Instituto Federal de Educação, Ciência e Tecnologia do Ceará		
Disciplina:	**Redes de Computadores**	**Prof. Nídia S. Campos**
Aluno:	**Francisco Jorge M. Jr.**	
Trabalho 2 - Criptografia e o SSL		

TAREFAS

TAREFA 1. A **criptografia** implementa a confidencialidade de dados do SSL. O que é criptografia? Pesquise e descreva um esquema de criptografia composto por: **texto claro**, **algoritmo de criptografia**, **texto cifrado** e **chave**.

É a conversão de dados de um formato legível em um formato codificado, que só podem ser processados e lidos depois de serem descriptografados pelo receptor. É um elemento fundamental da segurança de dados. É a forma mais simples e mais importante de garantir que as informações do sistema de um computador não sejam roubadas e lidas por alguém que deseja usá-las para fins maliciosos.

A criptografia de segurança de dados é amplamente usada por usuários individuais e grandes corporações para proteger desde dados de pagamento até informações pessoais dos usuários enviadas entre um navegador e um servidor. Os softwares de criptografia de dados, também conhecidos como algoritmo de criptografia ou codificação, são usados para desenvolver um esquema de criptografia que teoricamente pode ser desvendado apenas com uma grande capacidade de processamento.

Criptografia AES (Advanced Encryption Standard)

Utiliza a criptografia do tipo de Chaves de Criptografia Simétrica, ou seja, faz uso de uma única chave de criptografia privada, que é compartilhada entre o emissor e o destinatário de um conteúdo, essa chave é uma cadeia própria de bits, que define a forma como o algoritmo vai codificar/decodificar um conteúdo.

Esta permite usar chaves criptográficas de 128, 192 e 256 bits para criptografar e descriptografar dados em blocos de 128 bits (quanto maior a chave criptográfica, maior será o poder computacional exigido para quebrar a criptografia sem a chave, ou seja, maior a segurança fornecida). Entre alguns dos aplicativos mais comuns de algoritmo AES incluem-se aplicativos de mensagens, como o Signal ou WhatsApp, e o programa de compactação de arquivos WinZip.

TAREFA 2. O SSL usa dois tipos de criptografia: criptografia de **chave simétrica** e de **chave pública**. Explique como eles funcionam.

Chave simétrica: também conhecida como criptografia de chave privada. Neste tipo de criptografia a mesma chave usada para codificar é a usada para decodificar os dados, sendo assim é o tipo de criptografia mais indicado para usuários individuais e sistemas fechados. Caso contrário, a chave deve ser enviada ao destinatário. Isso aumenta o risco de comprometimento se for

interceptada por um terceiro, como um hacker. Esse método é mais rápido do que o método assimétrico.

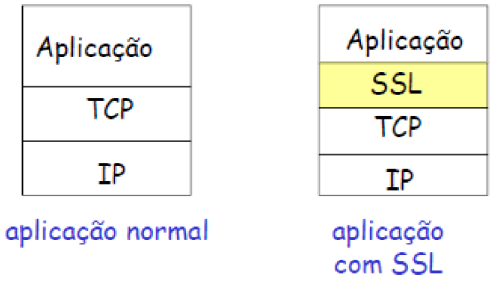
Como vantagem, esta criptografia tem uma boa performance e a possibilidade de manter uma comunicação contínua entre várias pessoas simultaneamente. Caso a chave seja comprometida, basta efetuar a troca por uma nova, mantendo o algoritmo inicial.

Chave pública: também conhecida como Chaves de criptografia assimétrica, esse tipo usa duas chaves diferentes, uma pública e uma privada, que são vinculadas matematicamente. É mais utilizada para cifrar mensagens e verificar a identidade de um usuário. A chave privada é usada para decodificar mensagens, enquanto a pública é utilizada para codificar o 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.

Essencialmente, as chaves são apenas grandes números que foram emparelhados um ao outro, mas não são idênticos, daí o termo assimétrico. A chave privada é mantida em segredo pelo usuário, e a chave pública também é compartilhada entre destinatários autorizados ou disponibilizada ao público em geral.

TAREFA 3. No lado do remetente, os protocolos da camada de aplicação enviam suas mensagens para que o SSL as codifique e repasse para o TCP, da camada de transporte. No lado do receptor, o TCP recebe as mensagens codificadas e as entrega ao SSL, que as decodifica e as repassa para os protocolos da camada de aplicação.

Pesquise e cite protocolos da camada de aplicação que utilizam o SSL.



Resposta: Sua utilização mais frequente é na World Wide Web, ou seja, nas aplicações que utilizam o protocolo HTTP (HyperText Transfer Protocol), categoria na qual os web browsers são maioria, e geralmente utilizados por leigos.