Kenneth Woodard

CS366

Nov 1, 2022

Question 1

A. Alice will construct the message to be transmitted by implementing a digital signature. This will make sure the integrity of the message is intact. First, the data will go through a hash algorithm to compress the data. Next, Alice will use her private key to encrypt (sign) the compressed data. The data and her public key will then be sent somehow, someway to Bob.
B. Bob is going to receive the digitally signed data (as well as Alice's public key) and then verify if the data still has its integrity. To begin, Bob will use the hash algorithm to get the first hash value from the data. He will then use the public key sent by Alice to decrypt the data and get a second hash value. Finally, Bob will compare the two hash values. If the hash values are equivalent, then the data is valid. Otherwise, Bob should realize the data has been compromised.

Question 2

Here are my screenshots because the assignment on canvas only accepts pdfs.

```
(base) jakewoodard@Jakes-MacBook-Air-3 WA3 % cat input.txt | openssl enc -aes-256-cbc -K 'E8B6C00C9ADC5E75BB656ECD429CB1643A25B111FCD22C6622D53E0722439993'
 -iv  'E486BB61EB213ED88CC3CFB938CD58D7' > output.dat
(base) jakewoodard@Jakes-MacBook-Air-3 WA3 % ls
input.txt       output.dat
(base) jakewoodard@Jakes-MacBook-Air-3 WA3 %
```

```
(base) jakewoodard@Jakes-MacBook-Air-3 WA3 % cat -n output.dat | openssl dgst -sha256 -hmac "key"
(stdin)= 75fec2cb33b1c44946c4fbcb911ae5d1fac6ee49a380e59c75924681b0e797ab
```

```
(base) jakewoodard@Jakes-MacBook-Air-3 WA3 % cat output.dat
-k_???MV????I?3yBeH?tMR?K'??c??U曙 R$??%
(base) jakewoodard@Jakes-MacBook-Air-3 WA3 % cat input.txt
The quick brown fox jumps over the lazy dog - [Kenneth Woodard]
(base) jakewoodard@Jakes-MacBook-Air-3 WA3 %
```