

**ESCOLA POLITÉCNICA DA
UNIVERSIDADE DE SÃO PAULO**



**Exercício prático
PCS
Segurança**

Aluno: Rafael Camargo Leite – 7629953

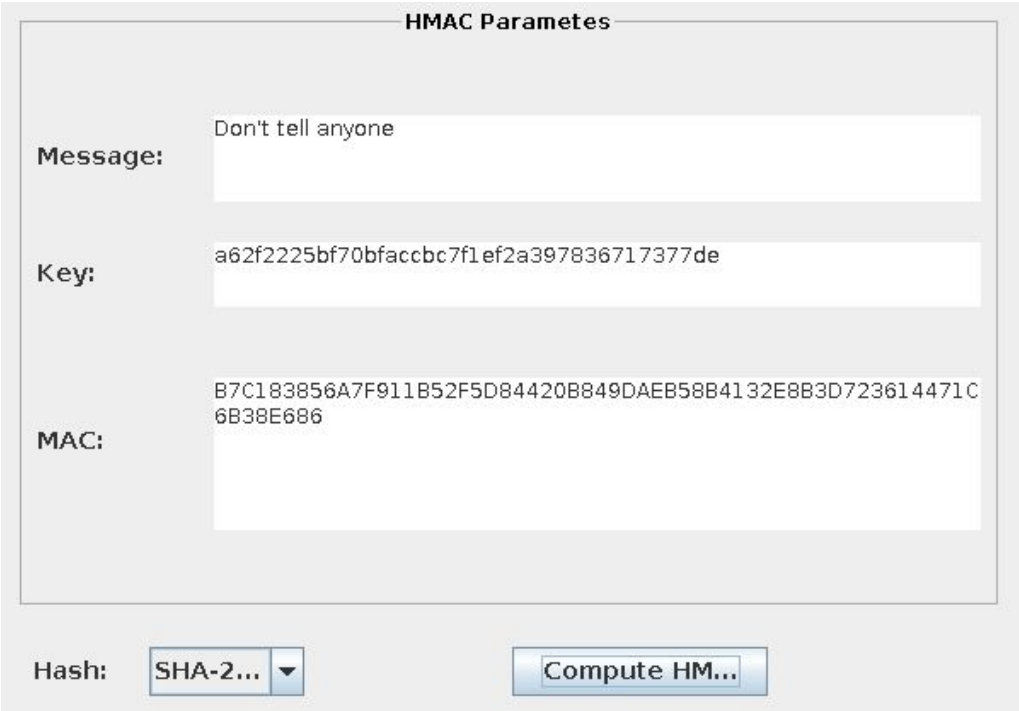
Índice

1. Introdução
2. HMAC
3. DSA
4. RSA
5. AES
6. Referências

1. Introdução

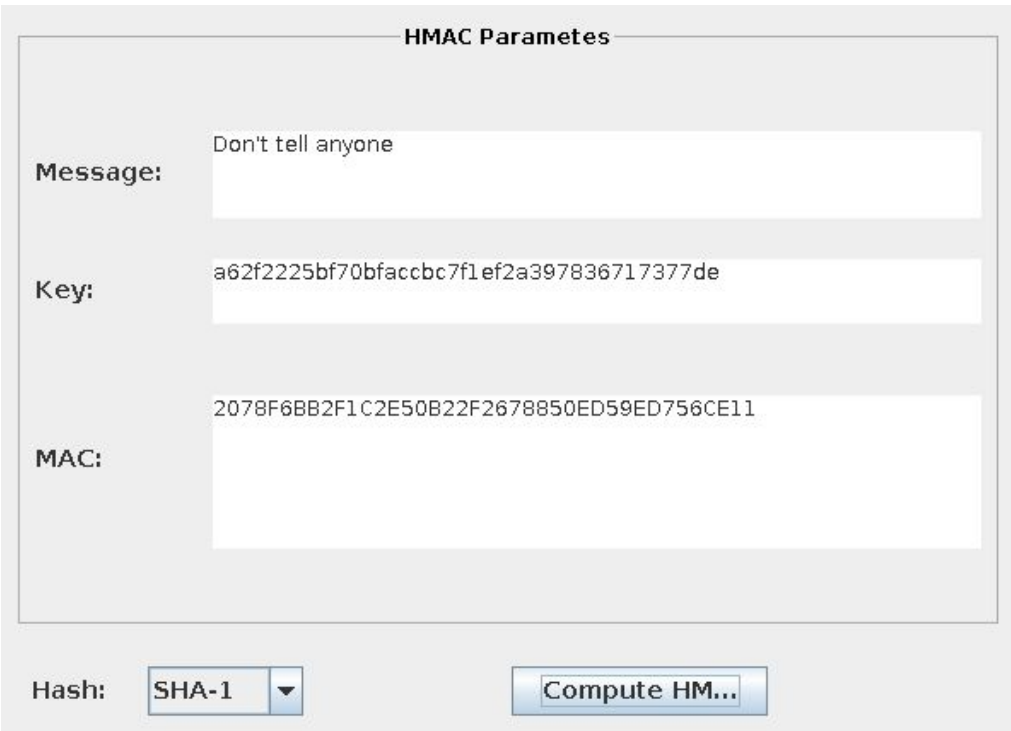
Para a implementação do exercício foram utilizadas as bibliotecas da oracle - javax.crypto

2. Hmac



The screenshot shows a window titled "HMAC Parametes" (note the typo). It contains three text input fields: "Message:" with the text "Don't tell anyone", "Key:" with the text "a62f2225bf70bfaccbc7f1ef2a397836717377de", and "MAC:" with the text "B7C183856A7F911B52F5D84420B849DAEB58B4132E8B3D723614471C6B38E686". Below the fields, there is a "Hash:" label followed by a dropdown menu showing "SHA-2..." and a "Compute HM..." button.

Figura 1 - HMAC usando SHA-256



The screenshot shows a window titled "HMAC Parametes" (note the typo). It contains three text input fields: "Message:" with the text "Don't tell anyone", "Key:" with the text "a62f2225bf70bfaccbc7f1ef2a397836717377de", and "MAC:" with the text "2078F6BB2F1C2E50B22F2678850ED59ED756CE11". Below the fields, there is a "Hash:" label followed by a dropdown menu showing "SHA-1" and a "Compute HM..." button.

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

The screenshot shows a window titled "DSA Parametes" (note the typo). It contains several text boxes and buttons. The "Message:" box contains "AAABBB". The "Private K..." box contains a long hexadecimal string. The "Public Key:" box contains another long hexadecimal string. The "Hash:" box contains a hexadecimal string. The "Signature:" box contains a long hexadecimal string. Below these boxes are three buttons: "SHA-2..." with a dropdown arrow, "Sign", and "Verify". At the bottom, the "Result:" box displays "SUCCESS - Signature is Valid!".

Field	Value
Message:	AAABBB
Private K...	3082014B0201003082012C06072A8648CE3804013082011F02818100FD7F53811D75122952DF4A9C2EECE4E7F611B7523CEF4400C31E3F80D6512660A55D402251ED502D0D50EABEC5E5DA20E6CB0D556CD7012B
Public Key:	308201B73082012C06072A8648CE3804013082011F02818100FD7F53811D75122952DF4A9C2EECE4E7F611B7523CEF4400C31E3F80B6512660A55D402251ED502D0D50EABEC5E5DA20E6CB0D556CD7012B001D24
Hash:	80EA94CDC6E8A55A68C457DFC11D1B52813B23FBDC71380FD7ED563C435A732A
Signature:	302C021465AC363E728694B694E1A812F2A9132D0A3894B402144A65D78B79DFAFA97FB5705D20F9D0AA59B77F69
Result:	SUCCESS - Signature is Valid!

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 dígito da assinatura. Com isso, percebe-se que a verificação falha.

DSA Parametes

Message:	AAABBB
Private K...	3082014B0201003082012C06072A8648CE3804013082011F02818100 FD7F53811D75122952DF4A9C2EECE4E7F611B7523CEF4400C31E3F80 B651266B455D402751ED5B2D0D50EADFC5E5DA20E6CD0D556CD7012D
Public Key:	308201B73082012C06072A8648CE3804013082011F02818100FD7F53 811D75122952DF4A9C2EECE4E7F611B7523CEF4400C31E3F80B65126 6B455D402751ED5B2D0D50EADFC5E5DA20E6CD0D556CD7012D001D24
Hash:	26B0DA18D000ABC9F5804395CB5BCFE22F253151
Signature:	302D021500843F9A785AF0BBA46CB28993FA2819FA0E34FD2002143A 68EBD0C5471E06FBCD021790FEEB314611CE33

SHA-1 ▼

Sign

Verify

Result:

SUCCESS - Signature is Valid!

Figura 4 - DSA usando SHA-1

DSA Parametes

Message:	AAABBB
Private K...	3082014B0201003082012C06072A8648CE3804013082011F02818100 FD7F53811D75122952DF4A9C2EECE4E7F611B7523CEF4400C31E3F80 B651266B455D402751ED5B2D0D50EADFC5E5DA20E6CD0D556CD7012D
Public Key:	308201B73082012C06072A8648CE3804013082011F02818100FD7F53 811D75122952DF4A9C2EECE4E7F611B7523CEF4400C31E3F80B65126 6B455D402751ED5B2D0D50EADFC5E5DA20E6CD0D556CD7012D001D24
Hash:	26B0DA18D000ABC9F5804395CB5BCFE22F253151
Signature:	302D021500843F9A785AF0BBA46CB28993FA2819FA0E34FD2002143A 68EBD0C5471E06FBCD021790FEEB314611CE34

SHA-1 ▼

Sign

Verify

Result:

FAILURE - Signature is not valid

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

4. RSA

RSA Parametes

Generate a Ke...

Private K...

30820277020100300D06092A864886F70D0101010500048202613082025D020100028181009AD83B1E2EB1978A162BABE284ACD58256BBC

Public Key:

30819F300D06092A864886F70D010101050003818D00308189028181009AD83B1E2EB1978A162BABE284ACD58256BBC6A9AB83116458DF23AAABBB

Plan Text:

Cypher T...

4E0A90DBA77678997A56066AFB8ED7CC7E82315FCBBEB33C9FFECD527391B96241D885659B8BA9F00CAE2998EB61AC4F84A6A5D80B7820C4930CB3988640FAF37CA7BA4A9413B821200C2F957314DF17A93AE367DEB83DD0159F8E806134E5984CBC1A697253BEE0E4B8C87AA56183004516AFC48B66DF3368FFD6135EADE000

Encrypt

Decrypt

Figura 6 - RSA encrypt

RSA Parametes

Generate a Ke...

Private K...

30820277020100300D06092A864886F70D0101010500048202613082025D020100028181009AD83B1E2EB1978A162BABE284ACD58256BBC

Public Key:

30819F300D06092A864886F70D010101050003818D00308189028181009AD83B1E2EB1978A162BABE284ACD58256BBC6A9AB83116458DF23Decrypted text: AAABBB

Plan Text:

Cypher T...

4E0A90DBA77678997A56066AFB8ED7CC7E82315FCBBEB33C9FFECD527391B96241D885659B8BA9F00CAE2998EB61AC4F84A6A5D80B7820C4930CB3988640FAF37CA7BA4A9413B821200C2F957314DF17A93AE367DEB83DD0159F8E806134E5984CBC1A697253BEE0E4B8C87AA56183004516AFC48B66DF3368FFD6135EADE000

Encrypt

Decrypt

Figura 7 - RSA decrypt

5. AES

a. ECB

AES Parameters

Generate IV:	10B79DB325A7CB3EE65CA32F38EDC13F
Generate ...	2b7e151628aed2a6abf7158809cf4f3c
	6bc1bee22e409f96e93d7e117393172a
Plan Text:	
Cypher T...	3AD77BB40D7A3660A89ECAF32466EF977DF76B0C1AB899B33E4 2F047B91B546F

Mode: ECB ▼ Encrypt Decrypt

Figura 8 - AES encrypt usando modo ECB

AES Parameters

Generate IV:	10B79DB325A7CB3EE65CA32F38EDC13F
Generate ...	2b7e151628aed2a6abf7158809cf4f3c
	Decrypted data: 6BC1BEE22E409F96E93D7E117393172A
Plan Text:	
Cypher T...	3AD77BB40D7A3660A89ECAF32466EF977DF76B0C1AB899B33E4 2F047B91B546F

Mode: ECB ▼ Encrypt Decrypt

Figura 9 - AES decrypt usando modo ECB

b. CBC

AES Parametes

Generate IV:	10B79DB325A7CB3EE65CA32F38EDC13F
Generate ...	2b7e151628aed2a6abf7158809cf4f3c
Plan Text:	6BC1BEE22E409F96E93D7E117393172A
Cypher T...	3C2AE5B00DD65795AC3C9819C882C8327DF76B0C1AB899B33E42F047B91B546F

Mode: CBC ▼ Encrypt Decrypt

Figura 10 - AES encrypt usando modo CBC

AES Parametes

Generate IV:	10B79DB325A7CB3EE65CA32F38EDC13F
Generate ...	2b7e151628aed2a6abf7158809cf4f3c
Plan Text:	Decrypted data: 6BC1BEE22E409F96E93D7E117393172A7DF76B0C1AB899B33E42F047B91B546F
Cypher T...	3C2AE5B00DD65795AC3C9819C882C8327DF76B0C1AB899B33E42F047B91B546F

Mode: CBC ▼ Encrypt Decrypt

Figura 11 - AES decrypt usando modo CBC

C. CTR

AES Parametes

Generate IV:

10B79DB325A7CB3EE65CA32F38EDC13F

Generate ...

2b7e151628aed2a6abf7158809cf4f3c

Plan Text:

6BC1BEE22E409F96E93D7E117393172A7DF76B0C1AB899B33E42F047B91B546F

Cypher T...

34FF80282FE6C031A755FB0701B4A8419AEEC2F4B110B6B04F183A0DCDED4868BFC0693C7DDA5C0989FD8D895692C1E4

Mode:

CTR

Encrypt

Decrypt

Figura 12 - AES encrypt usando modo CTR

AES Parametes

Generate IV:

10B79DB325A7CB3EE65CA32F38EDC13F

Generate ...

2b7e151628aed2a6abf7158809cf4f3c

Plan Text:

Decrypted data: 6BC1BEE22E409F96E93D7E117393172A7DF76B0C1AB899B33E42F047B91B546F

Cypher T...

34FF80282FE6C031A755FB0701B4A8419AEEC2F4B110B6B04F183A0DCDED4868BFC0693C7DDA5C0989FD8D895692C1E4

Mode:

CTR

Encrypt

Decrypt

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/>