Encryption : $c = p^e \pmod{n}$ → Cipher Text

Decryption : $p = c^d \pmod{n}$

* Two prime number (Large) p & q

* $n = p*q$; $z = (p-1)*(q-1)$

* d relatively prime to z

* e such that ⇒ $e*d \pmod{z} = 1$

* public key : (e, n)

* private key : (d, n)

* For Coding →

* Input : Text (Capital P)

  ↓

  number (output — show)

* Input : # of bits for the large prime #

  min (50 .....)

* Output : public key & private key

* output : Encrypted msg

* Output : Decrypted msg

  ↳ plain text

* Cryptography note ; its application