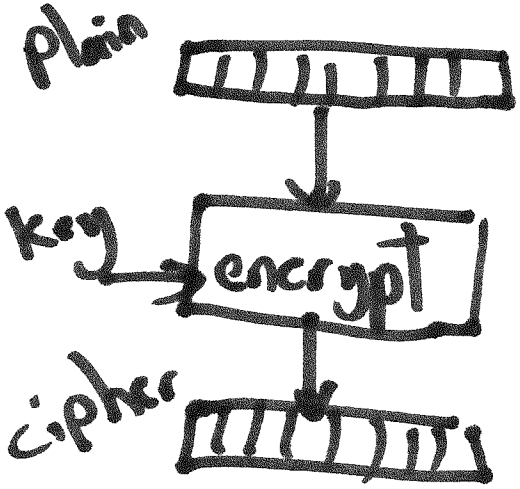
9/5

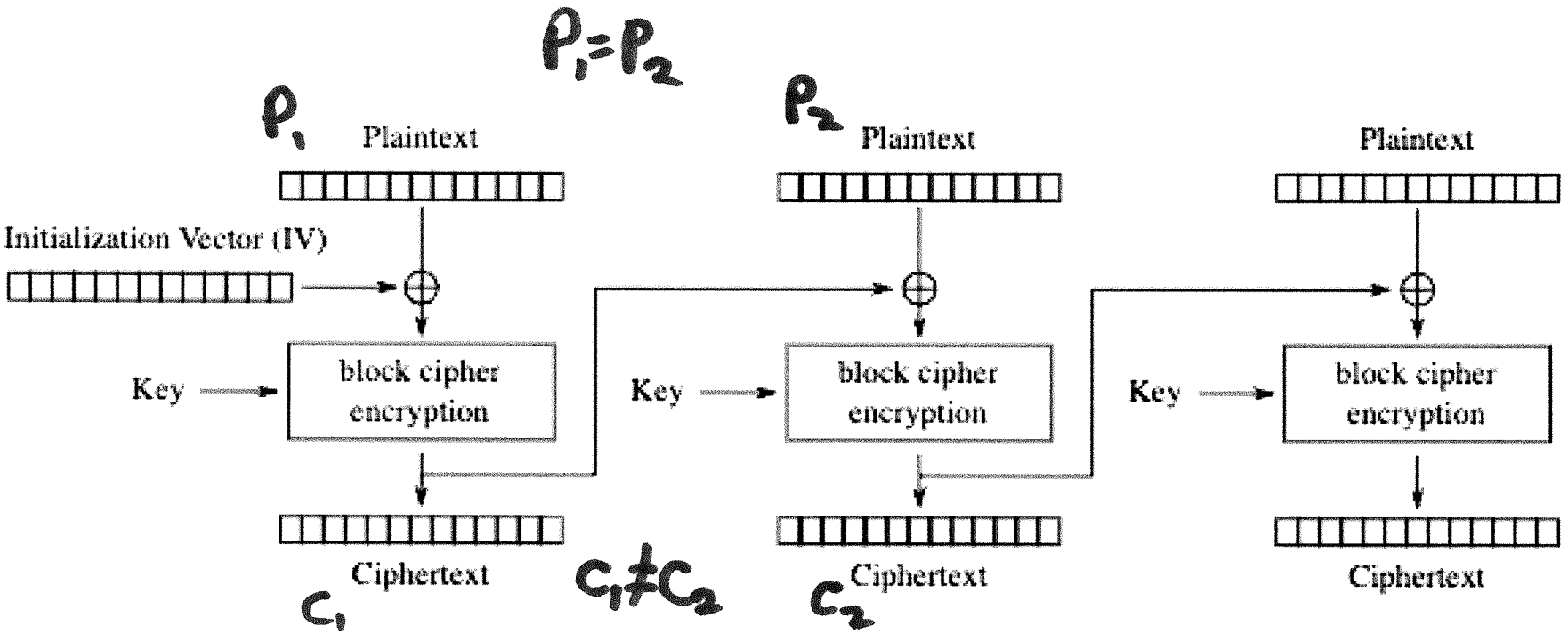
Stream Cipher: one char/byte at a time

Block Cipher: groups of bytes (8 or 1)



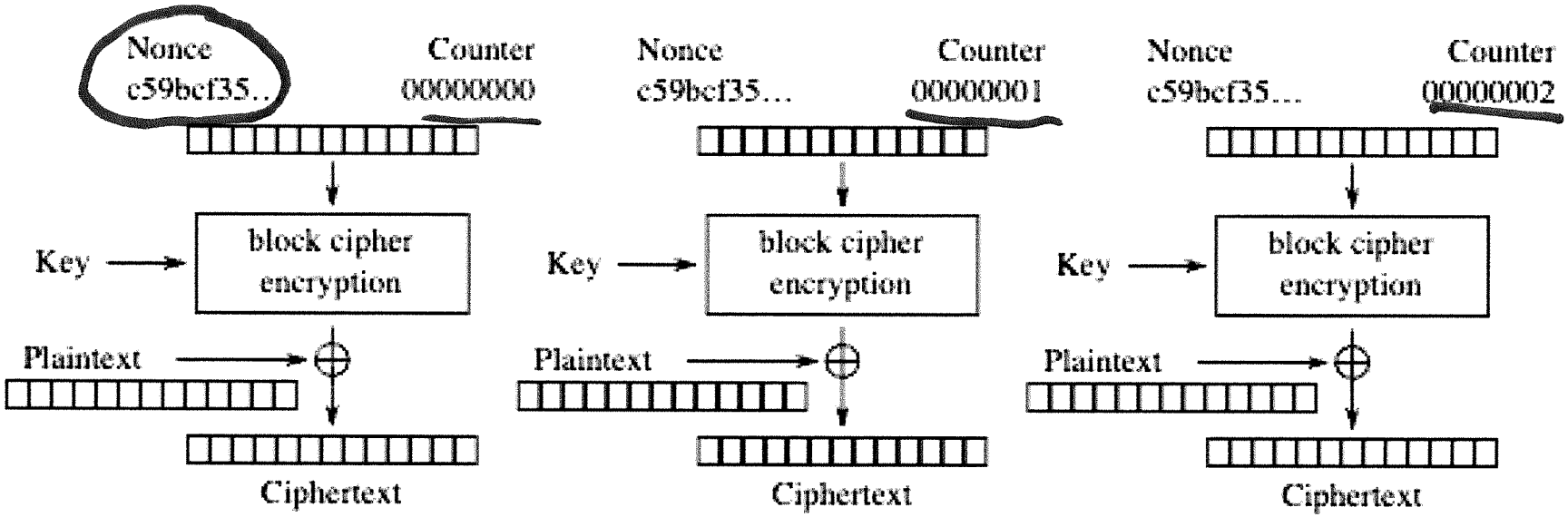
Electronic Codebook

Cipher Block Chaining



Cipher Block Chaining (CBC) mode encryption

Counter

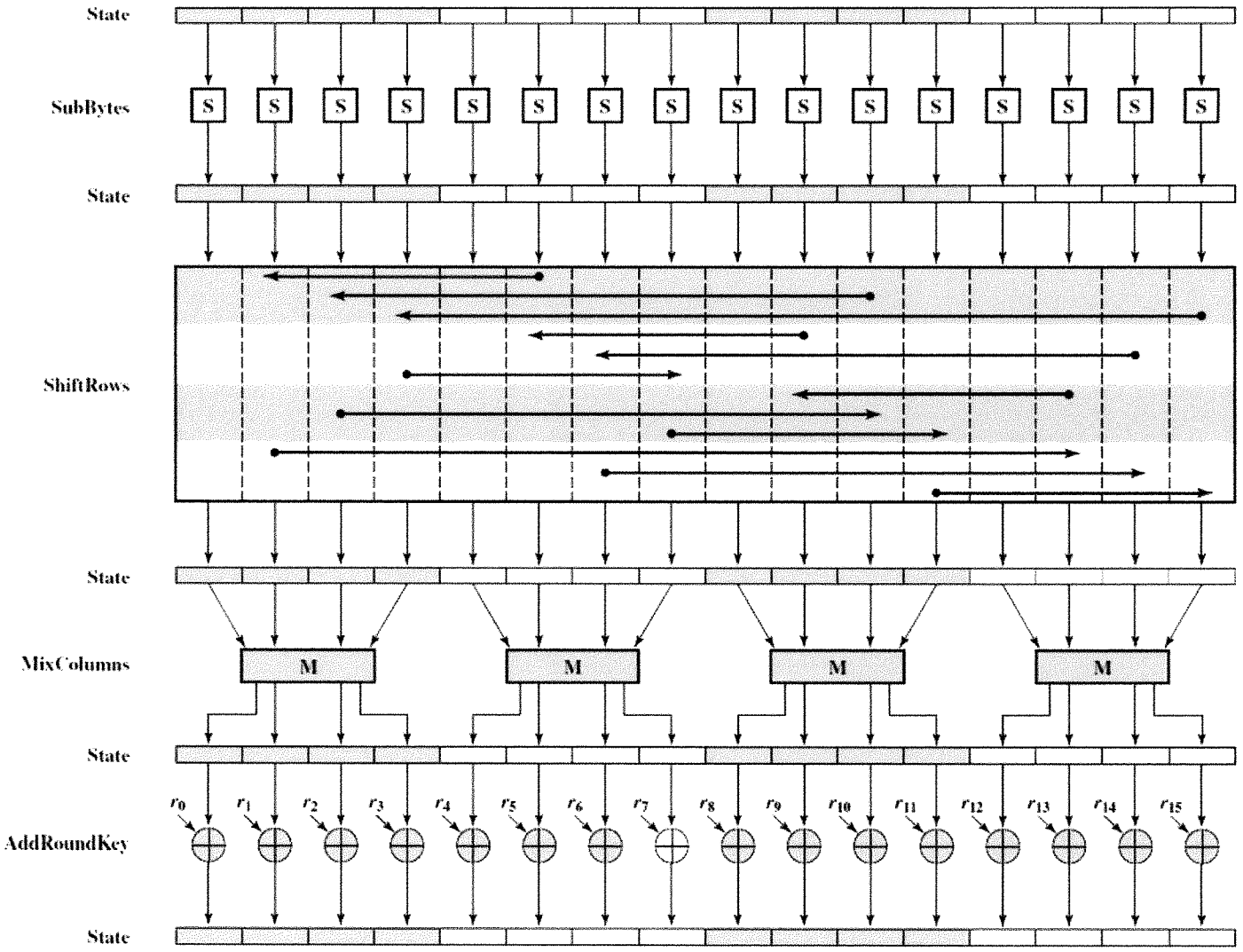


Counter (CTR) mode encryption

Advanced Encryption Standard

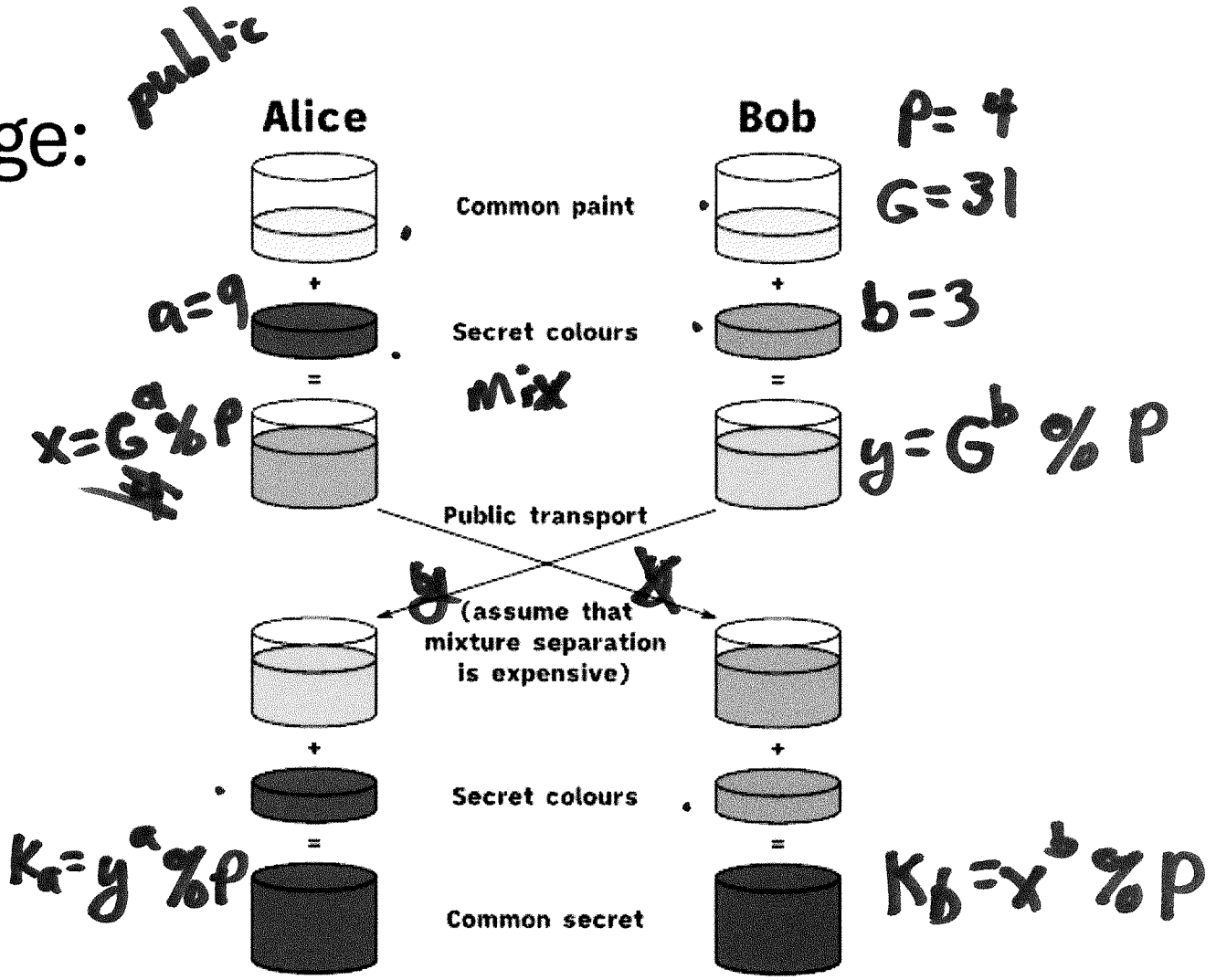
AES

- Block 128 bits
- Keys: 128, 192, 265 bits.
- 10-14 Rounds.
- Create round keys.



Key Exchange:

- Diffie-Hellman
- Generate a key
- Do not transmit



Hashes

- function: many to one
  e.g. length of a word

  hello ⇒ 5
  there ⇒ 5

  can't decode

---

passwords
- store a hash of the password