22-S2-Q2

Q (a) SSL/TLS

DH → RSA ✗ 不考

TLS 3.1

(b) DH

$p = 37$ $g = B$

$a = 10$ $b = 7$

(i) $A = ?$ $B = ?$

(ii) $s = ?$

(iii) $a \to s$? $b \to s$? ✓

Solution (b) (i)

① we define Alice public key A
pravite key a
Bob public key B
pravite key b
share key s
prime nurber p
generator g

② Alice generate A

$$A = g^a \bmod p$$
$$= 13^{10} \bmod 37$$
$$= (13^5)^2 \bmod 37$$
$$= (35)^2 \bmod 37$$
$$= 4$$

③ Bob → B

$$B = g^b \bmod p$$
$$= 13^7 \bmod 37$$

$= 32$

(ii) ① Alice

$s = B^{a} \bmod p$

$= 32^{10} \bmod 37$

$= (32^{5})^{2} \bmod 37$

$= 20^{2} \bmod 37$

$= 30$

② Bob

$s = A^{b} \bmod p$

$= 4^{7} \bmod 37$

$= 30$

(iii) ① can find

② due to $s = A^{b} \bmod p$ or $s = B^{a} \bmod p$

③ So no security remains.