CPSC 353
Project 6

Katie Stevens

(1) $d \equiv e^{-1} \bmod (p-1)(q-1)$

$\boxed{d = 113}$

(2a) $c \equiv m^e \bmod n$

$\boxed{c = 99}$

(2b) $m \equiv c^d \bmod n$

$\boxed{m = 99}$

3,4,5 Bob has a message, m that he wants to encrypt to Alice. For RSA encryption Alice will need 2 random large numbers, p and q. Let $n = p \cdot q$ and $phi = (p-1)(q-1)$. She will then choose a number that is co-prime to phi $gcd(e, (p-1)(q-1)) = 1$. She then can compute d using $d \equiv e^{-1} \bmod (p-1)(q-1)$. She keeps d as her private key for decryption and she can upload her public key (e n) to Bob for encryption. Bob can encrypt his message, m, to cipher text, c, using the theorem, $c = m^e \bmod n$. Alice can decrypt Bob's cipher-text using her private key, d, and the theorem, $m = c^d \bmod n$. Alice did not have to share keys in order to decrypt Bob's message so RSA is valid in not having to share keys.

6.18 "complexion dimm'd"

(9) $n = 119143$

$n = a^2 - b^2$

$n = (a+b)(a-b)$

$a = \lceil \sqrt{119143} \rceil$

$a = 346$

$b = \sqrt{346^2 - n}$ b is not a whole number

increase $a+1$ until $b = \sqrt{a^2 - n}$ results in a whole number

$\boxed{a = 352 \quad b = 69}$

$n = (352+69)(352-69) = 119143$ ✓

(10) Given two different cipher texts, $c_1 = m^{e_1}$ and $c_2 = m^{e_2}$ and two numbers, s and t that satisfy $se_1 + te_2 = 1$ then

$$c_1 \cdot c_2 = (m^{e_1})^s + (m^{e_2})^t$$
$$= m^{se_1} + m^{te_2}$$
$$= m^{se_1 + te_2}$$
$$= m^1$$
$$= m$$

The common modulus attack is correct.