RSA enc dec

P = 13

G = 7

Alice

A <- {2..11}

A = 4

Bob

B <- {2..11}

B = 5

7^4 mod 13

= 7^2 x 7 x 7 mod 13

= (49 mod 13) \* 7 x 7 mod 13

= 10 \* 7 x 7 mod 13

= (70 mod 13) \* 7 mod 13

= 5 \* 7 mod 13

= 9

7^5 mod 13

= 11

Alice Bob

a = 4 b = 5

B = 11 A = 9

B^a mod 13 A^b mod 13

= 11 ^4 mod 13 = 9^5 mod 13

= 3 = 3