazes a partir de então.

Modelo de Dados Relacional

Segundo (DATE, 2000), o modelo relacional que foi introduzido em 1970 por Edgar F. Codd baseia se em uma teoria matemática fundamentada principalmente na teoria dos conjuntos e na lógica de predicados, esse modelo trouxe maior rigor para a área de gerenciamento de dados, qualidade rara até então.

> Lógica de predicados, usado extensivamente em matemática, fornece um quadro em que uma afirmação (declaração de fato) pode ser verificada como verdadeira ou falsa [...] A teoria dos conjuntos é uma ciência matemática que lida com conjuntos ou grupos de coisas, e é usado como a base para a manipulação de dados no modelo relacional. (CORONEL, MORRIS, ROB, 2011 p 59).

Procedimentos Armazenados

Segundo (ELMASRI, 2005), são conjunto de comandos SQL, em forma estruturada, que são compilados e armazenados no servidor.

Podem ser armazenados no banco de dados e acionados por qualquer programa aplicativo que tenha autorização para execução, sendo esse comando de execução, por padrão, CALL.

Uma Stored Procedure (sp) é executada no lado do servidor e seu plano de execução fica na memória, agilizando as próximas chamadas, podendo receber um ou mais parâmetros formais e pode retornar diversos valores como parâmetro de saída (output).

Criptografia

“A palavra criptografia é de origem grega e significa ‘escrita secreta’. Entretanto, usamos o termo para nos referirmos à ciência e à arte de transformar mensagens de modo a torna-las seguras e imunes a ataques.” (FOROUZAN, 2008 p 931).

Segundo (FOROUZAN, 2008), no processo de criptografia, a mensagem original é chamada ‘texto limpo’ ou ‘texto em claro’ e depois de criptografada é chamada de ‘texto cifrado’, ‘texto criptografado’ ou ainda ‘criptograma’, são chamados ‘cifras’ os algoritmos de criptografia e descriptografia enquanto dá se o nome de ‘chave’ a um número sobre o qual uma cifra opera. São necessários um algoritmo de criptografia, uma chave e o texto claro para criptografar uma mensagem e para descriptografar uma mensagem são necessários o texto cifrado, uma chave descriptográfica e um algoritmo de descriptografia.

Na criptografia clássica, todos os algoritmos desenvolvidos foram divididos em dois grupos - algoritmos de criptografia com chave simétrica (também chamadas de chave secreta ou chave privada) e os algoritmos de criptografia com chave pública (também chamada de chave assimétrica).

Criptografia com Chave Simétrica

Na criptografia com chave simétrica, tanto o emissor quanto o receptor utilizam a mesma chave, o emissor utiliza essa chave e o algoritmo de criptografia para cifrar a mensagem e o receptor utiliza a mesma chave e um algoritmo de descriptografia correspondente para decifra-la, ou seja, a chave é compartilhada sendo necessário que apenas emissor e receptor tenham acesso a ela.

Conforme a figura 1, em criptografia com chave simétrica, o algoritmo de cifragem e o de decifragem são recíprocos, se o primeiro utiliza uma combinação de adição e multiplicação, o segundo decifra utilizando uma combinação de divisão e subtração.

Figura 1 - Criptografia de Chave Simétrica
Fonte: (FOROUZAN, 2008, p 933)

Criptografia com Chave Assimétrica

Na criptografia de chave assimétrica ou pública, conforme demonstrado na figura 2, são utilizadas uma chave privada e uma chave pública, a primeira é guardada pelo receptor e a segunda está disponível para o público, a chave pública é utilizada para criptografar a mensagem e a chave privada é utilizada para descriptografá-la, sendo que são chaves diferentes.

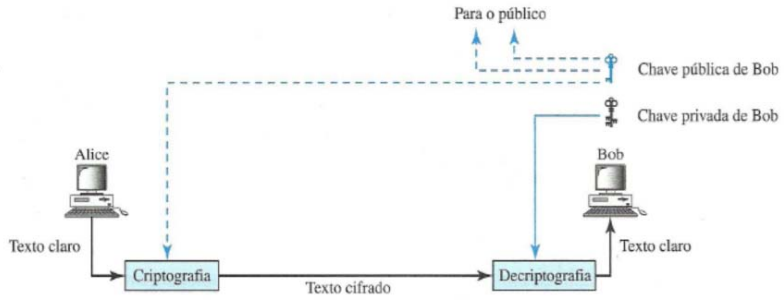

Figura 2 - Criptografia de Chave Assimétrica
Fonte: (FOROUZAN, 2008, p 933)

Cifras Cíclicas Modernas

Estas cifras são chamadas cíclicas, pois operam em ciclos onde cada um é uma cifra complexa composta por cifras mais simples. Exemplos de cifras de chave simétrica modernas são o DES e AES que dividem o texto claro em blocos usando a mesma chave para criptografar e descriptografar os mesmos:

- DES (Data Encryption Standard) – desenvolvido pela IBM e adotado pelo governo dos Estados Unidos como padrão para uso não militar e não confidencial, o algoritmo criptografa blocos de texto claro de 64 bits usando uma chave de 64 bits;
- Triplo DES – desenvolvido para resolver a questão do comprimento da chave do DES então considerada curta, o método é utilizado com duas ou três chaves, na versão com duas chaves ou três, com comprimentos de 112 ou 168 bits;
- AES (Advanced Encryption Standard) – foi desenvolvido devido ao fato da chave do DES ser pequena, apesar do triplo DES ter aumentado o tamanho da chave o método se tornou lento, o AES utiliza três comprimentos de chave: 128, 192 ou 256 bits.

Outras cifras de chave simétrica foram criadas durante as duas últimas décadas, a maioria deles semelhante ao DES e AES, diferindo normalmente quanto ao tamanho do bloco e chave, número de ciclos e funções utilizadas:

- IDEA (International Data Encryption Algorithm) – desenvolvido por Xuejia Lai e James Massey, o tamanho de bloco e chave é de 64 e 128 bits, pode ser implementado por meio de hardware ou software;
- Blowfish – criado por Bruce Schneier, manipula blocos de 64 bits utilizando chave de comprimento entre 32 e 448 bits;
- CAST-128 – desenvolvido por Carlisle Adams e Stafford Tavares, opera com blocos de 64 bits e chave de 128 bits de comprimento;
- RC5 – desenvolvido por Ron Rivest, é uma família de cifras com tamanhos de blocos, chaves e números de ciclos diferentes.

Certificados e *Hashing*

Para (TILBORG, 2005), um certificado é uma estrutura de dados assinada por uma entidade considerada por outras entidades como oficial, a assinatura na estrutura de dados está ligada á informação certificada de modo que a informação não pode ser alterada sem que isso seja detectado.

Entidades que obtém e utilizam certificados, podem confiar na informação certificada, pois podem determinar se a autoridade certificadora é confiável e porque é possível ter certeza de que a informação não foi alterada, uma vez que tenha sido certificada por uma autoridade.

Os principais tipos de certificados são certificados de chave pública utilizados em protocolos ou troca de mensagens envolvendo autenticação das partes envolvidas.

Segundo (HICKS, 2008), um '*hash*' é um número gerado a partir da leitura de uma mensagem ou documento sendo que diferentes mensagens deveriam gerar diferentes valores '*hash*', o termo 'deveriam' foi utilizado aqui, pois existe a possibilidade de duas mensagens diferentes originarem o mesmo valor '*hash*' mas a probabilidade é muito pequena.

Um bom algoritmo de '*hashing*' possui três qualidades importantes: Sensibilidade a pequenas alterações na mensagem original, impossibilidade de reversão, eficiência.

Garantia de Confidencialidade em Banco de Dados

Segundo (KENAN, 2006) os ataques ao banco de dados podem partir de um agente externo ou um agente interno que já possui acesso à rede local, estes ataques ameaçam um ou mais dentre três princípios básicos da segurança da informação, integridade, disponibilidade e 'confidencialidade' – que é o foco neste trabalho.

Um banco de dados pode conter informações confidenciais ou informações que não devem ser divulgadas a alguns usuários, em um ataque desse tipo uma pessoa não autorizada acessa a informação e a partir daí pode utilizá-las de modo prejudicial à instituição.

Em geral as organizações utilizam controle de acesso para proteger o banco de dados, o controle de acesso é um componente importante para a segurança, porém da maneira que é utilizado normalmente, apresenta alguns pontos fracos com relação a possíveis ataques a confidencialidade dos dados: usuários com permissão de 'somente leitura' em ambiente produtivo, ambientes não produtivos (ambientes de testes), cópias de segurança, acesso de administradores.

Uma vez que os dados são criptografados, estão mais seguros quanto ao risco de acesso não autorizado, porém, a criptografia diminui o risco, mas não o elimina, pois quando se utiliza a criptografia para proteger dados passa a ser necessário proteger a chave e ou certificado utilizados para a encriptação desses dados, são necessários controles de acesso eficazes para permitir o acesso direto ou indireto a chave, estes controles estão além do escopo deste trabalho.

Um indivíduo com acesso direto a chave pode copiá-la e utiliza-la sem temer ser detectado, no caso do acesso indireto, o indivíduo teria que interceptar uma aplicação ou serviço com permissões de acesso aos dados, portanto acesso a chave e utilizar este acesso para descriptografar a informação.

Estudo de Caso

Para esse artigo, o SGBD utilizado será o Microsoft SQL SERVER 2008 e o estudo de caso demonstrado, como feito por Souza (2012).

De acordo com (HIERARQUIA, s.d.), o SQL Server 2008 utiliza criptografia hierárquica de modo que cada camada criptografa a camada abaixo dela utilizando uma combinação de certificados, chaves simétricas e assimétricas, para a utilização de criptografia de dados, o SGBD, por meio de sua linguagem padrão de programação, fornece meios para a criação e manutenção de mecanismos como funções, chaves simétricas e assimétricas, certificados criptografia dos arquivos de dados do banco e suas cópias de segurança, funcionalidade chamada de criptografia transparente de dados.

Ainda segundo (HIERARQUIA, s.d.), ao utilizar criptografia de informações no banco de dados, é aconselhável utilizar chaves simétricas em lugar de chaves assimétricas ou certificados devido à diferença de complexidade dos mecanismos e, portanto diferente nível de utilização de recursos de processamento do servidor.

Um ponto fraco da abordagem usual de controle de acesso é a questão das permissões irrestritas de leitura dos administradores do banco de dados. Este risco poderia ser reduzido utilizando outro mecanismo de segurança do SGBD em conjunto com os métodos de criptografia descritos anteriormente, colocando o código de decriptação dos dados em procedimentos armazenados (*stored procedures*) ou visões (*views*),desse modo, as senhas ou frases chave podem ser encapsuladas utilizando-se o recurso de encriptação do código destes objetos do banco de dados.

> A opção WITH ENCRYPTION é outro recurso de segurança. Quando *views* ou *stored procedures* são criadas, o texto pode ser recuperado através das *views* de sistema sys.sql_modules e sys.syscomments. O código é, portanto, disponível para visualização. A *view* pode conter uma cláusula WHERE que deve ser mantida confidencial, ou pode haver alguma outra razão para

criptografar o código. A opção 'WITH ENCRYPTION' criptografa o código nas tabelas do sistema, esconde-o de sys.sql_modules e sys.syscomments e impede qualquer um de ver o código original. (NIELSEN, WHITE e PARUI, 2009 p344).

Para demonstrar o uso da opção WITH ENCRYPTION, foram criadas duas *stored procedures,* figura 3, cujo código retorna o numero descriptografado, selecionado da tabela TB_CARTAO a partir do CLI_ID fornecido, ambas utilizam a mesma chave para descriptografar o dado da coluna NUMERO_CRIPTOGRAFADO, primeiro demonstrando como o código da *procedure* pode ser visualizado e a seguir como este pode ser escondido utilizando a opção.

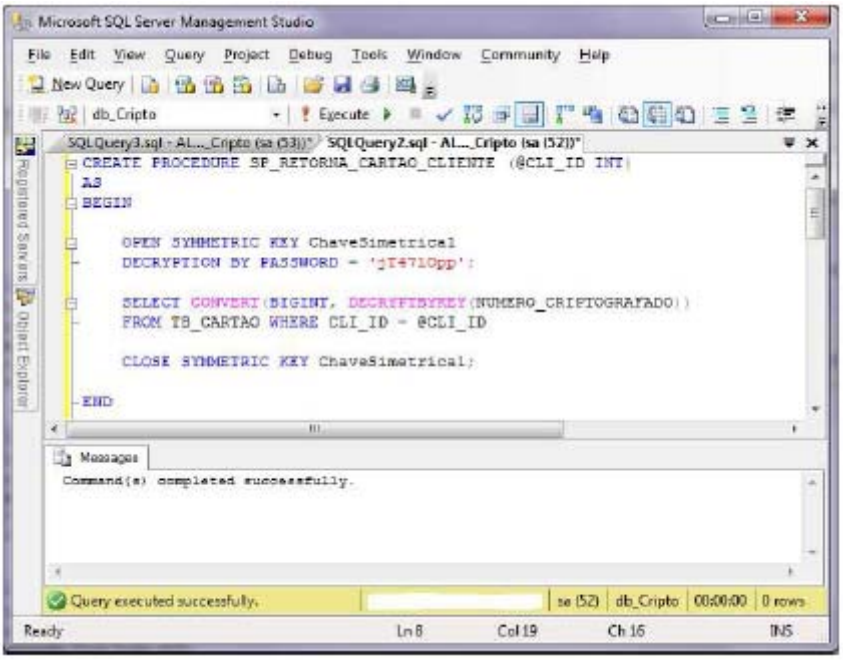

Figura 3 - Procedure SP_RETORNA_CARTAO_CLIENTE

Esta *procedure* não utiliza o recurso WITH ENCRYPTION, portanto, para um administrador do banco de dados seu código fonte pode ser visualizado nas *views* de sistema sys.sql_modules e sys.syscomments, como pode ser observado na figura 4:

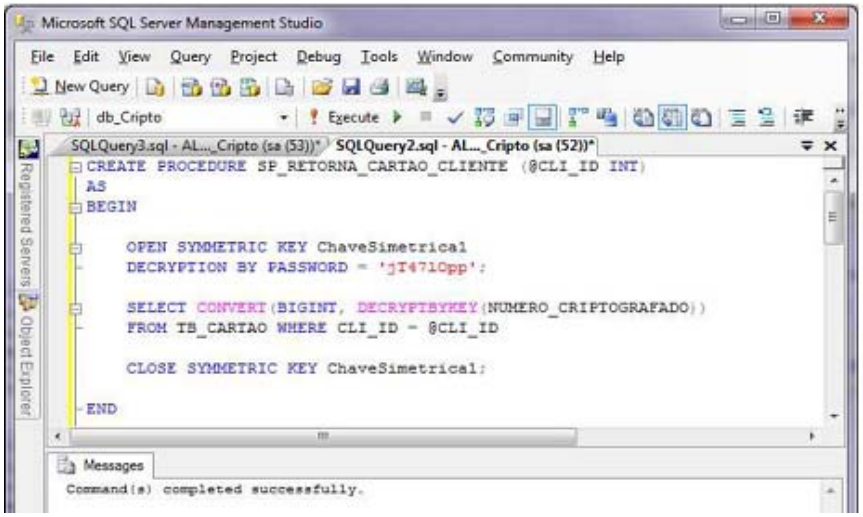

Figura 4 - Código exposto nas *views* de sistema

Neste caso, um administrador do banco de dados teria acesso ao código da *procedure*, inclusive a senha utilizada para descriptografar a informação com a chave simétrica.

Agora vejamos na figura 5 uma *procedure* com o mesmo código, porém utilizando a opção WITH ENCRYPTION:

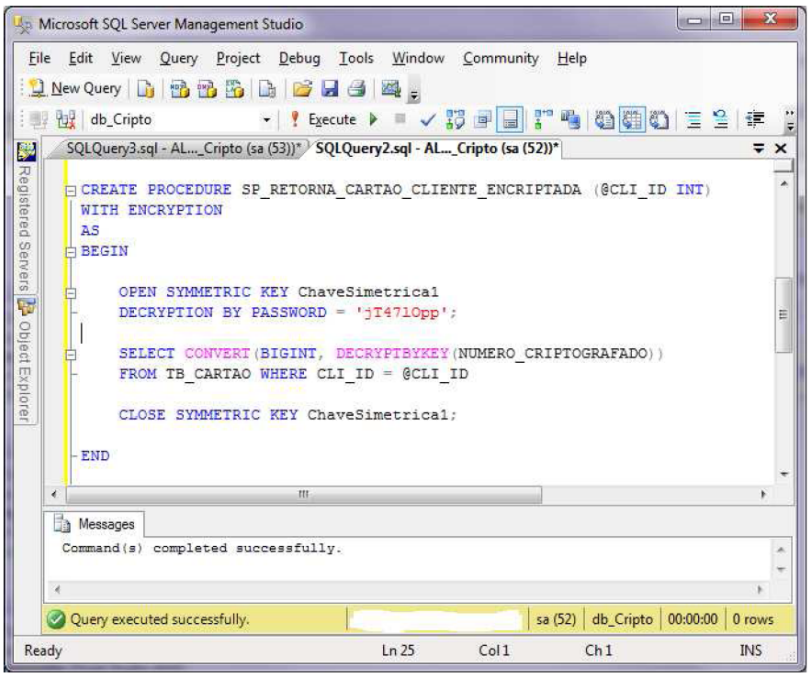

Figura 5 - Procedure utilizando a opção WITH ENCRYPTION

Desse modo, o código fonte da *procedure* não fica disponível nas *views* de sistema, mesmo para o administrador do banco de dados, conforme verificado na figura 6:

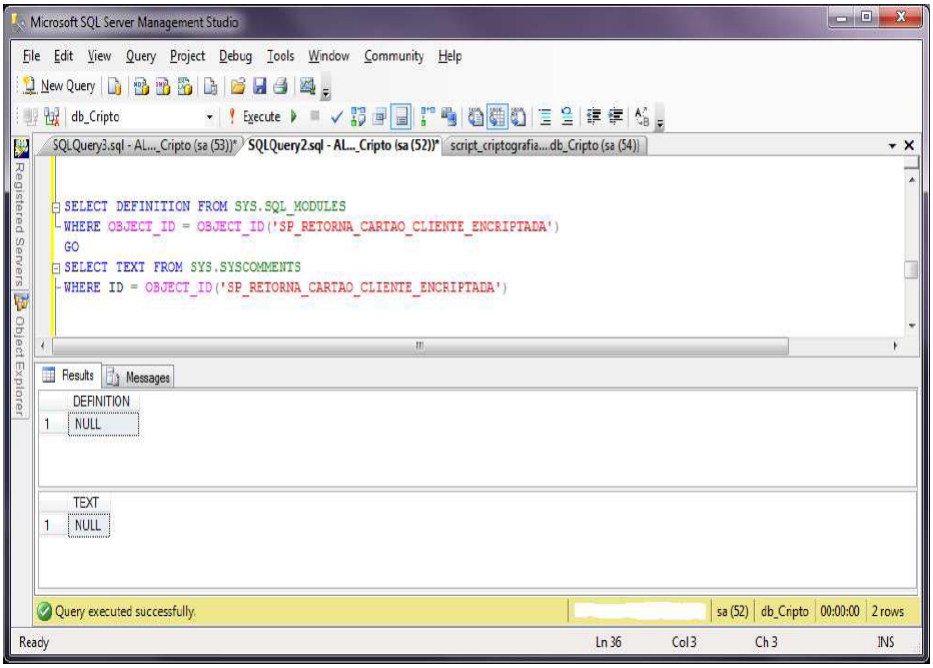

Figura 6 - *Select* retornando valor nulo para código fonte

Considerações Finais

O trabalho teve como objetivo demonstrar a possibilidade de garantir da confidencialidade de procedimentos armazenados em bases de dados, buscando uma solução para a questão de como garantir a confidencialidade de informações sigilosas mesmo que o intruso tenha conseguido acesso ao banco de dados, tendo demonstrado meios de reduzir o risco de violação desse princípio utilizando recursos de encriptação de informações.

Este artigo tratou a questão da confidencialidade de informações armazenadas em banco de dados, levantando a possibilidade de tornar ocultas *stored procedures* que não podem ser vistas por outros usuários do sistema.

A pesquisa, desenvolvida por Souza(2012), demonstra que, utilizando os conceitos apresentados na fundamentação teórica, criação de stored procedures, associados ao conceito de criptografia, em ferramentas já disponíveis no SGBD SQL Server 2008, podemos tornar procedimentos armazenados invisíveis aos usuários, protegendo seu conteúdo ou, até mesmo, seu código fonte.

Bibliografia

Coronel, C., Morris, S., Rob, P. (2011) “Database systems: design, implementation and management” 9 ed. Boston: Course Technology.

Date, C. J. (2000) “Introdução a sistemas de banco de dados” 7 ed. Rio de Janeiro: Campus.

Elmasri, R., Navathe, S. B. (2005) “Sistemas de banco de dados” 4 ed, São Paulo: Addison Wesley.

Forouzan, B. A. (2008), “Comunicação de dados e redes de computadores” 4 ed, São Paulo: McGraw-Hill.

Hicks, J.(2008), “Cryptography in SQL Server”, disponível em: http://msdn.microsoft.com/en-us/library/cc837966%28v=sql.100%29.aspx acessado em 19/04/2012 20:50.

Hierarquia de criptografia s.d. “Manual online do software”, disponível em: http://msdn.microsoft.com/pt-br/library/ms189586(v=sql.100).aspx acessado em 08/05/2012 19:04.

Kenan, K. (2006) “Cryptography in the database: the last line of defense”, Pearson Education Inc.

Mullins, C. S. (2002) “Database administration”, Boston: Pearson Education Inc.

Nielsen, P., White, M., Parui, U. (2009), “Microsoft sql server 2008 bible”, Indianapolis: Wiley Publishing, Inc.

Rodriguez, M. V., FERRANTE, Augustin J. (2000), “Tecnologia de informação e gestão”, Rio de Janeiro: E-Papers.

Souza, A., A., P., “Criptografia em Gerenciador de Banco de Dados SQL Server 2008”, Monografia de Conclusão de Curso – Informática para a Gestão de Negócios, Fatec Zona Leste, São Paulo, 2012.

Sumathi, S., Esakkirajan, S. (2007), “Fundamentals of relational database management systems”, Varsóvia: Springer.

Tilborg, Henk, C., A. (2005), “Encyclopedia of cryptography and security”, Nova Iorque: Springer.