Objetivo

Desenvolvimento de uma aplicação web que armazene arquivos com segurança, utilizando de criptografia para proteger os dados.

Introdução a internet

A transferência de informações sempre foi muito importante, visando velocidade e segurança, com isso o durante a guerra fria, o Departamento de Defesa americano, queria dispor de um meio de comunicação militar que interligasse seus centros. Um meio que conseguisse suportar uma destruição parcial e continuasse funcionando.

Então se criou ARPAnet, a qual foi fruto de pesquisas da Advanced Research Project Agency (ARPA), a primeira rede nacional de computadores criada em 1969, era uma rede privada que ligava os centros de pesquisas, universidades e instituições militares americanas, usada para compartilhamento de recursos entre pesquisadores que trabalhavam em projetos militares.

Em 1972 o governo americano expos o projeto pioneiro para sociedade, a ideia expandiu-se entre as universidades, interessadas em desenvolver trabalhos em conjunto. Com objetivo de interligar computadores de diferentes centros de pesquisas, em 1980 a internet adotou o protocolo TCP/IP para conectar sistemas heterogêneos, que com o tempo passou a se comunicar com diferentes dispositivos.

O nome internet foi definido em 1983 e três anos depois, a National Science Foundation criou a ligação em alta velocidade com seu centro de supercomputadores e passou a promover o compartilhamento das informações cientificas. Então o governo decidiu financiar a formação de redes regionais em todo pais.

Uma parte importante para a internet ficar com a cara que ela tem hoje, ocorreu em 1990, quando o pesquisador do Conselho Europeu para a Pesquisa Nuclear em Genebra(Cern), Tim Berners-Lee, criou o protocolo HTTP(Hyper Texte Transfer Protocol) e a linguagem HTML(Hyper Texte Markup Language), que permite que naveguemos entre sites. A Word Wide Web (www) apareceu para o mundo e abriu a internet ao publico, empresas particulares e privadas.

Introdução a criptografia

A segurança na transmissão de informações sempre foi muito importante, antigamente a cifragem era muito utilizada nas épocas de guerra, para trocar mensagens sem que o inimigo conseguisse descobrir a mensagem se a mesma fosse interceptada. Eram trocadas mensagens cifradas desde estratégias de guerras á cartas de amor. O registro do primeiro uso de criptografia documentado foi em torno de 1900 a.c., no Egito, quando um escriba usou hieróglifos fora do padrão numa inscrição.

Os hebreus, entre 600 a.c. e 500 a.c., utilizavam a cifra de substituição simples(fácil para reverter e fazendo uso de cifragem duplar para obter o texto original), sendo monogrâmica e monoalfabético(os caracteres são trocados um a um por outros), assim escreveram o Livro de Jeremias.