Capítulo 02 - A web segura - HTTPS

Nesse capítulo aprendemos:

- Quando usamos apenas o HTTP os dados trafegados na comunicação vão no formato texto, sem criptografia, ou seja, qualquer um no meio dessa comunicação pode ler os dados e isso é PERIGOSO! (podemos comprovar isso na aba network do navegador);

- Numa comunicação WEB entre Cliente e Servidor há a internet, e a internet é composta por diversas máquinas (inclusive de sua operadora), logo utilizar HTTP na WEB é INSEGURO!

- Para navegar com SEGURANÇA devemos utilizar o HTTPS, o 'S' é que antes a segurança era feito por SSL, mas atualmente é utilizado o TLS (podemos encontrar a sigla SSL/TLS).
  Significados: SSL/TLS = Secure Sockets Layer / Transport Layer Security;

- Como sabemos que ao acessar o site www.alura.com.br o servidor que irá responder é realmente do Alura? Simples, quem comprova a identidade de um servidor é o CERTIFICADO DIGITAL;

- O CERTIFICADO DIGITAL ainda guarda a CHAVE PÚBLICA que irá criptografar os dados que serão trafegados entre Cliente e Servidor;

- A CHAVE PÚBLICA fica do lado do Cliente (Navegador);

- A CHAVE PRIVADA fica do lado do servidor, apenas ela consegue DESCRIPTOGRAFAR uma mensagem,

- Esse método de ter duas chaves, uma para codificar e outra para decodificar chama-se Criptografia assimétrica. Ela é lenta, mas é segura. Outro método é a simétrica, que usa a mesma chave, ela é rápida, mas menos segura!

- HTTPS usa tanto o método Simétrico e Assimétrico,

- Como funciona no HTTPS? Quando vamos utilizar o HTTPS já sabemos que o cliente tem um certificado ditigal para verificar a identidade do servidor, ou seja, o cliente por ter o certificado já tem a chave pública e o servidor tem a chave privada, acontece que quando o cliente vai enviar uma mensagem ele gera uma chave simétrica somente para ele e o servidor e vai enviar essa chave ao servidor usando a chave assimetrica (ninguem vai conseguir ver essa chave),

depois as próximas requisições vai utilizar apenas a cahve pública. Resumindo: a primeira mensagem trocada entre Cliente e Servidor usa a chave ASSIMETRICA (e nessa mensagem envia-se a chave simetrica), nas outras irá utilizar a chave SIMETRICA (há um prazo para renovar sessão).