22-S2 - Q3

Q (a)(i) Sy VS Asy

(ii) ECC + reason

(b) RSA

Solution : (a) (i) Symmetric advantages

①very fast and secure

② key are relatively short

disadvantage ①key exchange issue

(ii) Asymmetric advantage

solve the key exchange issus

. Disadvantages

① Too many keys

② Slow and less secure.

(iii) ECC

①Reasons : ECC even with smaller key (faster), and more secure than RSA

② I think that prediction will come true

(b) (i) ① Define : $p=3$, $q=11$, $e=7$,

we define Tony private key $d=7$

② $n = p \times q = 3 \times 11 = 33$

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

factor $\phi(n)$: $2, 5$

$e = 7$

$$d = \frac{k\phi(n)+1}{e} = \frac{20k+1}{7}$$

If $k=1$, $d = \frac{21}{7} = 3$ ✓

So, $d=3$

(ii) $m=15$

$$S = m^d \bmod n$$

$$= 15^3 \bmod 33$$

$$= 9$$

(iii) $m = s^e \bmod n$

$$= 9^7 \bmod 33$$

$$= 15$$