

Design Thinking

Entrega 3 - Lista 4

Definição do Contexto

Considere que você foi contratado por uma empresa de grande porte no Brasil. Esta empresa sofreu recentemente ataques de espionagem. Ocorreram trocas de mensagens entre funcionários da empresa e contatos de empresas rivais – com o principal objetivo de criar um esquema para interceptação de mensagens.

A criptografia é um método de proteção e privacidade de dados muito importante e cada vez mais presente nas nossas vidas. A criptografia nada mais é do que um conjunto de regras que visa codificar a informação de forma que o emissor e o receptor consigam decifrá-la.

Definição do Problema

Sem a criptografia qualquer pessoa poderia interceptar senhas e dados que trafegam por uma rede de computadores.

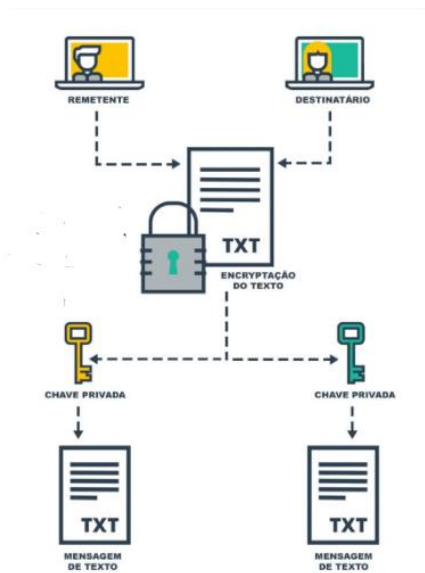
O principal problema da empresa, é a vulnerabilidade do sistema de chat, o que propicia ataques de espionagem de empresas rivais, onde ocorre dentro da empresa e troca de mensagens entre os funcionários com essas outras empresas.

Ideias

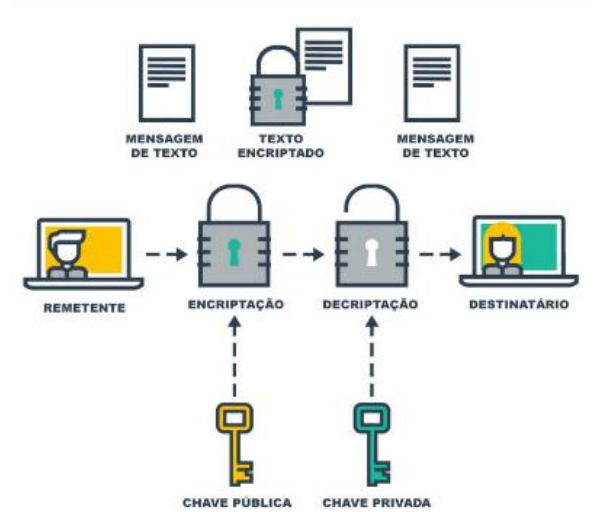
- Será necessário criar um sistema de criptografia ponta a ponta;
- Criar chaves de segurança para cada chat de conversa (privada ou pública);
-
- Será utilizado um sistema Assimétrico para criptografar e descriptografar das informações

Funcionamento Estrutural

A criptografia reforça a segurança de uma mensagem ou arquivo embaralhando o conteúdo. Para criptografar uma mensagem, você também precisa da chave certa para decodificá-la. É o modo mais eficaz para ocultar comunicações através de informações em código, onde o remetente e o destinatário têm a chave para decifrar os dados.



Modelo chave privada



Modelo chave pública

Protótipo do Programa

