

Q1
a)

{ 7, 187 }

public keys {e, n}

$$e = 7$$

$$n = 187$$

Two prime numbers \Rightarrow

$$17 \quad 11$$

$$17 \times 11 \Rightarrow 187$$

$$\phi(n) = (p-1)(q-1)$$
$$= 160$$

$$d = ?$$

$$\Rightarrow (\phi(n), e) = 1$$

$$\therefore e = 7$$

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

$$d \times 7 \bmod 160 = 1$$

$$d = 23$$

$$C_2 \Rightarrow P = 24^{23} \bmod (187)$$

$$P = 63$$

private key {23, 187}

d, n

$$P = c^d \bmod n$$

$$C_1 \Rightarrow P = 16^{23} \bmod 187$$

$$\Rightarrow 169$$

(b)

$$p = 47$$

$$g = 11$$

Alice's Secret = 9

Bob's Secret = 16

$$A = 11^9 \bmod 47$$

$$= 38$$

$$B = 11^{16} \bmod 47$$

$$= 3$$

$$S_A = 3^9 \bmod 47$$

$$\Rightarrow 37$$

$$S_B = 38^{16} \bmod 47$$

$$\Rightarrow 37$$

Both have the same
shared secrets.

Q#2

$$p = 7$$

$$q = 11$$

$$e = 7$$

$$n = p \times q$$

$$n = 11 \times 7$$

$$\Rightarrow 77$$

$$\phi(n) = (p-1)(q-1)$$

$$\Rightarrow (7-1)(11-1)$$

$$\Rightarrow 60$$

$$\gcd(e, \phi(n)) = 1$$

$$e = 7$$

$$d \times 7 = 1 \pmod{60}$$

$$d = 43$$

$$\text{public key} = (e, n) \\ (7, 77)$$

$$\text{private key} = (d, n) \\ (43, 77)$$

$$m = 13$$

Encrypt

$$c = p^e \bmod n$$

$$c = 13^7 \bmod 77$$

$$= 35$$

Decrypt

$$p = c^d \bmod n$$

$$p = 35^{43} \bmod 77$$

$$= 13$$

Q#3

(a)

$$n = p \times q$$

$$= 61 \times 53$$

$$\Rightarrow 3233$$

$$\phi(n) = (p-1)(q-1)$$

$$= 60 \times 52$$

$$\Rightarrow 3120$$

$$\gcd(\phi(n), e) = 1$$

$$e = 17$$

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

$$d = 2753$$

public key (e, n)
 $(17, 3233)$

private key (d, n)
 $(2753, 3233)$

Encryption

$$\begin{aligned}c &= p^e \bmod n \\&= 10^{17} \bmod 3233 \\&= 1096\end{aligned}$$

$$\begin{aligned}p &= c^d \bmod n \\&= 1096 \bmod 3233 \\&\Rightarrow 10\end{aligned}$$

⑥

$$\begin{aligned}p &= 11 \\q &= 13 \\e &= 7 \\m &= 9\end{aligned}$$

$$\begin{aligned}n &= 11 \times 13 \\n &= 143\end{aligned}$$

$$\begin{aligned}\phi(n) &= (p-1)(q-1) \\&\Rightarrow 10 \times 12 \\&\Rightarrow 120\end{aligned}$$

$$e = 7$$

$$\begin{aligned}dxe &= 1 \bmod \phi(n) \\d &= 103\end{aligned}$$

$$m = 9$$

Encrypt

$$\begin{aligned}C &= p^e \bmod n \\C &= 9^7 \bmod 143 \\&= 48\end{aligned}$$

Decrypt

$$\begin{aligned}&\Rightarrow c^d \bmod n \\&\Rightarrow 48^{103} \bmod 143 \\&\Rightarrow 9\end{aligned}$$

Q4+

$$p=23, g=5$$

$$\begin{aligned} A &= g^a \mod p \\ &\Rightarrow 5^6 \mod 23 \\ &\Rightarrow 8 \end{aligned}$$

$$\begin{aligned} B &= g^b \mod p \\ &\Rightarrow 5^{15} \mod 23 \\ &\Rightarrow 19 \end{aligned}$$

$$\begin{aligned} S_A &= 19^6 \mod 23 \\ &\Rightarrow 2 \end{aligned}$$

$$\begin{aligned} S_B &= 8^{15} \mod 23 \\ &\Rightarrow 2 \end{aligned}$$

(b) $p=11, g=2$

$$x=5, y=12$$

$$\begin{aligned} A &= g^x \mod p \\ &\Rightarrow 2^5 \mod 11 \\ &\Rightarrow 10 \end{aligned}$$

$$\begin{aligned} B &= g^y \mod p \\ &\Rightarrow 2^{12} \mod 11 \\ &\Rightarrow 4 \end{aligned}$$

$$\begin{aligned} S_A &= 4^5 \mod 11 \\ &\Rightarrow 9 \end{aligned}$$

$$\begin{aligned} S_B &= 10^{12} \mod 11 \\ &= 9 \end{aligned}$$