UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Tarefa Prática – Criptografia assimétrica e autenticação com passkeys

Suponha que você está implementando a autenticação com *passkeys* entre um cliente e alguns servidores diferentes. O cliente deve conseguir se autenticar no servidor da sua escolha.

Você deve:

1. Desenvolver um programa que permite a um cliente gerar uma passkey para acessar um servidor.
2. O programa deve permitir ao cliente autenticar no servidor escolhido.
3. Usar o código do projeto testeOAEPRSA para ver como funciona o uso do RSA em Java. NÃO use o BaseRSAExample.java. USE APENAS o OAEPPaddedRSAExample.java como base para usar o RSA.
4. Use o keystore Java para armazenar as chaves privadas (*passkeys*) no lado do cliente. Olhe o código disponível nos exemplos. O keystore Java é um arquivo especial Java para armazenar chaves. Tem keystore em outras linguagens também. Caso não tenha, deve ser usada criptografia autenticada para cifrar o arquivo que guardará as *passkeys* do cliente. No lado do servidor deve ser guardado o certificado digital.

Exemplo de fluxo entre cliente e servidor usando passkey está representado na Figura 1.

Figura 1 – Autenticação com passkey

Fonte: https://www.delasign.com/blog/passkey-authentication/

Para entregar/apresentar:

A. O código fonte deve ser postado no moodle, juntamente com um tutorial de execução da aplicação. Deve ser possível executar a aplicação com os arquivos anexados dentro do código.

B. Apresentação desta questão será feita de maneira presencial ou online via Google Meet. Todos os membros da equipe devem apresentar para receber nota.

A apresentação deve ser agendada para 2ª feira, 3ª feira ou 4ª feira da semana seguinte à entrega do trabalho (períodos da tarde e noite).

Avisos:

**** Se tiver cópias de código, todos os envolvidos receberão nota zero nesta tarefa.**