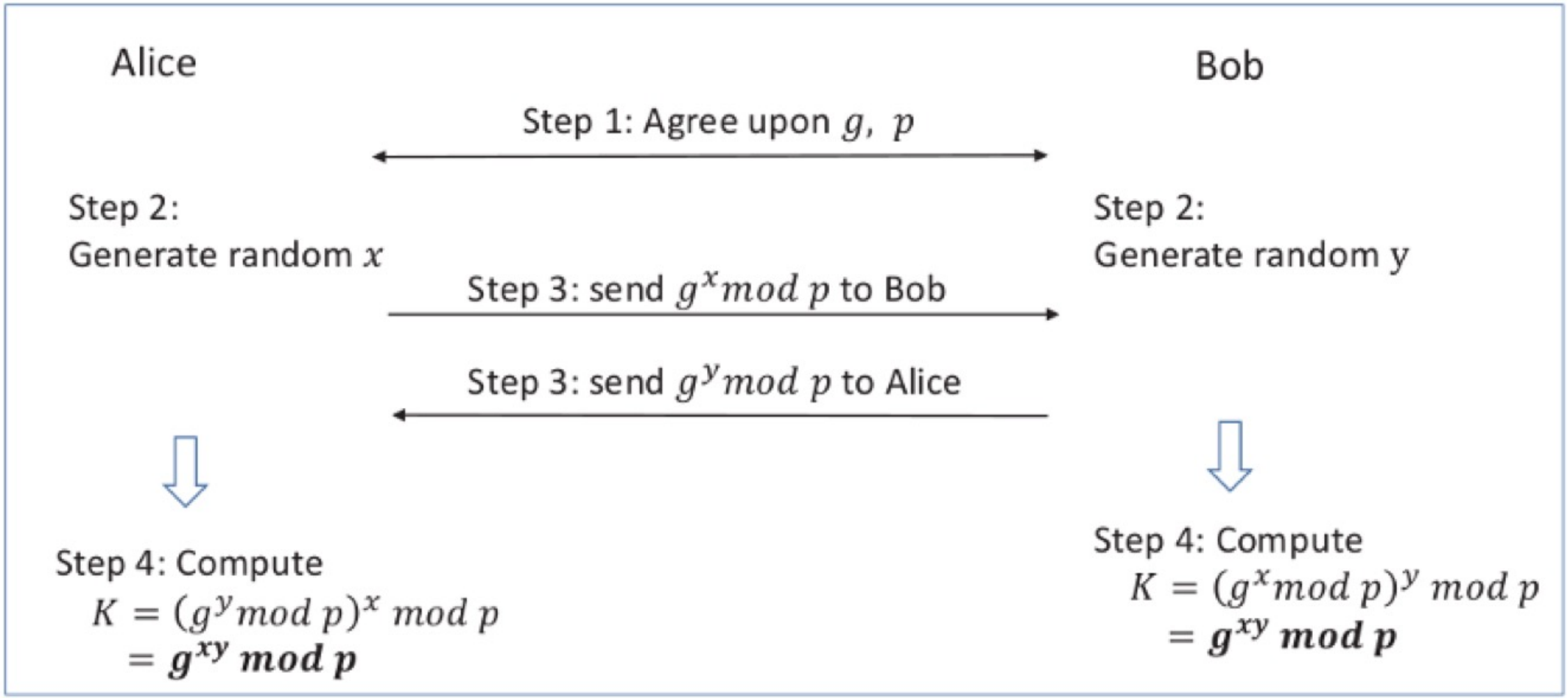
Diffie-Hellman Key Exchange

- The DH key exchange protocol
- How to exchange (symmetric) keys

Diffie-Hellman Key Exchange (High-Level)

Allows communicating parties **with no prior knowledge**
to **exchange shared secret keys**, **over an insecure channel**

Diffie-Hellman Key Exchange

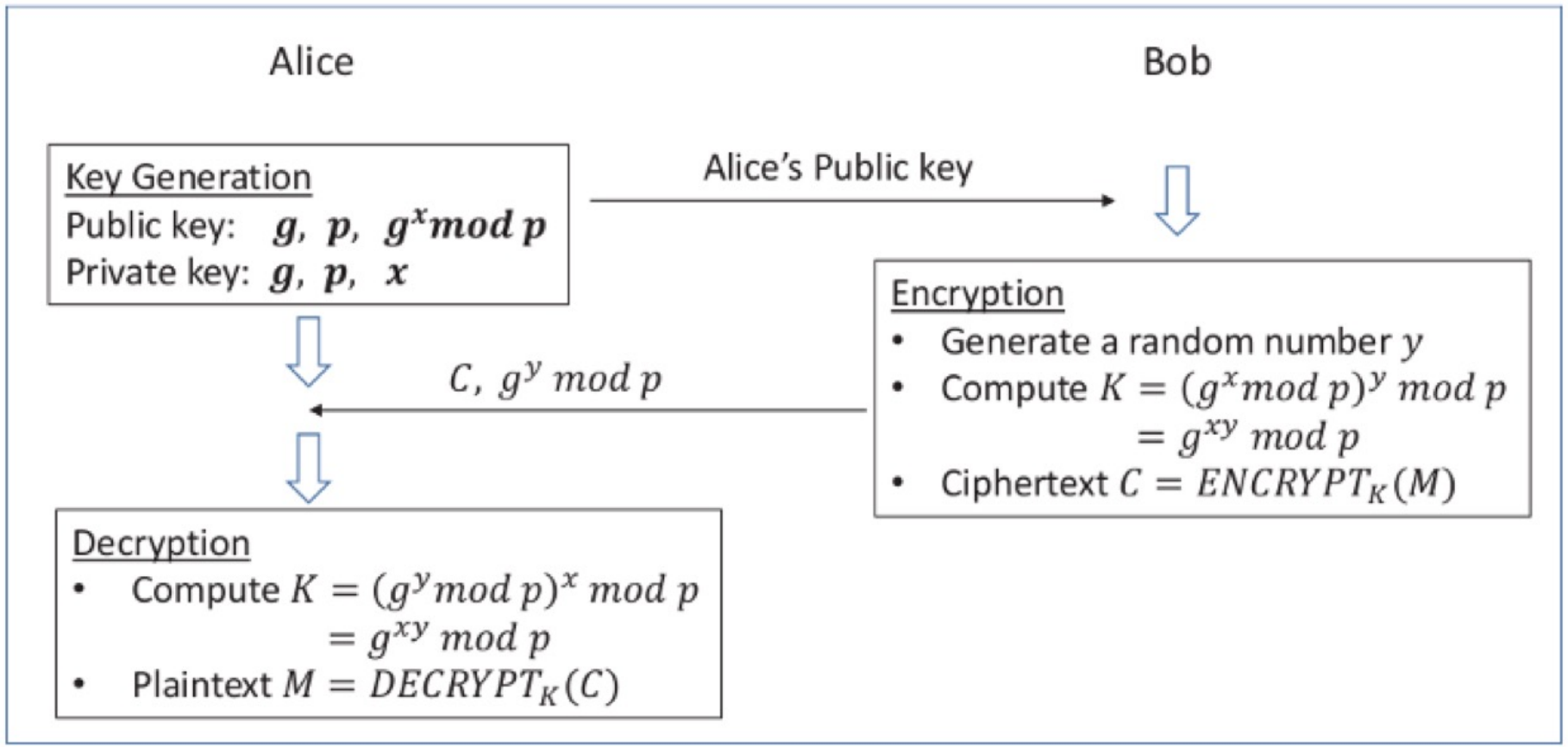


Turn DH Key Exchange into a Public-Key Encryption Algorithm!

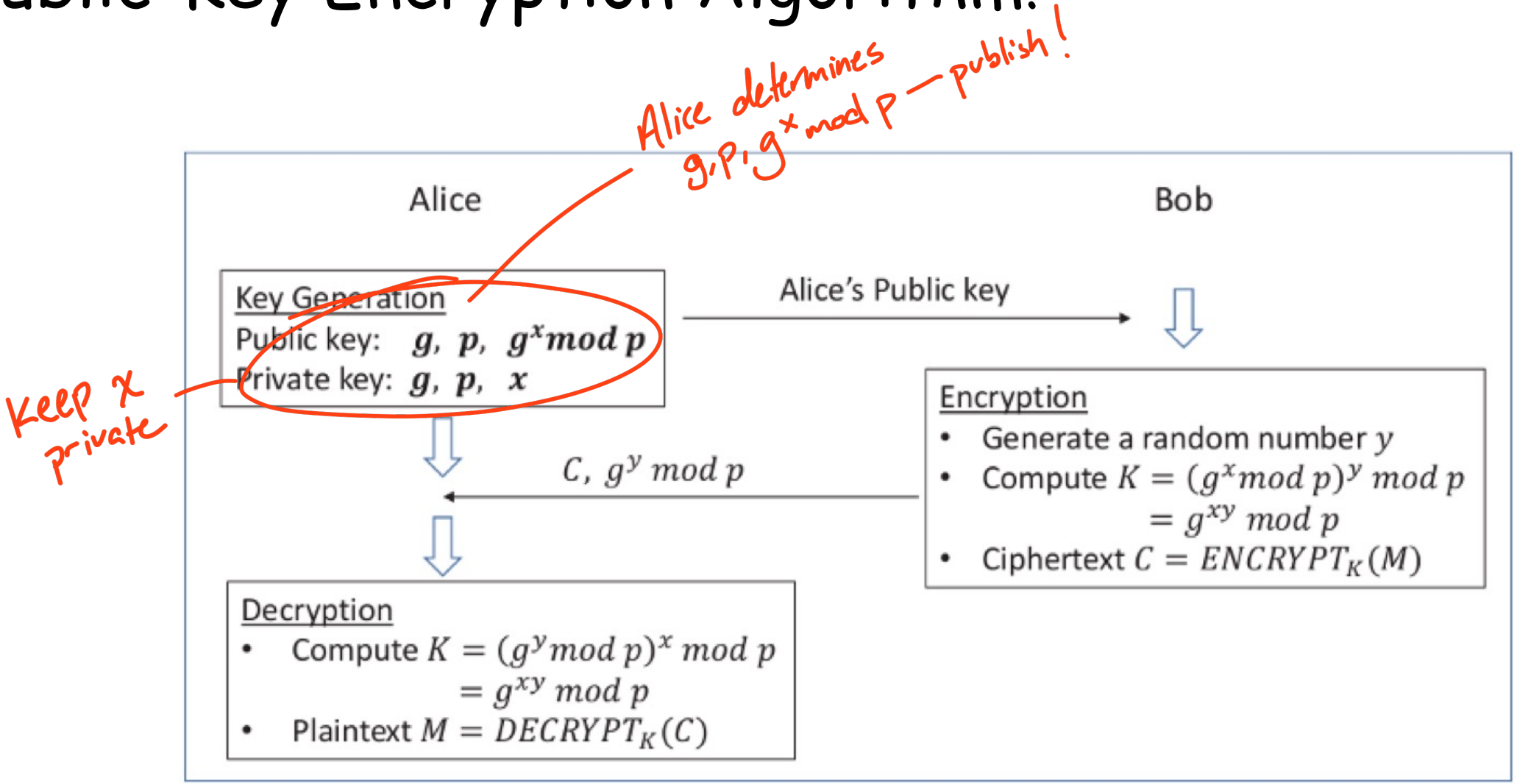
- DH key exchange protocol allows two parties to exchange a secret

- Protocol can be tweaked to turn into a public-key encryption scheme if…
  - **Public key**: known to the public and used for encryption
  - **Private key**: known only to the owner, and used for decryption
  - Establish algorithm(s) for encryption and decryption

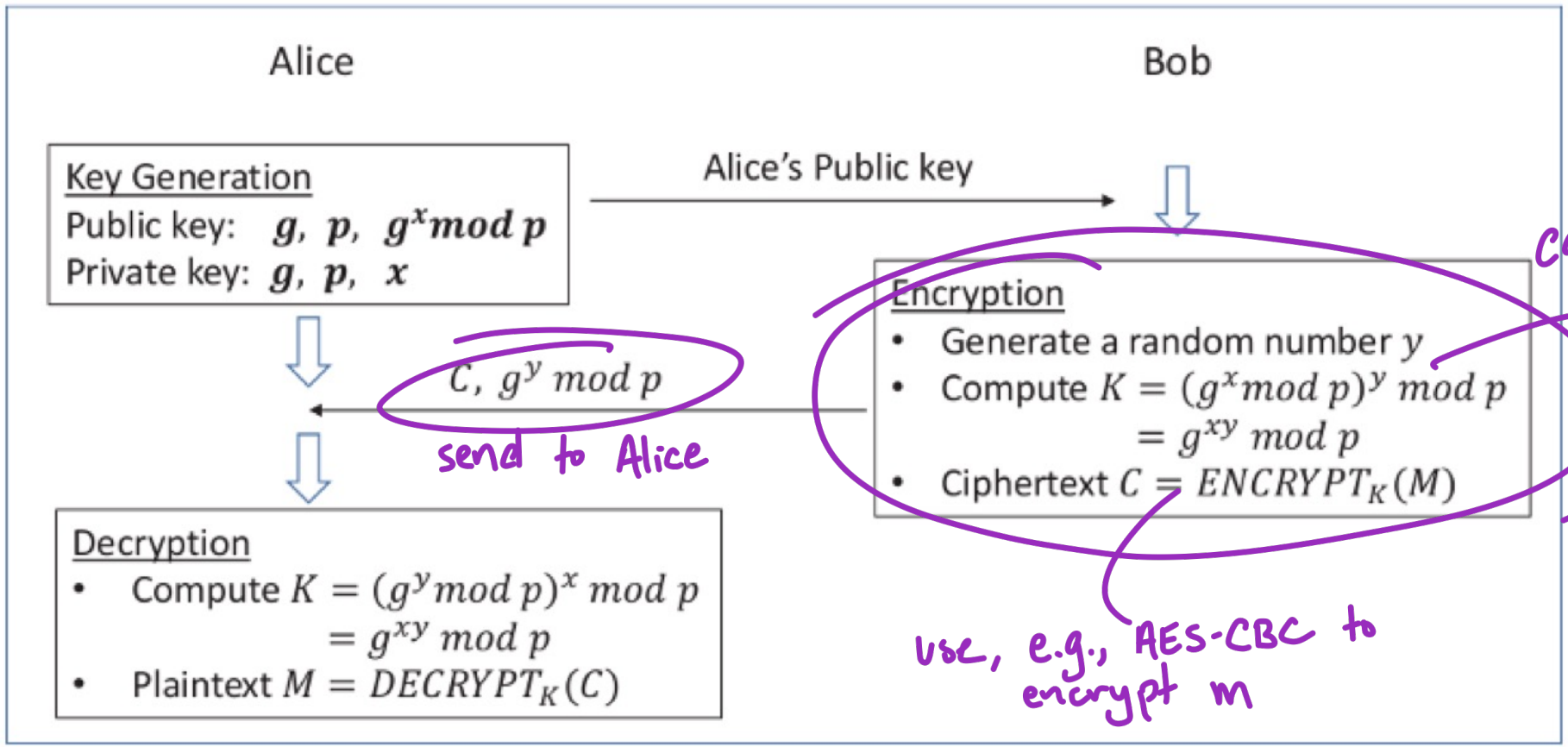
Turn DH Key Exchange into a Public-Key Encryption Algorithm!



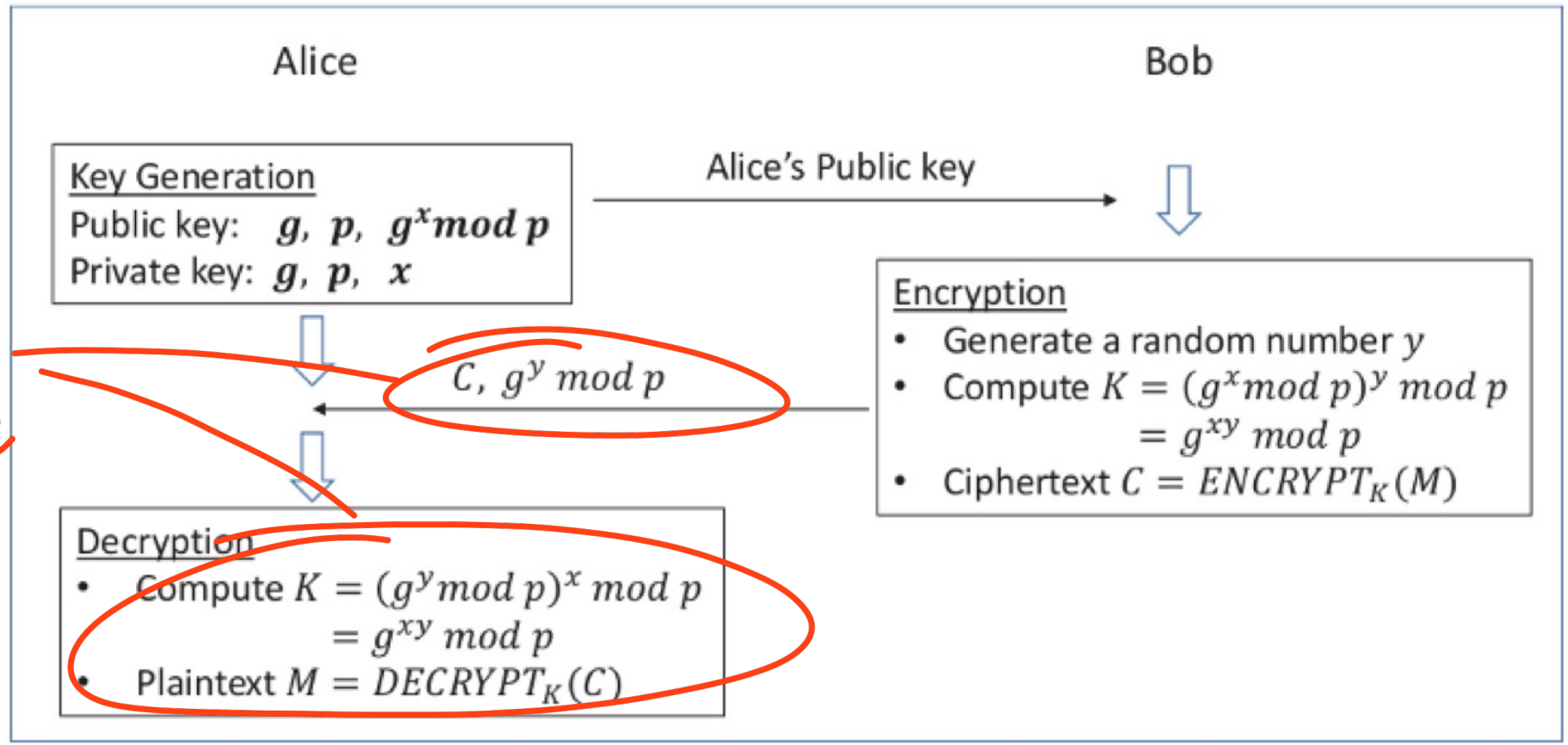
Turn DH Key Exchange into a Public-Key Encryption Algorithm!



Turn DH Key Exchange into a Public-Key Encryption Algorithm!



Turn DH Key Exchange into a Public-Key Encryption Algorithm!



Given info from Bob, compute K & decrypt C