4.3.4.4 Example 1 : RSA

① $p = 5$ $\quad q = 11$

$n = 5 \times 11 = 55$

$\phi(n) = (p-1) \times (q-1) = 4 \times 10 = 40$

$p-1 = 4$ $\quad$ Factor = 2, 4

$q-1 = 10$ $\quad$ Factor = 2, 5

② First prime number : 1, 2, 3, 5, 7

X X ✓ X ✓

③ let us choose $e = 3$

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

$e \times d = k \cdot \phi(n) + 1$

$d = \frac{40k + 1}{3}$

④ Solve for k in such a way that there is no remainder

Select $k=1$

$d = \frac{41}{3}$ X

$k = 2$

$d = \frac{81}{3} = 27$ ✓

(5) $D = 3 \quad C = 2 \quad DC = 32$

$C = p^e \bmod n$

$= 32^3 \bmod 55$

$= 43$

decryption $p = C^d \bmod n$

$p = 43^{27} \bmod 55$

$= 32$

Method 2: If we select public key $e = 7$

$$e \cdot d \bmod n = 1$$

$$d = \frac{kn+1}{e}$$

$$= \frac{40k+1}{7}$$

$k=1$, $d = \frac{41}{7}$ ✗

$k=2$, $d = \frac{81}{7}$ ✗

$k=3$, $d = \frac{121}{7}$ ✗

$k=4$, $d = \frac{40\times4+1}{7}$

$$= \frac{161}{7}$$

$$= 23 \checkmark$$

$$\begin{array}{r} 17 \\ 7\overline{)121} \\ 7 \\ \hline 51 \\ 49 \\ \hline 2 \end{array}$$

$$\begin{array}{r} 23 \\ 7\overline{)161} \\ 14 \\ \hline 21 \\ 21 \\ \hline 0 \end{array}$$

So $d = 23$