Criptografia em Java: Simétrica, Assimétrica e Hash (Trabalho Prático)

Este projeto demonstra três tipos de algoritmos de criptografia em Java:
1. Criptografia Simétrica (AES) – usa uma única chave para cifrar e decifrar.
2. Criptografia Assimétrica (RSA) – usa um par de chaves (pública e privada).
3. Função Hash (SHA-256) – gera um resumo único e irreversível da mensagem.

Código completo:

```
import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.MessageDigest;
import java.util.Base64;

public class Cripto_Implementacoes {

    public static void main(String[] args) {
        try {
            String textoOriginal = "Mensagem secreta";

            // ---------- Criptografia Simétrica (AES) ----------
            KeyGenerator geradorAES = KeyGenerator.getInstance("AES");
            geradorAES.init(128);
            SecretKey chaveAES = geradorAES.generateKey();

            Cipher cifraAES = Cipher.getInstance("AES");
            cifraAES.init(Cipher.ENCRYPT_MODE, chaveAES);
            byte[] textoCriptografadoAES = cifraAES.doFinal(textoOriginal.getBytes());
            String textoCifradoBase64 = Base64.getEncoder().encodeToString(textoCriptografadoAES);

            cifraAES.init(Cipher.DECRYPT_MODE, chaveAES);
            byte[] textoDecifradoAES = cifraAES.doFinal(Base64.getDecoder().decode(textoCifradoBase64

            System.out.println("=== Criptografia Simétrica (AES) ===");
            System.out.println("Texto original: " + textoOriginal);
            System.out.println("Texto cifrado: " + textoCifradoBase64);
            System.out.println("Texto decifrado: " + new String(textoDecifradoAES));

            // ---------- Criptografia Assimétrica (RSA) ----------
            KeyPairGenerator geradorRSA = KeyPairGenerator.getInstance("RSA");
            geradorRSA.initialize(2048);
            KeyPair parChaves = geradorRSA.generateKeyPair();

            Cipher cifraRSA = Cipher.getInstance("RSA");
            cifraRSA.init(Cipher.ENCRYPT_MODE, parChaves.getPublic());
            byte[] textoCriptografadoRSA = cifraRSA.doFinal(textoOriginal.getBytes());
            String textoCifradoRSA = Base64.getEncoder().encodeToString(textoCriptografadoRSA);

            cifraRSA.init(Cipher.DECRYPT_MODE, parChaves.getPrivate());
            byte[] textoDecifradoRSA = cifraRSA.doFinal(Base64.getDecoder().decode(textoCifradoRSA))

            System.out.println("\n=== Criptografia Assimétrica (RSA) ===");
            System.out.println("Texto original: " + textoOriginal);
            System.out.println("Texto cifrado: " + textoCifradoRSA);
            System.out.println("Texto decifrado: " + new String(textoDecifradoRSA));

            // ---------- Função Hash (SHA-256) ----------
            MessageDigest md = MessageDigest.getInstance("SHA-256");
            byte[] hash = md.digest(textoOriginal.getBytes());

            StringBuilder hex = new StringBuilder();
            for (byte b : hash) {
                hex.append(String.format("%02x", b));
            }
            System.out.println("\n=== Função Hash (SHA-256) ===");
```

```
            System.out.println("Texto original: " + textoOriginal);
            System.out.println("Hash gerado: " + hex.toString());

        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Instruções de uso:

1. Abra o BlueJ ou qualquer editor Java.
2. Crie um novo projeto e adicione este arquivo com o nome Cripto_Implementacoes.java.
3. Compile e execute o programa.
4. O terminal mostrará o texto original, cifrado, decifrado e o hash gerado.