Cryptography and digital signatures examples

All the examples use the following keys, and assume that RSA public key cryptography is used throughout:

Public key for Alice: modulus 22, exponent 3
Private key for Alice: modulus 22, exponent 7
Public key for Bob: modulus 34, exponent 5
Private key for Bob: modulus 34, exponent 13

The following table can be used for numerical calculations:

m	m^3 mod 22	m^7 mod 22	m^5 mod 34	m^{13} mod 34
01	01	01	01	01
02	08	18	32	32
03	05	09	05	29
04	20	16	04	04
05	15	03	31	03
06	18	08	24	10
07	13	17	11	23
08	06	02	26	26
09	03	15	25	25
10	10	10	06	28
11	11	11	27	07
12	12	12	20	14
13	19	07	13	13
14	16	20	12	22
15	09	05	19	19
16	04	14	16	16
17	07	19	17	17
18	02	06	18	18
19	17	13	15	15
20	14	04	22	12
21	21	21	21	21
22	00	00	14	20
23	01	01	07	27
24	08	18	28	06

Question: *A* would like to encrypt and send the message 06 to *B*. What is the encrypted message sent?

Answer: *A* encrypts using *B*'s public key. Formula is $c=m^e$ mod n. Here, m=6, e=5, n=34. So $c = 6^5$ mod 34 = 24.

Question: *A* has received the encrypted message 9 from *B*. What was the plaintext message sent by *B*?

Answer: *B*' s message to *A* is encrypted using *A*'s public key. *A* should decrypt using *A*'s private key. Formula is $m = c^d \bmod n$. Here, c=9, d=7, n=22. So $m = 9^7 \bmod 22 = 15$.

For the next questions, use the following hash function h, and assume it is a cryptographic hash function (it isn't, but don't worry about that):

h(m) = sum of decimal digits of m, mod 10

Question: *B* would like to send the message 3126 to *A*, without encryption but with a digital RSA signature. What is actually sent?

Answer: *B* computes h(m) = h(3126) = 12 mod 10 = 2. To sign, *B* encrypts the hash with *B*'s private key, so signature s is $s = 2^{13} \bmod 34 = 32$. Final data sent is the message (3126) followed by the signature (32), or 312632.

Question: *B* receives the message m=1314 followed by the signature s=15. *A* claims to have sent the message and signed it using RSA. (a) How can *B* verify that *A* sent the message? (b) How can *B* verify that the message received has not been tampered with?

Answer: Compute h(m) = h(1314)=9. Unsign 15 using *A*'s public key, obtaining $h' = 15^3 \bmod 22 = 9$. If h'=h(m), then message is from *A* and has not been altered, otherwise we have no information about the authenticity or integrity of the message. In this particular case, h'=h(m)=9, so the message is from *A* and has not been tampered with.