

Assignment Test .

Q

User A

User B

common elements
prime = 71
g = 7

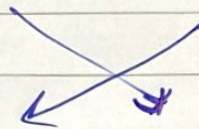
private key
 $x_a = 5$

private key
 $x_b = 12$

Cal Public key
 $y_a = g^{x_a} \text{ mod } p$
 $= 7^5 \text{ mod } 71$

Cal Public key
 $y_b = g^{x_b} \text{ mod } p$
 $= 7^{12} \text{ mod } 71$
 $= 4$

$y_a = 51$



$y_b = 4$

$y_a = 51$

$y_b^{x_a} \text{ mod } p$

$4^5 \text{ mod } 71$

$y_a^{x_b} \text{ mod } p$

$51^{12} \text{ mod } 71$

30

k =

Secret Key = 30