Assignment 5
Introduction to Information Security

Task 1:

1. F
2. T
3. F
4. T
5. T
6. T
7. T
8. F
9. F
10. F
11. T
12. F
13. T
14. T
15. T

Task 2:

1. D. Encryption
2. B. Sender cannot deny sending
3. C. Sender's public key
4. C. One-to-one relationship
5. B. Cannot control content of message
6. C. Harder to forge
7. C. 2048 bits
8. B. AES Digital Signature Scheme
9. B. Signature verification fails
10. C. Password management
11. B. Additional encryption needed
12. B. s = x^d mod n
13. C. Prevent attacks including existential forgery
14. B. Public key uses small exponent e
15. A. Digital signatures provide non-repudiation

Task 3:

Task 3 : RSA Signature and Cryptography

Bob's public key:

Given $N = 143$ and $e = 7$

We know that $p * q = 143$

$11 \times 13 = 143$

$$\phi(N) = (p-1) * (q-1)$$

$$= (11-1) * (13-1)$$

$$= 10 \times 12$$

$$\phi(N) = 120$$

we know that $d * e \bmod \phi(N) = 1$

$$d * 7 \bmod 120 = 1$$

$$103 * 7 \bmod 120 = 1$$

$$\therefore d = 103$$

Given $M = 3$

a) $S = M^d \bmod N$

$S = 3^{103} \bmod 143$

$S = 16$

$\therefore$ Signature value = 16

6) Alice's public key:

given $N = 39$ and $e = 5$

$$C = S^e \bmod N$$

$$C = 16^5 \bmod 39$$

$$\therefore C = 22$$

we know that $P * q = N$

$$P * q = 39$$

$$3 \times 13 = 39$$

$$\therefore p = 3 \text{ and } q = 13$$

$$\phi(N) = (P-1) * (q-1)$$

$$= (3-1) * (13-1)$$

$$= 2 * 12$$

$$\phi(N) = 24$$

We know that $e * d \bmod \phi(N) = 1$

$$5 * d \bmod 24 = 1$$

$$5 \times 5 \bmod 24 = 1$$

$$\therefore d = 5$$

c) Decrypt the recieved encrypted signature:

$$S = C^d \text{ Mod } N$$

$$S = 22^5 \text{ mod } 39$$

$$\therefore S = 16$$

d) Verity the signature and signer identity

We know that

Bob's public key:

$$M = S^e \text{ mod } N$$

Here $S = 16$, $e = 7$ and $N = 143$

$$M = 16^7 \text{ mod } 143$$

$$\therefore M = 3$$

Thus verified.