



Glumanda



Pikachu

Einigen auf zwei Zahlen:

P: Primzahl = 13

G: Generator von P = 6

13 

+

5 

=

2 

9 

+



=

3 

Privaten Schlüssel generieren

Öffentlichen Schlüssel berechnen
($G^{(\text{Private})} \text{ MOD } P$)

Austausch
Public

Geteilten Schlüssel berechnen
($\text{Shared}^{(\text{Private})} \text{ MOD } P$)

 13

+

 4

=

 9

 2

+



=

 3