Department of Defense
Cybersecurity Scholarship

ADVANTAGES

- Full cost of tuition and ALL fees provided for 2024-2025 academic year.
- A $27,000 (undergraduate) or $32,000 (graduate) stipend for room and board.
- The cost of all required books.

BASIC REQUIREMENTS

- Minimum cumulative GPA of 3.2 (undergraduate) or 3.5 (graduate).
- Must be entering junior or senior year or a graduate program in Fall 2024.
- Must be a U.S. Citizen.
- Agree to work for the DoD as a civilian for one year for each year of scholarship received.

INFORMATION MEETING:

November 7 from 12:15-1, lunch provided, in Computer Science room 130.

OPENING & DEADLINE:

November 1, 2023 - Submission portal opens and solicitation materials are available. Application deadline is **February 1, 2024.**

Visit **http://cybersecurity.colostate.edu** for detailed information and instructions on how to apply. Send questions to **compsci_dodcysp@colostate.edu**

Announcements

- Echo360 Recordings Fixed
- Due Date / Grade Error
  - Chapter 10 Quiz Due date caused 0's to appear in Canvas, has been fixed
- Office Hours are starting this week!
- Newshounds
  - Volunteers?
- Upcoming Due Dates
  - Security Overview Discussion Due Tomorrow
  - Security Overview Quiz Due Tomorrow
- The first programming assignment is open for you to view / start
  - Based on this module
  - Take time to read the instructions ASAP

Contacting Me: Rules of Engagement

- Teams!
  - Teams is preferable
  - Then email (greater possibility of being lost)
  - NEVER CANVAS MESSAGE!
- If I don't respond in 24 hours (not including weekends), message me again if urgent
- Be as specific as possible and let me know which course you're in
- General questions can be posted on the general channel
  - Let others see the answer!
- Office Hours
  - Mixed through teams and Office
  - By appointment
  - Fridays 4-6 CSB 450

Office Hours and TAs

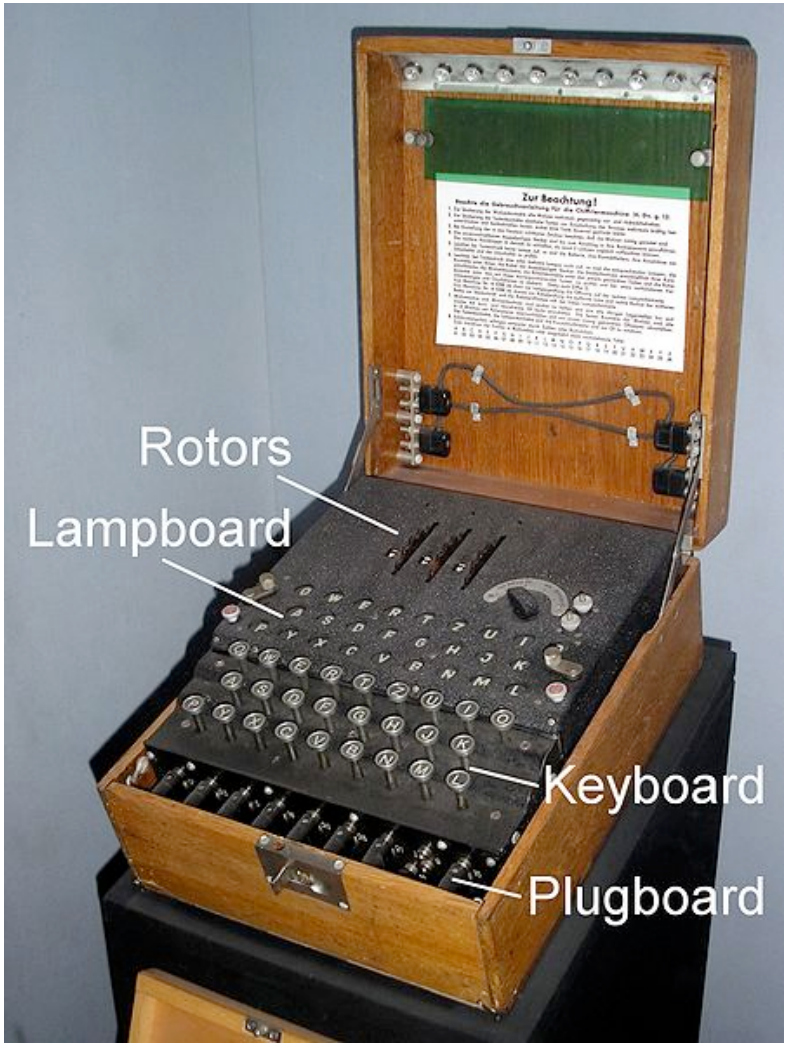
- Tanjim Faruk (GTA)
  - Office hours
    - Tuesday from 10-11 AM and 1-2 PM
    - Thursday 10-11 AM
    - All in CSB 120
- Oluwatosin Falebita (GTA)
  - Thursday 4-5 PM
  - CSB 120
- Zachary Schiro (UTA)
  - Monday, Wednesday 10-12 AM
  - Tuesday, Thursday 3-5 PM
  - Via Teams
- Ariana Mims (Instructor)
  - Friday 2-4 PM in CSB 450 or via Teams

Exercise

- Let's try an experiment!!!
- Break into 4 groups
  - Bank
  - Hospital
  - University
  - High-Tech Firm
- Each Group has 2 sub-teams
  - CISO
  - Hackers
- Discuss strategies for 6 minutes
- Each group (8) give 1 minute summary

CS 356 – Lectures for Week 2
Pelcgbtencuvp Gbbyf

CS 356 – Lecture 2
Cryptographic Tools



Chapter 2

Cryptographic Tools

Chapter 2

Cryptographic Tools

Chapter 2

Cryptographic Tools

History

- The “Caesar Cipher”
  - simple substitution
    - a ->b, b->c, etc
    - “Bring Food” -> “Csjoh Gppe”
- The Unix equivalent: “rot13”
  - rotates 13 characters
  - is its own inverse, so it encrypts and decrypts with the same command
  - pretty much useless

Another Example
Transposition Cipher

- Uses 1 or more shared secret keys

2 C	8 O	9 R	7 N	4 F	6 L	1 A	5 K	3 E	10 S
S	E	N	D	R	E	S	U	P	P
L	Y	T	O	T	H	E	B	R	I
D	G	E	B	Y	T	H	E	C	H
U	R	C	H	X	X	A	M	M	O
N	E	E	D	E	D	U	R	G	E
N	T	L	Y	W	I	T	H	M	A
G	A	Z	I	N	E	S	X	X	X

SEHAU TSSLD UNNGP RCMGM
XRTVU EWNUB EMRHX EHTXD
IEDOB HDYIE YGRET ANTEC
ELZPI HOEAX

Figure 1

2 B	7 L	1 A	3 C	6 K	5 H	8 O	9 R	10 S	4 E
S	E	H	A	U	T	S	S	L	D
U	N	N	G	P	R	C	M	G	M
X	R	T	V	U	E	W	N	U	B
E	M	R	H	X	E	H	T	X	D
I	E	D	O	B	H	D	Y	I	E
Y	G	R	E	T	A	N	T	E	C
E	L	Z	P	I	H	O	E	A	X

HNTRD RZSUX EIYEA GYHOE
PDMBD ECNTR EEHAH UPXXB
TIENR MEGLS CWHDN OSMNT
YTELG UXIEA

Figure 2

More Realistic Encryption

- Block and Stream Ciphers
  - Asymmetric: Public/Private Key-pairs
  - Symmetric: Shared Secret Keys
  - AES, DES, 3DES
  - Computationally fast
- Public Key Encryption
  - RSA, Elliptic Curve
  - Takes more computation time
- Serious Math required to design trapdoor functions:
  - easy to do, extremely hard to reverse

Key Management

- Just as hard a problem as encryption itself
  - why do cryptanalysis when all I have to do is steal your keys?
    - Typically they are just sitting in plaintext in a Linux file somewhere, so hack in
  - How do we distribute keys safely
  - How do we keep secrets safe

Another Crypto Tool

Secure Hashing

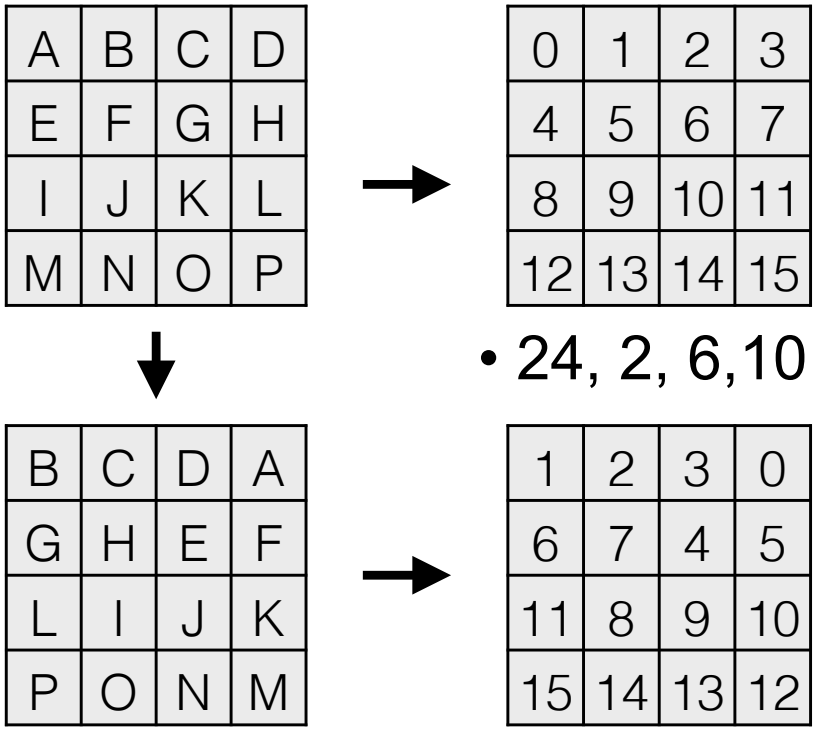
- Builds a one-way unique fingerprint of data to ensure data integrity
- Examples:
  - SHA1, SHA-256, SHA-512
  - MD5
- Linux: `shasum myfile` —>

```
2b725eb93ad70316d5afc76bee618f3e8a8b4588
( SHA1 gives 20 bytes (160 bits) )
2^160 = 1461501637330902918203684832716283019655932542 97
equals about 10^50
```

Simple Insecure Hash

TTH: Toy Tetragraph Hash

- From Problem 2.7 in the text:
  - message = "ABCDEFGHIJKLMNOP"



- 24, 2, 6,10

- step 0: Convert to integers in a 4x4 matrix (pad it to fill)
- step 1: add each column mod 26
- step 2: rotate rows by 1, 2, 3 and reverse last row, then add columns mod 26, then add to previous result mod 26
- step 3: do this for each subsequent 4x4 block of message
- step 4: Convert to alpha

- 7, 5, 3, 1 + previous = 5,7,9,11 —> "FHJL"

Extra Credit

Write a Python Program for TTH

```
python tth.py "I leave twenty million dollars to my friendly
cousin Bill."
Data to be hashed:
 [[[ 8 11  4  0]
  [21  4 19 22]
  [ 4 13 19 24]
  [12  8 11 11]]

 [[ 8 14 13  3]
  [14 11 11  0]
  [17 18 19 14]
  [12 24  5 17]]

 [[ 8  4 13  3]
  [11 24  2 14]
  [20 18  8 13]
  [ 1  8 11 11]]]


number of blocks:  3
numeric hash:  [ 1  5 16  6]

alpha hash:  BFQG
```

Why isn't TTH secure?

- only 26^4 possible hashes (456,976)
- Therefore there will be collisions
- Therefore we can craft a message that will give the same hash as some other message

The preceding was a brief overview

Now on to the real lecture

Cryptographic Tools

- Cryptographic algorithms important element in security services
- Review various types of elements
  - symmetric encryption
  - secure hash functions
  - public-key (asymmetric) encryption
  - digital signatures and key management
  - random numbers (and just how random are they?)
- Example use to encrypt stored data or networked data
  - “data at rest”
  - “data in motion”