Symmetric Key Cryptography

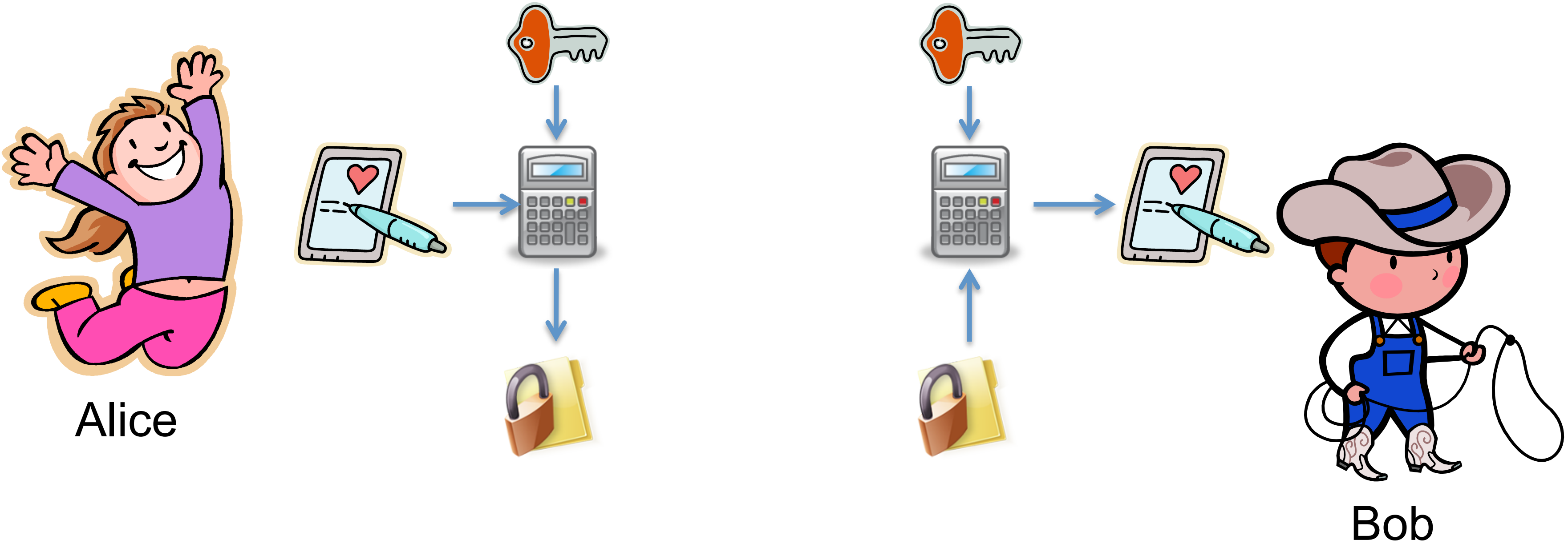
Introduction to Basic Cryptography

Dr. Ryan Riley

جامعة قطر
QATAR UNIVERSITY

Recall…

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



Two Types of Symmetric Crypto

- Stream Ciphers

- Block Ciphers

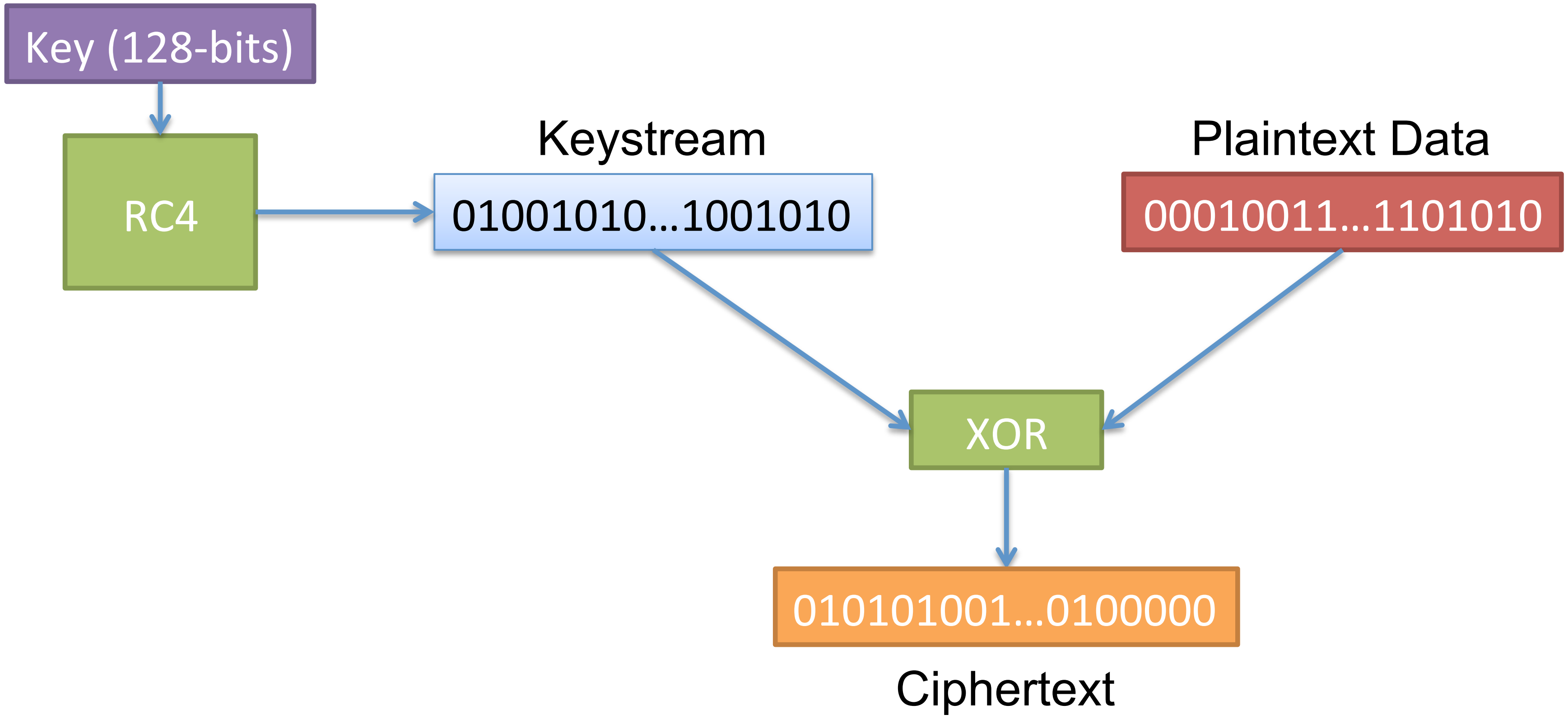
Stream Ciphers

- 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

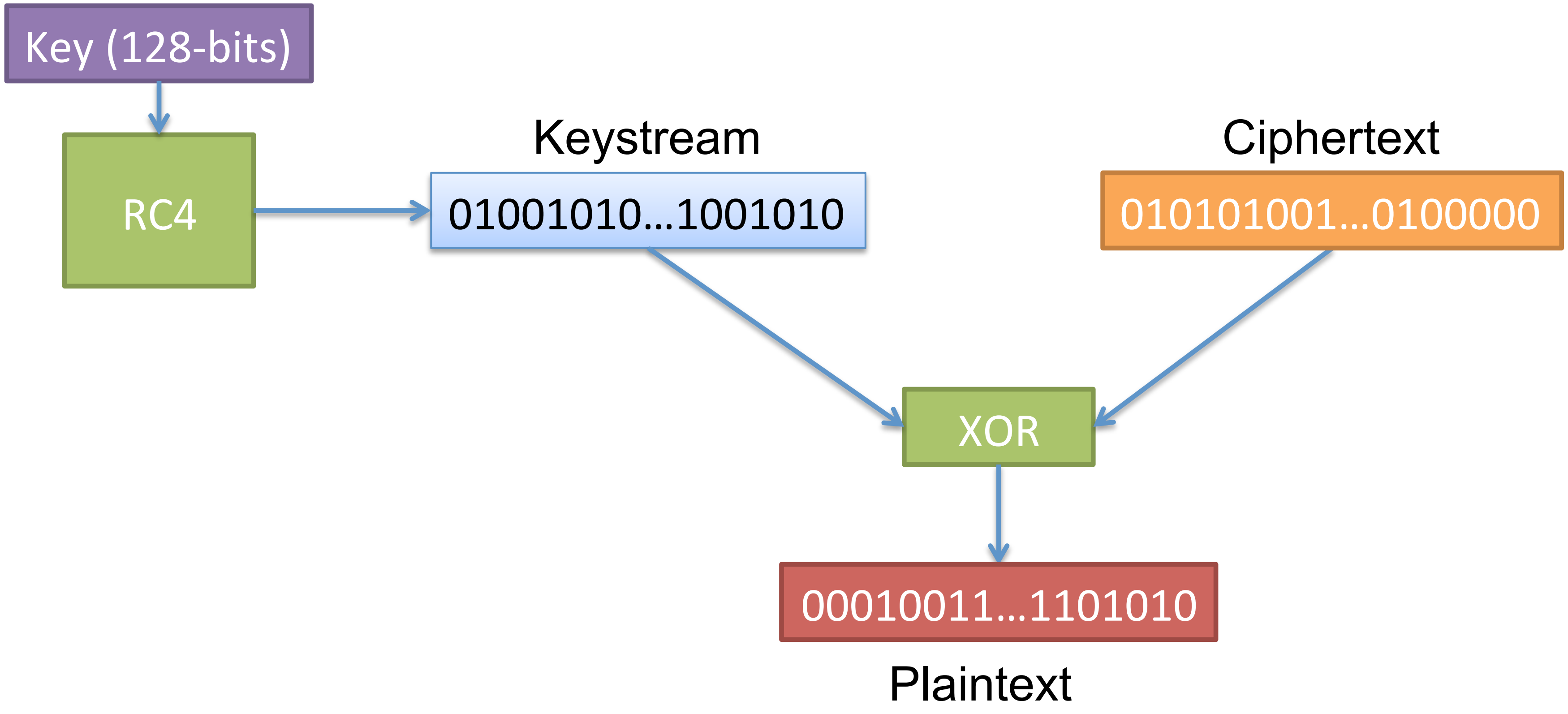
Real-Word Stream Ciphers

- 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



Stream Cipher Decryption Example



Using XOR with a Stream Cipher

- Using XOR for encryption:

$$CT = PT \oplus KS$$

- Using XOR for decryption:

$$PT = CT \oplus KS$$

XOR Example

- Encrypt

Plaintext:	0110
Key Stream:	1100
Ciphertext:	1010

- Decrypt

Ciphertext:	1010
Key Stream:	1100
Plaintext:	0110

XOR Truth Table

	1	**0**
1	0	1
0	1	0

Intro to Block Ciphers

- Type of symmetric key crypto
- Use a fixed length key to encrypted a fixed length block of data

- For example, a 64-bit block of data and a 128-bit key

Intro to Block Ciphers

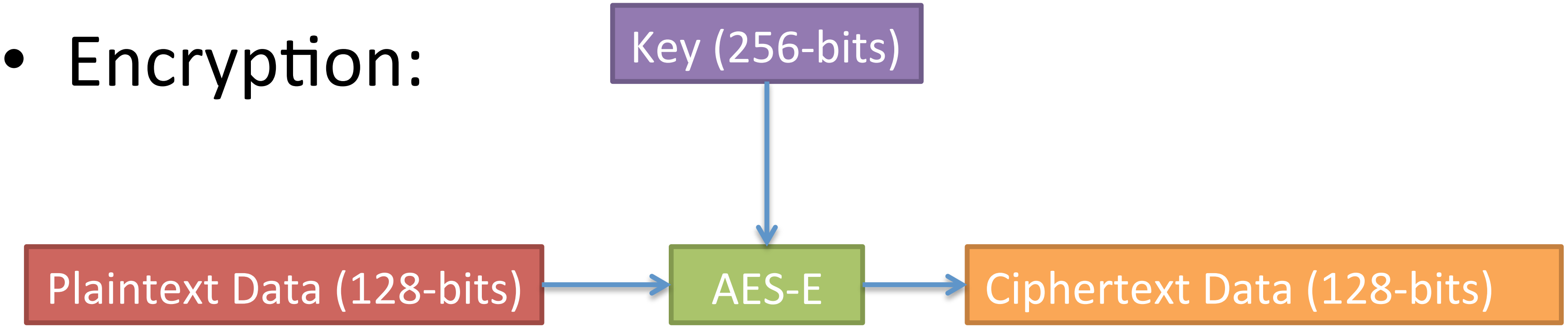
- Similar to a substitution cipher
  - Much larger alphabet!
- Example: If we have a 64-bit block cipher, then our substitution table has 2^{64} entries ($1.8 * 10^{19}$)
  - That's a big substitution table!
  - You would need 125 million 1-terabyte hard drives just to store the table
- Goal of a block cipher: Do this with an algorithm and a small key

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:



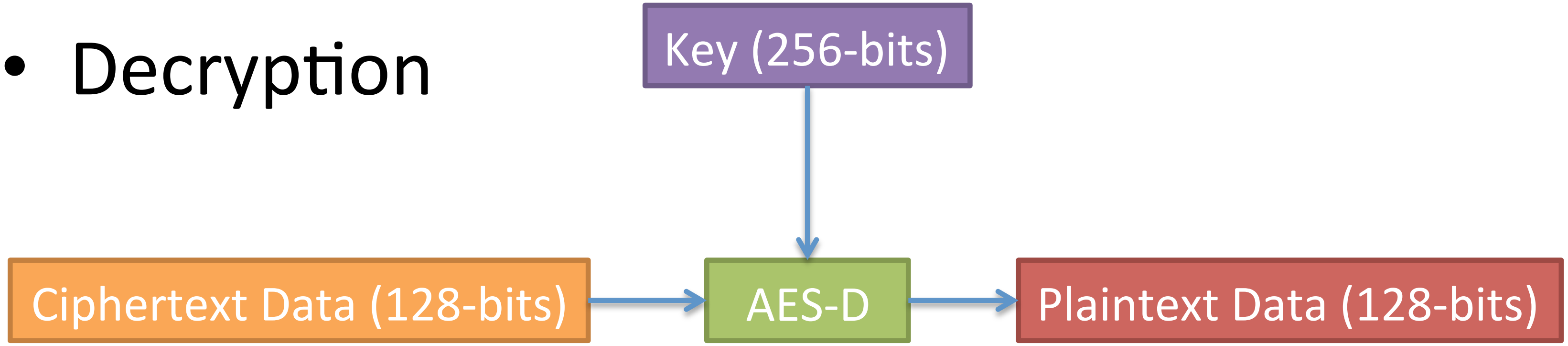
Key (256-bits)

Plaintext Data (128-bits)

AES-E

Ciphertext Data (128-bits)

- Decryption



Key (256-bits)

Ciphertext Data (128-bits)

AES-D

Plaintext Data (128-bits)

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

Features of Block Ciphers

- Block size
  - Bigger is more secure, but probably slower
- Key size
  - Bigger is more secure, but probably slower

Summing Up

- Stream ciphers produce a pseudo-random stream of bits that you XOR with your PT
- Block ciphers are used to encrypt data *one block at a time*
- Sender and receiver need to share the same key