RET Project #5: Cybersecurity

Faculty Mentor: Dr. Franco

Graduate Research Assistant: Shaunak Kapoor

Teachers:

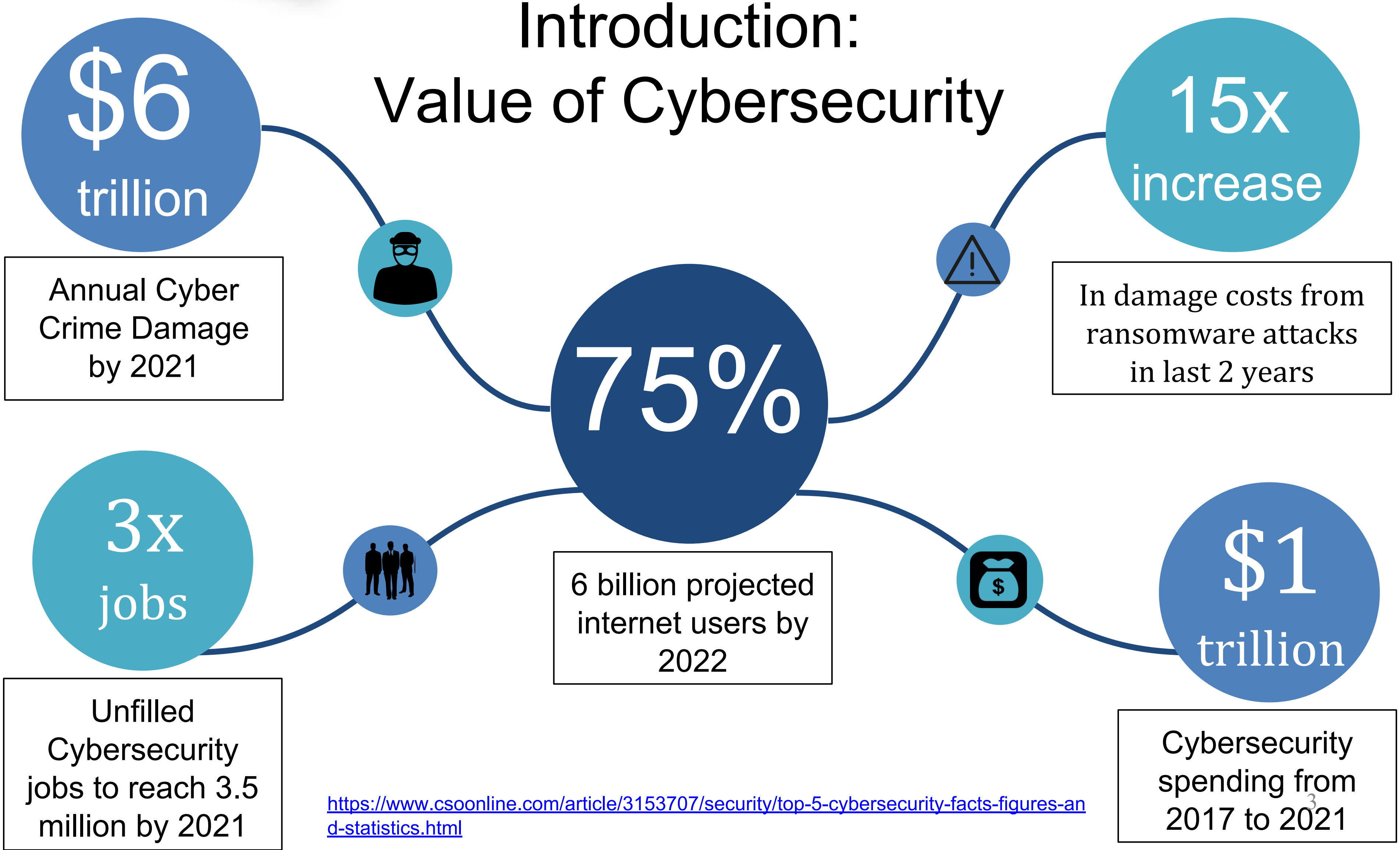
Adam Mesewicz

Kelly Hiersche

RET is funded by the National Science Foundation, grant # EEC-1710826

Table of Contents

Introduction:
Value of Cybersecurity



$6 trillion

Annual Cyber Crime Damage by 2021

15x increase

In damage costs from ransomware attacks in last 2 years

75%

6 billion projected internet users by 2022

3x jobs

Unfilled Cybersecurity jobs to reach 3.5 million by 2021

$1 trillion

Cybersecurity spending from 2017 to 2021

https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

Abstract

- Cybersecurity is a growing field.
- Trained cybersecurity experts are necessary for individual and national security.
- Math is a vehicle to teach students cybersecurity concepts and encourage students to consider a career in the field.
- Cybersecurity is a vehicle to motivate student learning in Algebra II.

Literature Review

<u>Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains</u>

✦ By Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D.
✦ Discusses the “Cyber Kill Chain” developed by Lockheed Martin.

<u>Logging and Monitoring to Detect Network Intrusions and Compliance Violations in the Environment</u>

✦ By Sunil Gupta.
✦ Introduces Various Methods of Network Intrusion Detection.

<u>Network Security: Private Communication in a Public World</u>

✦ By Charlie Kaufman, Radia Perlman, Mike Speciner.
✦ Gave background on fundamentals of cryptography.

Adam’s Research Training

- ✦ Learned about Networks, Protocols and Packet Transfer.
- ✦ Practiced ethical hacking techniques using tools built into Kali Linux OS.

Kelly’s Research Training

- How does secure transmission of information take place?
- What are viable ways to encrypt data?

- Can we develop a game to allow students to encrypt and decrypt information using Algebra 2 functions?

Image Sources: https://www.theverge.com/2016/1/28/10858250/oracle-java-plugin-deprecation-jdk-9l
https://betanews.com/2015/08/11/84-percent-of-enterprises-have-considered-encrypting-all-sensitive-data/

Background & Overview

Image Source: http://dreamstop.com/internet-dream-symbol/

The Internet

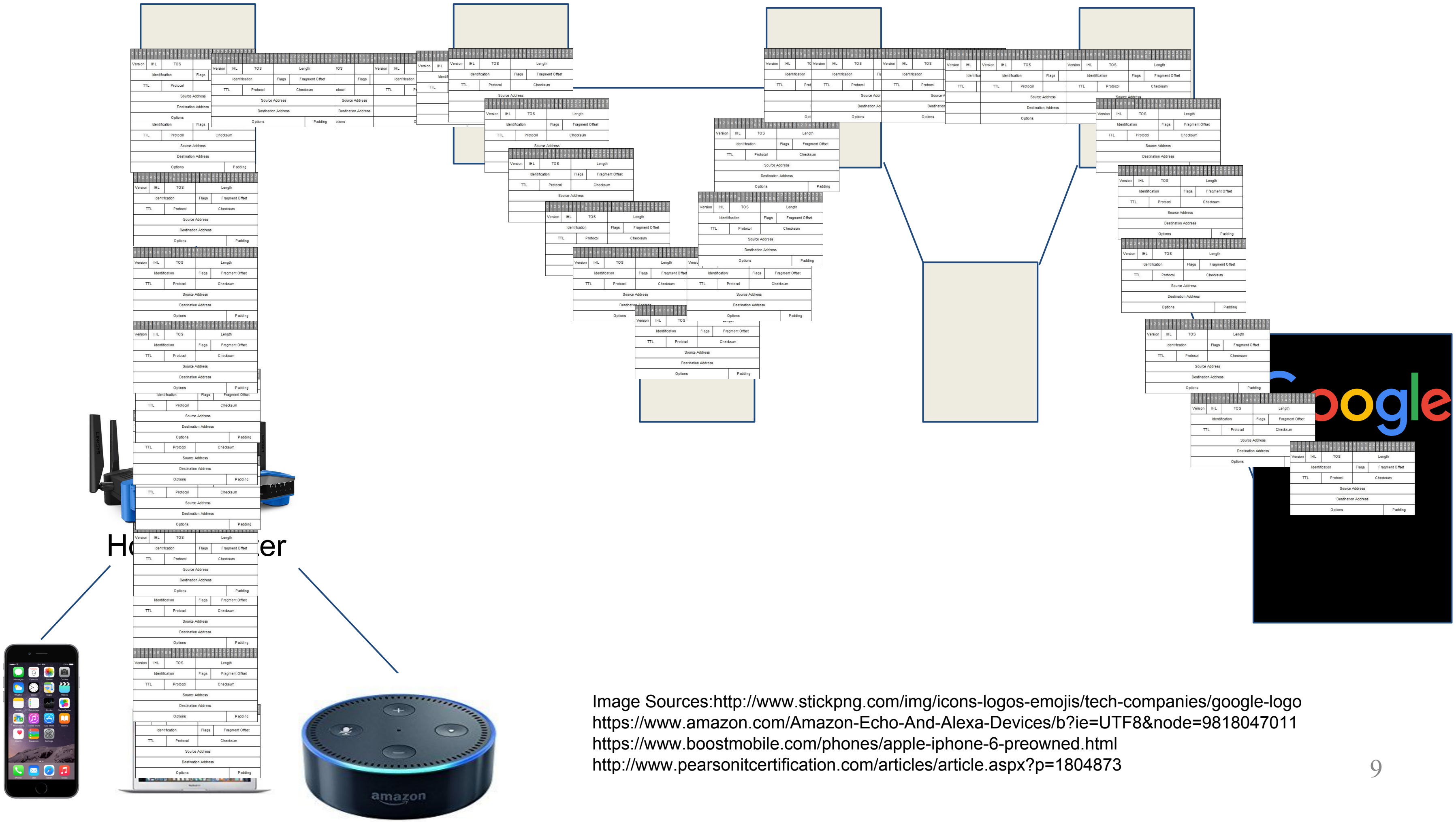


Image Sources:http://www.stickpng.com/img/icons-logos-emojis/tech-companies/google-logo
https://www.amazon.com/Amazon-Echo-And-Alexa-Devices/b?ie=UTF8&node=9818047011
https://www.boostmobile.com/phones/apple-iphone-6-preowned.html
http://www.pearsonitcertification.com/articles/article.aspx?p=1804873

The Internet

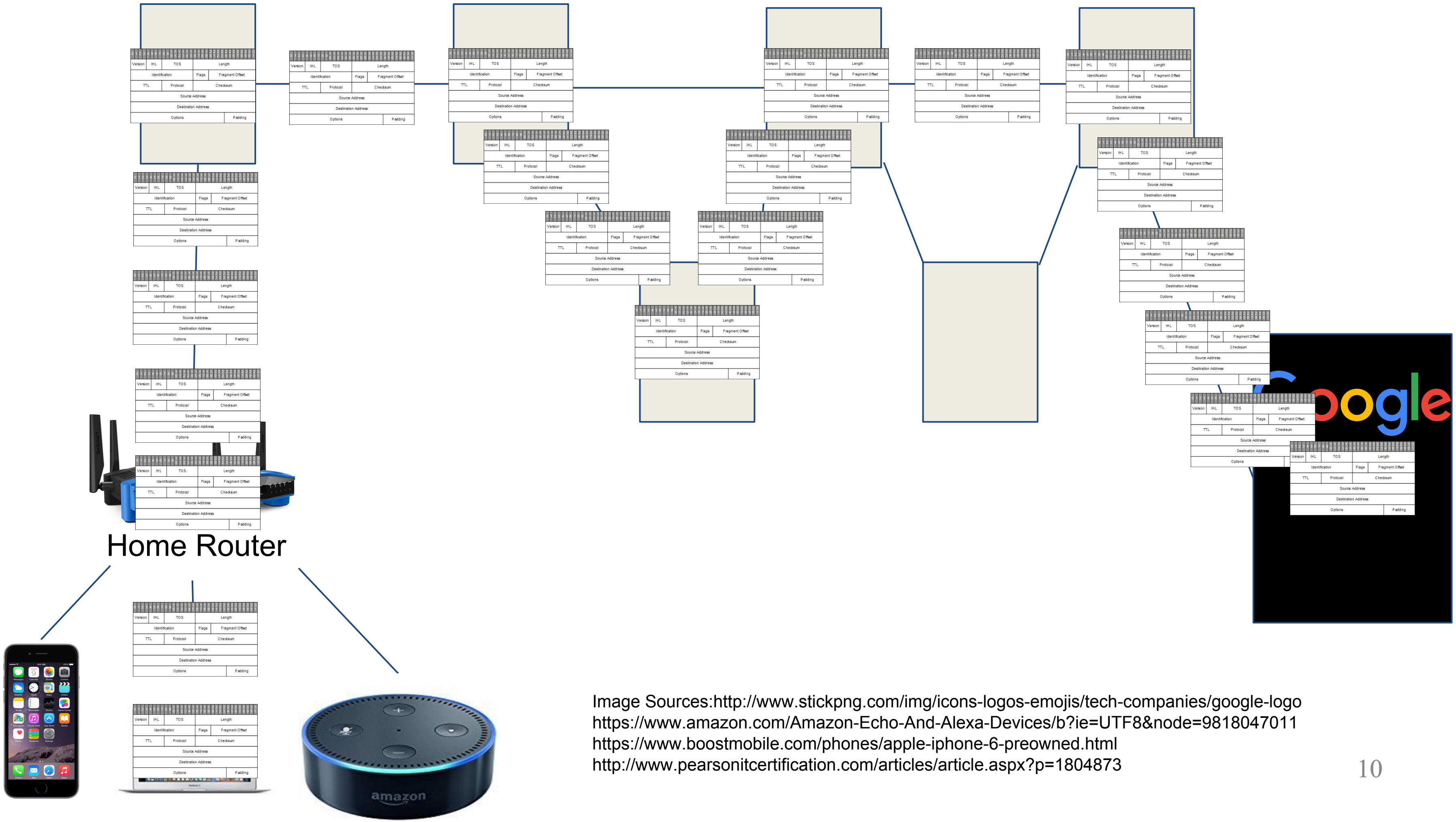
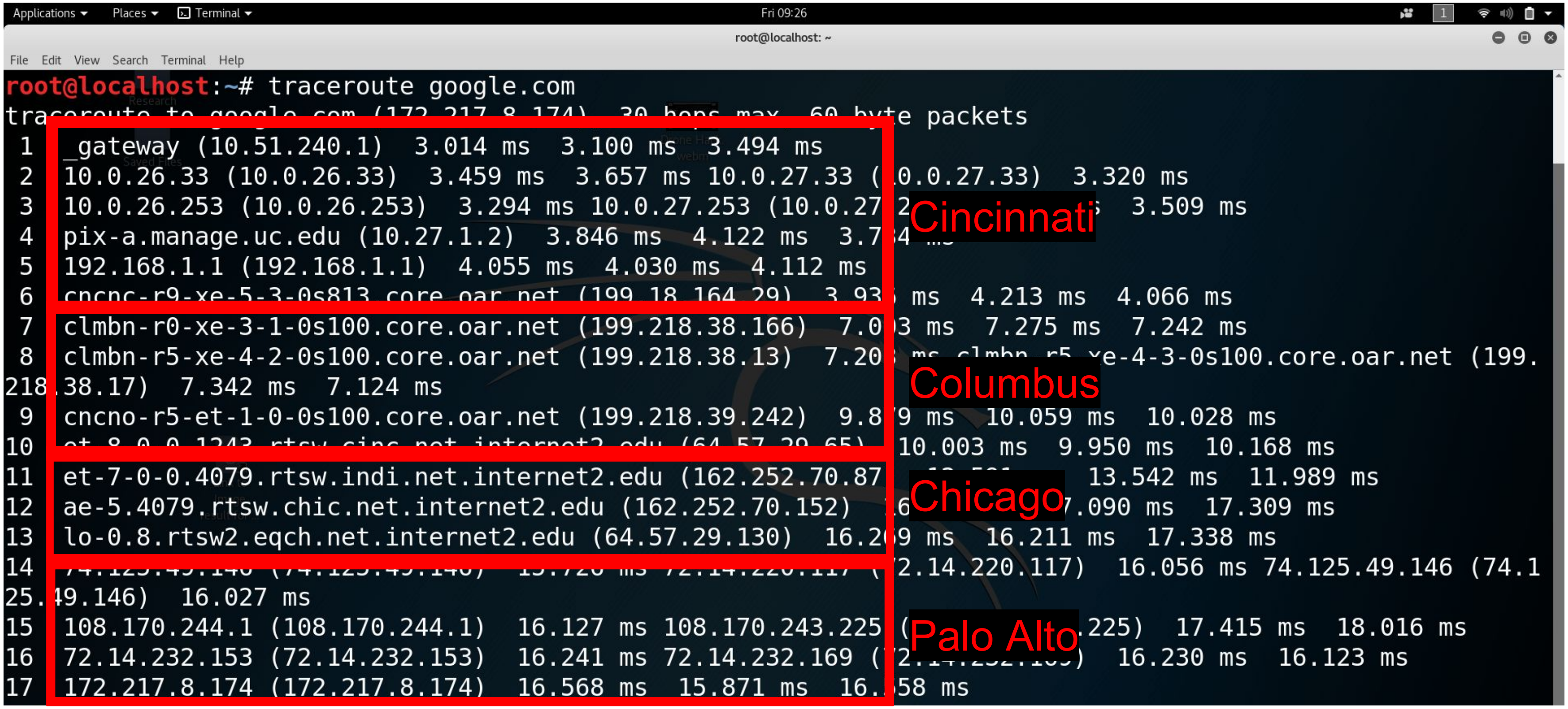


Image Sources:http://www.stickpng.com/img/icons-logos-emojis/tech-companies/google-logo
https://www.amazon.com/Amazon-Echo-And-Alexa-Devices/b?ie=UTF8&node=9818047011
https://www.boostmobile.com/phones/apple-iphone-6-preowned.html
http://www.pearsonitcertification.com/articles/article.aspx?p=1804873

The Internet



```
root@localhost:~# traceroute google.com
traceroute to google.com (172.217.8.174), 30 hops max, 60 byte packets
 1  _gateway (10.51.240.1)  3.014 ms  3.100 ms  3.494 ms
 2  10.0.26.33 (10.0.26.33)  3.459 ms  3.657 ms 10.0.27.33 (10.0.27.33)  3.320 ms
 3  10.0.26.253 (10.0.26.253)  3.294 ms 10.0.27.253 (10.0.27.2[illegible]s  3.509 ms
 4  pix-a.manage.uc.edu (10.27.1.2)  3.846 ms  4.122 ms  3.7[illegible]4 ms
 5  192.168.1.1 (192.168.1.1)  4.055 ms  4.030 ms  4.112 ms
 6  cncnc-r9-xe-5-3-0s813.core.oar.net (199.18.164.29)  3.93[illegible] ms  4.213 ms  4.066 ms
 7  clmbn-r0-xe-3-1-0s100.core.oar.net (199.218.38.166)  7.0[illegible]3 ms  7.275 ms  7.242 ms
 8  clmbn-r5-xe-4-2-0s100.core.oar.net (199.218.38.13)  7.20[illegible] ms clmbn-r5-xe-4-3-0s100.core.oar.net (199.
218.38.17)  7.342 ms  7.124 ms
 9  cncno-r5-et-1-0-0s100.core.oar.net (199.218.39.242)  9.8[illegible]9 ms  10.059 ms  10.028 ms
10  et-8-0-0.1243.rtsw.cinc.net.internet2.edu (64.57.29.65)  10.003 ms  9.950 ms  10.168 ms
11  et-7-0-0.4079.rtsw.indi.net.internet2.edu (162.252.70.87[illegible]  13.542 ms  11.989 ms
12  ae-5.4079.rtsw.chic.net.internet2.edu (162.252.70.152)  16[illegible]7.090 ms  17.309 ms
13  lo-0.8.rtsw2.eqch.net.internet2.edu (64.57.29.130)  16.2[illegible]9 ms  16.211 ms  17.338 ms
14  74.125.49.146 (74.125.49.146)  15.720 ms 72.14.220.117 (72.14.220.117)  16.056 ms 74.125.49.146 (74.1
25.49.146)  16.027 ms
15  108.170.244.1 (108.170.244.1)  16.127 ms 108.170.243.225 ([illegible].225)  17.415 ms  18.016 ms
16  72.14.232.153 (72.14.232.153)  16.241 ms 72.14.232.169 (72.14.232.169)  16.230 ms  16.123 ms
17  172.217.8.174 (172.217.8.174)  16.568 ms  15.871 ms  16.[illegible]58 ms
```

Principles of Security

- Confidentiality ➔ Encryption
- Integrity ➔ Checksum
- Authentication ➔ RSA

Confidentiality ensured through Cryptography

- Share information between two or more parties which can only be understood by the intended target

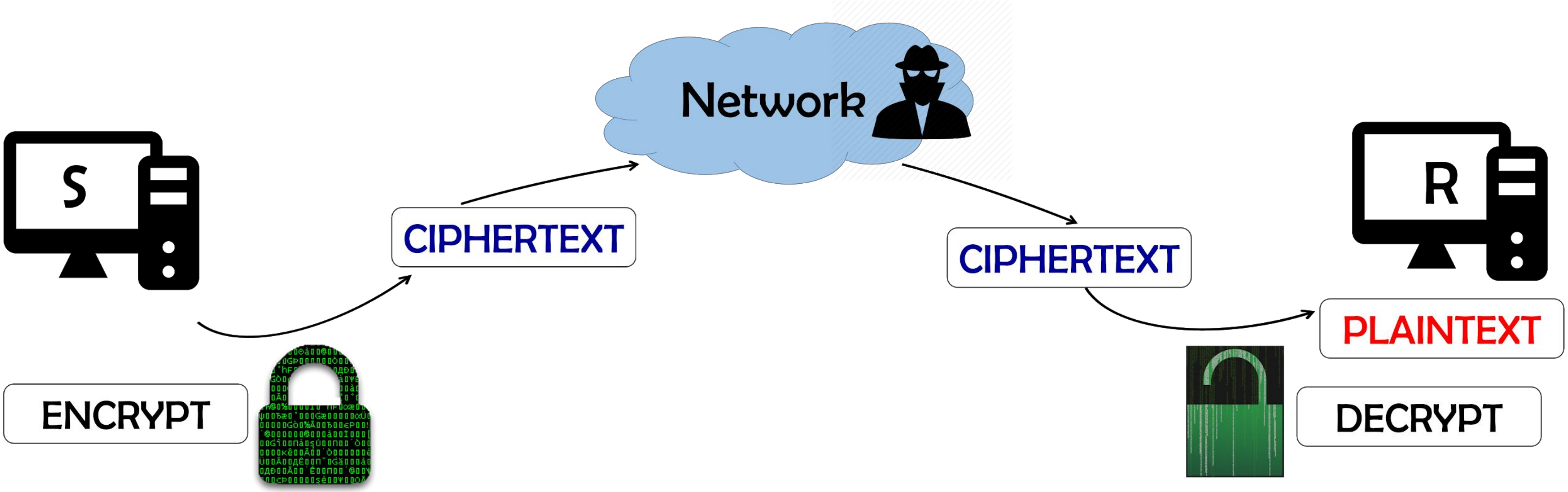


Image Source: https://techdifferences.com/difference-between-encryption-and-decryption.html

Modular Arithmetic

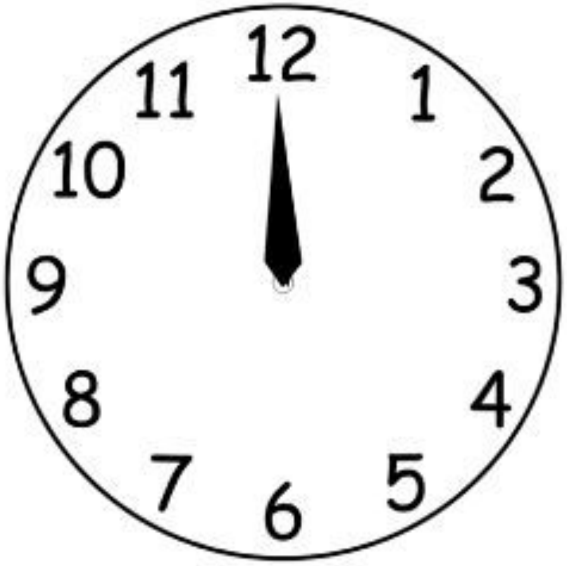
What is the remainder when you divide by a number?

Converting from military to civilian time:

23mod12 = 11

23:00 hours = 11pm

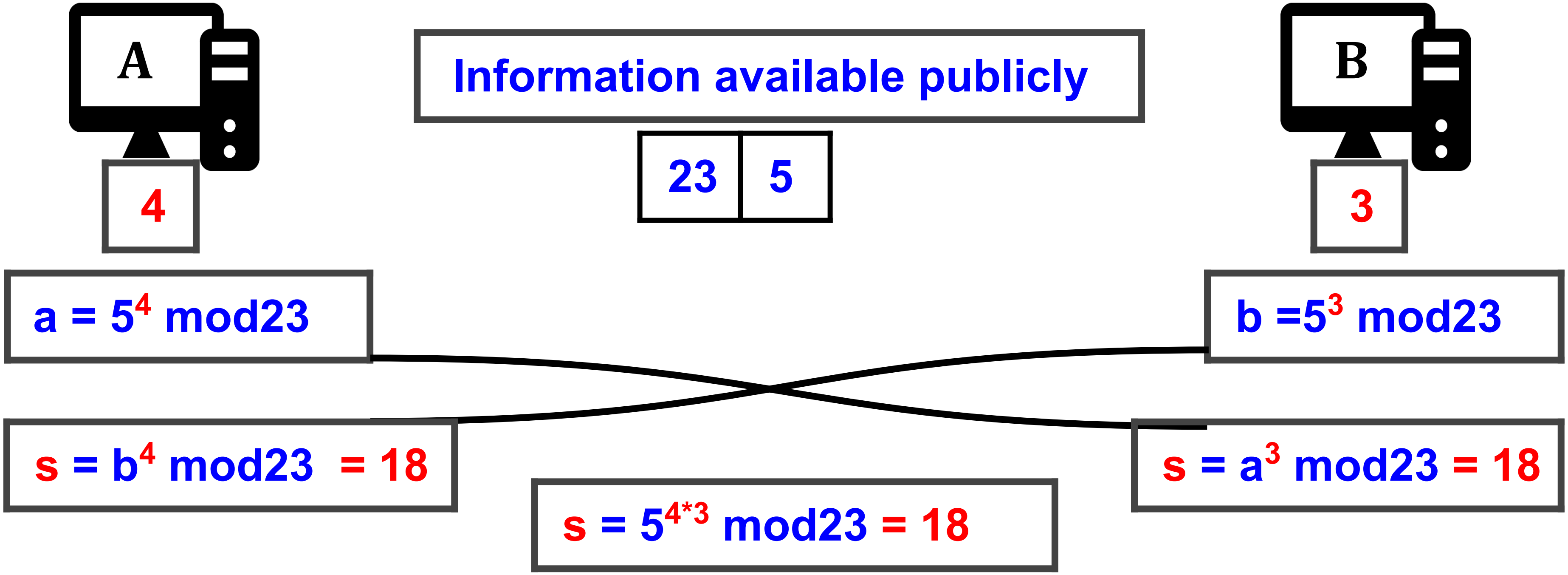
Modular/Clock Arithmetic



Modulus 12

Diffie-Hellman Exchange

- Way to establish a shared key over an insecure channel



A

B

Information available publicly

23 | 5

4

3

$a = 5^4 \bmod 23$

$b = 5^3 \bmod 23$

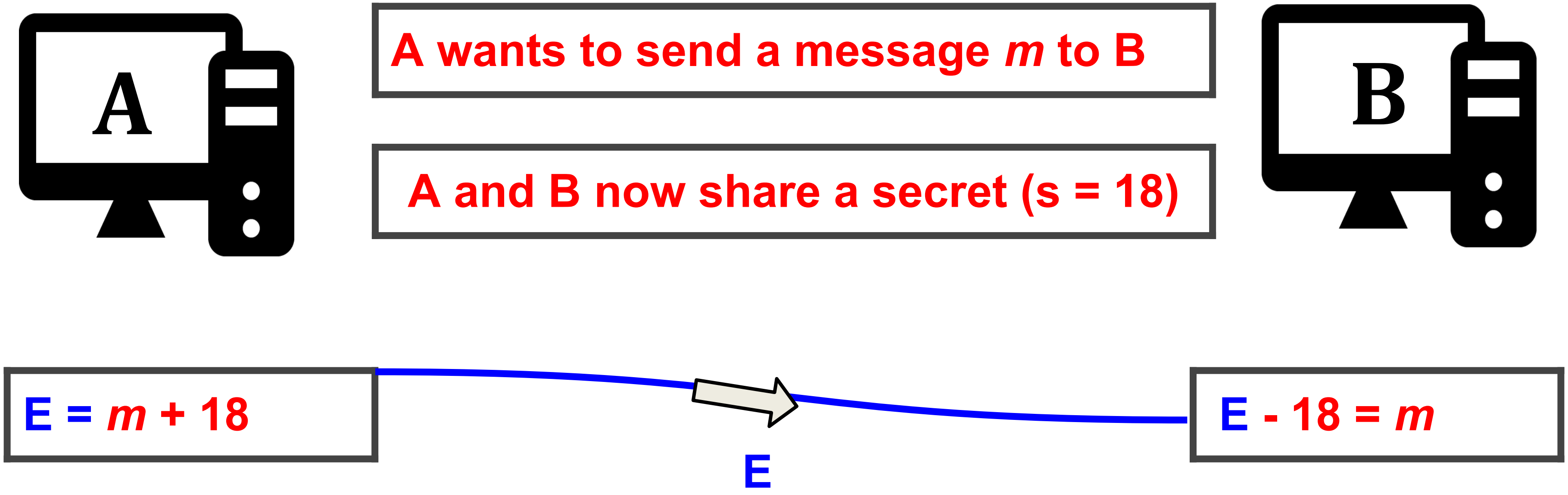
$s = b^4 \bmod 23 = 18$

$s = a^3 \bmod 23 = 18$

$s = 5^{4*3} \bmod 23 = 18$

- Utilizes exponent rules to share the secret key

Encryption



A wants to send a message *m* to B

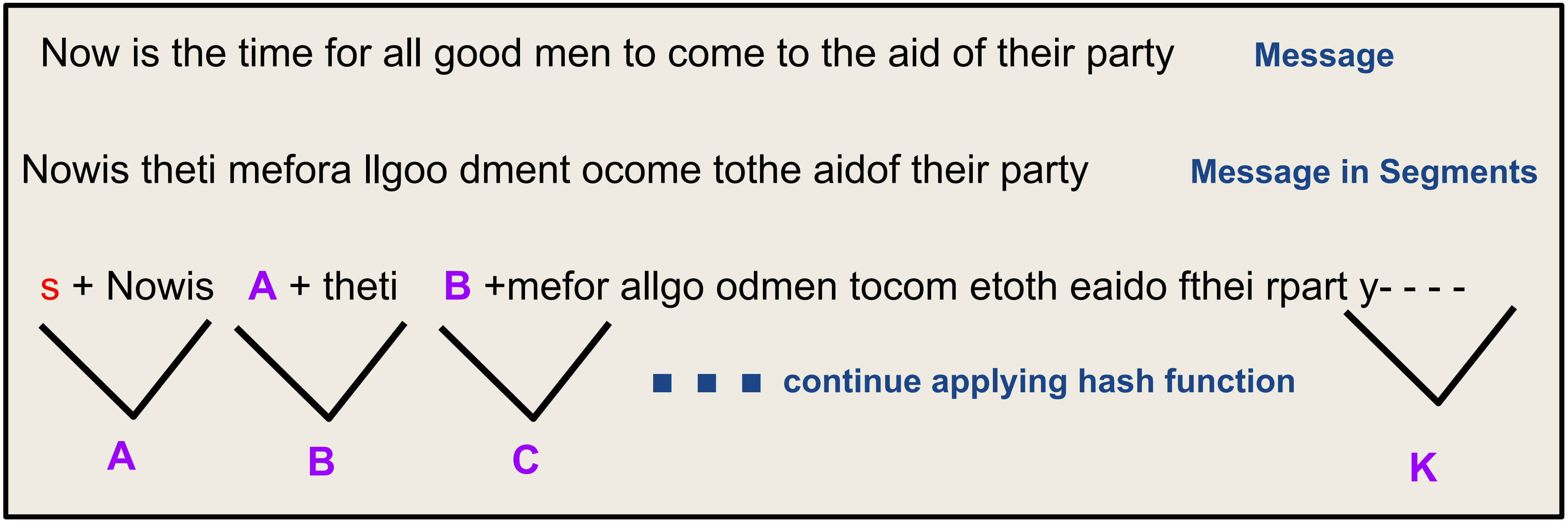
A and B now share a secret (s = 18)

E = *m* + 18

E - 18 = *m*

Integrity - Cryptographic Checksum

Hash Function: Takes an input of a known length and compresses it to a smaller, fixed length.



Now is the time for all good men to come to the aid of their party **Message**

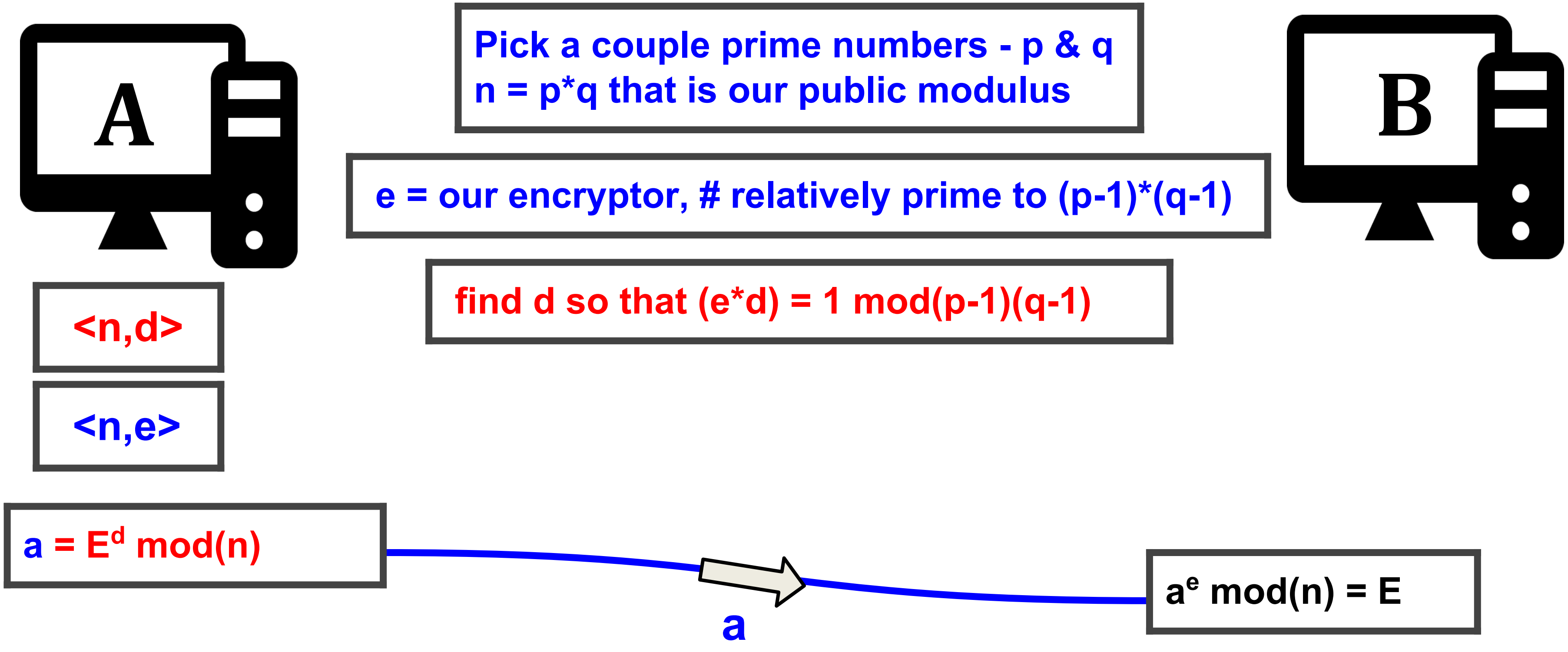
Nowis theti mefora llgoo dment ocome tothe aidof their party **Message in Segments**

s + Nowis A + theti B +mefor allgo odmen tocom etoth eaido fthei rpart y- - - -

■ ■ ■ **continue applying hash function**

Done by both the sender and receiver to make sure the message has not been changed.

Authentication - RSA



Pick a couple prime numbers - p & q
n = p*q that is our public modulus

e = our encryptor, # relatively prime to (p-1)*(q-1)

find d so that (e*d) = 1 mod(p-1)(q-1)

<n,d>

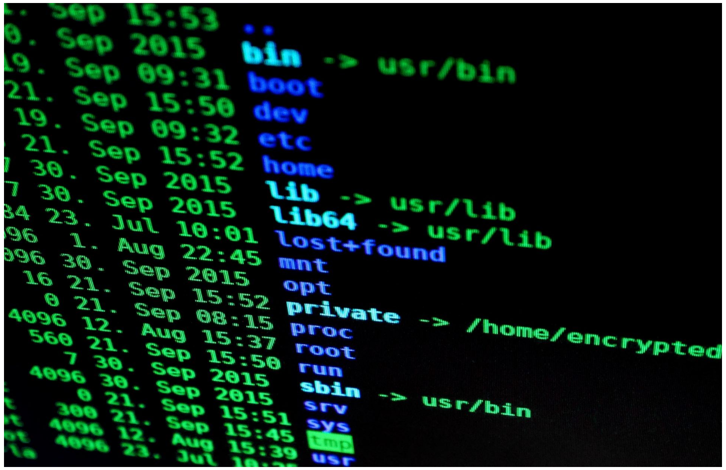
<n,e>

a = E^d mod(n)

a^e mod(n) = E

If the E that B calculates in this authentication is the same as it received in encryption phase, then we know the message came from where we thought.

Adam’s Goals and Objectives



```
. Sep 15:53 ..
0. Sep 2015 bin -> usr/bin
19. Sep 09:31 boot
21. Sep 15:50 dev
19. Sep 09:32 etc
21. Sep 15:52 home
7 30. Sep 2015 lib -> usr/lib
7 30. Sep 2015 lib64 -> usr/lib
34 23. Jul 10:01 lost+found
96 1. Aug 22:45 mnt
096 30. Sep 2015 opt
16 21. Sep 15:52 private -> /home/encrypted
0 21. Sep 08:15 proc
4096 12. Aug 15:37 root
560 21. Sep 15:50 run
7 30. Sep 2015 sbin -> usr/bin
4096 30. Sep 2015 srv
0 21. Sep 15:51 sys
t 300 21. Sep 15:45 tmp
t 4096 12. Aug 15:39 usr
la 4096 23. Jul 10:
```

✦ Cybersecurity is a growing field, in need of new talent and more manpower. My goal is to incorporate concepts of Cybersecurity into my AP Statistics class to increase my students’ knowledge of this field and ultimately guide them towards an exciting career.

Adams’s Unit

Image Source: https://www.villanovau.com/resources/iss/growing-need-for-cybersecurity-professionals/#.WzUehVVKipo

Adam’s AP Statistics Unit

Essential Question: Can we use statistics to analyze network traffic and detect potential intrusion?

Challenge: Identify the Occurrence of a Cyberattack Based on Statistical Analysis of Network Traffic.

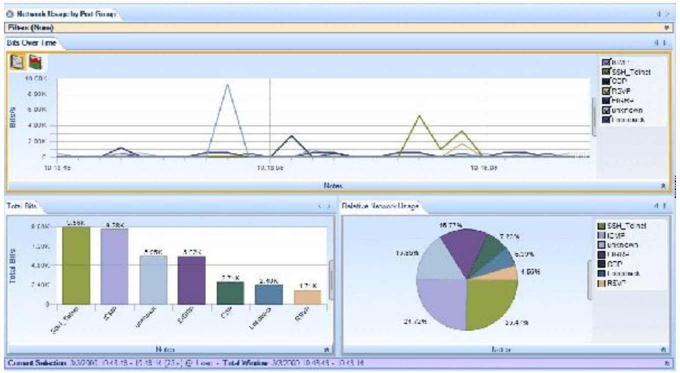


Image Source: https://www.wireshark.org/

Adams’s Unit

Kelly’s Goals and Objectives

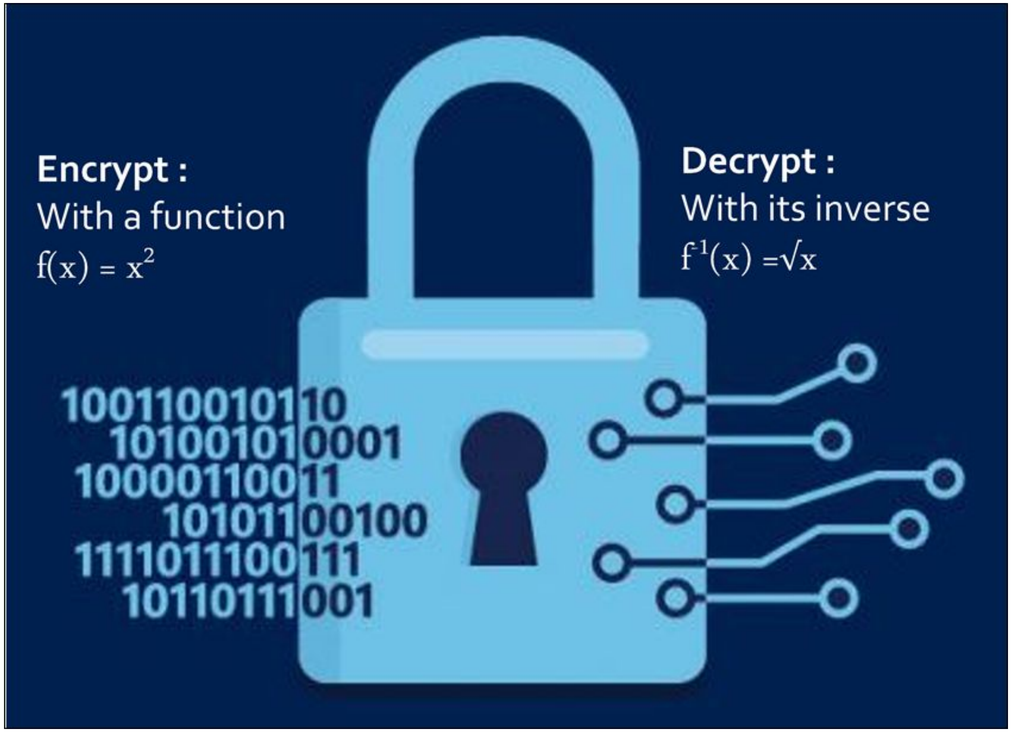
- To show the real world applications of Algebra II, so that students will be more invested in the content, more interested in the class, and better prepared for the newly written Algebra II End of Course exam.

Image Source: https://demmelearning.com/learning-blog/welcome-to-the-real-world-math-in-action/

Kelly’s Algebra II Unit

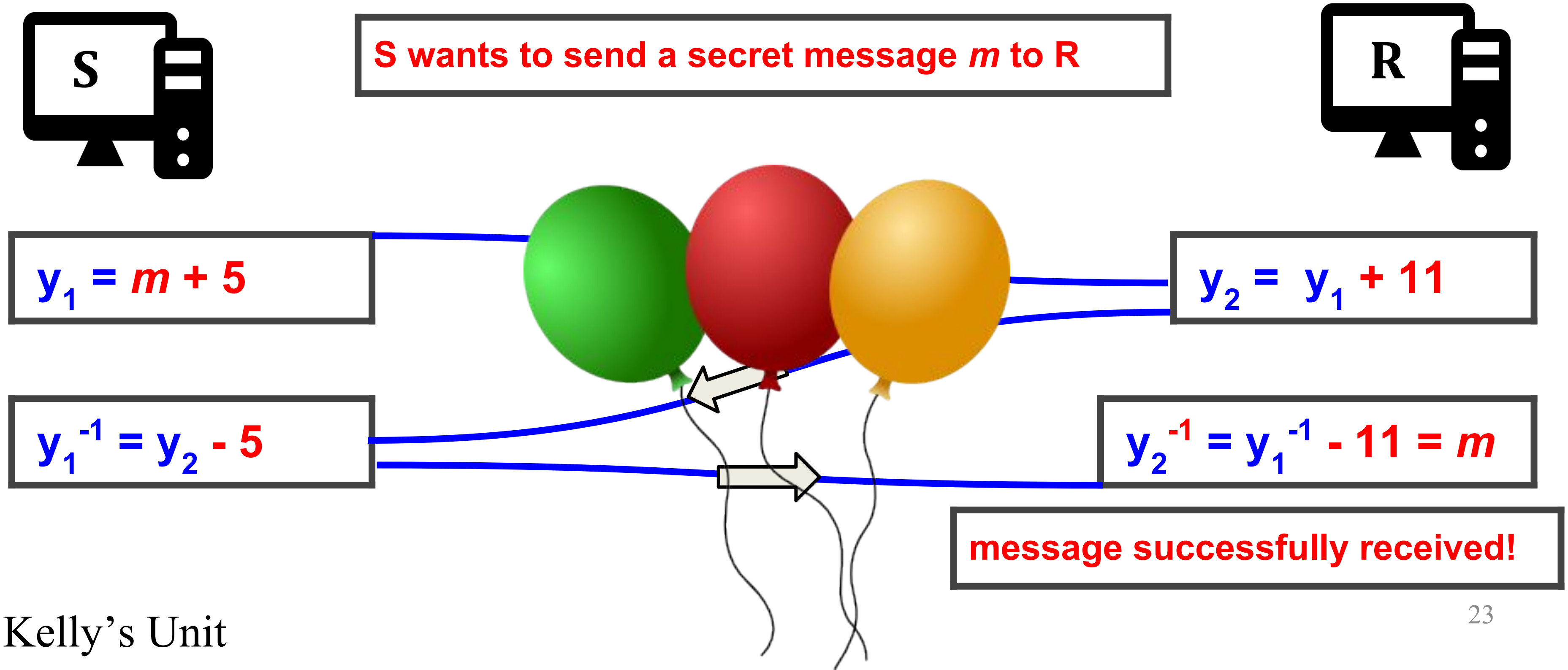
Essential Question:

How can math be used to reliably and effectively encrypt information sent online?



Encrypting with Algebra II

The Challenge: Develop as many *viable* ways as you can to encrypt a message between you and your teammates



S wants to send a secret message *m* to R

$y_1 = m + 5$

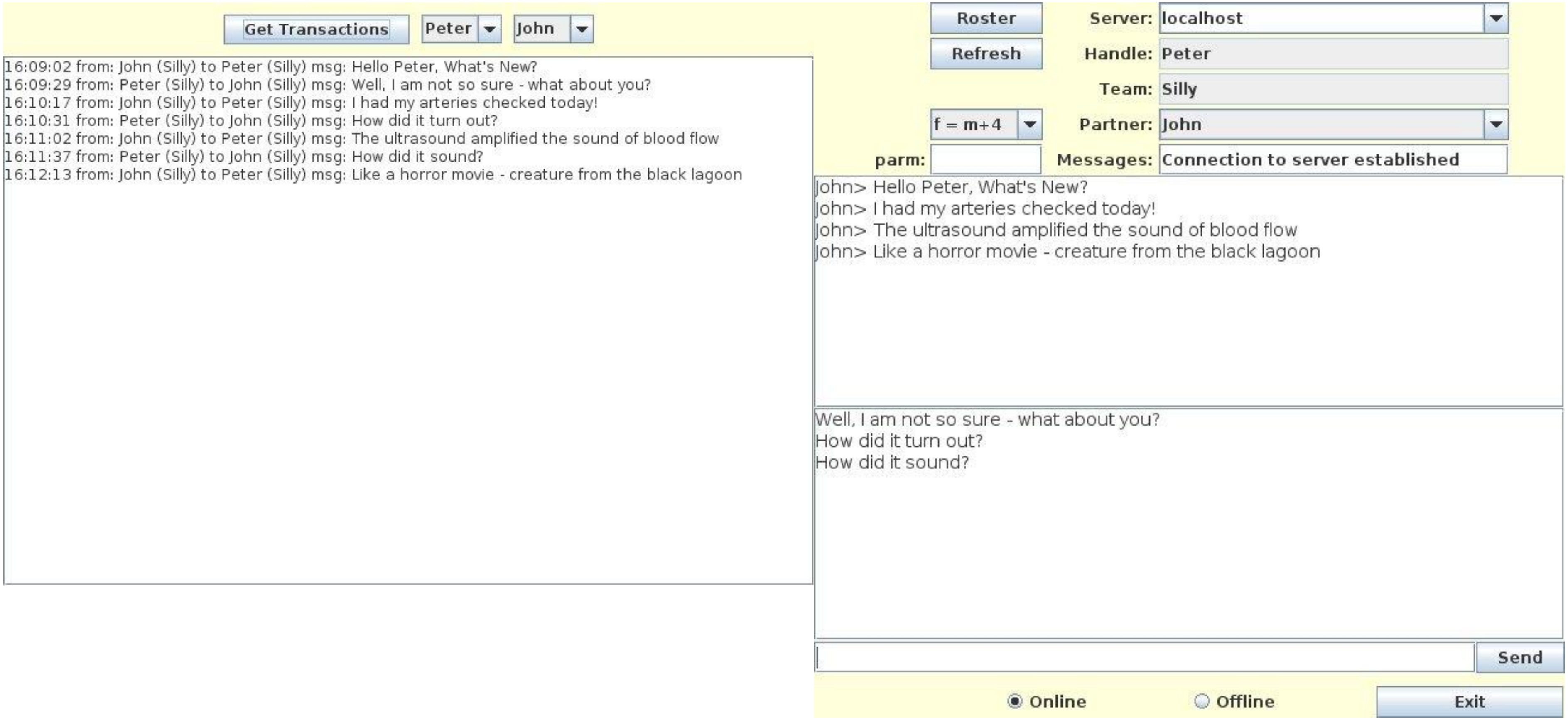
$y_2 = y_1 + 11$

$y_1^{-1} = y_2 - 5$

$y_2^{-1} = y_1^{-1} - 11 = m$

message successfully received!

The Game



```
16:09:02 from: John (Silly) to Peter (Silly) msg: Hello Peter, What's New?
16:09:29 from: Peter (Silly) to John (Silly) msg: Well, I am not so sure - what about you?
16:10:17 from: John (Silly) to Peter (Silly) msg: I had my arteries checked today!
16:10:31 from: Peter (Silly) to John (Silly) msg: How did it turn out?
16:11:02 from: John (Silly) to Peter (Silly) msg: The ultrasound amplified the sound of blood flow
16:11:37 from: Peter (Silly) to John (Silly) msg: How did it sound?
16:12:13 from: John (Silly) to Peter (Silly) msg: Like a horror movie - creature from the black lagoon
```

Server: localhost

Handle: Peter

Team: Silly

f = m+4

Partner: John

parm:

Messages: Connection to server established

```
John> Hello Peter, What's New?
John> I had my arteries checked today!
John> The ultrasound amplified the sound of blood flow
John> Like a horror movie - creature from the black lagoon
```

```
Well, I am not so sure - what about you?
How did it turn out?
How did it sound?
```

Timeline

	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7
Training		🟥	🟥	🟥			
Research		⬛	⬛	⬛	⬛	⬛	
Unit Design	🟥	🟥	🟥	🟥	🟥		
Report/ Summary			⬛	⬛	⬛	⬛	⬛
PPT			🟥	🟥	🟥	🟥	