Answer Key
November 24, 2020

Tutorial-11 Security

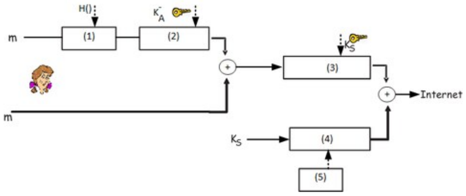
1. Alice encrypts a message m using her private key and sends the message to Bob. What is she doing?

- A Authentication
- B Confidentiality
- C Integrity
- ✓ D Signing m, non-repudiation (validated by a digital signature)

2. Alice creates a key "m" encrypts the key using Bob's public key and sends the encrypted key to Bob.

- A Authentication
- ✓ B Confidentiality
- C Integrity
- D Signing m, non-repudiation (validated by a digital signature

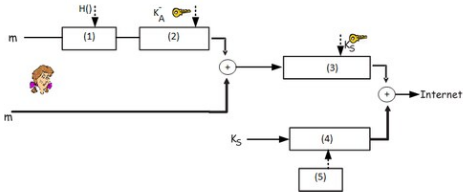
3. Alice wants to send a message (m) to Bob that is encrypted and authenticated and one can tell if the message has been tampered with or not.   Assume that Alice has Bob's public key and Bob has Alice's public key.



Using the diagram at the right, in (1) what is Alice doing?

- ✓ A Alice computes a message digest of M.
- B Alice signs the message with her public key.
- C Alice signs the message with her private key.
- D Alice signs the message with Bob's private key.
- E Alice signs the message digest with her private key
- F Alice sends the message and signed message digest encrypted with the key KS, along with the encrypted key KS to Bob
- G Alice encrypts the message with key KS.
- H Alice encrypts Bob's public key with KS.
- I Alice encrypts the message, message digest, and key KS with KS.
- J Alice encrypts the message and message digest with key KS.
- K Alice encrypts KS with Bob's public key.
- L Alice encrypts the shared key with Bob's public key.
- M Alice encrypts the message digest with her public key.
- N Alice encrypts the message with her public key.
- O Alice encrypts the message with Bob's public key.

4. Alice wants to send a message (m) to Bob that is encrypted and authenticated and one can tell if the message has been tampered with or not. Assume that Alice has Bob's public key and Bob has Alice's public key.



Using the diagram at the right, in (2) what is Alice doing?

A Alice computes a message digest of M.

B Alice signs the message with her public key.

C Alice signs the message with her private key.

D Alice signs the message with Bob's private key.

✓ E Alice signs the message digest with her private key

F Alice sends the message and signed message digest encrypted with the key KS, along with the encrypted key KS to Bob

G Alice encrypts the message with key KS.

H Alice encrypts Bob's public key with KS.

I Alice encrypts the message, message digest, and key KS with KS.

J Alice encrypts the message and message digest with key KS.

K Alice encrypts KS with Bob's public key.

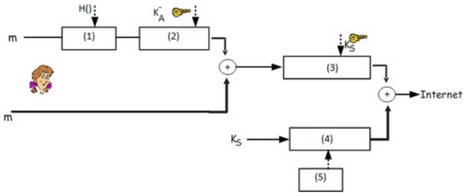
L Alice encrypts the shared key with Bob's public key.

M Alice encrypts the message digest with her public key.

N Alice encrypts the message with her public key.

O Alice encrypts the message with Bob's public key.

5. Alice wants to send a message (m) to Bob that is encrypted and authenticated and one can tell if the message has been tampered with or not. Assume that Alice has Bob's public key and Bob has Alice's public key.



Using the diagram at the right, in (3) what is Alice doing?

A Alice computes a message digest of M.

B Alice signs the message with her public key.

C Alice signs the message with her private key.

D Alice signs the message with Bob's private key.

E Alice signs the message digest with her private key

F Alice sends the message and signed message digest encrypted with the key KS, along with the encrypted key KS to Bob

G Alice encrypts the message with key KS.

H Alice encrypts Bob's public key with KS.

I Alice encrypts the message, message digest, and signed message digest with KS.

✓ J Alice encrypts the message and signed message digest with key KS.

K Alice encrypts KS with Bob's public key.

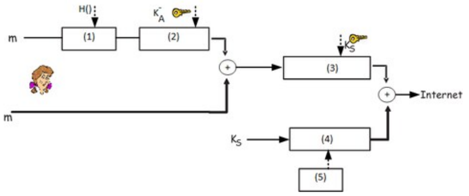
L Alice encrypts the shared key with Bob's public key.

M Alice encrypts the message digest with her public key.

N Alice encrypts the message with her public key.

O Alice encrypts the message with Bob's public key.

6. Alice wants to send a message (m) to Bob that is encrypted and authenticated and one can tell if the message has been tampered with or not. Assume that Alice has Bob’s public key and Bob has Alice’s public key.



Using the diagram at the right, what is Alice doing in applying (5) to box (4) with input KS?

A Alice computes a message digest of M.

B Alice signs the message with her public key.

C Alice signs the message with her private key.

D Alice signs the message with Bob's private key.

E Alice signs the message digest with her private key

F Alice sends the message and signed message digest encrypted with the key KS, along with the encrypted key KS to Bob

G Alice encrypts the message with key KS.

H Alice encrypts Bob's public key with KS.

I Alice encrypts the message, message digest, and key KS with KS.

J Alice encrypts the message and message digest with key KS.

✓ K Alice encrypts KS with Bob's public key.

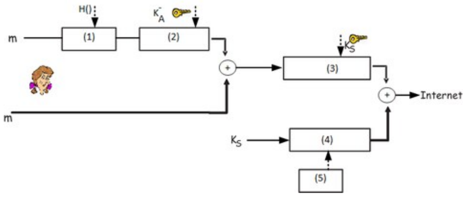
L Alice encrypts the shared key with Bob's public key.

M Alice encrypts the message digest with her public key.

N Alice encrypts the message with her public key.

O Alice encrypts the message with Bob's public key.

7. Alice wants to send a message (m) to Bob that is encrypted and authenticated and one can tell if the message has been tampered with or not. Assume that Alice has Bob’s public key and Bob has Alice’s public key.



Using the diagram at the right, what does Alice finally send to Bob?

A Alice computes a message digest of M.

B Alice signs the message with her public key.

C Alice signs the message with her private key.

D Alice signs the message with Bob's private key.

E Alice signs the message digest with her private key

✓ F Alice sends the message and signed message digest encrypted with the key KS, along with the encrypted key KS to Bob

G Alice encrypts the message with key KS.

H Alice encrypts Bob's public key with KS.

I Alice encrypts the message, message digest, and key KS with KS.

J Alice encrypts the message and message digest with key KS.

K Alice encrypts KS with Bob's public key.

L Alice encrypts the shared key with Bob's public key.

M Alice encrypts the message digest with her public key.

N Alice encrypts the message with her public key.

O Alice encrypts the message with Bob's public key.

8. Using the website

https://csfieldguide.org.nz/en/interactives/rsa-encryption/

Encrypt the short message "got it" for me. Use PKCS and "no padding".

The public key is (please tell everyone my public key):

```
-----BEGIN RSA PUBLIC KEY-----
MEgCQQCA8GLS1NhWTDyxyAU+gAkI9Rbj6RFdRMRlPvi/3DuzWOPrr+tPikypwGkh
ZigCC0/L2zjv8mz0c6Ka2AF/32a1AgMBAAE=
-----END RSA PUBLIC KEY-----
```

cmUS0dKS42m0OpESZZk5CTrKEChIKTAXzNSIQ35AY+wL+mzW/gx4lGBF8a4ff7SRgTMw6vX8YKzlnL74hlJ63Q==

9. Using the website

https://csfieldguide.org.nz/en/interactives/rsa-decryption/

Decrypt the following message for me. Use PKCS.

TeFo+Lzyt5Lv9GoCpwHgg3tE0wbohkOnoXvY78Y21g4E8NdUX7hR+OG1jQHeSnvLEgyceYNCznXStGsc5AXP+w==

My private key is (don't tell anyone it is a secret):

```
-----BEGIN RSA PRIVATE KEY-----
MIIBOQIBAAJBAIDwYtLU2FZMPLHIBT6ACQj1FuPpEV1ExGU++L/cO7NY4+uv60+K
TKnAaSFmKAILT8vbOO/ybPRzoprYAX/fZrUCAwEAAQJAeob1AjCtXGSaEL9o7Fmz
PEXbeL0UeTNOBoBu1bOtL+HfvvzTNc+Vw+0vmDgUt7peeQbf67hAaMX2SbzGsANy
gQIhAMjEL6fPkF+MeAzk493nQCmYvJoYYhSXoXC6IV0JzCNxAiEApGl1FxpRXmFA
a6uFavtmiY4uKbIZYCkIwSywfcCoTYUCIB2tor3T2SvGwBhn3ad3/+wmP/snj5gr
shnP6g6u3BaBAiBgeqoFZqI9GiCtjjd6shBXxCF+wk51yV6jzU+8W6Pn6QIgK1+V
QEAgVlBt2Qtsk9CoRMUUdHd+U1dnKIx3SfX2dzs=
-----END RSA PRIVATE KEY-----
```

I know a UDP joke, but you probably wouldn't get it.

10. Alice and Bob decide that the best way to settle the question of who gets the house in the divorce is to toss a coin and communicate the results with an independent arbitrator to decide the issue. Alice and Bob will each toss their coin and Alice gets to decide to call it DIFFERENT or SAME. If she correctly guesses whether the two coins are the same or different she wins the house.

Given the instructions the arbitrator sends out a message to both Alice and Bob to use the arbitrator's pubic key for Bob to send his coin toss and for Alice to send her coin toss and whether or not she believes the two coins are different or the same The arbitrator received two messages and based on those messages declared Bob the winner and published the messages she received. Alice however appealed and refused to concede. She claimed that she didn't send the message that was published.

Now it turns out Bob knows a bit of cryptography and when he received the instructions from the arbitrator he sent out his message, and then immediately sent out a second message saying he was Alice and giving a coin toss and an answer to ensure he received the house. Alice could not prove that the messages did not come from her.

Can you suggest a protocol for this problem to make sure this travesty can not occur and that you can make the process fair and also allow everyone to see and to validate the decision? What techniques would you include?

playfair key: sxfcpautmonyrkdivebhzlgwq
(http://www.practicalcryptography.com/ciphers/classical-era/playfair/)

nonce
sequence numbers
signatures

i NICZGEOEVTFITPDAKSITYNAZZRHRTBXFTZIFTNBVOCTDMURAOEITKEEANTMAKFATQYAXITDAKSGRTHIATYGRIOMEAMIOZVFBNIKHMHTNVGVEIFIBQMYXNOZXAOMNI