Descrição do Trabalho

1. A segurança é hoje um dos maiores desafios da Internet, senão o maior. A base das soluções de segurança é a criptografia. Existem, na verdade, 3 tipos de criptografia: *hash*, criptografia com chave pública e criptografia com chave secreta. Esta última é o tema do Trabalho Prático. A criptografia com chave secreta é usada para armazenar e transmitir informações sigilosas. Um algoritmo de criptografia de chave secreta recebe os dados originais como entrada e produz os dados criptografos como saída, que depois podem ser então descriptografos.
2. Um algoritmo de criptografia de chave secreta recebe também como entrada uma chave, usada tanto para criptografar como para descriptografar os dados. A chave, como o nome diz, deve ser *secreta*, apenas quem está autorizado a acessar os dados originais pode conhecer a chave. Para a transmissão de informações sigilosas em redes de computadores como a Internet surge um problema básico: como as partes que comunicam vão trocar a chave? Repare que a mesma chave secreta é usada para criptografar e descriptograr uma mensagem.
3. A solução para troca de chave secreta de Diffie-Hellman é muito clássica. Ela permite justamente isso: que duas partes se comuniquem para estabelecer uma chave secreta, sem nunca revelar a chave. Outros dados são comunicados, mas mesmo que toda a comunicação seja observada por uma parte não autorizada que tenta descobrir a chave, isso é computacionalmente inviável. Entre outros recursos disponíveis para estudarem, recomendo a página da Wikipedia a troca de chave de Diffie-Hellman.
4. Neste Trabalho Prático você deve implementar o estabelecimento de chave secreta de Diffie-Hellman, para em seguida utilizar a chave construída para fazer a comunicação sigilosa em cliente servidor. Assim o TP tem duas partes: (1) implementar um sistema cliente-servidor sobre TCP/IP para estabelecer a chave secreta com Diffie-Hellman, e (2) usar um algoritmo de criptografia com a chave secreta estabelecida. Atenção: o algoritmo e criptografia em si não deve ser implementado pela dupla, vcs devem usar um algoritmo como DES ou IDEA, investiguem o que está disponível nas bibliotecas da linguagem que vcs escolheram.
5. Devem ser apresentados logs para múltiplas execuções. Mostre também execuções em que se tenta descriptografar com a chave secreta errada.

Cada dupla pode fazer a implementação na linguagem que escolher, o professor sugere Python pela produtividade, mas são muito bem vindos trabalhos em C, C++, Java ou qualquer outra linguagem.

ENTREGA DO TRABALHO

Deve ser construída uma página Web, que contém em documentos HTML, os seguintes itens:

1. Relatório de como foi feito o trabalho e quais foram os resultados obtidos. Use desenhos, diagramas, figuras, todos os recursos que permitam ao professor compreender como a dupla estruturou o trabalho e quais resultados obteve. O

objetivo é o professor entender como a dupla fez o trabalho, como o trabalho funciona.

2. Código Fonte comentado. ATENÇÃO: acrescente a todo programa a terminação ".txt" para que possa ser diretamente aberto em um browser. Exemplos: cliente.py.txt ou servidor.c.txt
3. Logs de execução dos processos cliente/servidores, que demonstrem a execução correta destes processos. Os testes devem ser exaustivos até o ponto que demonstrem com clareza a funcionalidade correta do sistema.

Observações:

- Não serão aceitos trabalhos impressos, nem em meio ótico/magnético.
- Como neste semestre a turma não está grande, todos os trabalhos serão defendidos no laboratório, portanto certifique-se que seu trabalho funciona aqui.
- Pode ser usada qualquer linguagem de programação. A diversidade é bem vinda!