4.3.3.3 Example Diffie – Hellman Algorithm

Q:

Agree upon two number

P: prime Number 13

G: Generate of P 6

Random generate a Private key

public: $G^{Private} \bmod P$

Alice

Private = 5

$6^5 \bmod 13$

$7776 \bmod 13$

public = 2

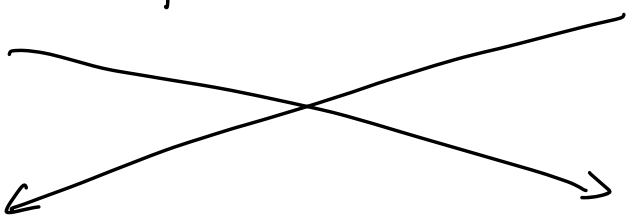
Bob

Private = 4

$6^4 \bmod 13$

$1296 \bmod 13$

public = 9



$9^5 \bmod 13$

$59049 \bmod 13$

Shared secret = 3

Shared secret

Shared public $^{Private} \bmod P$

$2^4 \bmod 13$

$16 \bmod 13$

Shared Secret = 3