7.(a) $47_{10} = \underbrace{101111_2}_{6 \text{ bits}}$: factors = (1, 47)

$GF(47) = \{0, 1, 2, \ldots, 46\}$

g is a primitive element of GF(p) if
- $g^{p-1} = 1$
- $g^r \neq 1 \ \forall \ 1 \leq r < p-1$

① $g^{47-1} = 5^{46} \pmod{47} = 1$

② only need to check $g^r \neq 1$ for $r = 2, 23$ since $g^{46} = g^{2 \times 23}$

$\Rightarrow 5^2 \pmod{47} = 25 \neq 1$

$5^{23} \pmod{47} = 46 \neq 1$

∴ g=5 is a primitive element in GF(p=47)

(b) $pk_A = g^{x_A} = 5^3 \pmod{47} = 31$

$pk_B = g^{x_B} = 5^{11} \pmod{47} = 13$

$pk_C = g^{x_C} = 5^7 \pmod{47} = 11$

(c) AB: $g^{x_A x_B} = 5^{33} \pmod{47} = 35$

AC: $g^{x_A x_C} = 5^{21} \pmod{47} = 15$

BC: $g^{x_B x_C} = 5^{77} \pmod{47} = 29$