Diffie-Hellman key Exchange

① Agree upon a base and a modulus value

base = x , modulus = z

- modulus needs to be large prime number
- Base does not need to be a large number but it should be a primitive root.

share the (x, z) pair as the publically shared value.

② Both participants should generate a secret value for themselves.

Alice ; S_A Bob ; S_B

③ Each participant calculates $x^s \bmod z$

Alice $\Rightarrow$ $x^{S_A} \bmod z$

Bob $\Rightarrow$ $x^{S_B} \bmod z$

④ share the generated value with each other.

Then each participant does the following calculation

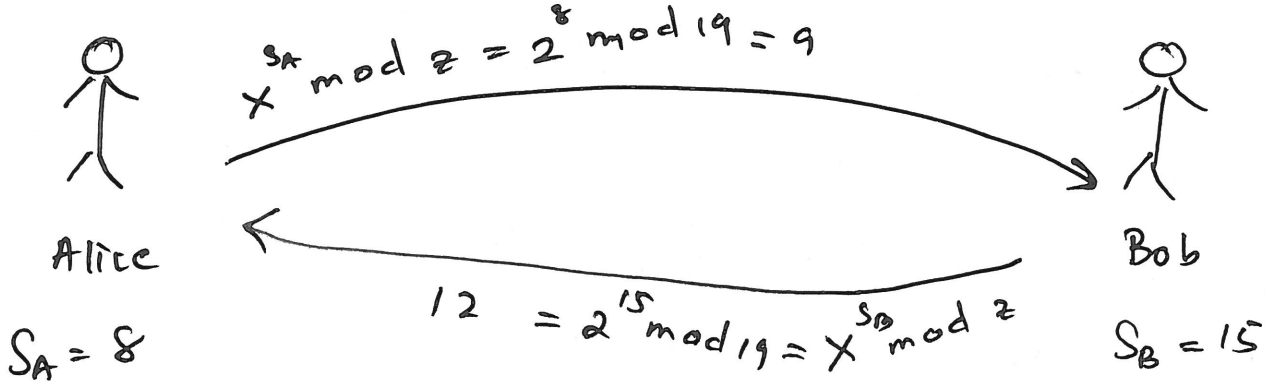
Alice $\Rightarrow$ $\underbrace{(x^{S_B} \bmod z)}_{\text{value received from Bob}}^{S_A} \bmod z = S$

Bob $\Rightarrow$ $\underbrace{(x^{S_A} \bmod z)}_{\text{value received from Alice}}^{S_B} \bmod z = S$

⑤ Both values generated are equal, and can be used as the shared secret, S. $S = (x^{S_A})^{S_B} \bmod z$

Ex!

$x = 2 \quad z = 19$



$S_A = 8$

$S_B = 15$

Alice

$S = (X^{S_B} \bmod z)^{S_A} \bmod z$

$S = (12)^8 \bmod 19 = 11$

Bob

$S = (x^{S_A} \bmod z)^{S_A} \bmod z$

$= 9^{15} \bmod 19 = 1$

$\boxed{S = 11}$ ← Shared Secret.