1. (i) Digital signature can ensure the message authentication and integrity of message while MAC produces MAC based on the message and the secret key using the algorithm.

(a) DS = the digital code is generated using the hash of the message and then encrypted using the sender's private key and it is added as signature. It protect the integrity of message and not altered by third party.

MAC: generated based on the message and the secret key using the hash of the message and encrypted using the sender's private key and added as signature append to the message. Using algorithm produce MAC, verify MAC for authentication. If true, then the integrity is without attack.

(b) Replay attack will not be detected by both DS and MAC as they only assure the identities.

(c) Yes, DS can verify the signature by decrypting and determine with the authenticated user. MAC can use secret key verify the user.

(d) DS: Alice can ask Bob for the received message and verify the signature to prove it wasn't from her.

MAC: MAC unable prove that Alice didn't send

2. RSA

a. $p=3$, $q=11$, $e=7$, $M=5$

$n = p \times q = 33$

$\phi(n) = (p-1)(q-1) = 2 \times 10 = 20$

$d \cdot e \bmod \phi(n) = 1$

$\Rightarrow d = 3$

public: $KU = \{7, 33\}$ $\quad M=5 < 33 = n$

private: $KR = \{3, 33\}$

b. $p=11$, $q=13$, $e=11$, $M=7$

$n = p \times q = 143$

$\phi(n) = (p-1)(q-1) = 10 \times 12 = 120$

$d \cdot e \bmod \phi(n) = 1$

$\Rightarrow d = 11$

public: $KU = \{11, 143\}$ $\quad M=7 < 143 = n$

private: $KR = \{11, 143\}$

c. $p=17$, $q=31$, $e=7$, $M=2$

$n = p \times q = 527$

$\phi(n) = (p-1)(q-1) = 16 \times 30 = 480$

$d \cdot e \bmod \phi(n) = 1$

$\Rightarrow d = 343$

public: $KU = \{7, 527\}$

private: $KR = \{343, 527\}$

3. $c=10 \quad e=5, n=35$, what is M

find d: $d \cdot e \bmod \phi(n) = 1$

$\because n = 35 = 5 \times 7$

$\phi(n) = 4 \times 6 = 24$

$\because e = 5$

$\Rightarrow d = 5$

$M = C^d \bmod n = 10^5 \bmod 35 = 5$ ($10^5 = 100000$, $35 \times 2857 = 99995$)

4. RSA, $e=31, n=3599$, find private key

$d \cdot e \bmod \phi(n) = 1$

$n = 3599 = 59 \times 61$

$\phi(n) = 58 \times 60 = 3480$

$d \cdot e \bmod \phi(n) = 1$

$\Rightarrow d = -449$

private key: $KR = \{-449, 3599\}$

5. $q=11, \alpha=2$

a. $Y_A = 9$, what is X_A ($55+9=64$)

$Y_A = \alpha^{X_A} \bmod q = 2^{X_A} \bmod 11 \Rightarrow X_A = 6$

b. $Y_B = 3$, what is key k ($11 \times 23 + 3 = 258$)

$Y_B = \alpha^{X_B} \bmod q = 2^{X_B} \bmod 11 \Rightarrow X_B = 8$

$K = (Y_B)^{X_A} \bmod q = 3^6 \bmod 11 = 729 \bmod 11 = 3$