ESCOLA POLITÉNICA DA UNIVERSIDADE DE SÃO PAULO

Exercício prático
PCS
Segurança

Aluno: Rafael Camargo Leite – 7629953

Índice

1. *Introdução*

Para a implementação do exercício foram utilizadas as bibliotecas da oracle - javax.crypto

2. *Hmac*

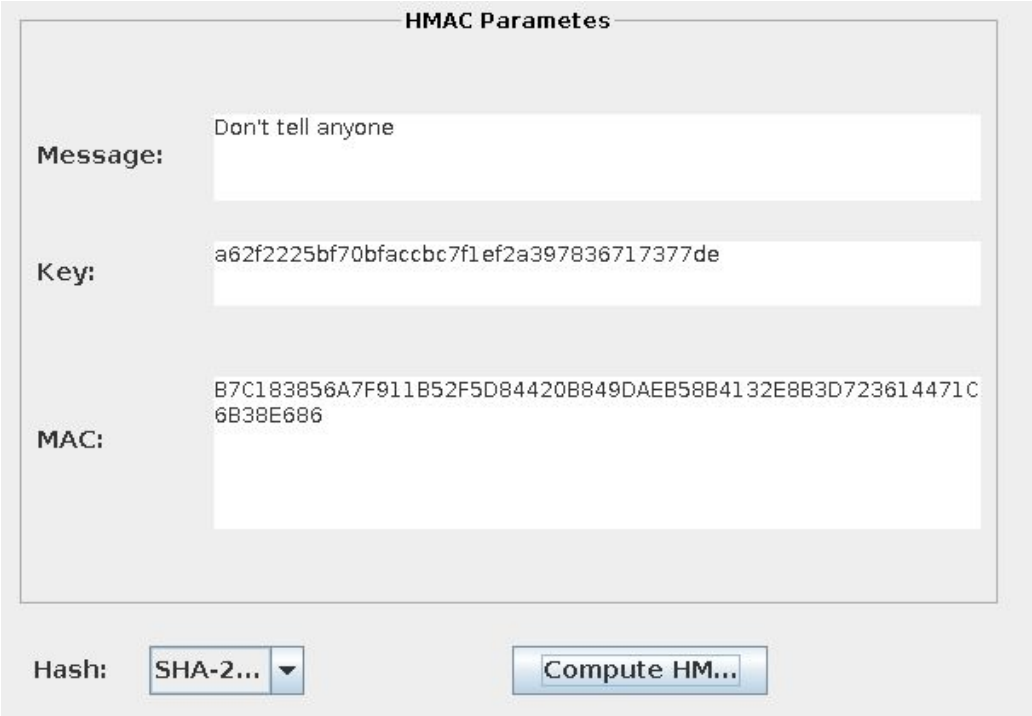

Figura 1 - HMAC usando SHA-256

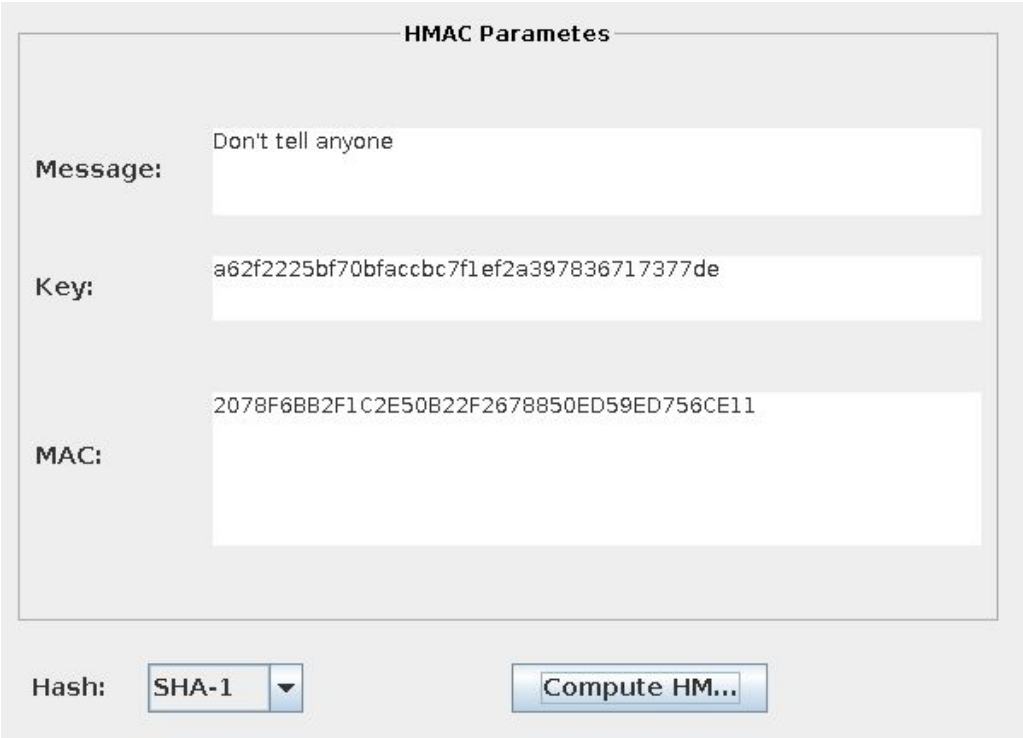

Figura 2 - HMAC usando SHA-1

3. *DSA Signature*

Para o DSA usei a interface antiga pois já havia acabado o EP quando a nova foi desenvolvida e eu havia alterado a interface para mostrar o resultado da verificação em um textBox. Por esse motivo, as chaves que usei estão dispostas na pasta raiz do projeto com os nome:

1. Private Key =generated_DES_rk
2. Public Key =generated_DES_uk

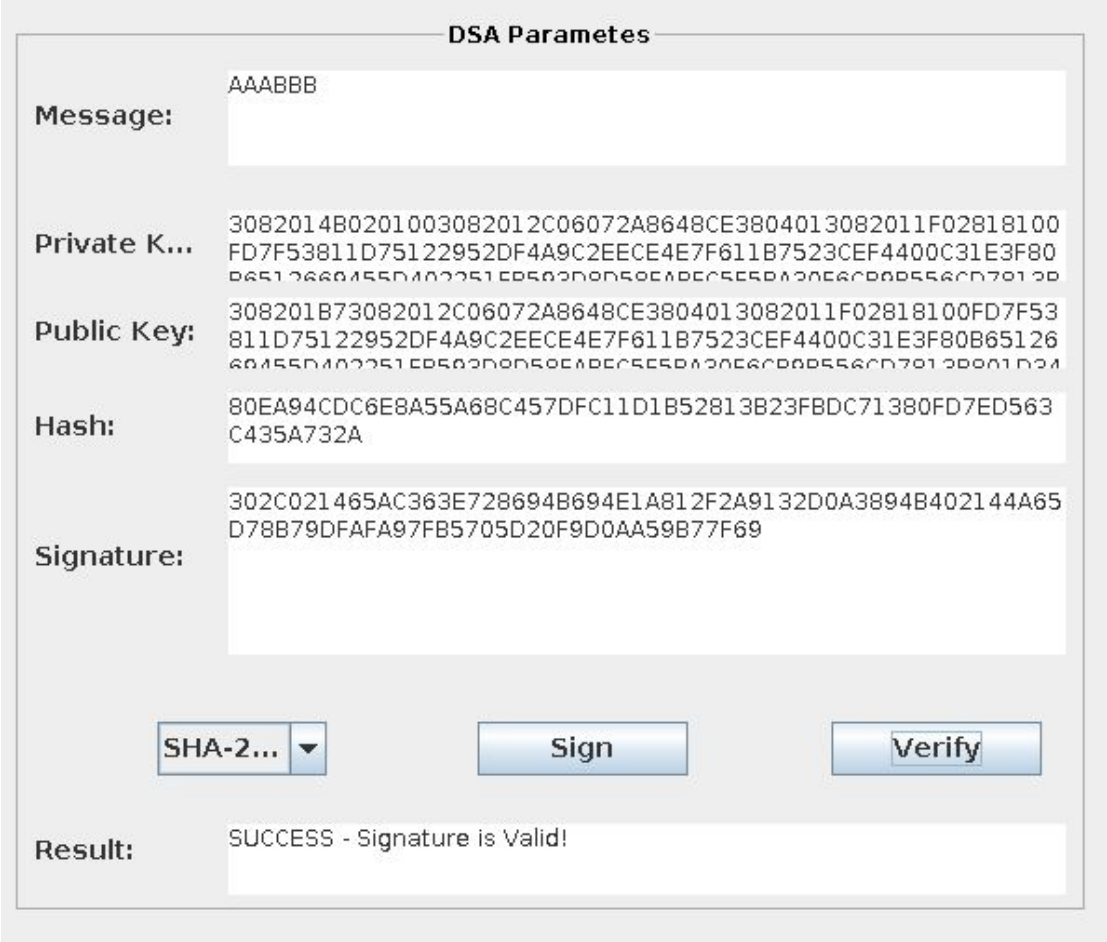

Figura 3 - DSA usando SHA-256

Pela Figura 3, pode-se observar que a assinatura foi verificada com sucesso.

Nas figuras 4 e 5 pode-se observar o DSA usando SHA-1. A primeira delas mostra que a assinatura foi verificada corretamente. Na segunda, alterei o último digito da assinatura. Com isso, percebe-se que a verificação falha.

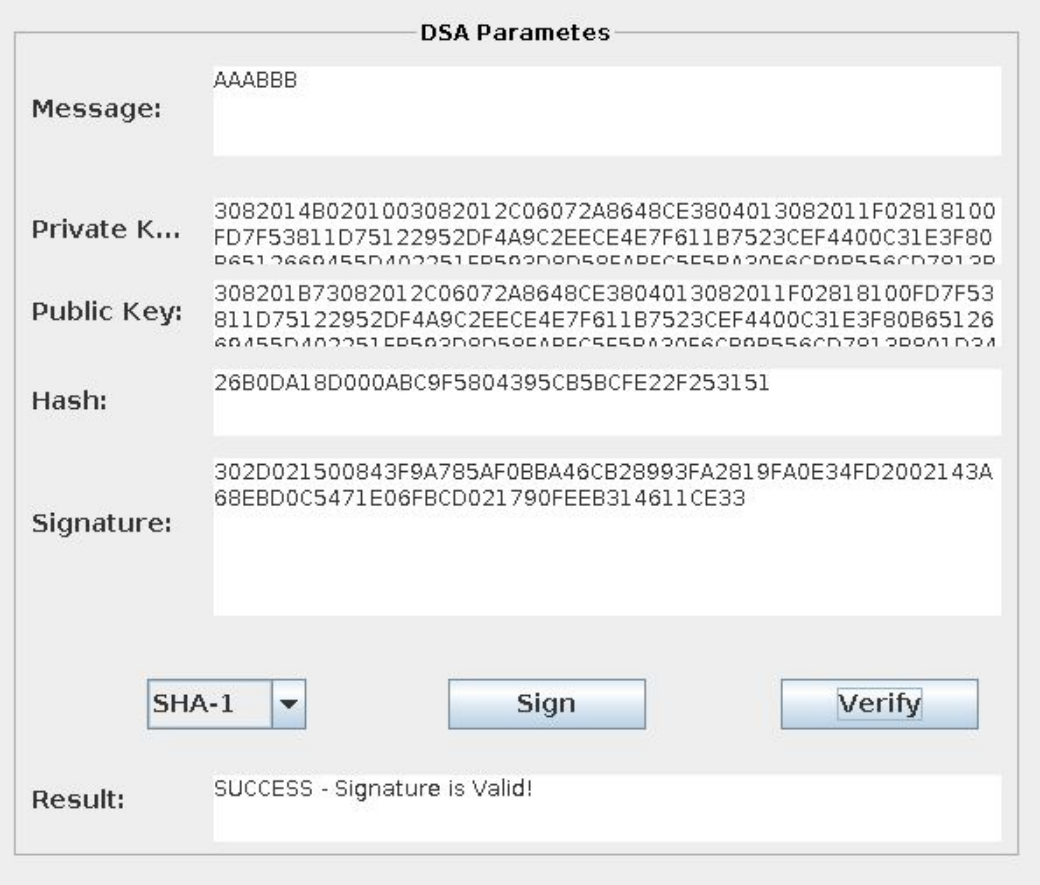

Figura 4 - DSA usando SHA-1

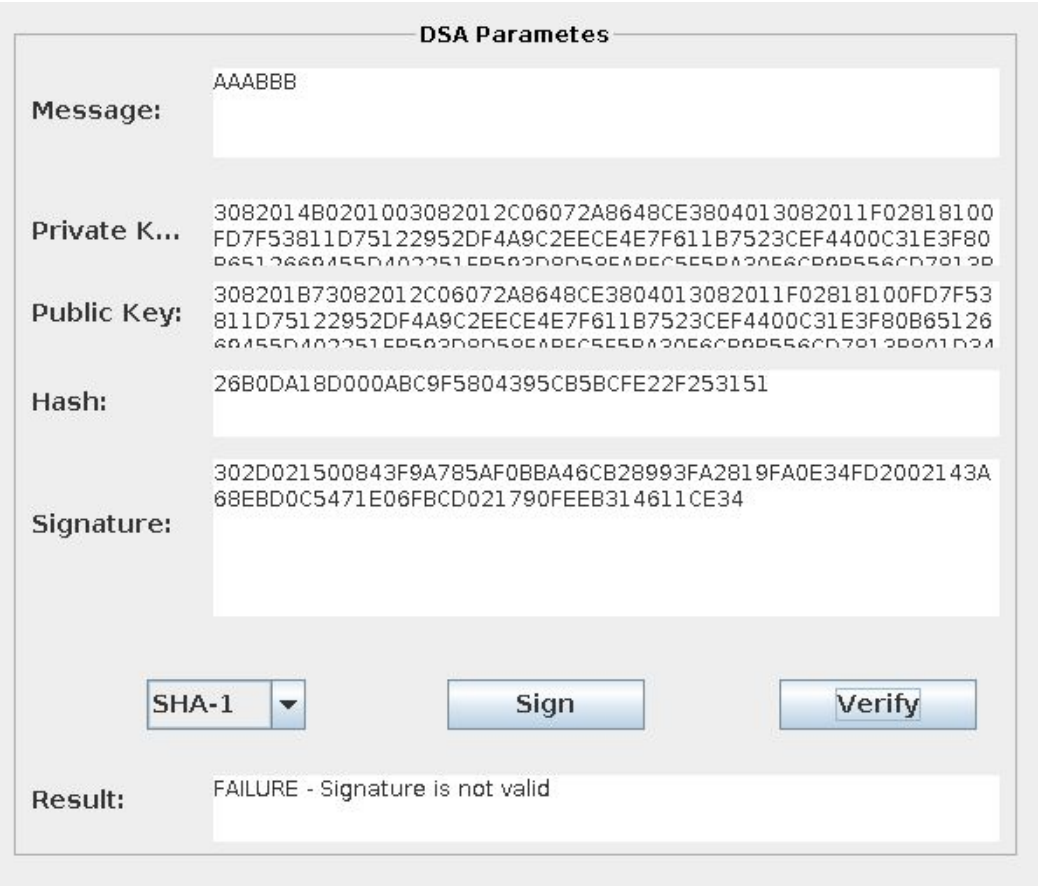

Figura 5 - DSA usando SHA-1 - Falha na verificação

4. RSA

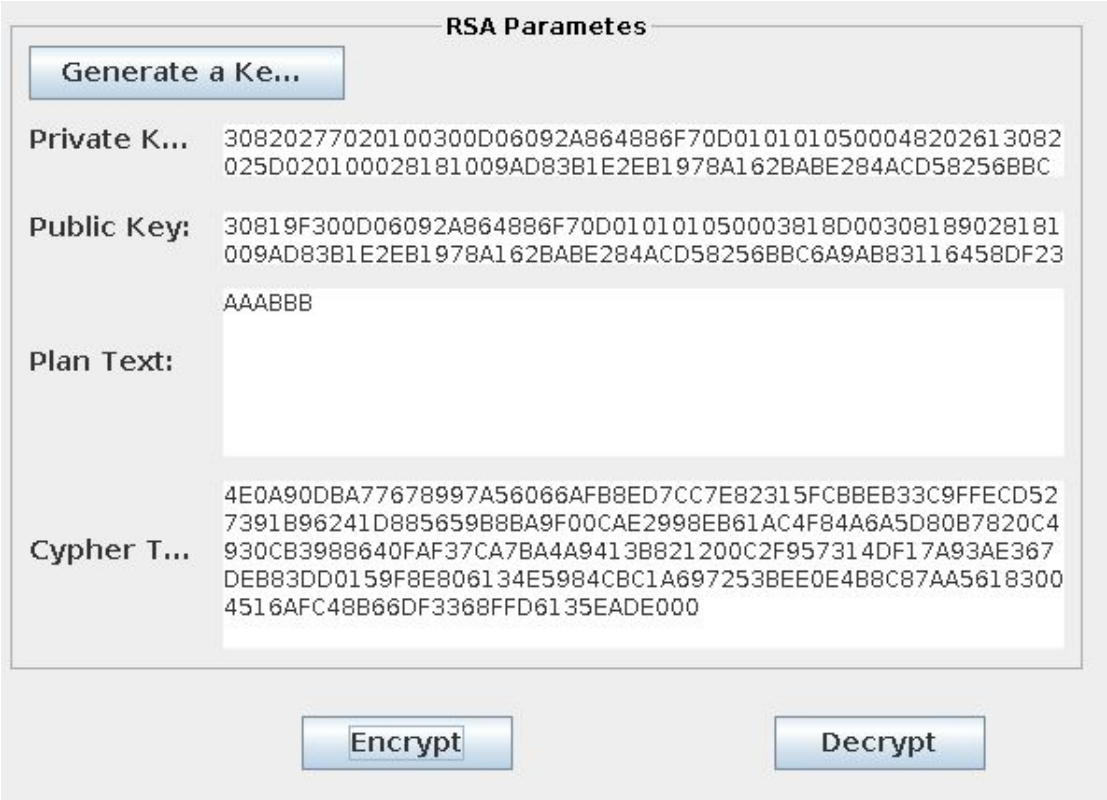

Figura 6 - RSA encrypt

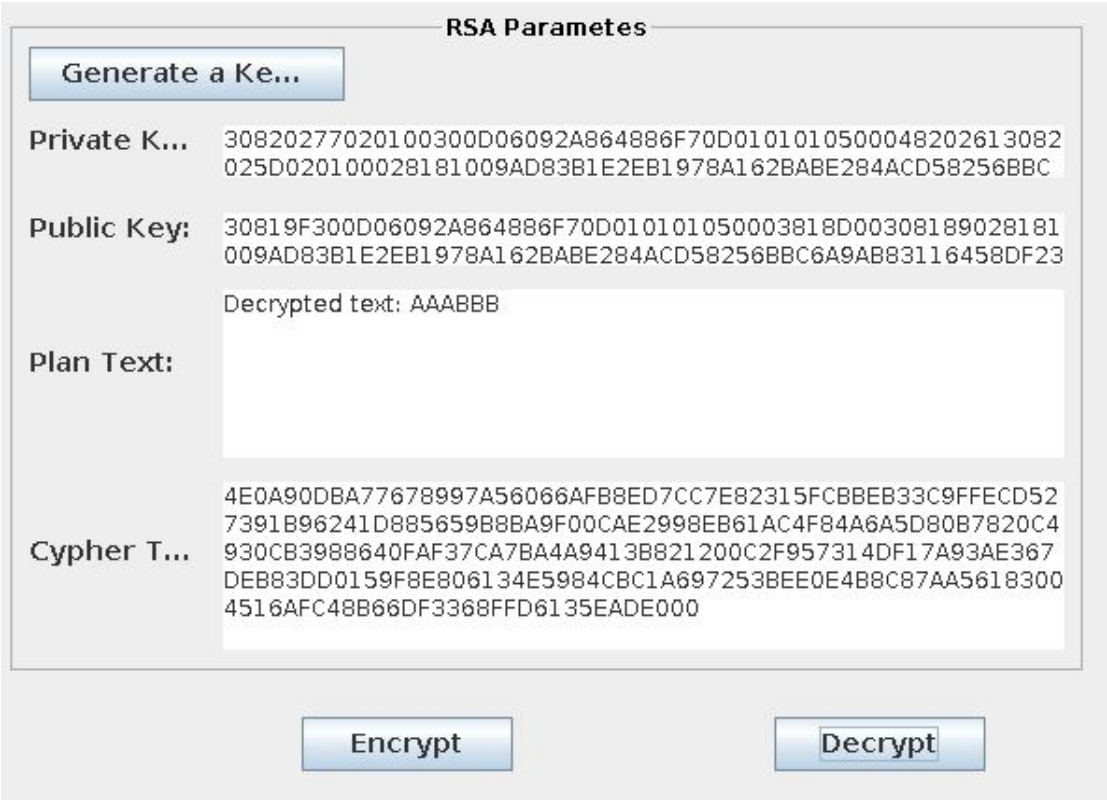

Figura 7 - RSA decrypt

5. AES

a. ECB

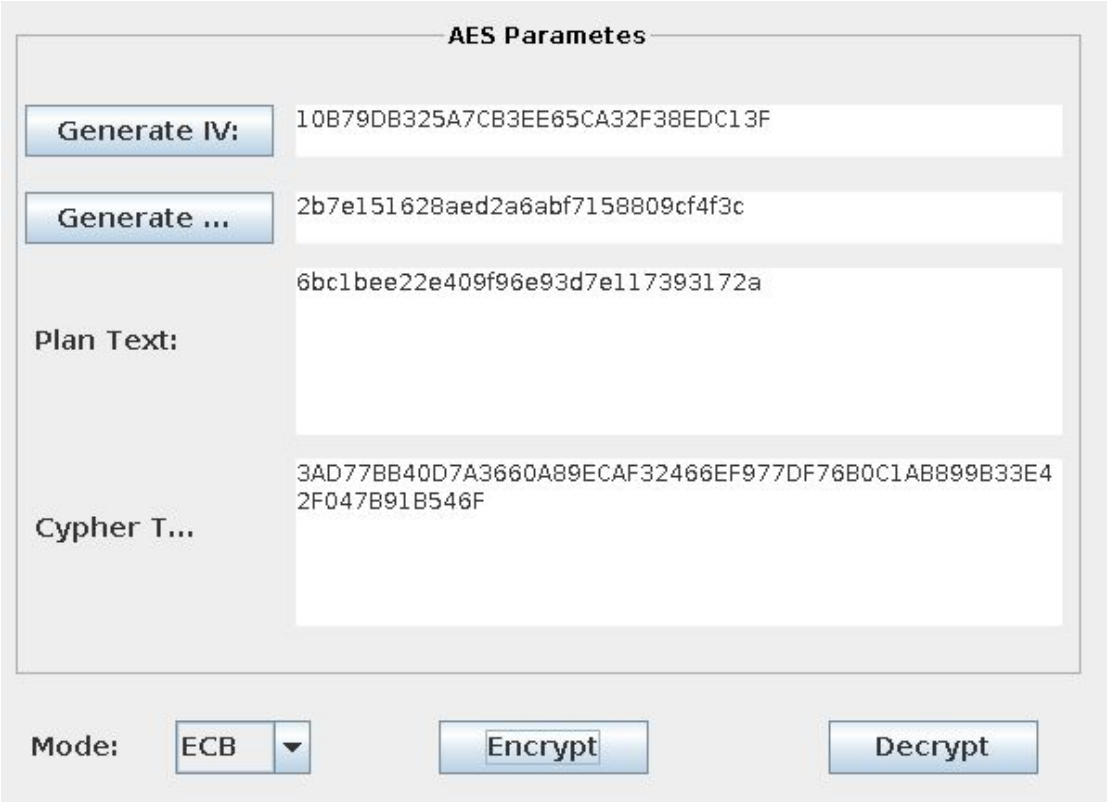

Figura 8 - AES encrypt usando modo ECB

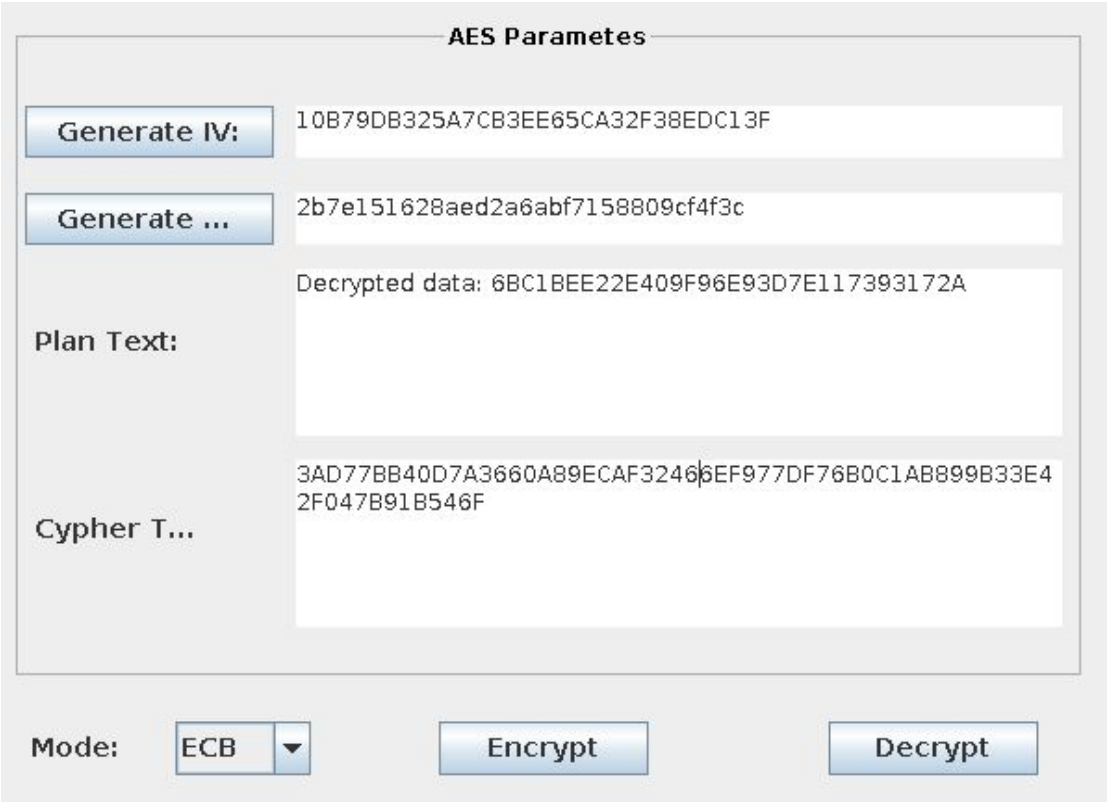

FIgura 9 - AES decrypt usando modo ECB

b. CBC

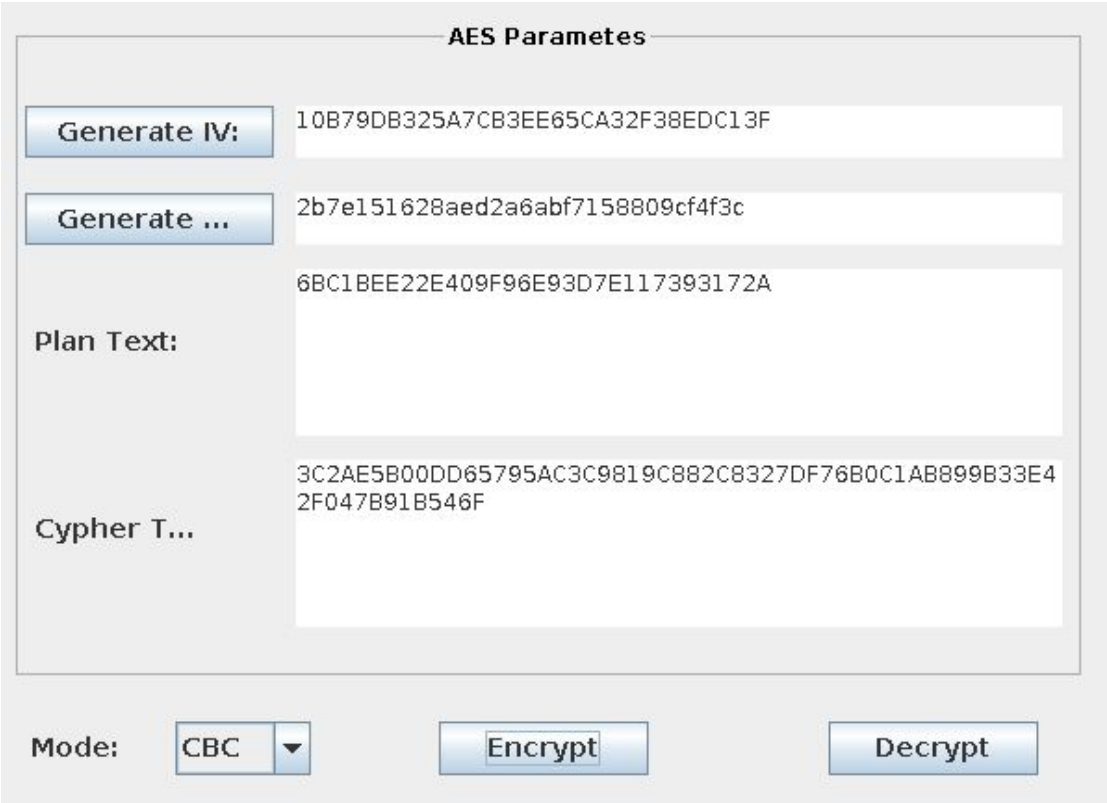

Figura 10 - AES encrypt usando modo CBC

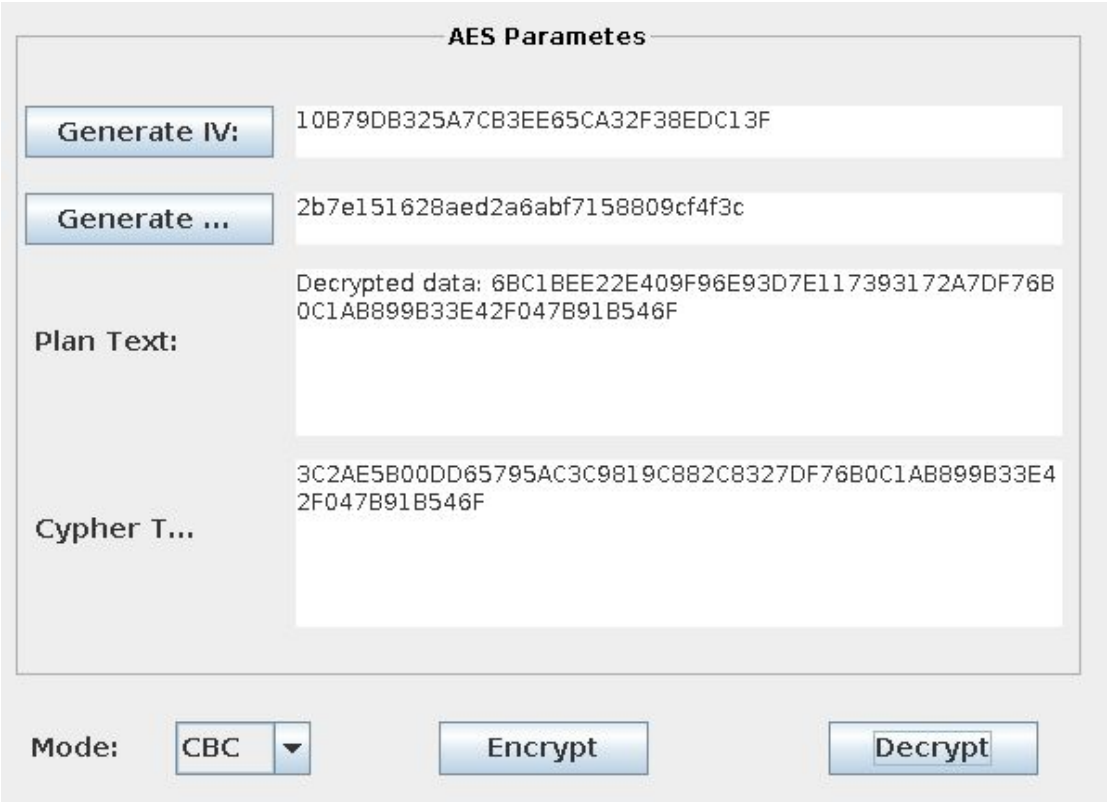

Figura 11 - AES decrypt usando modo CBC

C. CTR

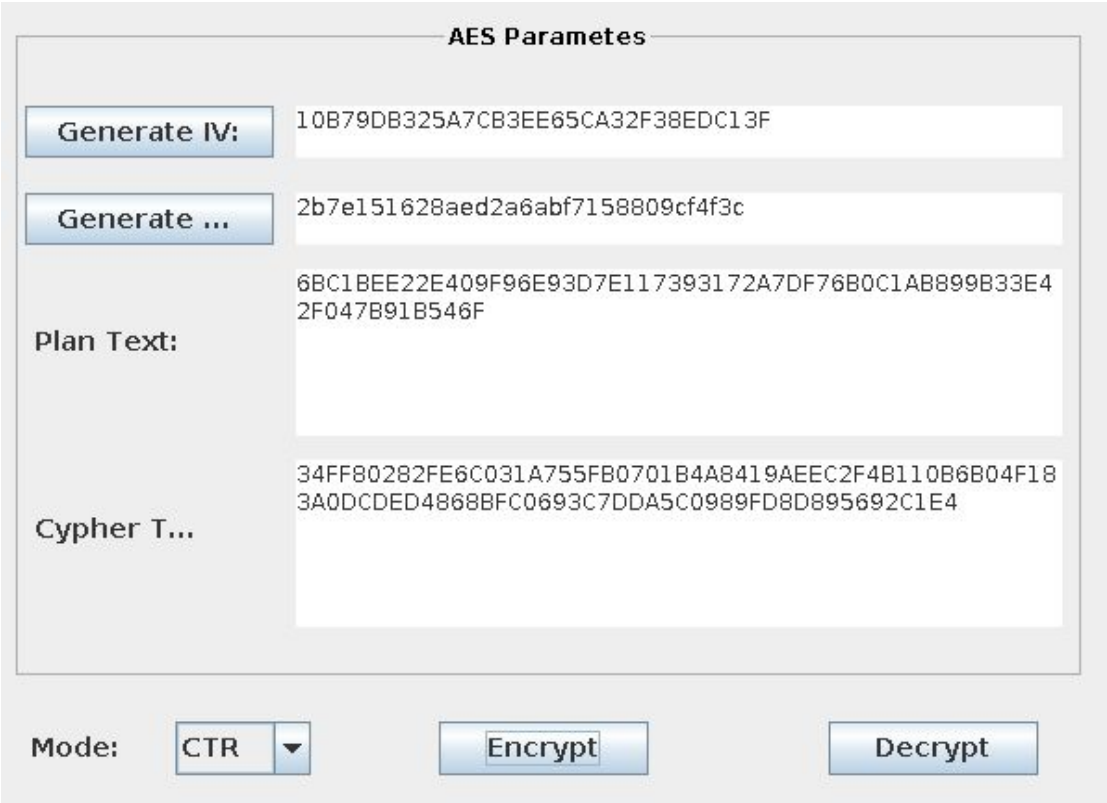

Figura 12 - AES encrypt usando modo CTR

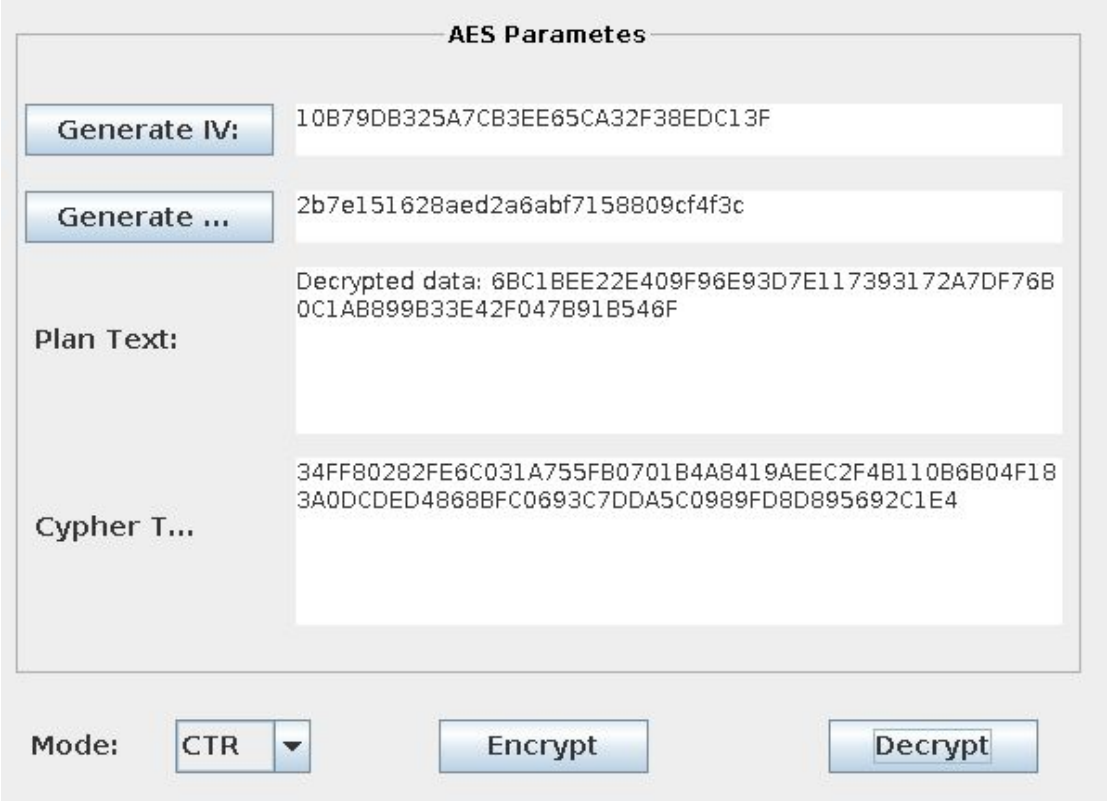

Figura 13 - AES decrypt usando modo CTR

6. *Referências*

a. *HMAC*

- http://docs.oracle.com/javase/7/docs/api/javax/crypto/Mac.html
- http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/AuthJavaSampleHMACSignature.html

b. *DSA*

- https://docs.oracle.com/javase/tutorial/security/apisign/step3.html

c. *RSA*

- https://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf
- https://javadigest.wordpress.com/2012/08/26/rsa-encryption-example/
- http://www.java2s.com/Tutorial/Java/0490__Security/BasicRSAexample.htm

d. *AES*

- http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
- https://github.com/golang/go/blob/master/src/crypto/aes/
- http://www.larc.usp.br/~pbarreto/
- https://n3vrax.wordpress.com/2011/08/14/aesrijndael-java-implementation/