TP4 - Criptografia

Iniciar tarefa

- Vencimento Segunda-feira por 23:59
- Pontos 4
- Enviando um URL de site ou um upload de arquivo
- Tipos de arquivo zip
- Disponível até 24 jun em 23:59

Para concluirmos o nosso projeto, vocês devem, agora, criar alguma função criptográfica para cifrar os dados das entidades. Isso deve ser feito nos métodos `toByteArray()` e `fromByteArray()` das classes das suas entidades.

Por exemplo, considere uma entidade `Usuario` que contém o seguinte método `toByteArray()`:

```
public byte[] toByteArray() throws Exception {
  ByteArrayOutputStream baos = new ByteArrayOutputStream();
  DataOutputStream dos = new DataOutputStream(baos);
  dos.writeInt(this.idUsuario);
  dos.writeUTF(this.nome);
  dos.writeUTF(this.email);
  dos.writeInt(this.hashsenha);
  byte[] dados = baos.toByteArray();
  byte[] dadosCifrados = cifrar(dados, chave);
  return dadosCifrados;
  }
```

Veja que, ao invés de retornarmos diretamente os dados do vetor criado, retornos os dados após a passagem por um processo de cifragem. E é aqui que você vai trabalhar: na implementação desse método `cifrar()`. Da mesma forma, você deve implementar um método `decifrar()` no método `fromByteArray()`.

Mas, atenção:

- Seu processo de cifragem e decifragem deve ter 2 etapas, isto é, deve **embaralhar os dados de 2 formas diferentes**, uma baseada na substituição e outra baseada na transposição.
- Você não pode usar classes prontas de criptografia. A implementação deve ser sua.
- Você deve usar uma única chave no processo de cifragem e decifragem. Armazene essa chave no código ou em um arquivo anexo (que, em situação real, não ficaria em uma pasta pública).

O QUE VOCÊ DEVE FAZER

Neste TP, você deve implementar uma função de cifragem e uma função de decifragem para os vetores de bytes de cada entidade. Essas funções devem envolver duas operações diferentes para embaralhamento dos dados, uma usando uma técnica de substituição e a outra usando uma técnica de transposição, ambas considerando uma única chave criptográfica.

Todas as suas entidades devem usar a criptografia.

RELATÓRIO

O projeto do seu grupo deve ter necessariamente um relatório em um arquivo readme.md corretamente formatado com Markdown. Nesse relatório, vocês devem descrever cada rotina (classe, método, função, ...) implementada, como se estivessem apresentando o código do seu projeto, isto é, explicando cada coisa que seu grupo implementou. **Coloquem os nomes dos componentes do grupo no relatório.**

Em seguida, relatem um pouco a experiência do grupo, explicando questões como: Vocês implementaram todos os requisitos? Houve alguma operação mais difícil? Vocês enfrentaram algum desafio na implementação? Os resultados foram alcançados? ... A ideia, portanto, é relatar como foi a experiência de desenvolvimento do TP. Aqui, a ideia é entender como foi para vocês desenvolver este TP.

No relatório, descrevam cada uma das operações usadas nas funções de cifragem e de decifragem, explicando como elas embaralham os dados e como usam a chave criptográfica.

Finalmente, vocês devem, necessariamente, responder ao seguinte *checklist* (copiem as perguntas abaixo para o seu relatório e responda sim/não em frente a elas). Ao responderem esse questionário, vocês estão me dizendo o que fizeram ou não fizeram.

- Há uma função de cifragem em todas as classes de entidades, envolvendo pelo menos duas operações diferentes e usando uma chave criptográfica?
- Uma das operações de cifragem é baseada na substituição e a outra na transposição?
- O trabalho está funcionando corretamente?
- O trabalho está completo?
- O trabalho é original e não a cópia de um trabalho de um colega?

Lembre-se de que, para essa atividade, eu avaliarei tanto o esforço quanto o resultado. Portanto, escreva o relatório de forma que me ajude a observar o resultado.

FORMA DE ENTREGA

Vocês devem postar o seu trabalho no GitHub e enviar apenas o URL do projeto. O relatório deve estar nesse mesmo repositório. Não se esqueçam de colocar comentários em todo o código que criarem. **Se o repositório de vocês for de vários trabalhos e não apenas deste TP, anexe o código respondente ao TP em um arquivo ZIP (e não ARJ, RAR, ...) no formulário de entrega.**

AVALIAÇÃO

Essa atividade vale 4 pontos. A avaliação será feita por meio do relatório. Dessa forma, um relatório incompleto ou ausente impactará na perda significativa de pontos na avaliação do projeto.

Atenção: Trabalhos copiados de colegas, que não evidenciem um esforço mínimo do próprio aluno, serão anulados.

Se tiver dúvidas sobre o trabalho a fazer, me avise. Não deixe de observar que o URL com o código no GitHub deve ser entregue até o dia especificado na atividade.