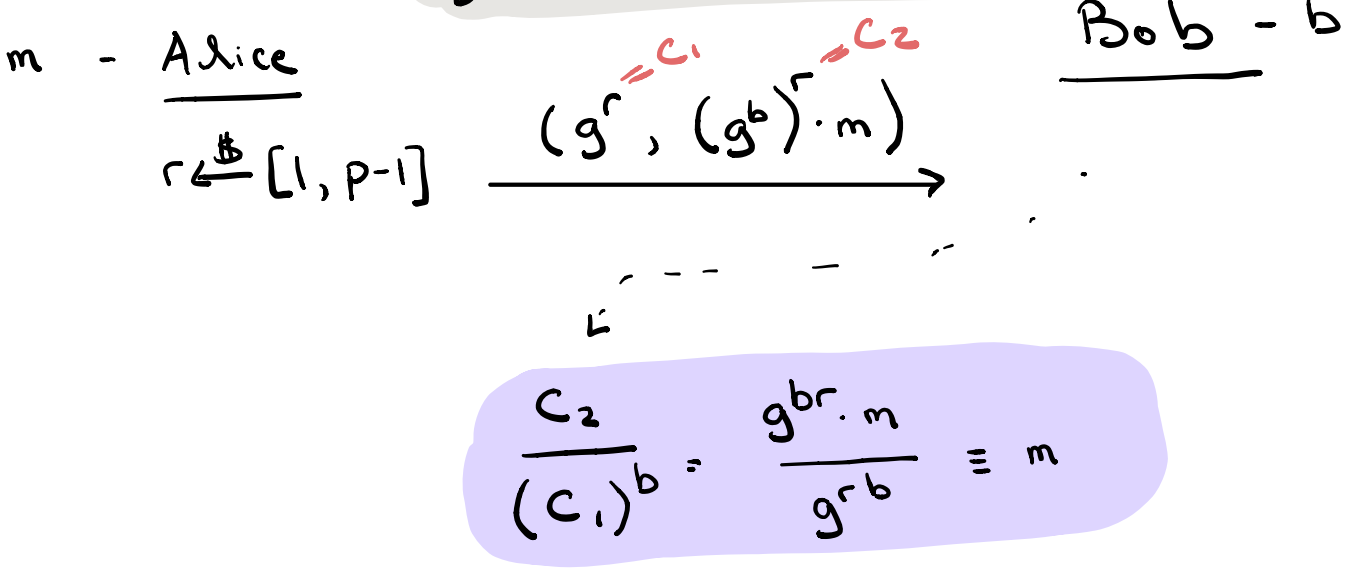
El-Gamal Encryption Scheme

p - large prime
$g \in [2, p-2]$ - generator
g^b - Bob's public key



$$\frac{c_2}{(c_1)^b} = \frac{g^{br} \cdot m}{g^{rb}} \equiv m$$

- We know discrete log is hard... how to build encryption from it?

.... Embed message in exponent? ie. g^m

→ This hides the message but isn't decryptable

- We want something like $m \cdot k$ where k is only known to Alice & Bob

→ This is just a OTP!

Idea: Use DH Key exch. to create a new K for every ciphertext

For each encryption:

- $K = g^{br}$ → Alice can compute since she knows r & g^b
  → This is DH Key exch. where g^b is static
- $c = (g^r, K \cdot m)$ → Bob can compute K & decrypt since he knows g^r & b

⟹ El-Gamal Encryption can be thought as a OTP where the key is randomly generated on each encryption via DH Key Exch.