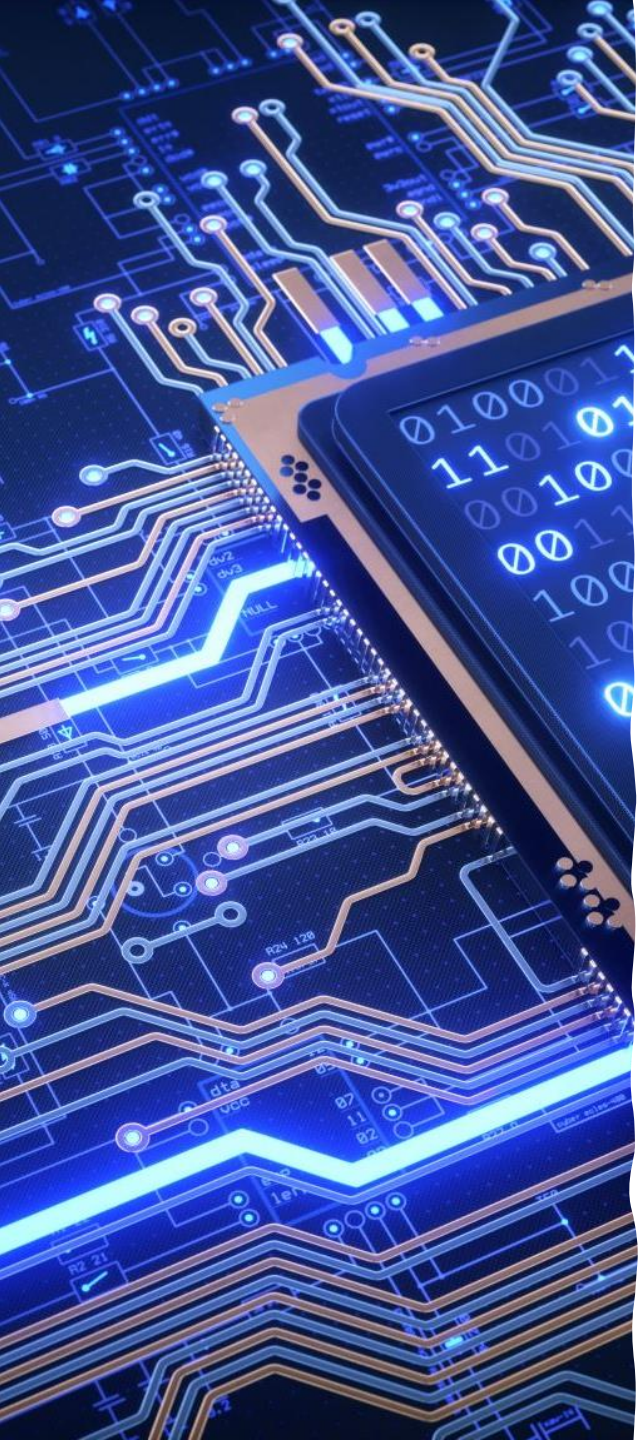


IoT-Cloud and Blockchain

Two virtual RPis

Dr. Phillip G. Bradford

University of Connecticut, Stamford CT. **USA**

phillip.bradford@uconn.edu,

Outline

Two virtual RPIs

Simple network model

SSH on RPIs

Message-digest hashing and public keys systems

Two Raspberry Pis

Running two QEMU VMs

Communication with Raspberry Pis

Running Two RPIs

Duplicate RPi folder

RPi_1

RPi_2

Both contain the files:

2021_01_11-raspios-…-lite.img
2021_01.qcow2
qemukernel
versatile-pb.dtb

QEMU State model

The system state is saved on the image (qcow2 file)

Multiple autonomous VMs require multiple images

~/Rpi_1/

~/Rpi_2/

Simple network model

Both RPIs

hostfwd=tcp::5022-:22

hostfwd=tcp::5023-:22

Simple network model

Both RPIs

hostfwd=tcp::5022-:22

hostfwd=tcp::5023-:22

Running Two RPIs

Two terminals

Term1> cd Rpi_1

Term2> cd Rpi_2

qemu-system-arm -M versatilepb

-cpu arm1176

-m 256 -hda "./2021-01.qcow2"

-net nic -net user,hostfwd=tcp::5022-:22

-dtb "./versatile-pb.dtb"

-kernel "./qemukernel"

-append "root=/dev/sda2 panic=1 rootfstype=ext4 rw" -no-reboot

Running Two RPIs

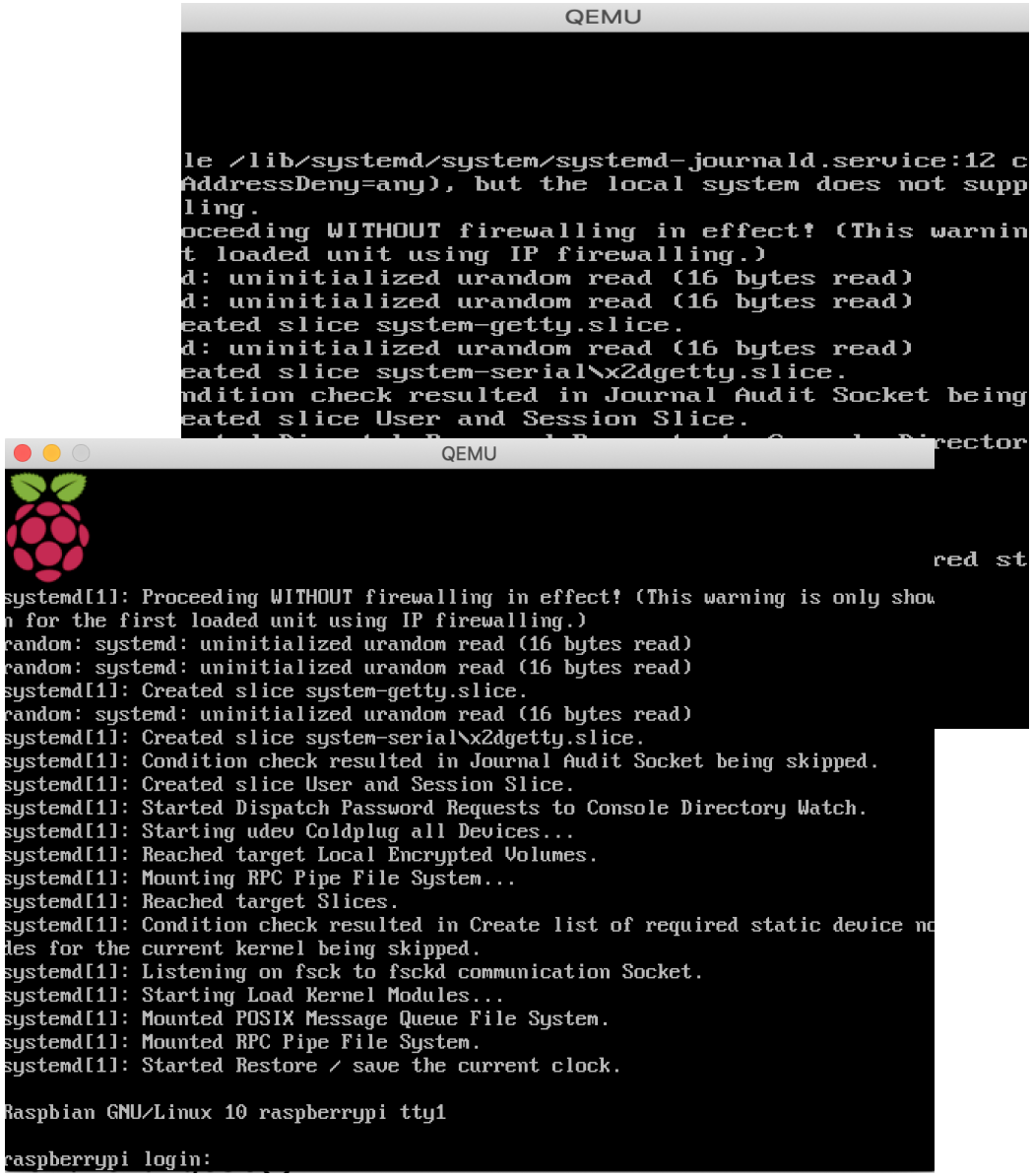
Duplicate RPi folder:

Rpi_1

Rpi_2

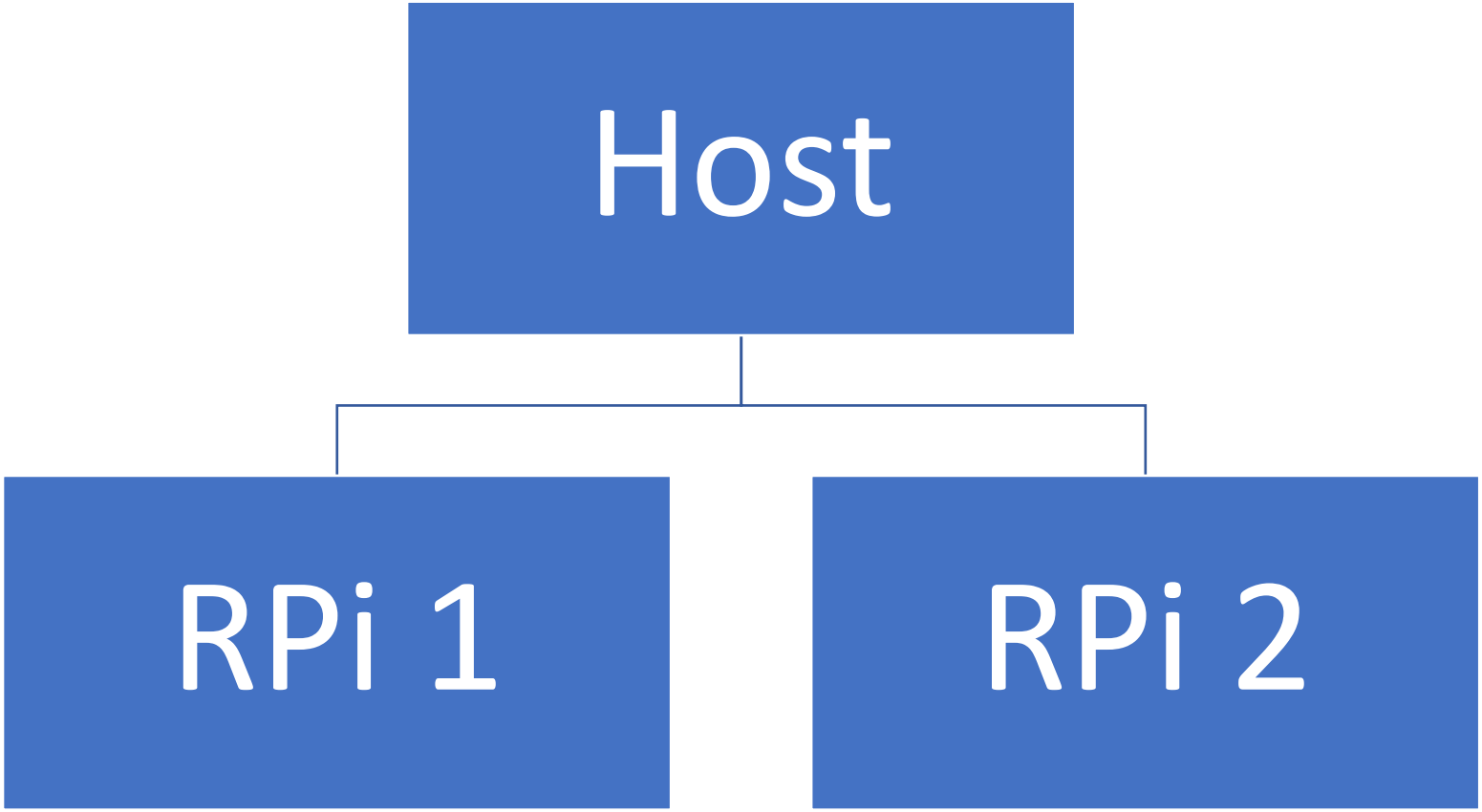
The qcow2 file should be different for each RPi

Run qemu from both folders



Guests and Hosts

System virtualization



SSH

Secure shell via ports 502X

Communication path

Host → RPI_1

Host → RPI_2

Installation

Install git on RPIs

Windows 10: easy ssh

MacOS: generate public-secret key pairs

put public key hash in known_hosts

secret key in keychain

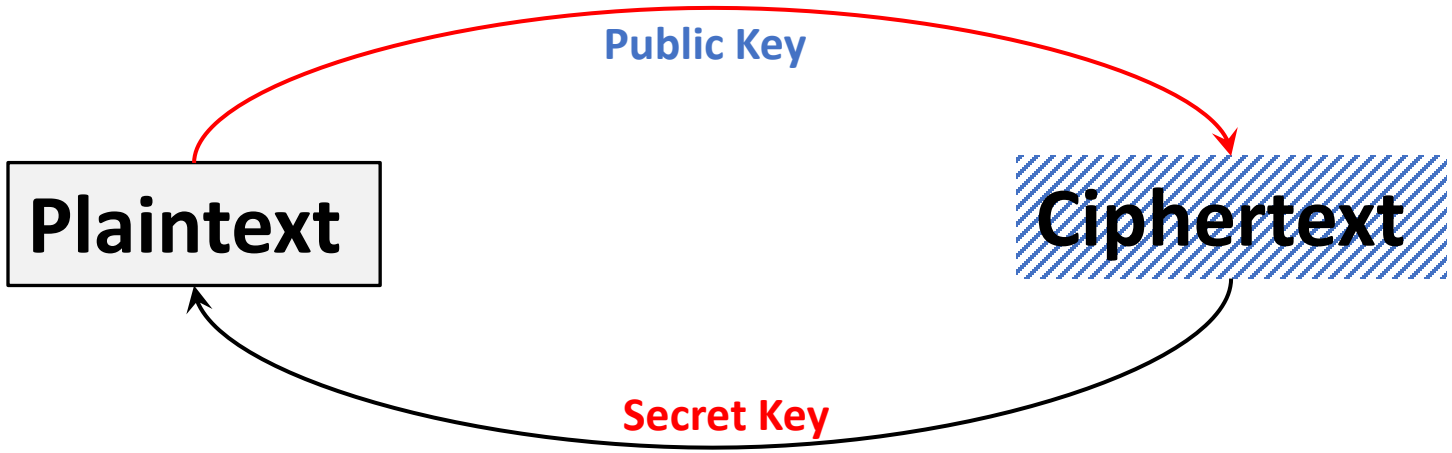
push public key to RPIs

Message digest hash functions
Public key systems

Public key systems: RSA

SHA message digest function

Public Key Systems: secret message



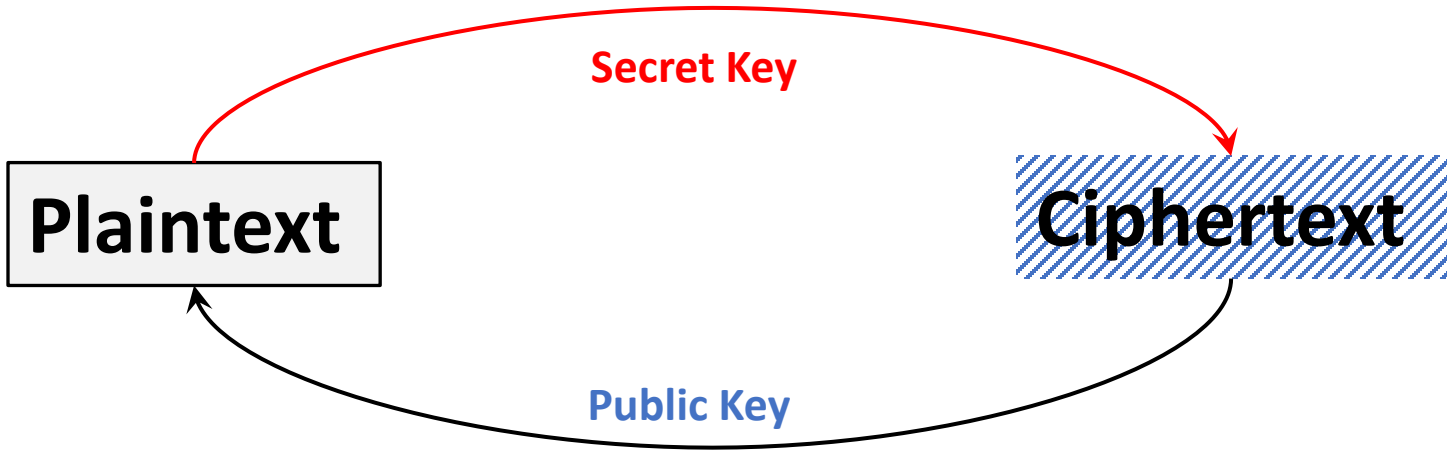
Generate two keys

- The public Key is open to the world
- The secret key is secret, **only** you know it

Knowing the public key, intractable to find secret key

Each key is the other's cryptographic inverse

Public Key Systems: proving secret key

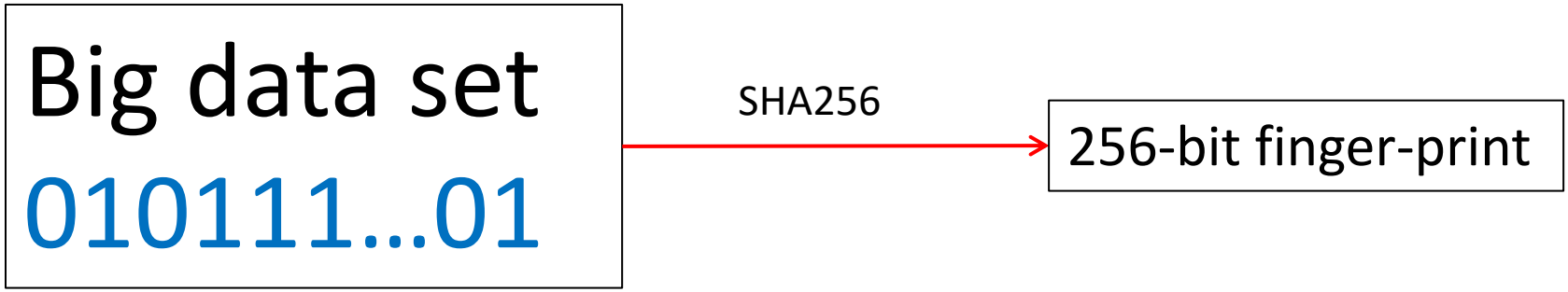


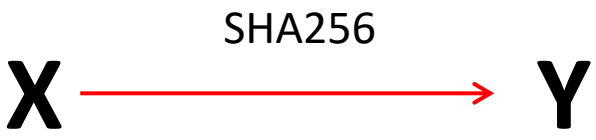
Take today's news as plaintext

Encrypt it with secret key and post cipher text

Anyone with public key can get the plaintext

SHA256 finger-prints





Given SHA256 output **Y**, not feasible to find input **X** where **SHA256(X) = Y**

Hash functions: simplified

Outputs three decimal digits

Hash("Buy ETH") → 372
Hash("Buy BTC") → 281
Hash("Sell ETH") → 870

Any integer x in {0, 1, 2, …, 999} and any string X we have:

$$\mathbf{P[Hash(X) = x] = \frac{1}{1000}}$$

Collision intractability

SHA256 digests giant strings into 256 bits

How many decimal digits in 2^{256} ?

Log10(2^{256}) > 77

One third of 77 is about 25 decimal digits

$$\mathbf{P[SHA_{1/3}(X) = y]} = \frac{1}{10000000000000000000000000}$$

Public key systems

Proving you have a secret key

$$E_S[T] = C$$

$$D_P[C] = T$$

Letting anyone send you a secret message

$$E_P[T] = C$$

$$D_S[C] = T$$