

sd Diffie-Hellman

Alice

Bob

let g
let p

let a
let A = $g^a \% p$

let b
let B = $g^b \% p$

1 : A

2 : B

let s = $B^a \% p$

let s = $A^b \% p$

