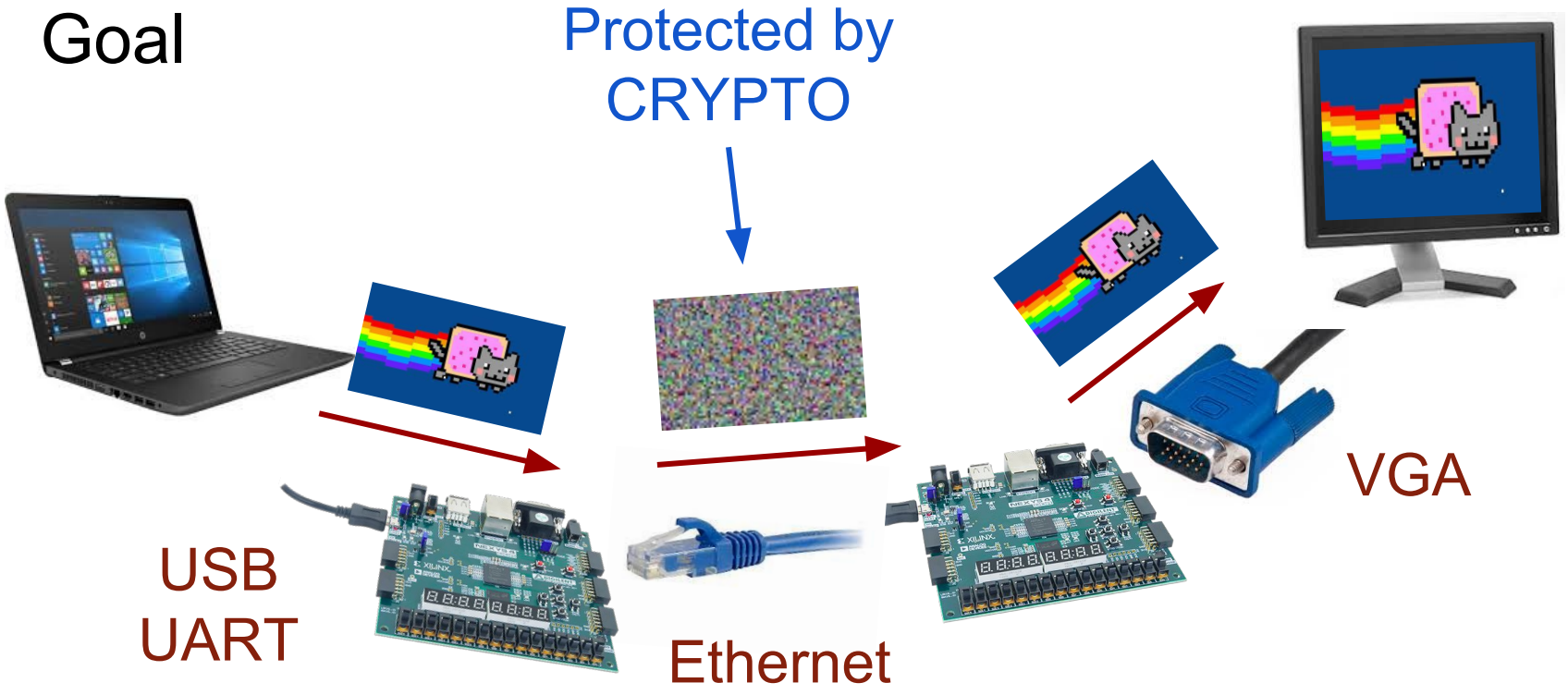
Encrypted Communication over Ethernet

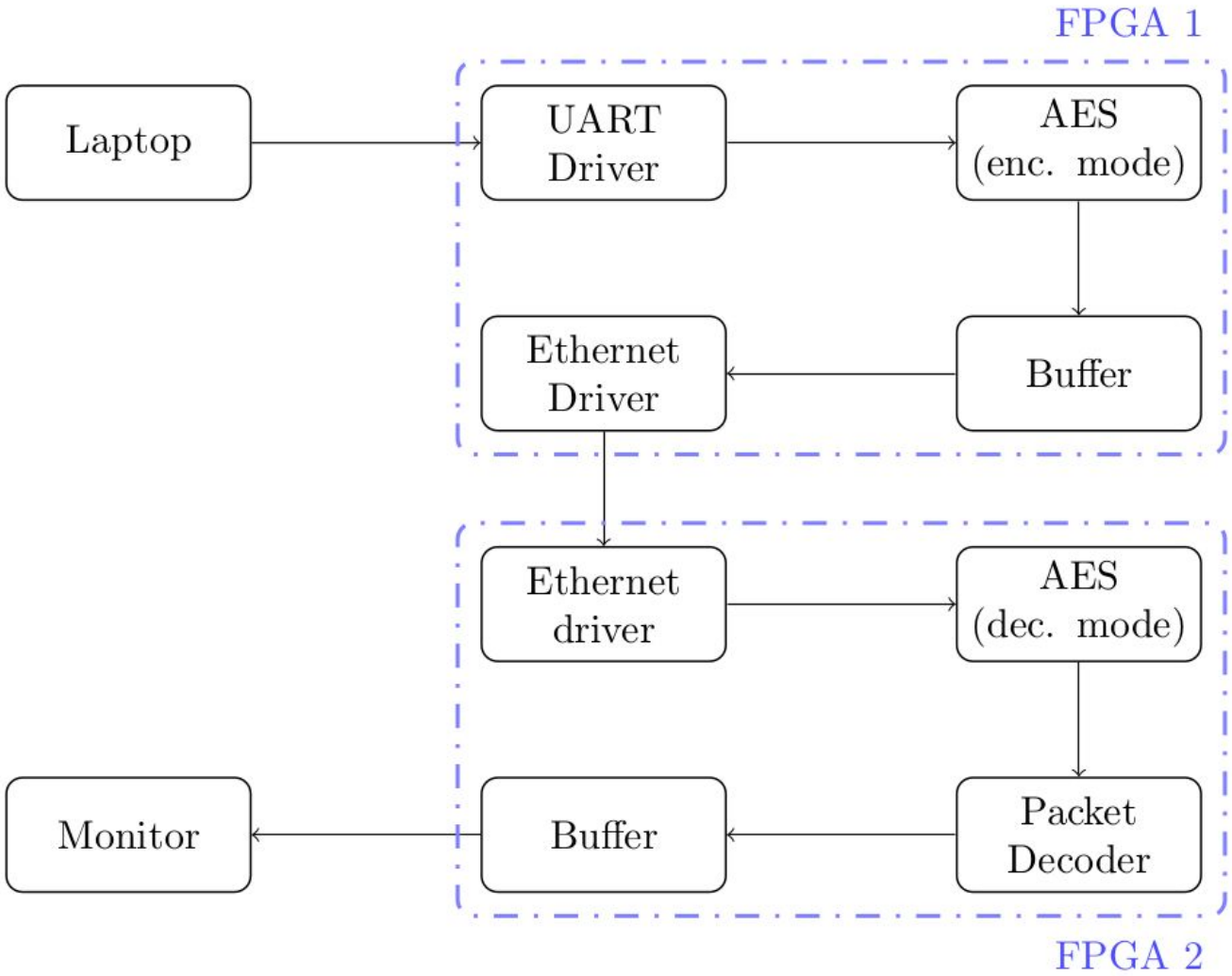
by Ashley and Mark

Overview

- Why do we want this?
  - You want to protect sensitive information
  - Protect the right of people to privacy
  - It’s easier to eavesdrop than users expect
- How do we do it?
  - Implement (minimal subset of) Ethernet standard
  - Use tried-and-true setup of AES

Goal

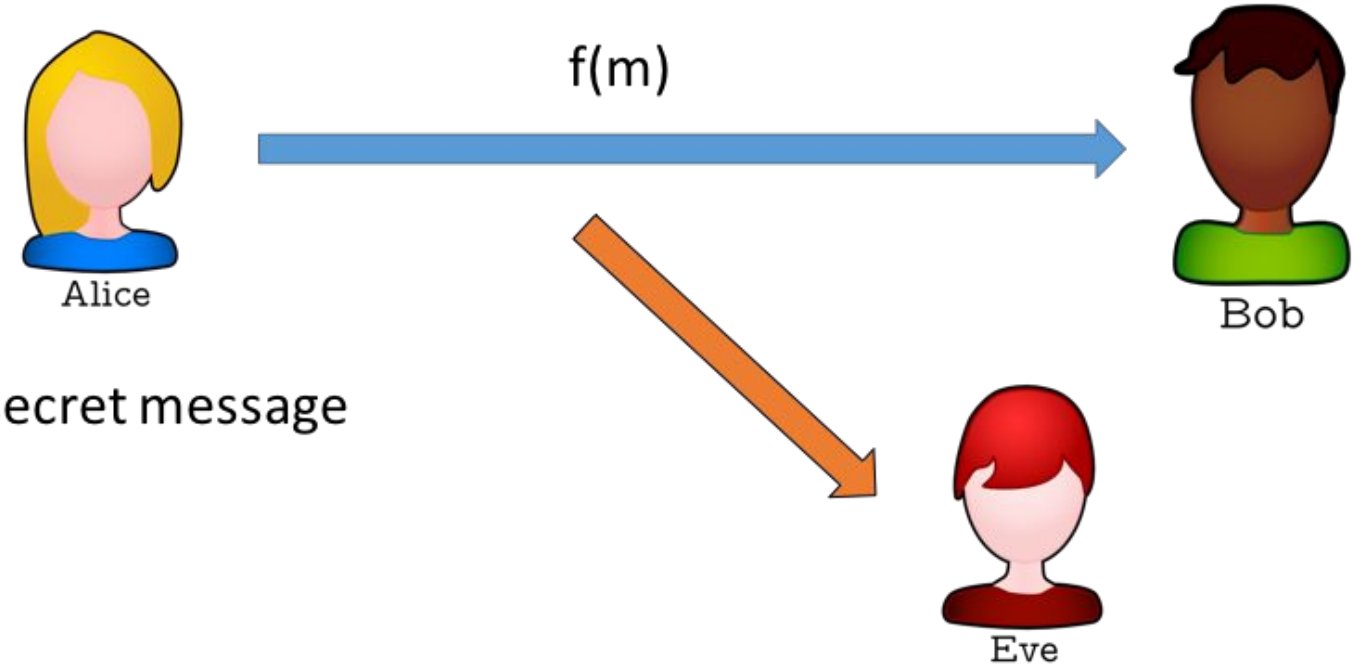




Daisy Chain Structure
=
No Global Coordination Required

(until stretch goals)

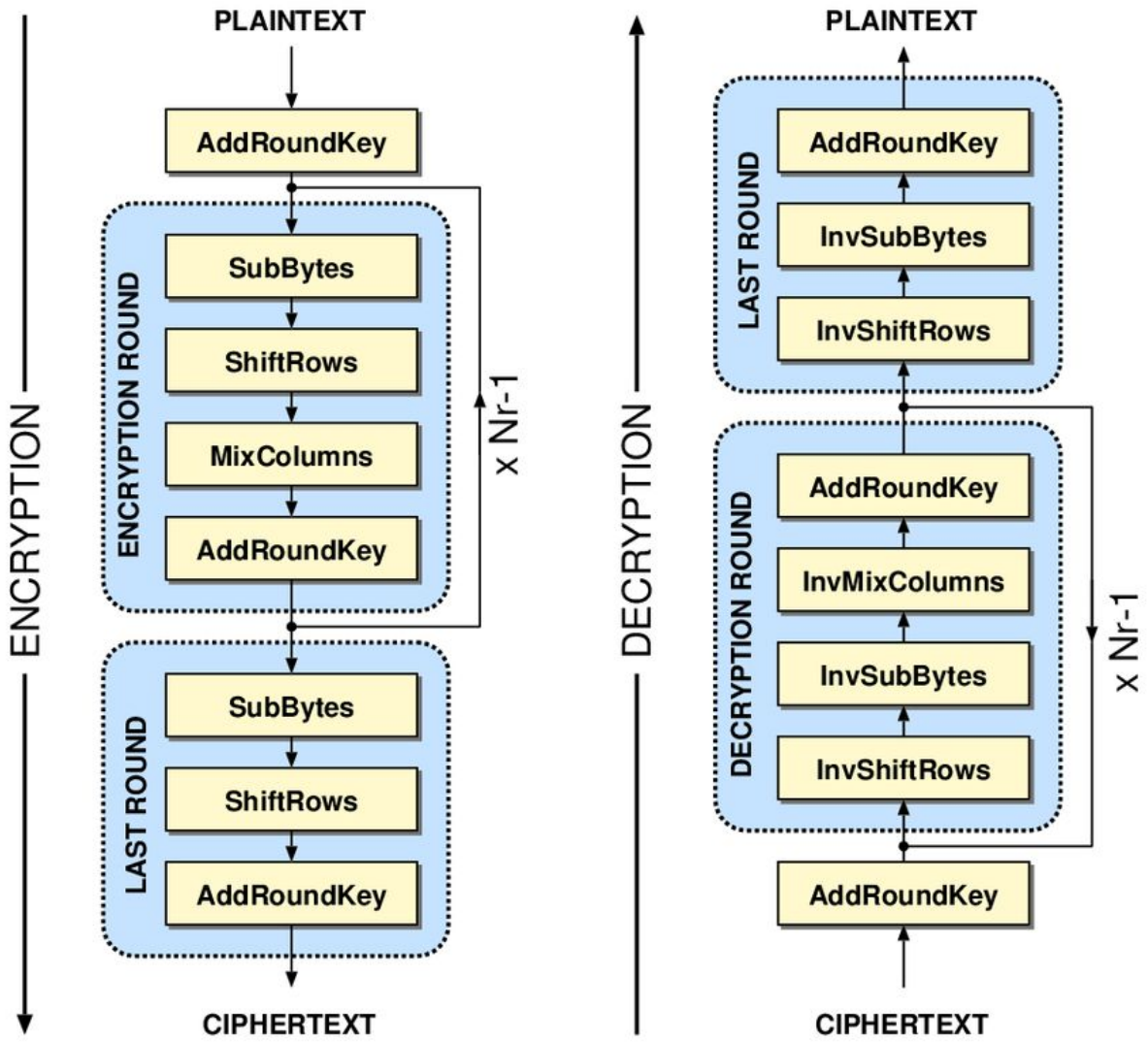
Encryption



m = secret message

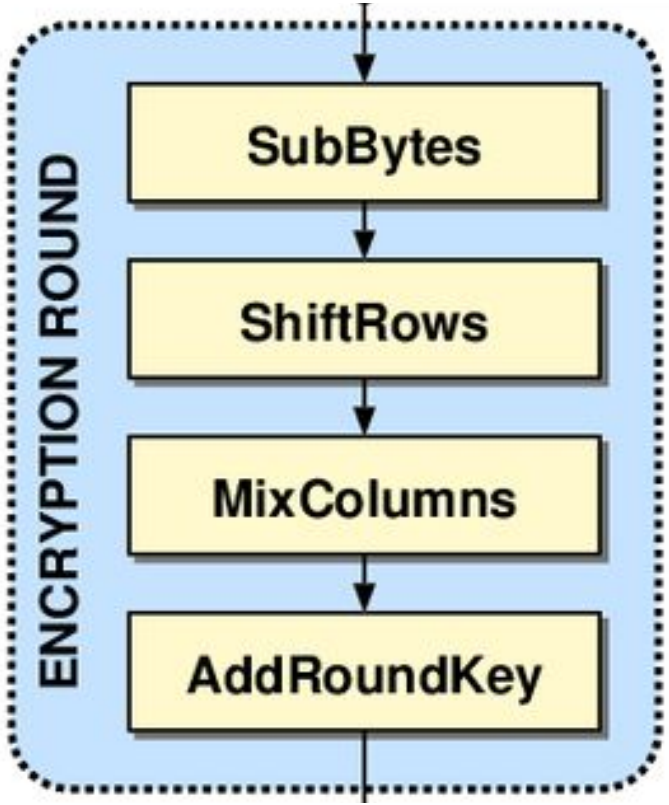
How can we stop Eve from eavesdropping?

AES

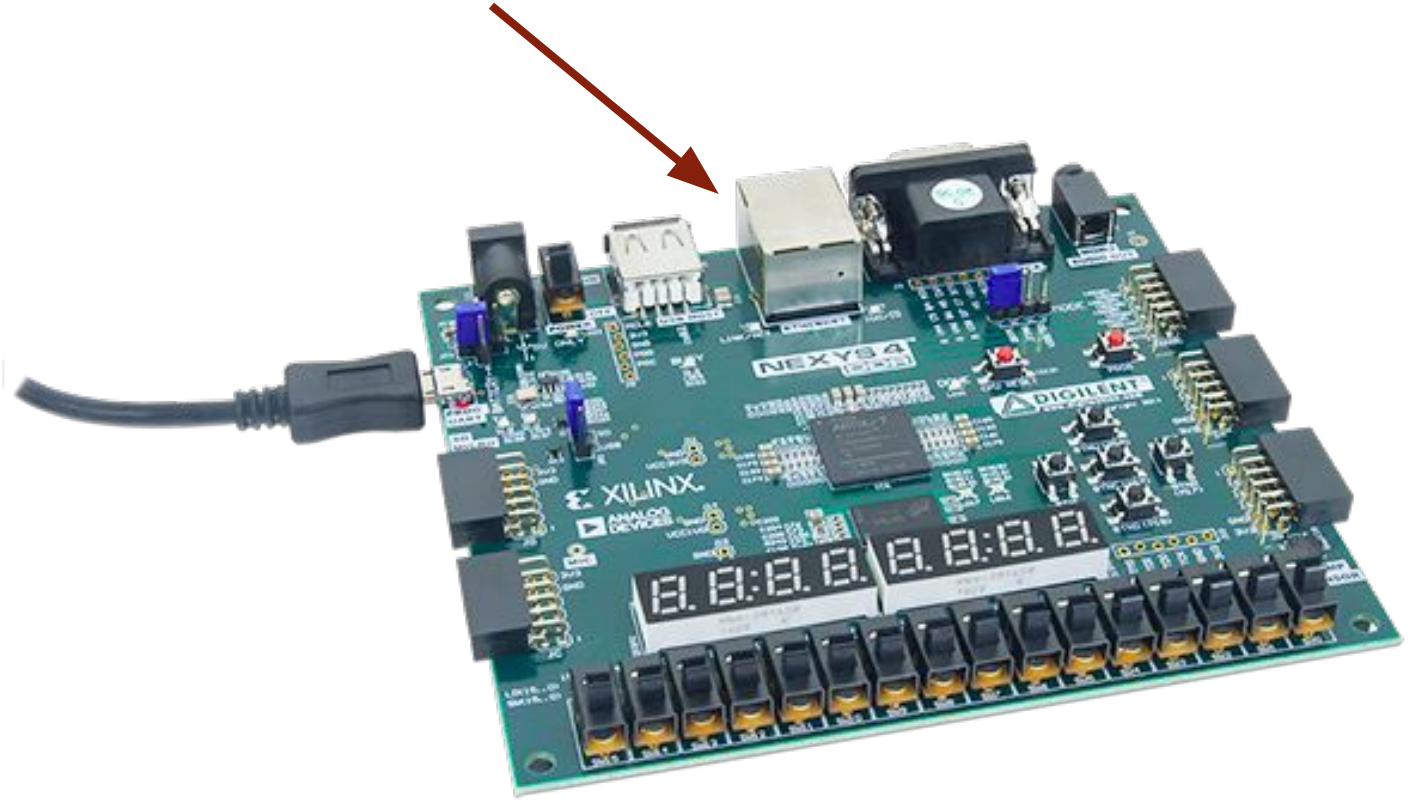

ENCRYPTION
PLAINTEXT
AddRoundKey
ENCRYPTION ROUND
SubBytes
ShiftRows
MixColumns
AddRoundKey
x Nr-1
LAST ROUND
SubBytes
ShiftRows
AddRoundKey
CIPHERTEXT
DECRYPTION
PLAINTEXT
LAST ROUND
AddRoundKey
InvSubBytes
InvShiftRows
DECRYPTION ROUND
AddRoundKey
InvMixColumns
InvSubBytes
InvShiftRows
x Nr-1
AddRoundKey
CIPHERTEXT

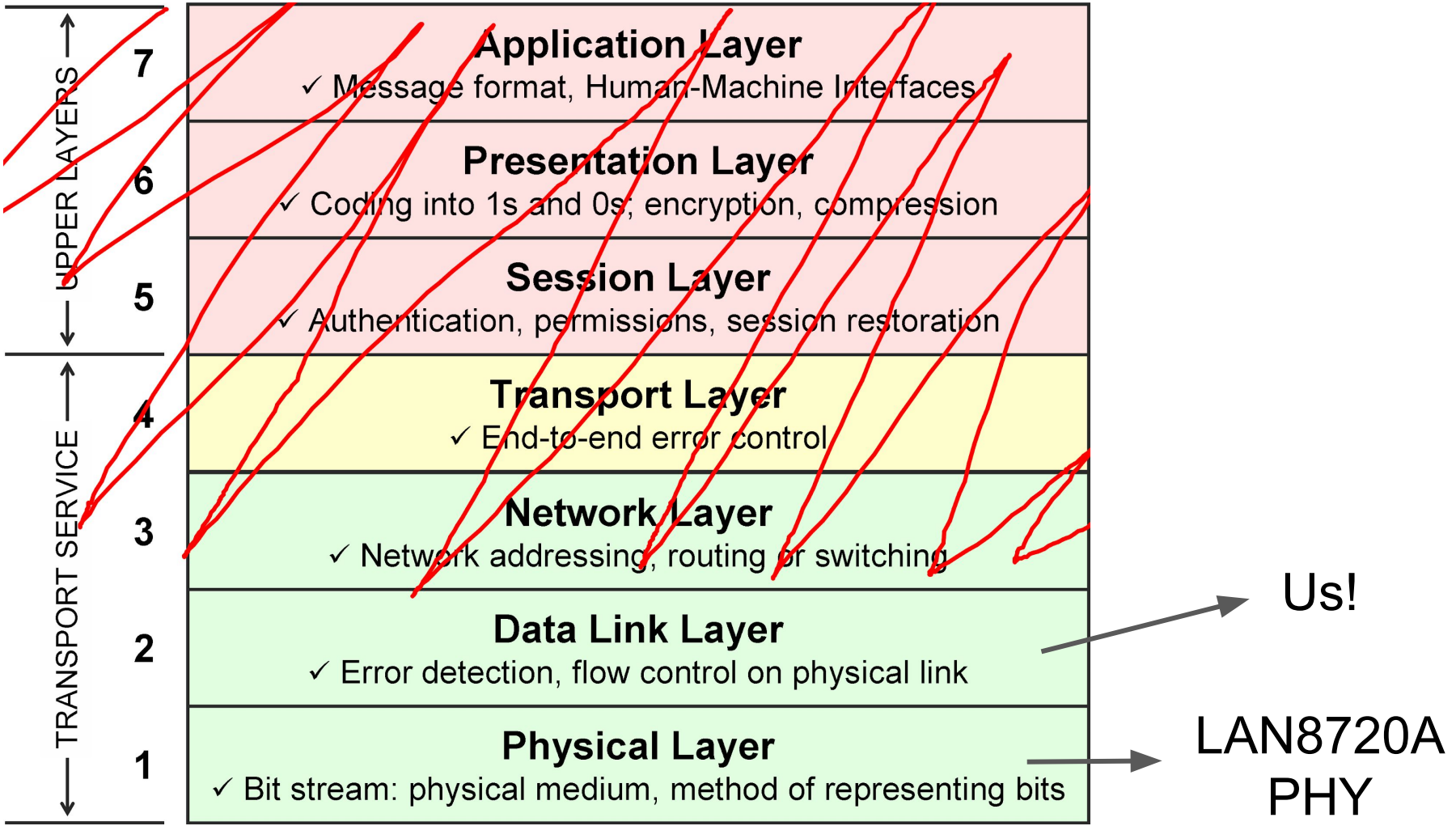
Single Round of Encryption

- Four main steps
  - SubBytes
    - Use a substitution table to replace the byte in the input with different bytes
  - ShiftRows
    - Cyclically shift rows to de-align the columns
  - MixColumns
    - Calculate new columns by taking linear combinations of the input
  - AddRoundKey
    - XOR each byte of input with byte of generated key

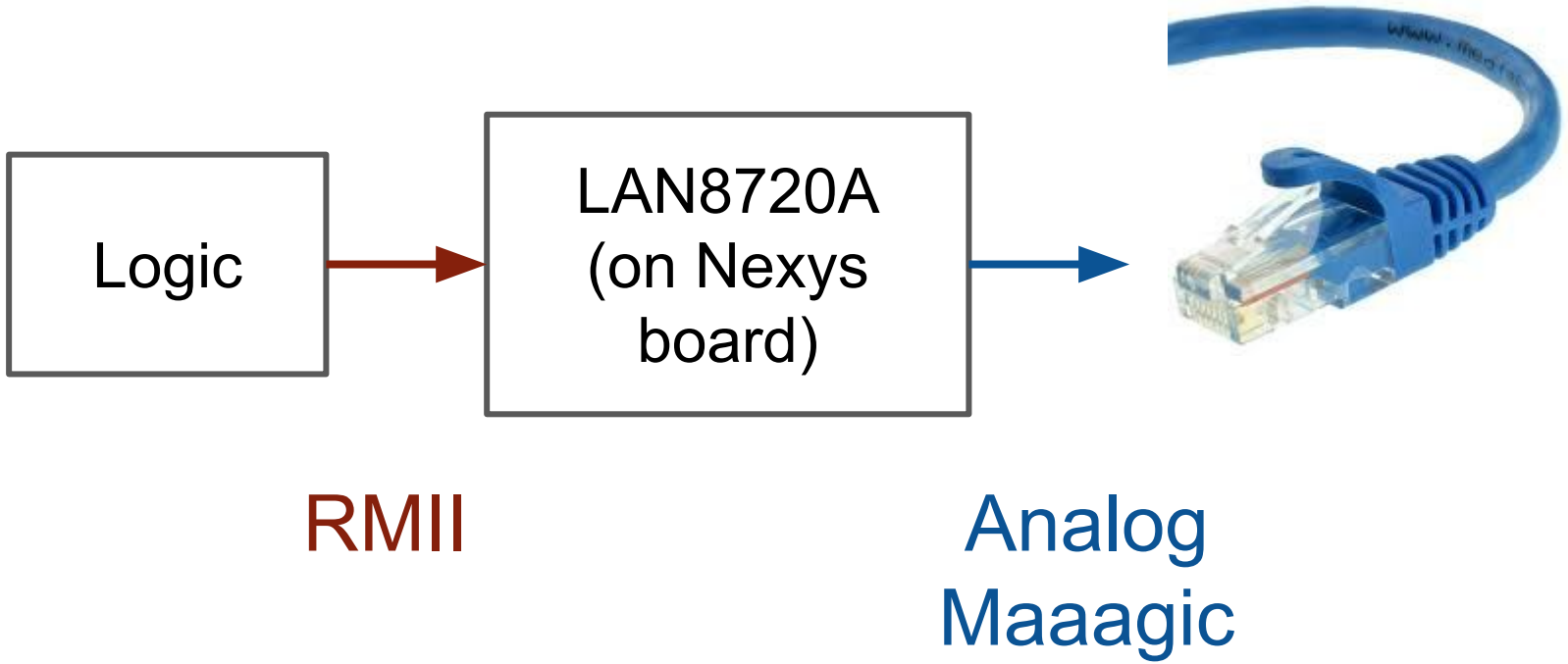


Ethernet Port!!!



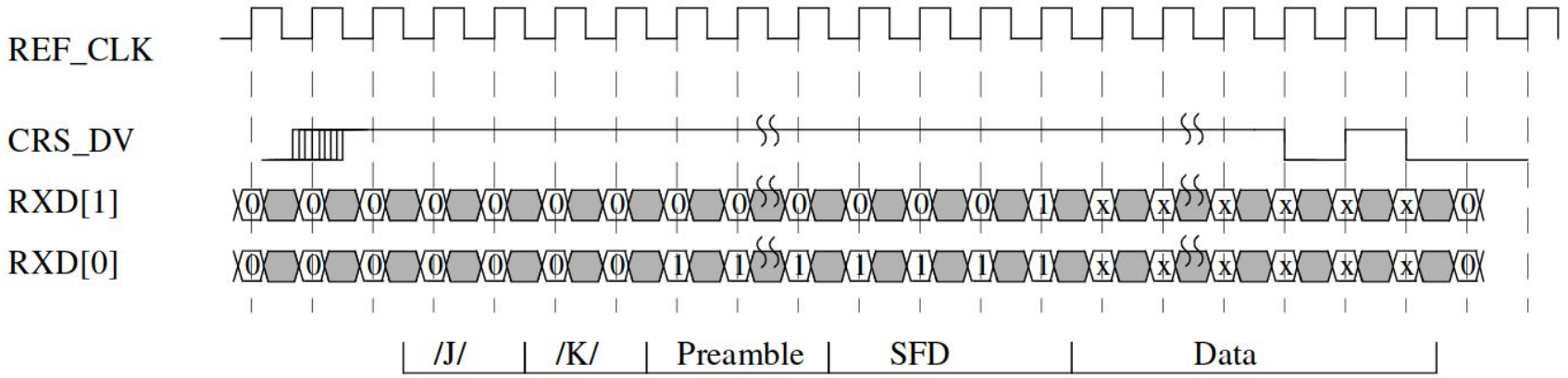

UPPER LAYERS
TRANSPORT SERVICE
7
6
5
4
3
2
1
Application Layer
✓ Message format, Human-Machine Interfaces
Presentation Layer
✓ Coding into 1s and 0s; encryption, compression
Session Layer
✓ Authentication, permissions, session restoration
Transport Layer
✓ End-to-end error control
Network Layer
✓ Network addressing, routing or switching
Data Link Layer
✓ Error detection, flow control on physical link
Physical Layer
✓ Bit stream: physical medium, method of representing bits
Us!
LAN8720A
PHY

Can’t access Ethernet cable directly



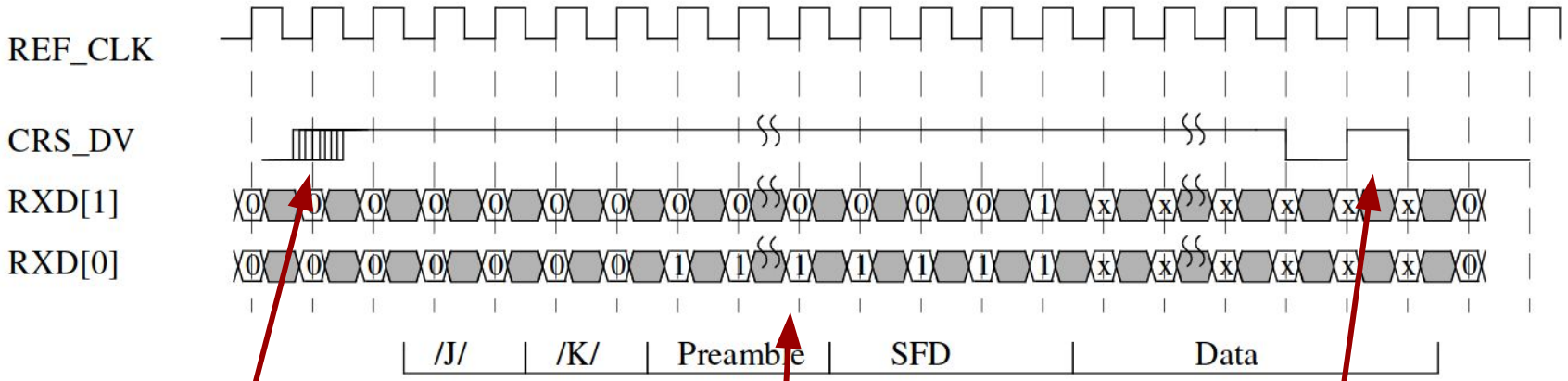
The RMII Interface

(this is just the receive part)



The RMII Interface

(this is just the receive part)

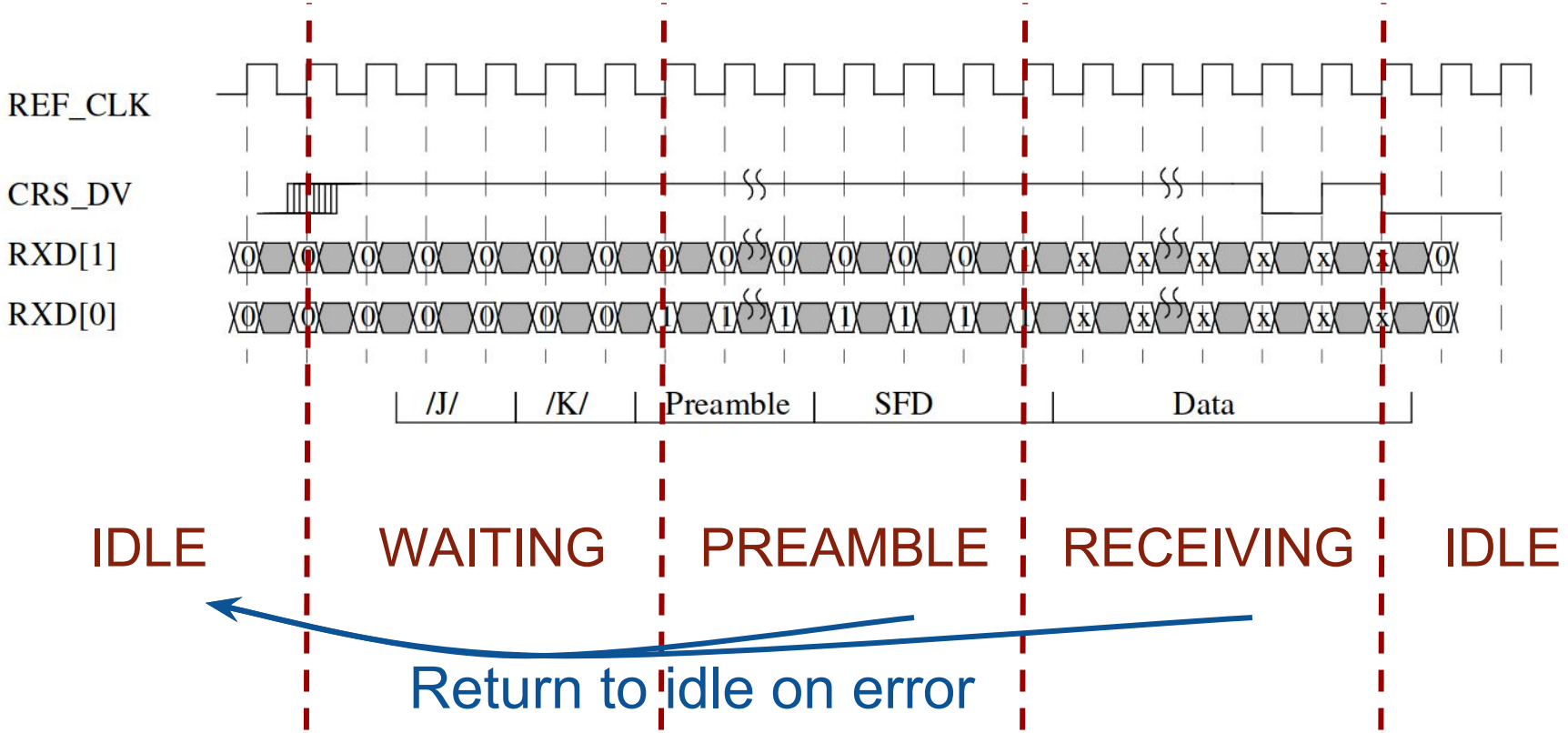


Asserted asynchronously

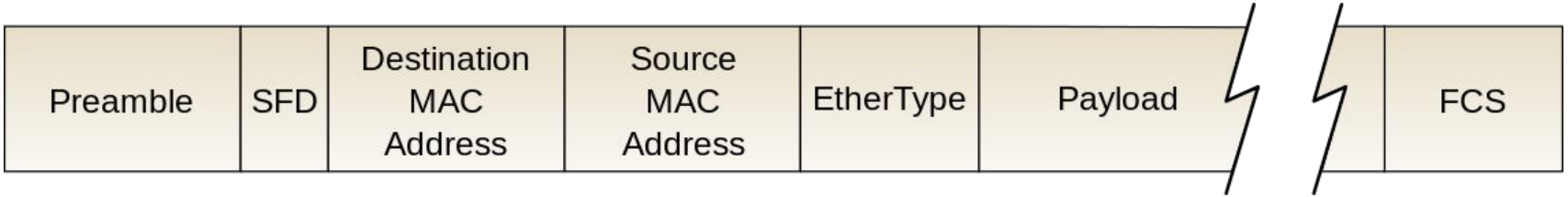
LSBit first, MSByte first???

Two signals mixed into one

The RMII Interface (State Diagram)



How Ethernet Works



String of "1010…", ending with "11"
(i.e. "11" is the *most significant* dibit of the last byte!)

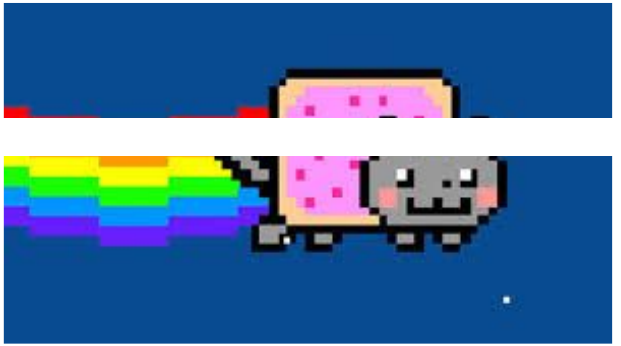
MAC Addressing
(ignore for now)

Min 64 bytes
Max 1518 bytes

CRC32
(there are 1000 ways to take a CRC, even with the same polynomial)

Robust to Dropped/Incomplete Packets

Missing/Incomplete packets not disastrous

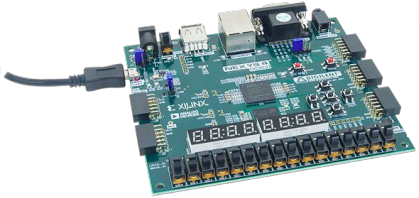


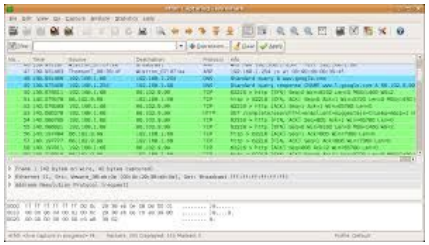
The sender cycles through same image data over and over again, so we will eventually receive all the data

BUT! AES has to operate in ECB mode (insecure) for this to work

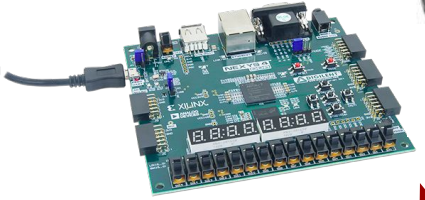
(Stretch goal: flow control and CBC mode)

Ethernet is Hard :(





Ethernet is Hard :(

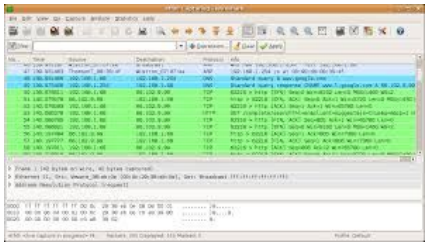


Logic wrong?

Constraints wrong?

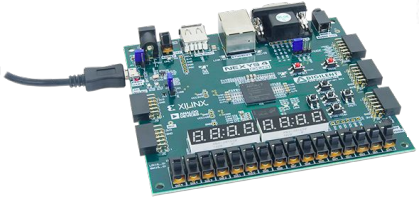
PHY misconfigured?

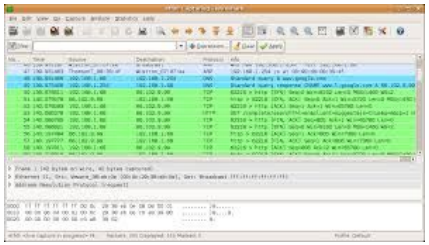
Frames dropped?



Wireshark misconfigured?

Ethernet is Hard :(

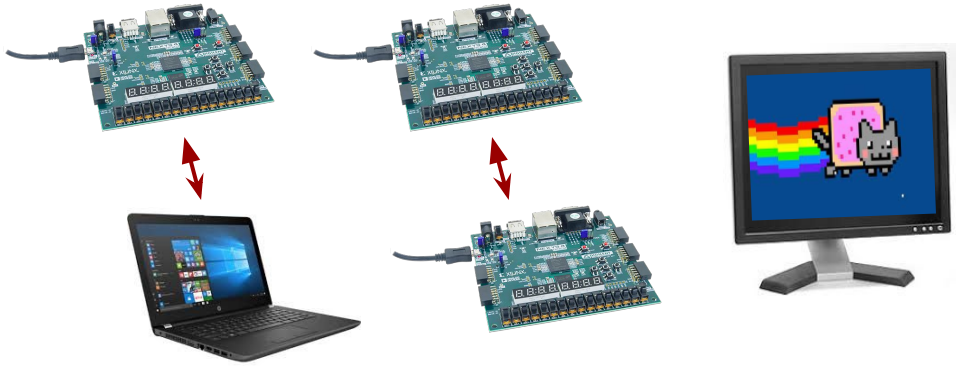




Can’t just probe!

Tradeoff: More reliable communication but harder to debug

Timeline



INTEGRATION!

Nov 5

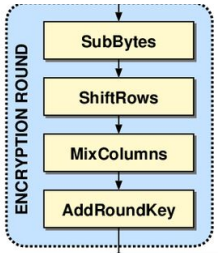
Nov 12

Nov 19

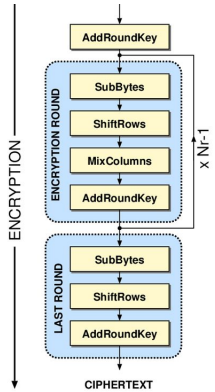
Nov 26

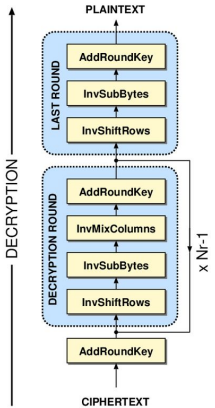
$$\int_a^b$$

Dec 3



(one round)





BUFFER / STRETCH