UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO - UFERSA
Departamento de Computação - DC
Graduação em Ciência da Computação
Disciplina: Segurança Computacional
Prof.: Paulo Henrique Lopes Silva

Prática offline 1 - Unidade 2

1. Descrição geral

O objetivo do projeto é o desenvolvimento de um sistema que utilize uma cifra clássica (exceto a cifra de César) e a cifra simétrica AES para garantir a confidencialidade das comunicações entre emissores (cliente de um banco) e receptores (banco ou agência virtual).

2. *User Stories*

User Stories são uma forma de expressar requisitos funcionais desejados para o sistema (o que o sistema deve fazer). Elas focam nos objetivos dos usuários e como eles conseguem alcançá-los. *User stories* devem ser curtas, simples e escritas sob o ponto de vista do usuário. Observe que, no mundo real, o cliente poderá mudar de ideia com respeito a esses requisitos funcionais.

User Story	**Título**	**Descrição**
1.	Autenticação de usuários	Clientes do banco devem acessar o sistema por meio de autenticação usando o número da conta e a senha.
2.	Criar conta corrente	Cada conta possui, no mínimo, atributos como: cpf, nome do cliente, endereço e telefone.
3.	Saque	Cada cliente pode sacar algum valor de sua conta, desde que a mesma não esteja vazia.
4.	Depósito	Cada cliente pode depositar algum valor na sua conta.
5.	Transferência	Clientes podem transferir valores entre contas (correntes) do banco.
6.	Saldo	Retorna o valor corrente contido na conta.
7.	Investimentos	**Poupança (criada automaticamente na criação da conta corrente):** rende 0,5% ao mês. **Renda fixa (o correntista escolhe investir na renda fixa):** rende 1,5% ao mês. Cada investimento deve ter uma tela única que mostrará o valor aplicado e uma simulação de rendimento para três, seis e doze meses.
8.	Autenticação de mensagens	O sistema bancário garante a autenticidade e integridade de mensagens enviadas por clientes legítimos.

3. Detalhamento dos requisitos da simulação.

- A distribuição da chave simétrica entre as entidades, tanto para a encriptação quanto para a autenticação de mensagens, pode ser feita manualmente ou usando um servidor auxiliar somente com a função de gerar e distribuir as chaves.
- O banco deve garantir que todas as comunicações com clientes (ida e volta) sejam criptografadas usando a cifra simétrica clássica e o AES e codificadas em Base64.

- Três contas devem estar criadas no início do programa.
- Todas as "*user stories"* devem ser testadas.
- Sobre a autenticação de mensagens, simule um cliente sendo um atacante e tentando enviar mensagens ao banco. Todas as mensagens que não puderem ser autenticadas, devem ser descartadas.

4. Observações.

- O prazo para a entrega dos projetos expira em 06/03/2024 às 23:59h, via SIGAA. Portanto, certifiquem-se do arquivo que vão enviar.
- Avaliação: o projeto vale 50% da nota da 2ª unidade.
    - O código do projeto deve ser enviado pelo Sigaa.
    - Um vídeo com a apresentação do projeto deve ser gravado (as instruções para a gravação estão no roteiro). Perguntas podem ser feitas, após a correção pelo vídeo
    - O link do vídeo deve ser enviado pelo Discord.
- Para os que enviarem por e-mail, depois do prazo, o projeto valerá 20% a menos.
- O projeto é individual.
- Utilize preferencialmente a linguagem Java para o desenvolvimento do trabalho.
    - Os projetos podem utilizar *threads* e *sockets* TCP e UDP.
- Sabe-se que a estrutura de projetos dessa natureza pode ser muito comum. No entanto, a lógica de funcionamento, o armazenamento e a visualização das informações da loja podem ser bem particulares. Cuidado com códigos iguais. A penalidade é a nota ZERO.