Atividade prática

Programação Orientada à Objeto

Professor Me. Eng. Gerson Neto.

Programas utilizados:

- Eclipse IDE.
- Plataforma Java SE.

Contextualização:

Atualmente é comum o uso de aplicativos multiplataforma de mensagens instântaneas e chamadas de voz, principalmente para smartphones – whatsapp como exemplo. Além de mensagens de texto, os usuários podem enviar imagens, vídeos e documentos.

Existem um questionamento quanto a segurança destes aplicativos. Em particular, no Brasil aconteceram vazamentos de mensagens que resultaram em escândalos políticos.

Uma das formas de se evitar que mensagens extraviadas sejam lidas é aplicando tecnicas de criptografia. A criptografia é um método de proteção e privacidade de dados muito importante e cada vez mais presente na nossa vida. Criptografia (em grego: kryptós, "escondido", e gráphein, "escrita") ou seja Escrita Escondida - funciona como códigos para assegurar a integridade da informação - Trata-se de um conjunto de regras que visa codificar a informação de forma que só o emissor e o receptor consiga decifrá-la. Sem a criptografia, qualquer pessoa poderia interceptar suas senhas e informações que trafegam por uma rede de computadores.

O que define o grau de segurança de uma criptografia é a quantidade de bits que são aplicados à codificação. Por exemplo, uma chave de 8 bits pode gerar até 256 combinações, já uma chave de 128 pode gerar mais de um trilhão de combinações.

Existem dois tipos de criptografia: a simétrica e a assimétrica. A criptografia simétrica é a mais comum, é quando uma mesma chave é utilizada para codificar e traduzir as mensagens - esse método é utilizado, por exemplo, no envio de emails. Já a criptografia assimétrica ou de ponta a ponta, é baseada em algoritmos que requerem duas chaves, uma delas é privada e a outra é pública. Mesmo sendo diferentes, as duas partes desse par de chaves são ligadas.

Em criptografia, a Cifra de César, também conhecida como cifra de troca, código de César ou troca de César, é uma das mais simples e conhecidas técnicas de criptografia. A origem é a seguinte: Júlio César, imperador romano de 100 a.C. a 44 a.C., utilizava um código para proteger as mensagens enviadas a seus generais. Assim, se a mensagem caísse em mãos inimigas, a informação não poderia ser compreendida. Cada letra do alfabeto era substituída pela letra três posições à frente, ou seja, o “A” era substituído pelo “D”, o “B” pelo “E”, o “C” pelo “F”, e assim sucessivamente. Qualquer código que tenha esse padrão é considerado uma Cifra de César, também conhecida como Código de César. A chave para cifrar/decifrar é exatamente a quantidade de posições que uma letra foi é trocada.

Atividade:

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

Para se proteger disto a empresa contratou você para desenvolver um chat interno privado apenas aos diretores da empresa contratante. O objetivo é criar um plataforma de envio de mensagens de texto – apenas mensagens de texto entre os diretores, durante o expediente de trabalho pela rede interna da empresa.

As mensagens enviadas deverão ser criptografadas com uma Cifra de César. A arquitetura do chat privado deverá seguir a forma:

- Um servidor central, será responsável por mediar a troca de mensagens entre cada uma das máquinas clientes.
- Cada máquina deverá enviar uma mensagem criptografada para o servidor e este deverá replicar as mensagens para os demais clientes. Sempre que uma mensagem for recebida pelo servidor esta deverá ser enviada para as demais máquina clientes conectadas ao servidor.
- Todas as mensagens deverão ser criptografas, antes do envio e descriptografadas antes da leitura, ou seja, a cifra/decifra ocorre nas máquinas clientes – o caminho feito até o servidor e depois para outros clientes é sempre com a mensagem criptografada.

Pontos a destacar:

O software será executado em terminais de linha de comando. Logo não é necessário a construção de uma interface gráfica, mas apenas de um menu interativo.

O software deverá funcionar em várias plataformas diferentes como Linux, Windows e IOS.

No fim deverão ser entregues ao cliente o software funcionando para testes bem como todos os códigos e diagramas desenvolvidos.