**Instituto Federal de Educação, Ciência e Tecnologia do Ceará**

**Disciplina: Redes de Computadores Prof. Nídia S. Campos**

**Trabalho 2 - Criptografia e o SSL**

**EQUIPE: Francisco Lucas // Juliana Cardoso**

**OBJETIVO**

* Conhecer princípios de criptografia.
* Conhecer o protocolo SSL e as aplicações que o utilizam.

**Introdução**

Os programas que usam redes de computadores para se comunicarem fazem com que os protocolos da camada de aplicação enviem e recebam mensagens através da camada de transporte. A maioria dessas mensagens usam a codificação ASCII. Ou seja, em uma rede compartilhada, como as redes sem fio, essas mensagens podem ser lidas e entendidas com muita facilidade por outros usuários com um analisador de pacotes (ex. Wireshark, tcpdump). O **SSL (Secure Socket Layer)** foi criado para oferecer serviços de segurança em conexões TCP entre dois processos na Internet. Entre estes serviços, está a **confidencialidade** dos dados, onde, a leitura e entendimento da mensagem só pode ser feita pelo remetente e destinatário dessa mensagem.

**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**.

Segundo a Wikipédia, criptografia “é o estudo e prática de princípios e técnicas para [comunicação segura](https://pt.m.wikipedia.org/w/index.php?title=Comunica%C3%A7%C3%A3o_segura&action=edit&redlink=1) na presença de terceiros, chamados "[adversários](https://pt.m.wikipedia.org/wiki/Advers%C3%A1rio_(criptografia))". Mais geralmente, a criptografia refere-se à construção e análise de [protocolos](https://pt.m.wikipedia.org/wiki/Protocolo_de_comunica%C3%A7%C3%A3o) que impedem terceiros, ou o público, de lerem mensagens privadas”. É um sistema de algoritmos matemáticos que codificam dados do usuário para que só o destinatário possa ler.

Em um esquema de criptografia simples, uma mensagem em sua forma original é conhecida como texto aberto ou texto claro. A mensagem em texto aberto que será enviada é criptografada usando um algoritmo de criptografia, de modo que a mensagem criptografada, conhecida como texto cifrado, pareça ininteligível para qualquer intruso.



Figura – Componentes criptográficos

Observando pela Figura 1, um emissor fornece uma chave *KE*, uma cadeia de números ou de caracteres, como entrada para o algoritmo de criptografia. O algoritmo pela essa chave e o texto aberto da mensagem *m* como entrada e produz um texto cifrado como saída, com notação *KE(m)*. De maneira semelhante, um destinatário fornecerá uma chave *KD*, ao algoritmo de decriptação, que pega o texto cifrado e a chave como entrada e produz o texto aberto original com saída, isto é, se o destinatário receber uma mensagem criptografada *KE(m)*, ele a descriptará calculando *KD(KE(m)) = m*.

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

A criptografia de chave simétrica usa a mesma chave tanto para criptografar como para descriptografar dados. Os algoritmos que são usados para a criptografia simétrica são mais simples do que os algoritmos usados na criptografia assimétrica. Em função desses algoritmos mais simples, e porque a mesma chave é usada tanto para criptografar como para descriptografar dados, a criptografia simétrica é muito mais rápida que a criptografia assimétrica. Portanto, a criptografia simétrica é adequada à criptografia e à descriptografia de uma grande quantidade de dados.

Uma das principais desvantagens da criptografia simétrica é o uso da mesma chave tanto para criptografar como para descriptografar os dados. Por isso, todas as partes que enviam e recebem os dados devem conhecer ou ter acesso à chave de criptografia.

A criptografia simétrica fornece autorização para dados criptografados. Por exemplo, ao usar a criptografia simétrica, uma organização pode estar razoavelmente certa de que apenas as pessoas autorizadas a acessar a chave de criptografia compartilhada podem descriptografar o texto codificado. No entanto, a criptografia simétrica não fornece não-repúdio. Por exemplo, em um cenário em que vários grupos têm acesso à chave de criptografia compartilhada, a criptografia simétrica não pode confirmar o grupo específico que envia os dados.

Já a criptografia de chave pública (ou assimétrica) usa duas chaves diferentes, porém matematicamente relacionadas, para criptografar e descriptografar dados. Essas chaves são conhecidas como chaves privadas e chaves públicas. Em conjunto, essas chaves são conhecidas como par de chaves. A criptografia assimétrica é considerada mais segura do que a criptografia simétrica, porque a chave usada para criptografar os dados é diferente da que é usada para descriptografá-los. Contudo, como a criptografia assimétrica usa algoritmos mais complexos do que a simétrica, e como a criptografia assimétrica usa um par de chaves, o processo de criptografia é muito mais lento quando uma organização usa a criptografia assimétrica do que quando usa a simétrica.

Com a criptografia assimétrica, somente uma parte mantém a chave privada. Essa parte é conhecida como o assunto. Todas as outras partes podem acessar a chave pública. Os dados criptografados por meio da chave pública só podem ser descriptografados com o uso da chave privada. Por outro lado, os dados criptografados por meio da chave privada só podem ser descriptografados com o uso da chave pública. Por conseguinte, esse tipo de criptografia fornece confidencialidade e não-repúdio.

**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.

IMAP (TCP/993); POP3 (TCP/995); FTP (TCP, UDP/989) – dados; FTP (TDP, UDP/990) – controle; LDAP (TCP, UDP/636); HTTPS (TCP/443); NNTP (TCP, UDP/563); Telnet (TCP, UDP/992).