Rebecca Dias -19
182027
TECMDN A

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
$Y_a = g^{x_a} \bmod p$
$= 7^5 \bmod 71$

Cal Public key
$Y_b = g^{x_b} \bmod p$
$= 7^{12} \bmod 71$
$= 4$

$Y_a = 51$

$Y_b = 4$

$Y_a = 51$

$Y_b^{x_a} \bmod p$

$Y_A^{x_b} \bmod p$

$4^5 \bmod 71$

$51^{12} \bmod 71$

30

k =

Secret key = 30