Secure Storage and Communications in IoT

Class 1: Security Concepts in the IoT

6/25/18
Warren Miller

Presented by:

DesignNews

CEC CONTINUING EDUCATION CENTER

Digi-Key ELECTRONICS

This Week’s Agenda

6/25/18	Security Concepts in the IoT
6/26/18	MCU-based Security Features
6/27/18	Implementation Examples- Storage
6/28/18	Implementation Examples- Communications
6/29/18	A Hands-on Design

Course Description

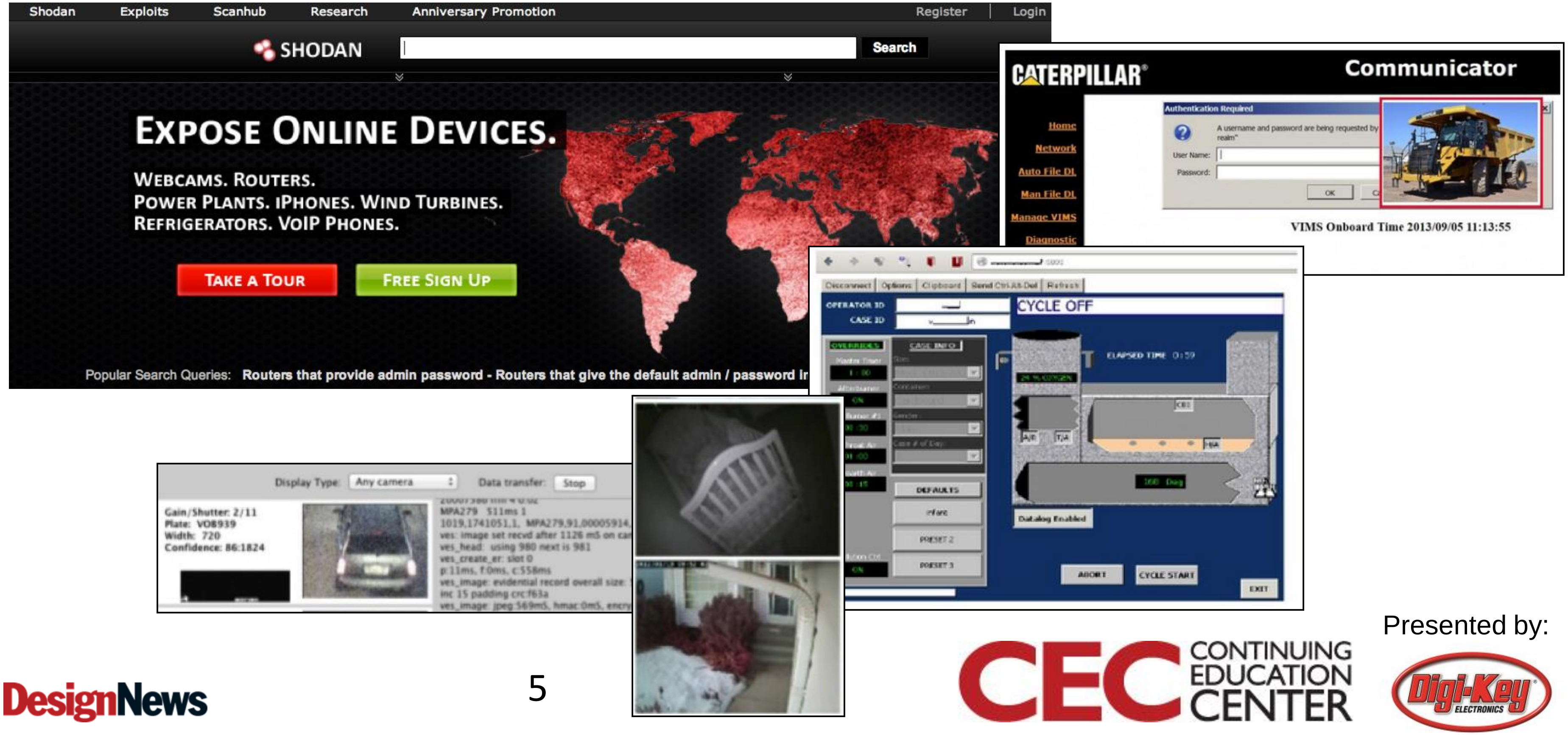
- The Internet of Things is connected
- Connected Things make it easy to steal...
- Must protect Storage
- Must protect Communications
- Must protect your IP!
- Lots of techniques are available to help you protect your IoT device

Today’s Topics and Goals

- Security Threats
  - Understand them
- Cryptography
  - Know about key techniques and uses
- Your Designs…
  - Provide me with information for class on Friday

Threats are Real

- Additional tools become available every day
- Shodan, Metasploit, etc.



Shodan | Exploits | Scanhub | Research | Anniversary Promotion | Register | Login

SHODAN [ ] Search

EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

TAKE A TOUR | FREE SIGN UP

Popular Search Queries: **Routers that provide admin password - Routers that give the default admin / password ir**

CATERPILLAR® Communicator

Home
Network
Auto File DL
Man File DL
Manage VIMS
Diagnostic

Authentication Required

A username and password are being requested by
realm"

User Name: [ ]
Password: [ ]

OK | C

VIMS Onboard Time 2013/09/05 11:13:55

Disconnect | Options | Clipboard | Send Ctrl-Alt-Del | Refresh

OPERATOR ID
CASE ID

CYCLE OFF

Display Type: Any camera | Data transfer: Stop

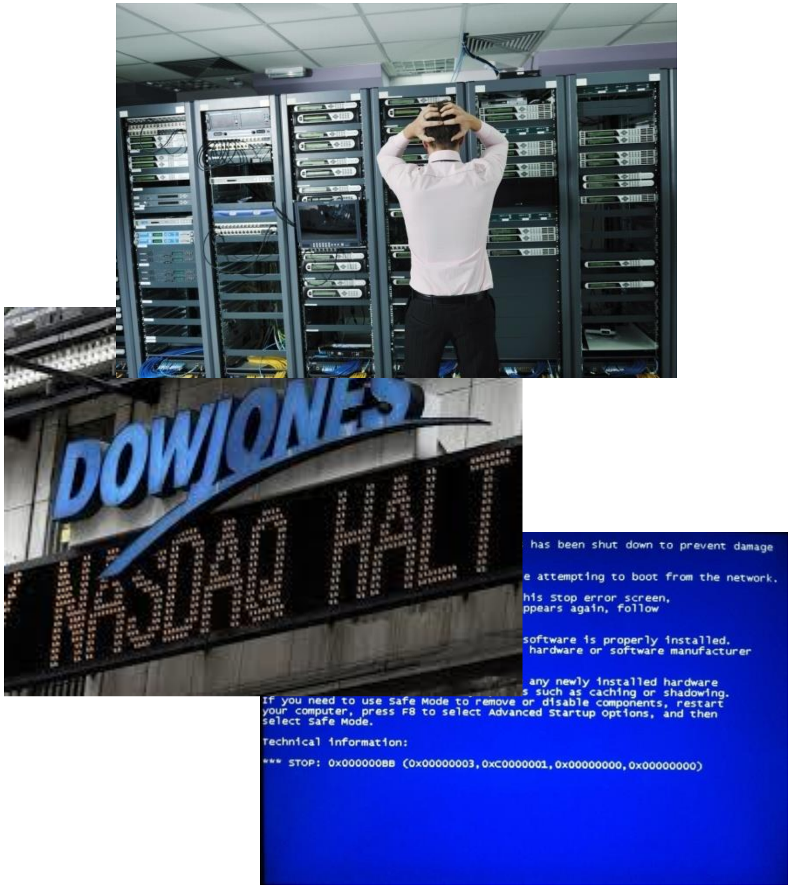
Gain/Shutter: 2/11
Plate: VO8939
Width: 720
Confidence: 86:1824

```
MPA279   511ms 1
1019,1741051,1,  MPA279,91,0000591
ves: image set recvd after 1126 mS on ca
ves_head:  using 980 next is 981
ves_create_er: slot 0
p:11ms, f:0ms, c:558ms
ves_image: evidential record overall size:
inc 15 padding crc:f63a
ves_image: jpeg:569mS, hmac:0mS, encry
```

Presented by:

Responses to Threats

- Commercial Avionics
  - New DO-326, Airworthiness Security Process Specification
- Industrial
  - IEC61508
    - Security is now part of Functional Safety for any networked device
    - Over 100 field bus protocols
- Communications
  - Secure Boot enables proper operation of the nations communications infrastructure.
- Defense
  - Anti-tamper and Design Assurance



```
 has been shut down to prevent damage

e attempting to boot from the network.

his Stop error screen,
ppears again, follow

software is properly installed.
 hardware or software manufacturer

 any newly installed hardware
s such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000BB (0x00000003,0xC0000001,0x00000000,0x00000000)
```

Threats to Your Hardware (Supply Chain)

- Counterfeit Devices
  - Devices remarked as a different part!
  - E-Waste as the source
    - Apply a flame to PCB
    - Treat devices to 'clean'
    - Remark and sell
- Fraud
  - Recovered devices
  - Correct devices marked as higher grade
  - Difficult to catch!

- SIA Reports on Counterfeiting show a growing threat
- Threat grows when parts are in short supply
- Need to manage purchasing
- Need to decommission devices

Threats to Your Hardware (Manufacturing and Deployment)

- Hardware Threats
  - Copying
  - Overbuilding
  - Cloning
  - Reverse Engineering
- Deployed Hardware Threats
  - Invasive Threats
  - Remote Threats
    - Upgrades, Boot code
    - Sensitive Data

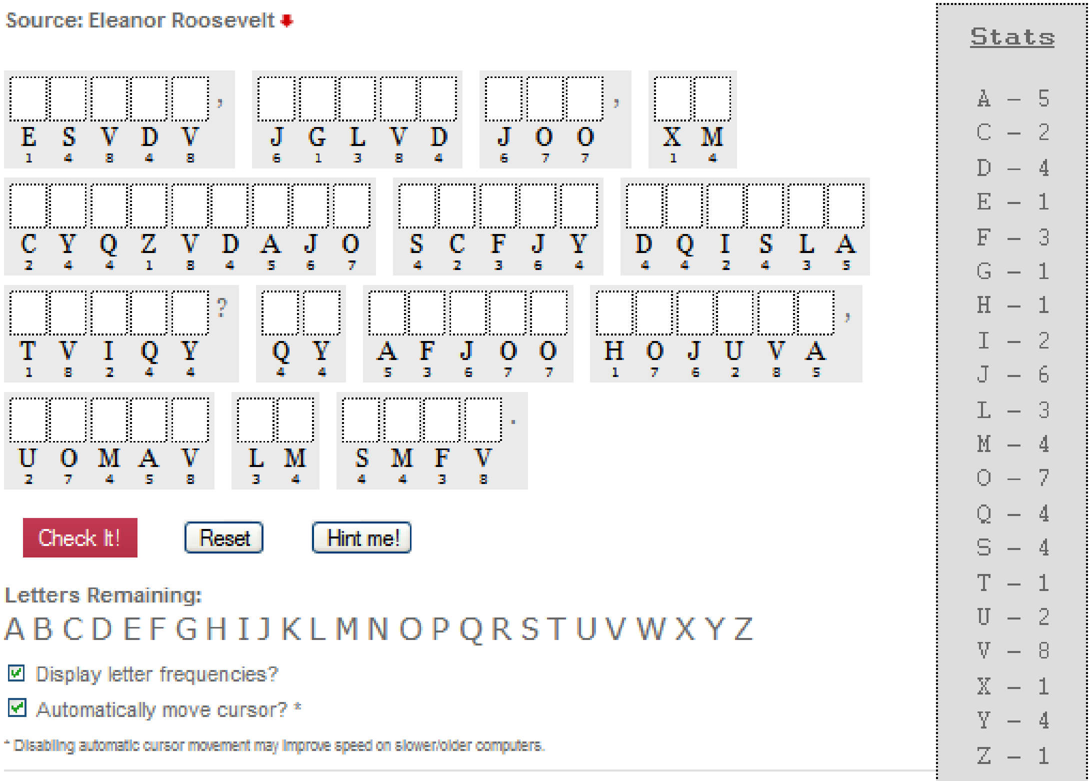
Technology to Thwart Threats

- Typical Hardware (for this course)
  - MCU, FPGA, ASIC, Analog, Standard Devices, etc
  - All interconnected on a circuit board
  - Can be accessed when used in the field
- Thwarting Threats (Keep design secret)
  - MCU code, FPGA code, Flash memory contents
  - Secret keys, SRAM data, Data going on/off board
  - Devices used, Board layout, Tamper detection

Cryptography (Technique)

- Substitution Ciphers
- Each letter -> Another letter
- One Time Pad
- Pseudo Random Numbers

http://www.cryptograms.org/play.php



Source: Eleanor Roosevelt

E S V D V , J G L V D J O O , X M
1 4 8 4 8 6 1 3 8 4 6 7 7 1 4

C Y Q Z V D A J O S C F J Y D Q I S L A
2 4 4 1 8 4 5 6 7 4 2 3 6 4 4 4 2 4 3 5

T V I Q Y ? Q Y A F J O O H O J U V A ,
1 8 2 4 4 4 4 5 3 6 7 7 1 7 6 2 8 5

U O M A V L M S M F V .
2 7 4 5 8 3 4 4 4 3 8

Letters Remaining:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

☑ Display letter frequencies?

☑ Automatically move cursor? *

* Disabling automatic cursor movement may improve speed on slower/older computers.

Stats

A	5
C	2
D	4
E	1
F	3
G	1
H	1
I	2
J	6
L	3
M	4
O	7
Q	4
S	4
T	1
U	2
V	8
X	1
Y	4
Z	1

Modern Cryptography

- Standards
- Shared Secrets and Encryption/Decryption Algorithms
- Keys (Small- 256bits or so)
  - Symmetric and Asymmetric
- Standard Algorithms for Encrypt/Decrypt
  - One Way Functions with Trapdoor Information
    - The ideal- standards try to approach this ideal

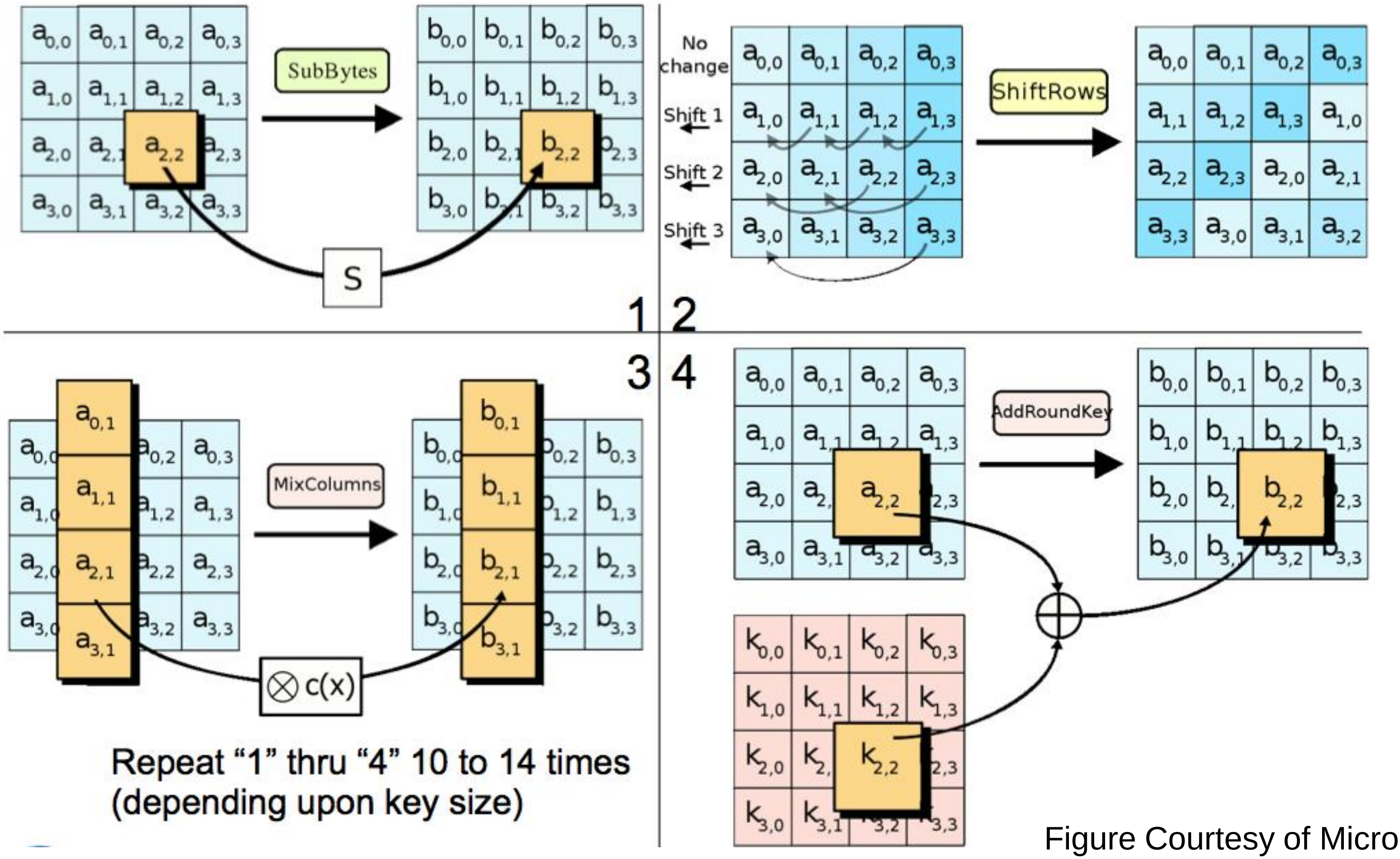
Some Key Standards

- DES- Data Encryption Standard
- AES- Advanced Encryption Standard
- SHA- Secure Hash Algorithm
- Diffie-Hellman Key Exchange
- RSA- Rivest, Shamir, Adleman
  - Public Key Cryptosystem
- ECC- Elliptic Curve Cryptography

AES Standard Overview

- A more recent standard for en/decryption
  - – Rijndael Cipher: Selected by NIST in 2001
    - 128, 192 and 256 bits
    - Symmetric Key
- Substitution and permutation network
- Multiple repetitions based on key size
  - – 10, 12 or 14 cycles
- High-speed, Low-RAM and hard/software ease

AES- Basic Operation Elements



Repeat “1” thru “4” 10 to 14 times (depending upon key size)

Figure Courtesy of Microsemi

Presented by:

AES- Typical Encryption Round

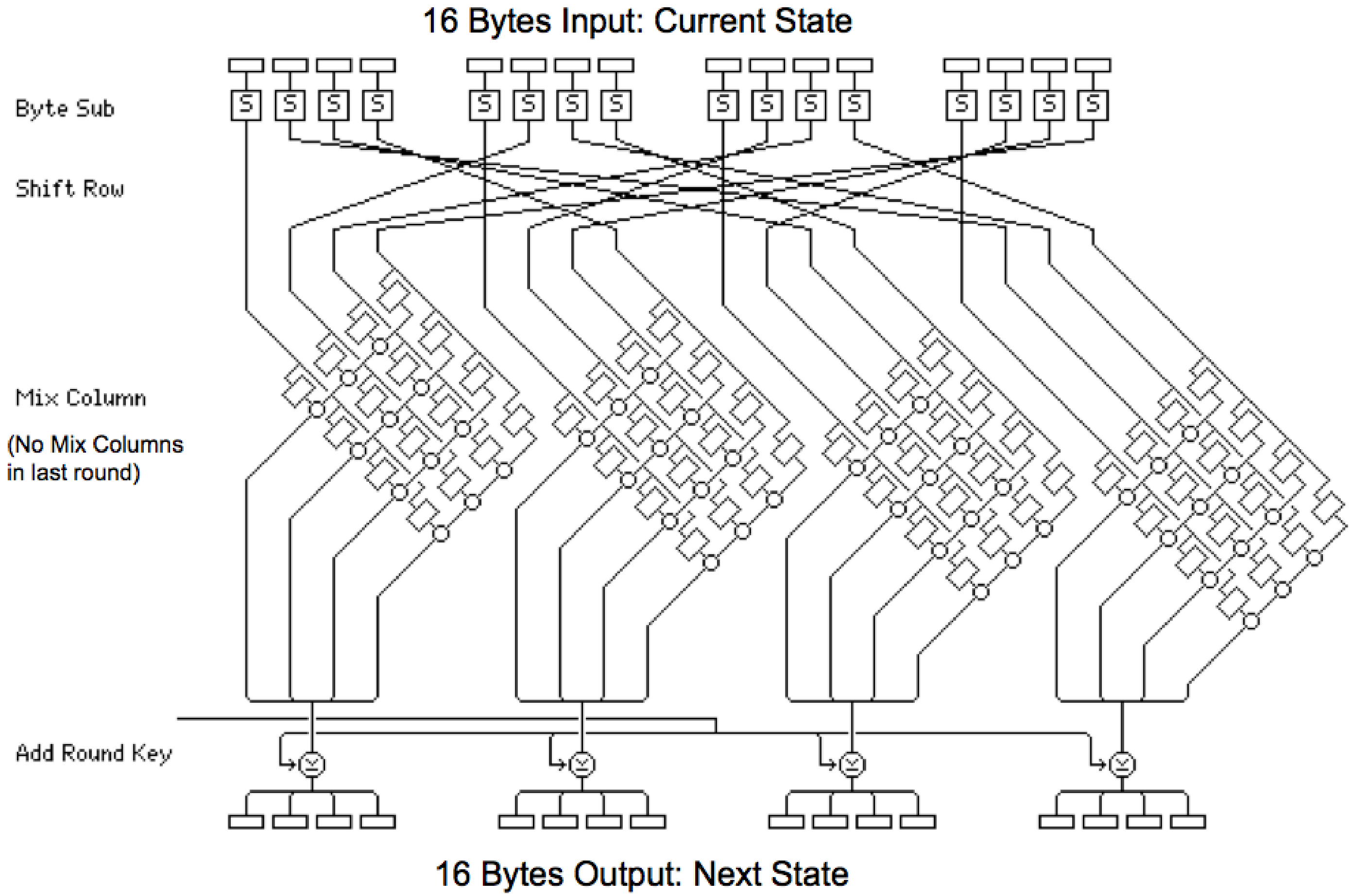

16 Bytes Input: Current State
Byte Sub
S
Shift Row
Mix Column
(No Mix Columns in last round)
Add Round Key
16 Bytes Output: Next State

Figure Courtesy of Microsemi

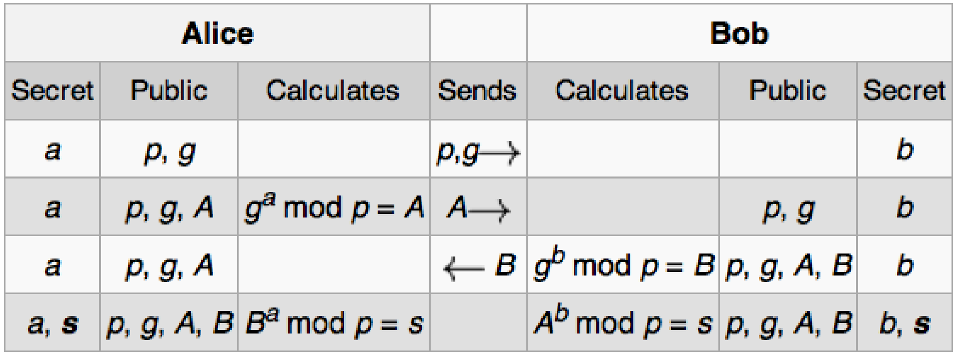
Presented by:

SHA

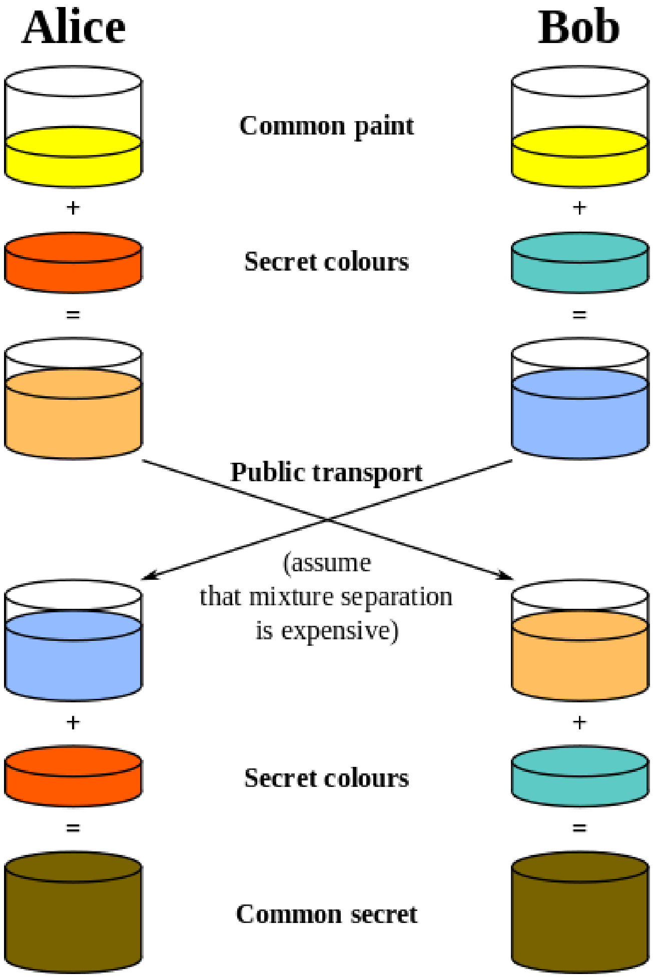
- Secure Hash Algorithm
  - Transforms a large data set into a small fixed length value
  - Avoid collisions so that an attacker can’t craft data sets to replace a set with a known hash
  - Used for authentication
    - Bitcoin, software packages, passwords, messages
- NIST and FIPS, NSA designs
- SHA-1/2/3

Diffie-Hellman Exchange

- The problem with symmetric keys…
- Exchange shared keys over an insecure channel
  - Example with color
  - Example with primes using modulo arithmetic



Alice				Bob		
Secret	Public	Calculates	Sends	Calculates	Public	Secret
a	p, g		$p,g \rightarrow$			b
a	p, g, A	$g^a \bmod p = A$	$A \rightarrow$		p, g	b
a	p, g, A		$\leftarrow B$	$g^b \bmod p = B$	p, g, A, B	b
a, s	p, g, A, B	$B^a \bmod p = s$		$A^b \bmod p = s$	p, g, A, B	b, s

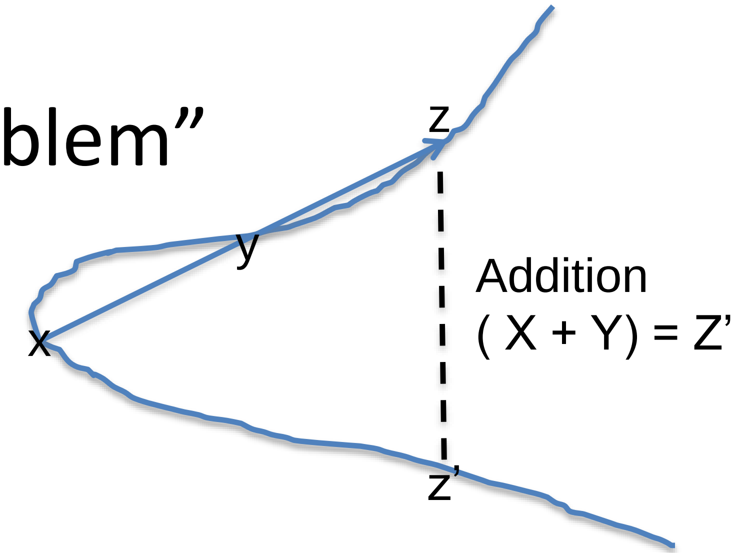


RSA

- Public-Key Cryptosystem
  - Encryption key is public
  - Decryption key is secret
- Based on the difficulty in factoring the product of two large prime numbers
- “Math Trick” simplifies decryption using prime factors

ECC

- Different "Intractable Problem"



- Elliptic Curve Arithmetic
- Much smaller key size for the same security
  - 3027-bit RSA vs. 256bit ECC

Additional Resources

Previous Course: http://www.designnews.com/lecture.asp?doc_id=269699
"Securing Your Embedded System"

Security Blog, Schneier on Security: https://www.schneier.com

Department of Homeland Security- Federal Network Resilience

SIA Report on Counterfeiting

Coursera Cryptography Courses: www.coursera.org (Search for Cryptography)

Digi-Key TechZone Article Library: MCUs , Securing MCU Designs, 11/06/2013

Optional No Cost HW and Software

Renesas Synergy Platform

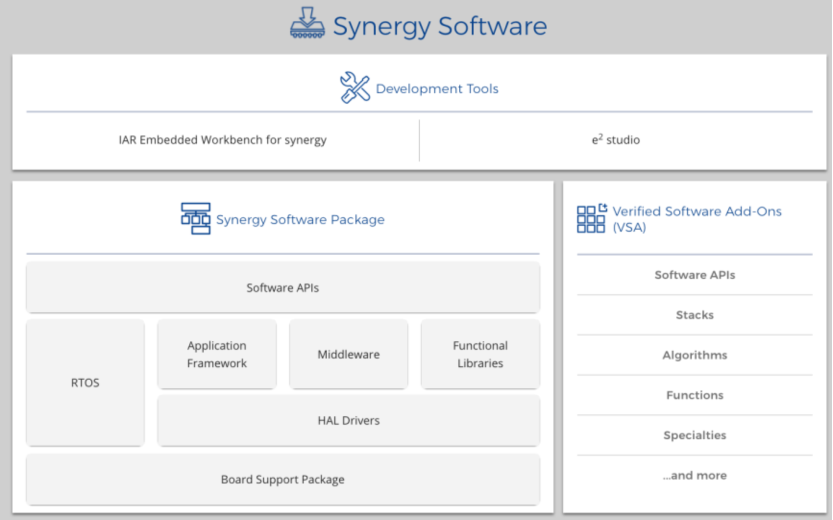
https://www.renesas.com/en-us/products/synergy/software/ssp.html

Synergy AE-Cloud1 Kit

https://www.digikey.com/product-detail/en/renesas-electronics-america/YSAECLOUD1/YSAECLOUD1-ND/8342110

Project Page

https://www.renesas.com/en-us/products/synergy/hardware/kits/ae-cloud1.html



Synergy Software

Development Tools

IAR Embedded Workbench for synergy

e^2 studio

Synergy Software Package

Software APIs

RTOS

Application Framework

Middleware

Functional Libraries

HAL Drivers

Board Support Package

Verified Software Add-Ons (VSA)

Software APIs

Stacks

Algorithms

Functions

Specialties

...and more

This Week’s Agenda

6/25/18	Security Concepts in the IoT
6/26/18	MCU-based Security Features
6/27/18	Implementation Examples- Storage
6/28/18	Implementation Examples- Communications
6/29/18	A Hands-on Design