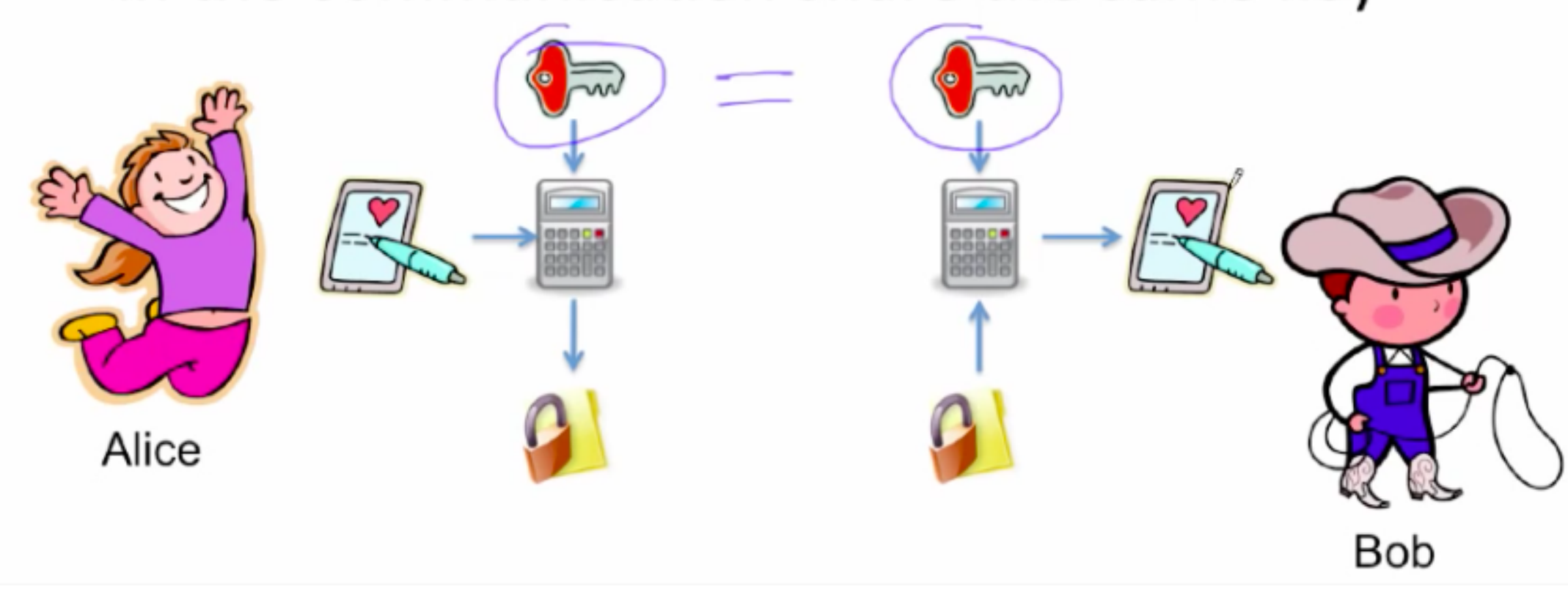
Symmetric Key Cryptography

- In symmetric cryptography both the parties in the communication share the same key.

- A cryptographic technique where both parties in the communication share the same key



There are two types of Symmetric key Cryptography

1. Stream Ciphers
2. Block Ciphers

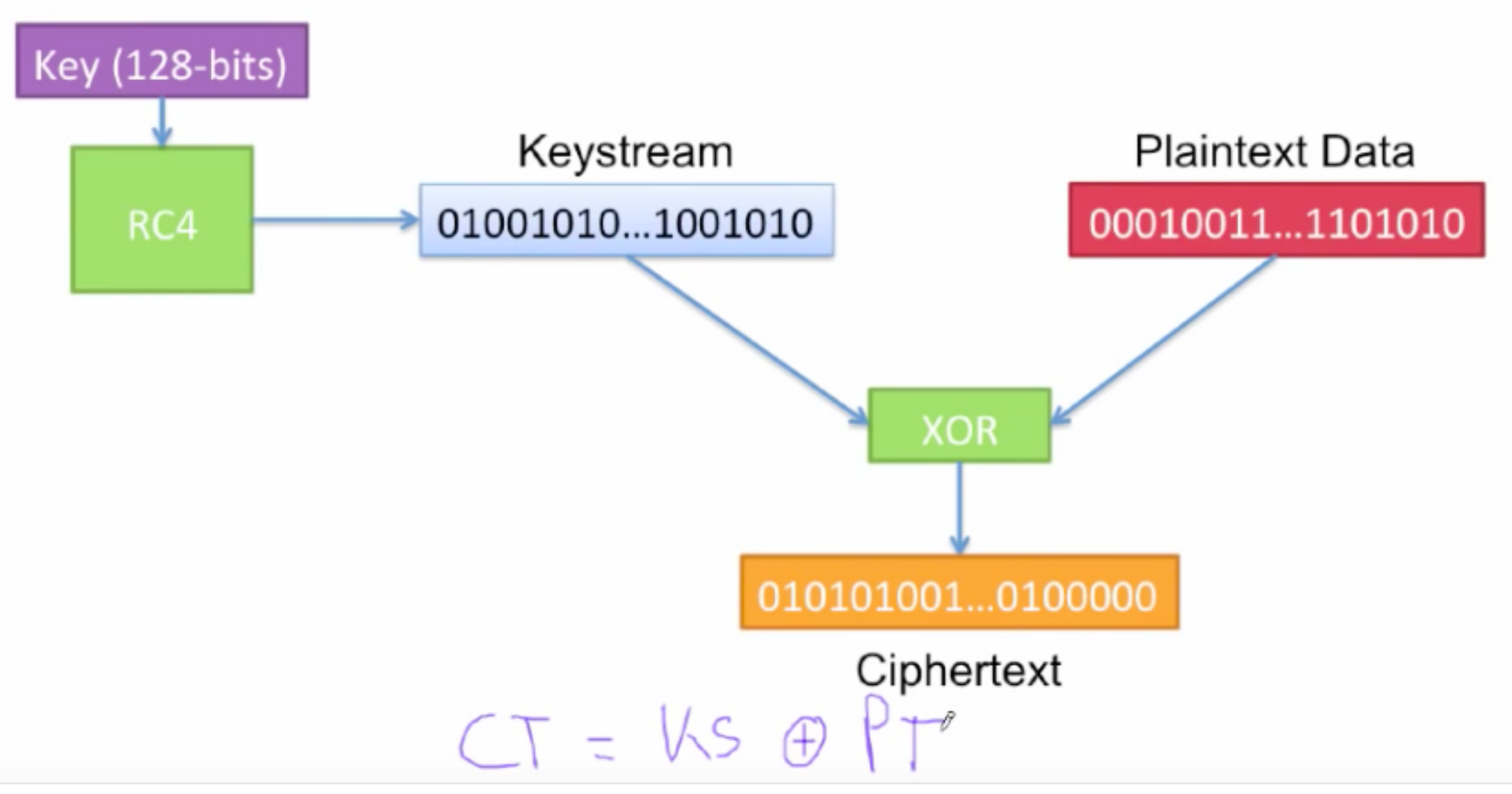
Stream Ciphers

- Type of symmetric key crypto
- Use a fixed length key to produce a pseudo-random stream of bits
  - Same key gets you the same stream
- XOR those bits with your PT in order to encrypt
- XOR those same bits with your CT in order to decrypt
- Tries to approximate a one-time-pad

Real-world stream ciphers

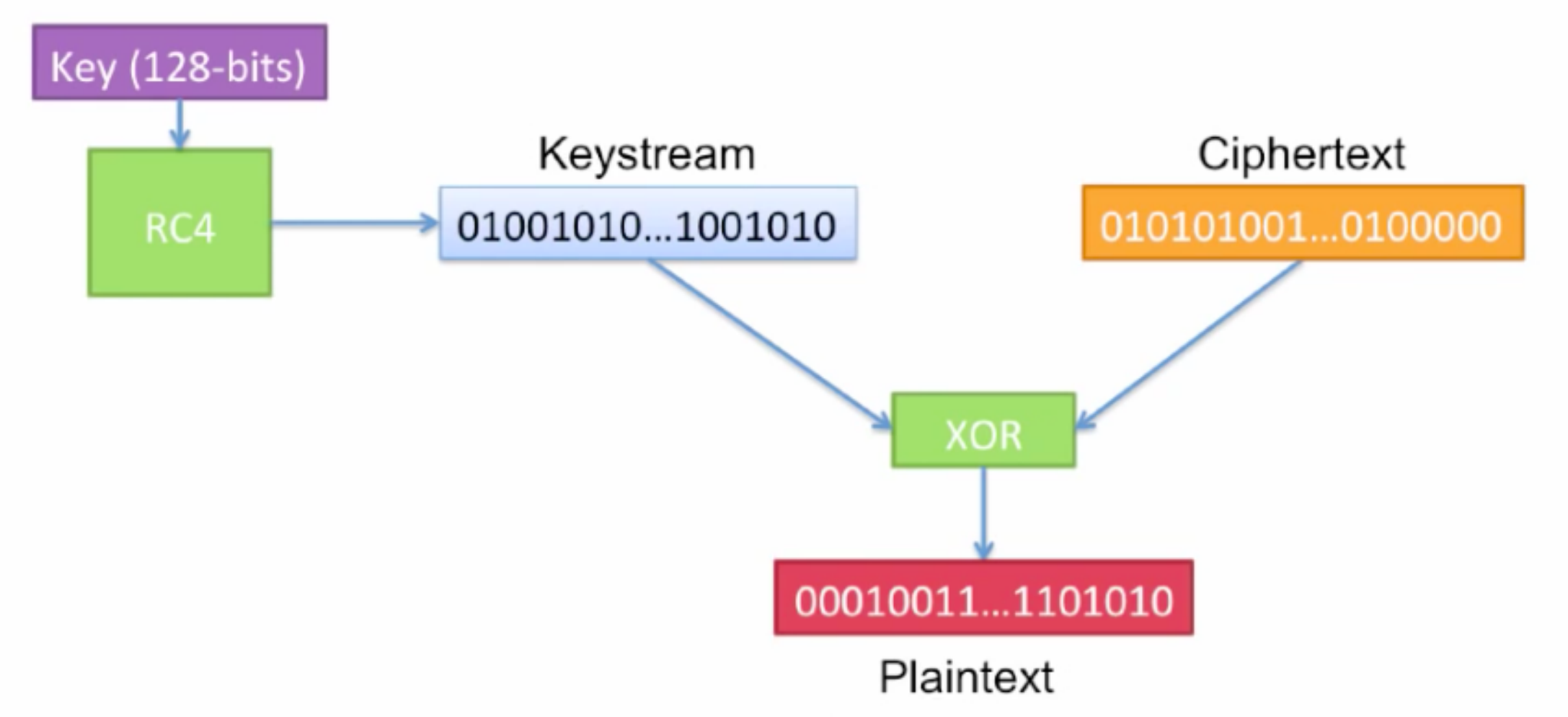
- RC4
  - Used in WEP for wireless network security
  - One option in TLS/HTTPS for encrypting web traffic
  - Not recommended for use anymore
- A5/1
  - Use for encrypting GSM phone data and conversations
  - NSA is known to be routinely breaking it

Stream Cipher Encryption Example:



$CT = Ks \oplus PT$

Stream cipher Decryption Example:



$PT = Ks \oplus CT$

XOR Example -

- Encrypt
  - Plaintext: 0110
  - Key Stream: 1100
  - Ciphertext: 1010
- Decrypt
  - Ciphertext: 1010
  - Key Stream: 1100
  - Plaintext: 0110

1010

0110

XOR Truth Table

	1	0
1	0	1
0	1	0

Stream - flow of bits.

s. 1) Clear text is shorter than key.
No problem in this case.

2) Clear text is longer than key *
1101 1011   1010

In this case we must reuse the key but we may face some security problems.
→ Multiple bits of the PT are encrypted with same key bit.

→ One-time-pad means key is longer than or equal to clear text.

Block Ciphers

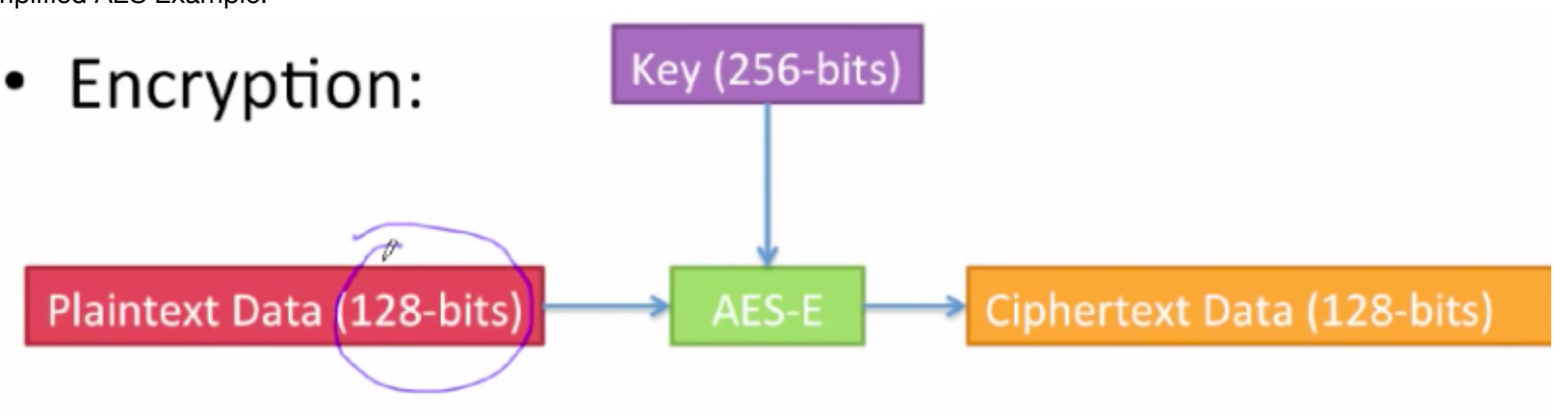
- Block Ciphers uses fixed length key to encrypt a fixed length block of data.

Real World Block Ciphers.

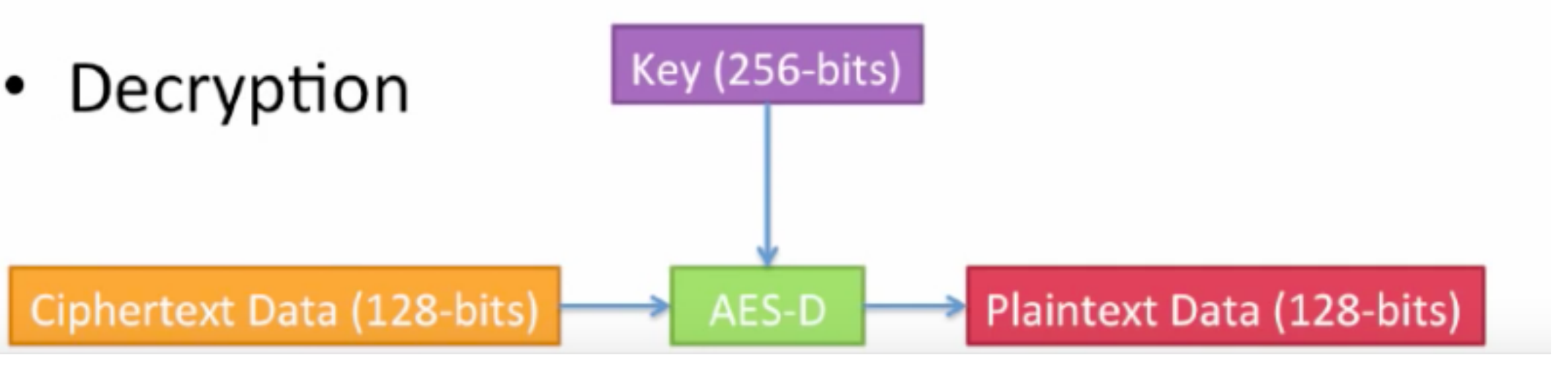
- Data Encryption Standard (DES)
  - 64-bit blocksize
  - 56-bit keysize
  - Released in 1976
  - US government standard until 2001
- Advanced Encryption Standard (AES)
  - 128-bit blocksize
  - 128, 192, or 256 bit key size
  - Current US government standard
  - Most widely used
  - Considered very secure

Simplified AES Example:

- Encryption:



- Decryption



Some of the properties of Block Ciphers

- Plaintext to CT mappings must be 1-to-1 for a given key
  - This means the same PT always become the same CT (and vice-versa)
- Input and output should have no correlation
  - Change 1-bit of the input block, and the change on the output should not be distinguishable from random

~50 % of bits should change

1 to 1 mapping

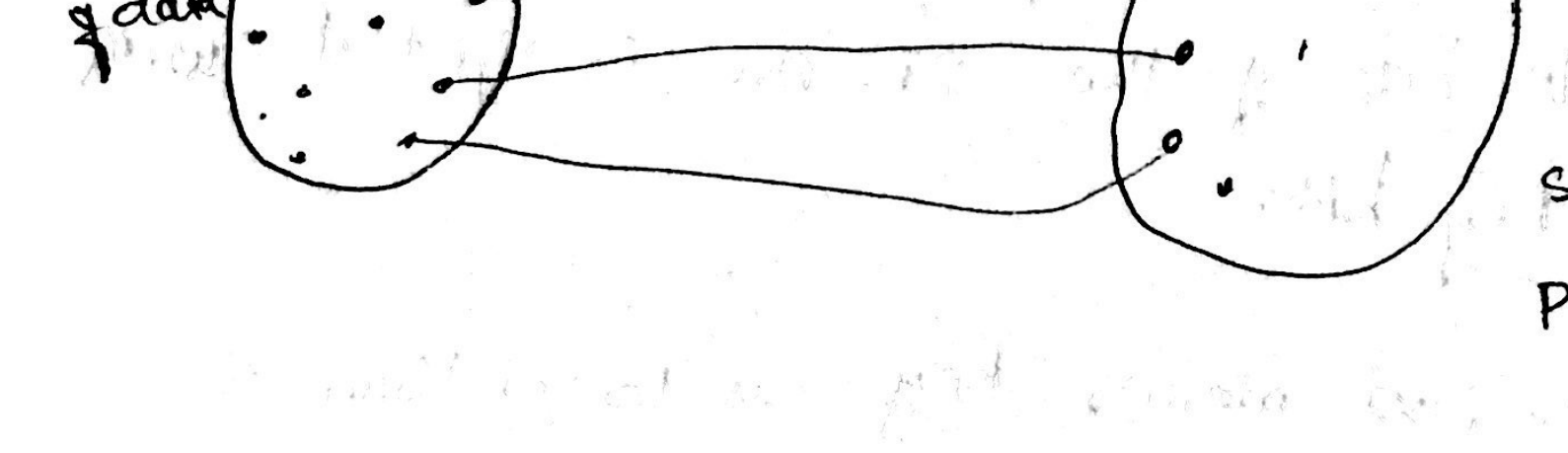
64 bit clear texting

128 bit key.   after Encryption → Cipher text
size ≥ clear Text.

∴ size of cipher Text ≥ clear Text.

64 bit clear Text ⇒ 2^{64} blocks   128 bit key
0 1 1 0 ...

space of plain Text (Clear Text)   space of Cipher Text



Since the mapping is one-to-one There should be same size of CT as P.T.