Section 6 Lecture 39 – RSA Messaging - Solutions

Q1)

(i)

$n = pq = 21$, $\varphi(n) = (p - 1)(q - 1) = 12$. d needs to satisfy $de = 1 \pmod{\varphi(n)}$, that is

$5d = 1 \pmod{12}$. This gives $d = 5$.

Alice sends $c = m^e \pmod{n} = 3^5 \pmod{21} = 12$.

Bob calculates $c^d \pmod{n} = 12^5 \pmod{21} = 3$ which is Alice's original message.

(ii)

$n = pq = 65$, $\varphi(n) = (p - 1)(q - 1) = 48$. d needs to satisfy $de = 1 \pmod{\varphi(n)}$, that is

$7d = 1 \pmod{48}$. This gives $d = 7$.

Alice sends $c = m^e \pmod{n} = 5^7 \pmod{65} = 60$.

Bob calculates $c^d \pmod{n} = 60^7 \pmod{65} = 5$ which is Alice's original message.

(iii)

$n = pq = 55$, $\varphi(n) = (p - 1)(q - 1) = 40$. d needs to satisfy $de = 1 \pmod{\varphi(n)}$, that is

$3d = 1 \pmod{40}$. This gives $d = 27$.

Alice sends $c = m^e \pmod{n} = 10^3 \pmod{55} = 10$.

Bob calculates $c^d \pmod{n} = 10^{27} \pmod{55} = 10$ which is Alice's original message.

Q2)

(i)

The message actually encrypts to itself (so nothing happens to it!) Virtually impossible to happen for larger numbers.

(ii)

(a) e is not coprime to $\varphi(n) = 48$
(b) e is not smaller than $\varphi(n) = 48$