Engenharia de Segurança

Trabalho – Criptografia e Criptoanálise

Tamanho do grupo: 2
Data de entrega: 12/11

Descrição:
Escrever, na linguagem de programação de preferência do grupo, um algoritmo de criptografia permita codificar e decodificar uma mensagem de texto. O algoritmo pode ser simétrico ou assimétrico.

O grupo deverá criar uma mensagem cifrada com sua aplicação e rodar alguma ferramenta de criptoanálise (ex: GanzùA) sobre a mesma para ver se, ao menos por força bruta, a ferramenta consegue decifrar a mensagem.

Entrega:
Enviar via email para kalinka@icmc.usp.br com cópia para usp@paulogurgel.com.br até 12/11 às 23h59min:

1) **Código fonte documentado (compilável)**
2) **Relatório contendo as seguintes seções:**
   a) **Explicação do algoritmo, identificando a função da chave**
   b) **Estratégia sugerida para a troca de chave (se assimétrico)**
   c) **Instruções para compilação**
      i) **Deve conter a versão do compilador utilizado**
      ii) **No caso do uso de bibliotecas, especificar a fonte onde a mesma pode ser obtida e a versão utilizada**
   d) **Resultados da ferramenta de criptoanálise**

Importante: Não deve ser utilizada nenhuma biblioteca / framework / código disponível na internet sobre qualquer formato que faça a criptografia em si. Podem ser utilizadas bibliotecas livres para qualquer outra função (ex: fazer uma UI opcional, ou facilitar a leitura e escrita do arquivo)

Importante 2: Se o código fonte não compilar o trabalho não será considerado entregue!