UNIVERSIDADE ANHANGUERA – UNIDERP

POLO DE (Porto Alegre-RS)

Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas

(BRUNO RAMIRES DE MORAES FERREIRA - 2931636229)

PRODUÇÃO TEXTUAL INTERDISCIPLINAR

Disciplinas Norteadoras:

INTERAÇÃO HUMANO-COMPUTADOR

ÉTICA, POLÍTICA E SOCIEDADE

SISTEMAS DE COMPUTAÇÃO E INFORMAÇÃO

SEGURANÇA DA INFORMAÇÃO

SEMINÁRIOS I

Tutor (a) EAD: JOICE SIQUEIRA LIMA

PORTO ALEGRE / RS

2018

SUMÁRIO

TAREFA 1

CADASTRO DE CLIENTES (OFICINA MECÂNICA);

CADASTRO DE CLIENTES (OFICINA MECÂNICA)												
CÓD.	NOME DO CLIENTE	CPF/RG	ENDEREÇO	BAIRRO	CIDADE/UF	TELEFONE/CELU	E-MAIL	SERVIÇO PRESTADO	PLACA	VEÍCULO	DESCONTO	DATA DE CADASTRO
1	Bruno Ramires	865.214.380-3X	Rua André C. Dutra, 50	Monte Cristo	Porto Alegre/RS	(51) 9 9104-9xx5	brunormferreira@XXX.com	SUSPENSÃO	BFG-4585	Ka Sedan Ltz 1.4	5%	16/04/2018
2	Marcelly Silva	025.837.250-8X	Rua André C. Dutra, 50	Monte Cristo	Porto Alegre/RS	(51) 9 8503-7xx1	marcellysantunes@XXX.com	FREIO	ASD-6955	Hb20 2.0 AT.	10%	22/04/2018
3	Igor Ramires	458.458.957-4X	Av. Juca Batista, 250	Cavalhada	Porto Alegre/RS	(51) 9 8671-6xx2	igorramirezz@XXX.com	MOTOR	KBC-4487	Onix Lt 1.0	0%	27/05/2018

TAREFA 2

a) Organização hierárquica dos dados

HIERARQUIA DOS DADOS

BANCO DE DADOS OFICINA MECÂNICA

Banco de dados

*Arquivo do curso
*Arquivo financeiro
*Arquivo de histórico pessoal

Arquivo

NOME	VEÍCULO	SERVIÇO	DESCONTO
Bruno Ramires	Ka Sedan	Suspensão	5%
Marcelly Silva	Hb20 2.0	Freio	10%
Igor Ramires	Onix Lt 1.0	Freio	0%

Registro

NOME	VEÍCULO	SERVIÇO	DESCONTO
Bruno Ramires	Ka Sedan	Suspensão	5%

Campo

Bruno Ramires

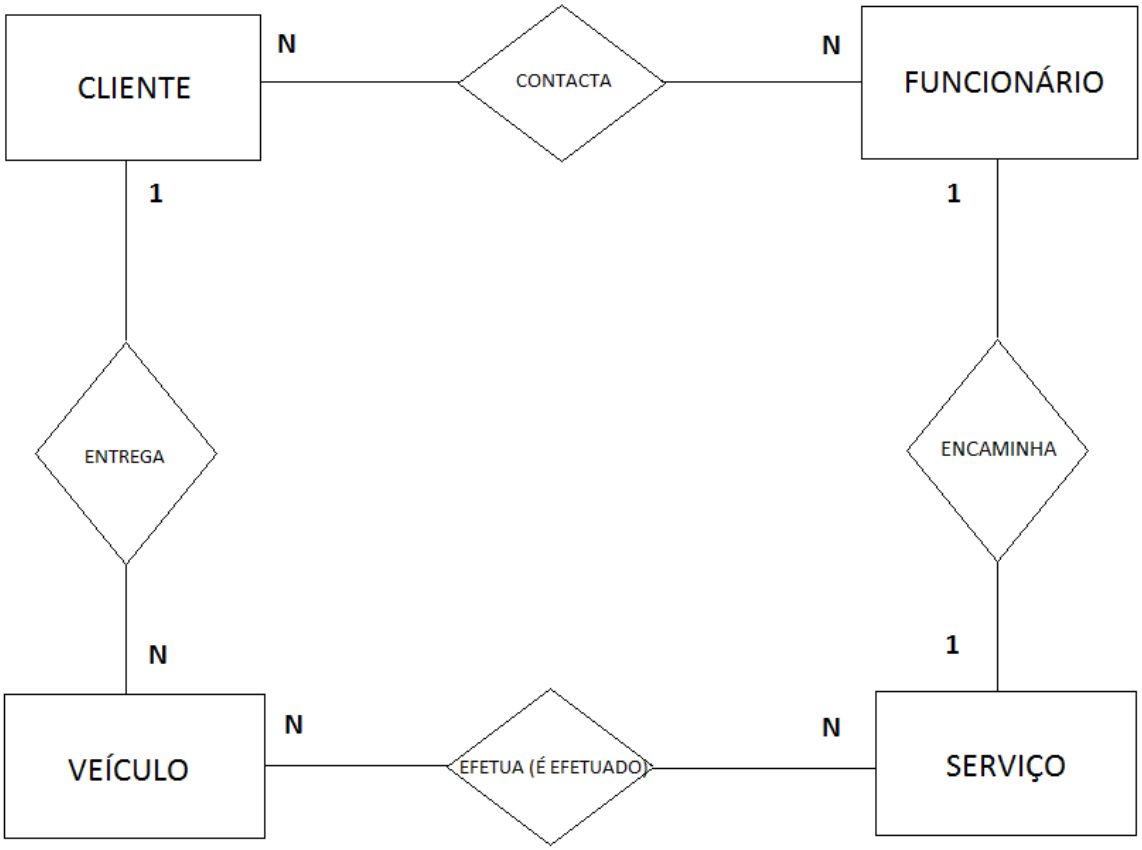
Byte

01001010

Bit

0

b) Diagrama de relacionamento quantitativo dos dados.



c) Explanação da análise realizada e representada nos dois itens apresentados.

- Cliente *contacta* Funcionário (um cliente pode contatar vários funcionários e um funcionário pode ser contatado por vários clientes).
- Funcionário *encaminha* Serviço (um funcionário encaminha apenas um serviço e apenas um serviço pode ser encaminhado por apenas um funcionário).
- Serviço *efetuado* Veículo (qualquer serviço pode ser efetuado em qualquer veículo e qualquer veículo pode receber qualquer serviço).
- Veículo *entrega* Cliente (qualquer veículo pode ser entregue a apenas um cliente e apenas um cliente pode receber qualquer veículo).

TAREFA 3

CRIPTOGRAFIA SIMÉTRICA

A criptografia simétrica é também conhecida por criptografia de chave secreta. DES, 3DES, AES e RC4 são alguns dos algoritmos que usam criptografia simétrica.

Algoritmos que usam criptografia simétrica tendem a ser mais rápidos, no entanto não são tão seguros como os que usam criptografia assimétrica, uma vez que a chave usada para cifrar a informação é partilhada entre as várias máquinas. Porém é uma ótima forma de criptografia enquanto não é abrangido um modo assimétrico (logo abaixo).

Como vantagem, a criptografia tem uma boa performance e a possibilidade de manter uma comunicação contínua entre várias pessoas simultaneamente. Caso a chave seja comprometida, basta efetuar a troca por uma nova, mantendo o algoritmo inicial.

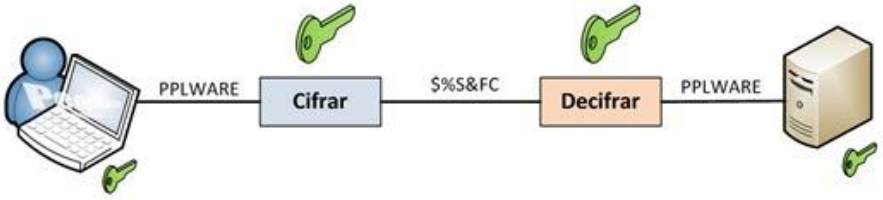
A criptografia de chave simétrica, quando comparada com a de chaves assimétricas, é a mais indicada para garantir a confidencialidade de grandes volumes de dados, pois seu processamento é mais rápido. Todavia, quando usada para o compartilhamento de informações, se torna complexa e pouco escalável, em virtude da:

- Necessidade de um canal de comunicação seguro para promover o compartilhamento da chave secreta entre as partes (o que na Internet pode ser bastante complicado) e;
- Dificuldade de gerenciamento de grandes quantidades de chaves (imagine quantas chaves secretas seriam necessárias para você se comunicar com todos os seus amigos).

Apesar do seu alto desempenho, a criptografia simétrica possui falhas graves de segurança. A gestão de chaves, por exemplo, torna-se mais complexa conforme o número de pessoas que se comunica aumenta. Para cada N usuários, são necessárias N2 chaves.

Funcionamento Criptografia Simétrica

É usada uma única chave que é partilhada entre o emissor e o receptor. Desta forma, a chave que é usada para cifrar é a mesma que é usada para decifrar.



CRIPTOGRAFIA ASSIMÉTRICA

Em comparação com a criptografia simétrica, a criptografia assimétrica tende a ser mais lenta e necessita de um maior poder computacional por parte das máquinas. No entanto, este é um excelente método para garantir segurança num canal público e inseguro (ex. Internet). Apenas a chave pública é partilhada entre emissor e receptor, e a chave privada é usada para decifrar a informação.

A criptografia assimétrica, também conhecida como criptografia de chave pública, é baseada em 2 tipos de chaves de segurança — uma privada e a outra pública. Elas são usadas para cifrar mensagens e verificar a identidade de um usuário.

Resumidamente falando, a chave privada é usada para decifrar mensagens, enquanto a pública é utilizada para cifrar um conteúdo. Assim, qualquer pessoa que precisar enviar um conteúdo para alguém precisa apenas da chave pública do seu destinatário, que usa a chave privada para decifrar a mensagem.

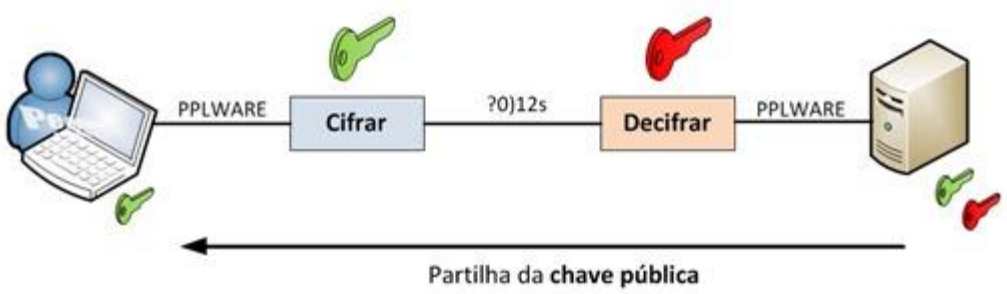
A criptografia de chaves assimétricas, apesar de possuir um processamento mais lento que a de chave simétrica, resolve estes problemas visto que facilita o gerenciamento (pois não requer que se mantenha uma chave secreta com cada um que desejar se comunicar) e dispensa a necessidade de um canal de comunicação seguro para o compartilhamento de chaves.

Para aproveitar as vantagens de cada um destes métodos, o ideal é o uso combinado de ambos, onde a criptografia de chave simétrica é usada para a codificação da informação e a criptografia de chaves assimétricas é utilizada para o compartilhamento da chave secreta (neste caso, também chamada de chave de

sessão). Este uso combinado é o que é utilizado pelos navegadores Web e programas leitores de e-mails. Exemplos de uso deste método combinado são: SSL, PGP e S/MIME.

Funcionamento Criptografia Assimétrica

*Usam um par de chaves distintas (chave privada e chave pública);
*A chave pública é usada para cifrar (encriptar);
*A chave privada é usada para decifrar (desencriptar).



Em síntese;

Criptografia de Chave Simétrica

- Mesma chave para cifrar e decifrar;
- Mais rápida;
- Problema de distribuição de chaves.

Criptografia de Chave Pública (assimétrica)

- Duas Chaves (uma privada e outra pública);
- Pode garantir confidencialidade ou autenticidade;
- Mais lenta (Problema de desempenho).

ASSINATURA DIGITAL

A assinatura digital permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isto e que ela não foi alterada.

A assinatura digital baseia-se no fato de que apenas o dono conhece a chave privada e que, se ela foi usada para codificar uma informação, então apenas seu dono poderia ter feito isto. A verificação da assinatura é feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo.

FUNÇÃO HASHING

A utilização da criptografia assimétrica na assinatura digital se torna inviável por causa da lentidão do seu algoritmo.

Como alternativa a este problema é empregado um mecanismo denominado função hashing. Este mecanismo gera um valor de tamanho fixo derivado da mensagem a ser assinada. Também conhecida como Message Digest, One-Way Hash Function, Função de Condensação ou Função de Espalhamento Unidirecional, a função Hashing funciona como uma impressão digital de uma mensagem, gerando a partir de uma entrada de tamanho variável, um valor fixo: o digest ou valor hash. Este valor está para o conteúdo da mensagem assim como o dígito verificador de uma conta-corrente está para o número da conta. Após o valor hash de uma mensagem ter sido calculado, qualquer modificação em seu conteúdo será detectada pois o valor hash da nova mensagem será diferente do valor hash da mensagem original.

Uma função de resumo é um método criptográfico que, quando aplicado sobre uma informação, independentemente do tamanho que ela tenha, gera um resultado único e de tamanho fixo, chamado hash.

As funções hashing mais utilizadas são: MD5, SHA-1, MD2 e MD4.

CRIPTOGRAFIA E CERTIFICADOS DIGITAIS

Os algoritmos de criptografia podem ser utilizados em conjunto para tornar vários processos de análise de dados e troca de informações mais seguros. Assim, o ciframento de mensagens, a verificação de identidades e a otimização de assinaturas digitais torna-se mais ágil e poderosa. Juntos, eles podem tornar mecanismos comerciais, como os certificados digitais, mais confiáveis e imunes a falhas de segurança.

Os certificados digitais modernos são usados para garantir a identidade de pessoas em ambientes digitais. Eles permitem a identificação de tentativas de alteração de chaves públicas por terceiros, tornando a comunicação entre pessoas mais segura. Todo certificado digital é assinado por uma autoridade de certificação ou CA (sigla para certification authority).

O padrão PKI (Public Key Infrastructure) regula o gerenciamento de chaves públicas. É ele quem define o local de armazenamento dos certificados digitais, de que forma serão armazenados, revogação de certificados, etc.

Para o usuário comum, o uso de certificados digitais pode ser visto como uma estratégia de segurança de alta eficácia. Em atividades como a declaração do Imposto de Renda, o uso de um certificado digital aumenta a confiabilidade do envio da declaração, tornando a comunicação com os órgãos do governo mais eficaz.

Garantir a confiabilidade em comunicações digitais é algo indispensável para o ambiente corporativo. Empresas devem implementar soluções que facilitem o uso de sistemas que trabalham com dados sensíveis com alto desempenho e confiabilidade. Dessa forma, sites como os de e-commerce podem ser mais confiáveis e imunes a ameaças digitais.

MÉTODO ADEQUADO PARA OFICINA MECÂNICA

Com base nas explicações e pesquisas acima, o melhor método que se aplica há um cadastro de clientes seria a criptografia simétrica que usa a mesma chave para encriptar e desencriptar, até o aperfeiçoamento da tecnologia de criptografia assimétrica na empresa de Oficina Mecânica.

TAREFA 4

Como um profissional e atuante da área, se faz necessário agir com plena ética e moral diante de seus clientes ou qualquer outra pessoa que venha a interagir. Jamais devemos se mostrar superior diante de alguém ou de algum projeto, não estabelecendo regras sem consultá-las antes, não agregando itens sem antes pesquisar com sabedoria e não com pressa. Há uma necessidade de extrema moral para um ambiente coerente e sadio e não um ambiente pesado para nenhum lado, por exemplo, em uma reunião sobre o software projetado. Cumprir esta responsabilidade exige, no mínimo, uma investigação e um posicionamento explícito sobre os aspectos éticos da atividade relacionada.

A inserção de projetos em novos ambientes com alto nível de competitividade deve ser muito cautelosa e de alto sigilo, pois qualquer descuido referente à nossa ética e moral, poderá acarretar no declínio do projeto e da ética estabelecida pelo profissional.

O produto de cadastro de clientes estará a disposição no mercado por uma empresa terceirizada denominada “C&A Vendas de Software”. Que estará fazendo a venda deste imenso sistema de tabelas que lhe trará inúmeros benefícios de organização em sua empresa, podendo lhe fornecer os dados necessários para os funcionários quando precisarem, contendo as informações de nome, endereço, tipo de serviço, desconto, veículo e muito mais! É um sistema adequado para você alavancar seus negócios com muita organização e sabedoria. Contrate agora mesmo este excelente software para sua empresa que conta com ótimos profissionais da área.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Junior; **Criptografia Simétrica X Criptografia Assimétrica (Criptografia de Chave Pública)** postado no site ITnerante em 18 de Agosto 2012. http://www.itnerante.com.br/profiles/blogs/criptografia-sim-trica-x-criptografia-assim-trica-criptografia-de

PINTO, Pedro; **Criptografia Simétrica e Assimétrica. Sabe a diferença?** Postado por Pedro Pinto no site Pplware em 07 de Dezembro de 2010. https://pplware.sapo.pt/tutoriais/networking/criptografia-simetrica-e-assimetrica-sabe-a-diferenca/

Cartilha de Segurança para Internet – **CERT.br** https://cartilha.cert.br/criptografia/

Valid Certificadora Digital – **Qual a diferença entre elas?** Postado em 01 de Novembro de 2017. http://blog.validcertificadora.com.br/?p=8897

SOTERO, Sergio; **Criptofrafia e Certificação Digital** – Postado por Sergio Sotero em 16 de Julho de 2003. https://imasters.com.br/artigo/1209/dotnet/criptografia-e-certificacao-digital?trace=1519021197&source=single

MAIA, Luiz Paulo; PAGLIUSI, Paulo Sergio; **Artigo Criptografia e Certificação Digital.** http://www.training.com.br/lpmaia/pub_seg_cripto.htm