Mason Competitive Cyber

Meeting 1: Welcome Back!

Welcome (or Welcome Back)!

- We're The Executive Board
  - **Michael Bailey** – President – Likely Speaker
  - **Paul Benoit** – Co President – Likely Speaker
  - **Ammar Al-Kahfah** – Secretary
  - **Ali Sharaf** – Treasurer
- Faculty Advisor: Jim Jones

What are we?

- Our Official Status: Tier II Registered Student Organization
- Cybersecurity Focus
- Competition Focus
- No barrier to entry

What do we do?

- Weekly meetings (you're at one)
- Different topics every week
  - Linked at competitivecyber.club
- Competes, largely over weekends, largely online

What's coming up?

- Metropolis – Feb 18th
  - Big competition and job/internship fair at UMD
  - Can't guarantee there'll be an in-person after this
  - Seems to be largely jeopardy-style CTF (see next slide)
  - Join **#metropolis** for more
- CryptoParty – Feb 25th
  - SRCT-LUG-CC co-run
  - Zero-experience-needed Cryptography workshop
  - Not related to competition, just for public awareness
  - Join **#cryptoparty** for more

AlexCTF: Disperse

- If you are done with this or know basic ciphers already, go to compete in AlexCTF
- Slides will be available on Slack/GDrive
- **Competing? JC Room D**

What's a CTF?

- Jeopardy Style
  - Question-Answer version
  - Questions worth points, sometimes bounty
  - Cryptography, Forensics, Reverse Engineering, etc
- Attack Defense Style
  - Less common
  - Harder to organize
  - Harder to compete in
  - Often in-person

What's a CND?

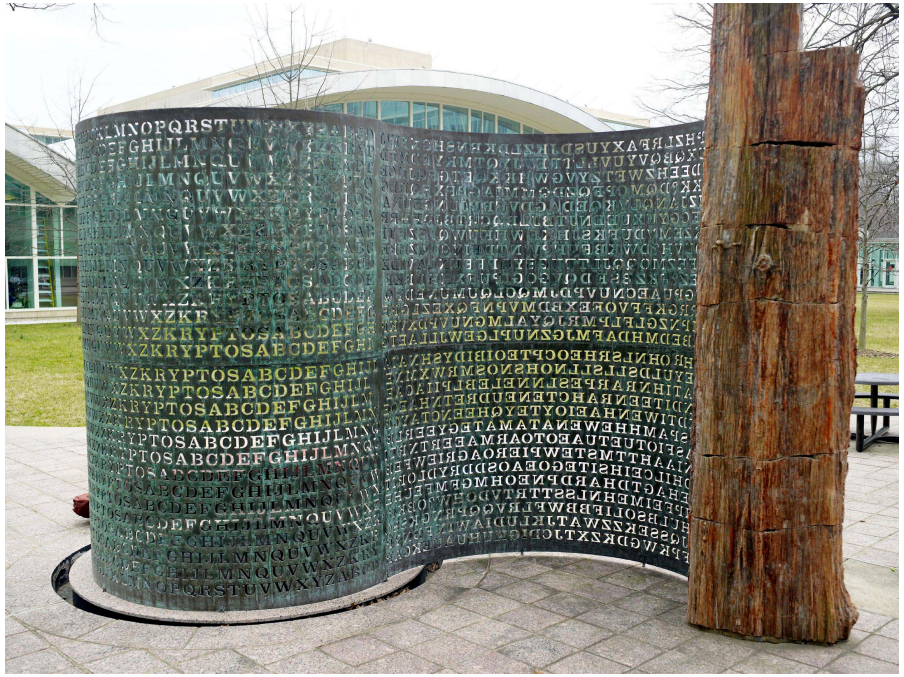
- Computer Network Defense
  - "Blue Team" – Common Industry Term beyond
  - Defending Computer Networks/Systems from Attackers
- CCDC
  - We are working on acquiring the rights to it
- MDC3
  - Defunct as of 2017 due to poor organization

Ciphers

- What are they?
  - Oftentimes (not always) shitty ways to protect information (pretty much except for OTP)
  - Oftentimes basic CTF problems
- Mason CC -> cc nosam
- More common in early historical wartime when nobody had real encryption
- Many kinds, some require keys, some require a code, some require literally just clear text
- **Ciphertext:** Ciphered text you can't immediately get ("cc nosam")
- **Clear text/Plain text:** Basic text you and I read (the "Mason CC")

CIA Statue Kryptos

- Huge statue of ciphertext in front of Langley CIA, partially solved
- Wikipedia has a solid breakdown



Rumkin

- rumkin.com/tools/cipher
- The mecca of basic cipher cracking
- Has every tool ever
- Try each one on all possible combinations, profit

- **Also useful, Cryptogram Solver: http://quipqiup.com/**

Spamming Online Solvers = You Suck at Crypto

- Many of the ciphers we will talk about can be easily solved online **if they are used on their own**
- Seeing ciphers is like “reading the field” in sports
  - It takes practice
  - Not everyone can do it

AlexCTF Crypto1

- ZERO ONE ZERO ZERO ONE ONE ZERO ZERO ZERO ONE ONE ZERO ONE ZERO ZERO ONE ZERO ZERO ONE ONE ZERO ZERO ZERO
- Decode to Binary → 01001100011010010011000001100111
- Decode to ASCII → Li0gLi0uLiAuIC0uLi0gLS4tLiAtIC4uLS4gLSAuLi4uIC4tLS0tIC4uLi4uIC0tLSAuLS0tLSAuLi4gLS0tIC4uLi4uIC4uLSAuLS0uIC4uLi0tIC4tLiAtLS0gLi4uLi4gLiAtLi0uIC4tLiAtIC4uLS4gLSAuLi4uIC4tLi4gLiAtLi0uIC4tLiAuLi4tLSAtIC0uLS4gLQ==
- Base64 decoded → .- .-.. . -..- -.-. - ..-. - .... .-
- Morse decoded → ALEXCTFTH15O1SO5UP3RO5ECR3TOTXT
- Flag → AlexCTF{TH15_1S_5UP3R_5ECR3T_TXT}

“An Enigma” by Edgar Allan Poe

"Seldom we find," says Solomon Don Dunce,
"Half an idea in the profoundest sonnet.
Through all the flimsy things we see at once
As easily as through a Naples bonnet-
Trash of all trash!- how can a lady don it?
Yet heavier far than your Petrarchan stuff-
Owl-downy nonsense that the faintest puff
Twirls into trunk-paper the while you con it."
And, veritably, Sol is right enough.
The general tuckermanities are arrant
Bubbles- ephemeral and so transparent-
But this is, now- you may depend upon it-
Stable, opaque, immortal- all by dint
Of the dear names that he concealed within 't.

“An Enigma” by Edgar Allan Poe

"Seldom we find," says Solomon Don Dunce,
"Half an idea in the profoundest sonnet.
Through all the flimsy things we see at once
As easily as through a Naples bonnet-
Trash of all trash!- how can a lady don it?
Yet heavier far than your Petrarchan stuff-
Owl-downy nonsense that the faintest puff
Twirls into trunk-paper the while you con it."
And, veritably, Sol is right enough.
The general tuckermanities are arrant
Bubbles- ephemeral and so transparent-
But this is, now- you may depend upon it-
Stable, opaque, immortal- all by dint
Of the dear names that he concealed within 't.

go.gmu.edu/ciphers

- Go there now

Caesar

- Regular Caesar: Shift every letter over one letter
- ROT13: So easy, literally just Caesar with a key shift of 13
- Affine Cipher: Adds multiplier to Caesar
- Keyed Caesar Cipher: Encodes alphabet with a key

Example Alphabets, No Shift	
Standard	ABCDEFGHIJKLMNOPQRSTUVWXYZ ABCDEFGHIJKLMNOPQRSTUVWXYZ
Keyed	ABCDEFGHIJKLMNOPQRSTUVWXYZ **rumkinco**ABDEFGHJLPQSTVWXYZ

- **To identify: Same character patterns and the like, just different characters**

Vigenere

- Vigenere Cipher: Like Caesar, changes shift number with each letter, kinda hard at least for beginners, uses a key
- Gronsfeld: Vigenere, but with numbers instead of a key
- Keyed Vigenere: Uses two keys to offset alphabet, for Kryptos sculpture
- Vigenere Autokey: Uses password once, then plaintext to encode

Atbash

- Reverse character set
- A<->Z, B<->Y, etc

Baconian

- Super common in CTFs
- All B's and A's
- Mason CC: ABBAAAAAAABAABAABBBAABBAB AAABAAAABA
- Two versions, one uses distinct codes for all whereas the other uses I and J as the same and U and V as the same
- Typefaces of 5 characters of As and/or Bs

Base64

- Form of encoding to make binary data safe to transport
- **Extremely common** in CTFs
- masoncc -> bWFzb25jYwo=
- How to identify: Alphanumeric blog ending in either nothing, or =’s
- Needs a certain character length so it pads the remainder with =s

Bifid

- Breaks message into row-column coordinate pairs
- Resets the coordinates in a linear format
- Optional alphabet key
- Often omits one letter like J

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

```
letter: A B C D
   row: 1 1 1 1
column: 1 2 3 4

The numbers: 1 1 1 1 1 2 3 4
    Encoded:  A   A   B   O
```

Columnar Transposition

- Write onto column, move columns around
- Simple, on Kryptos statue
- **Double Transposition: Do it twice**
- Übch: Adds number to pad characters

	Unencoded	Rearranged
Column #:	4 2 5 3 1 W H I C H W R I S T W A T C H E S A R E S W I S S W R I S T W A T C H E S	1 2 3 4 5 H H C W I T R S W I H A C W T E S R E A S W S S I T R S W I H A C W T S E

Morse Code

- Pretty sure we all know what this looks like
- “Dit”s and “Dah”s
- Direct conversion
- Pretty distinct
- CTF example: ”Boop Boop” MP3

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 --..	0 -----	1 .----	2 ..---	3 ...--
4 ....-	5	6 -....	7 --...	8 ---..	9 ----.	. .-.-.-	, --..--	? ..--..	- -....-
= -...-	: ---...	; -.-.-.	(-.--.	) -.--.-	/ -..-.	" .-..-.	$ ...-..-	' .----.	¶ .-.-..
_ ..--.-	@ .--.-.	! ---.	! -.-.--	+ .-.-.	~ .-...	# ...-.-	&	⁄ -..-.	

Letters Numbers

- Replace each letter with the number of its position in the alphabet
- Really easy
- masoncc is fun -> 13-1-19-15-14-3-3 9-19 6-21-14

One Time Pad

- The best one
- Pretty much uncrackable if done right
- Relies on truly random key (“the pad”) to encrypt message
- masoncc is fun -> mvsrsey yu jzd

Playfair

- As seen in National Treasure
- “Sliding square” function
  - Feel free to Google particulars
- Takes Optional Alphabet Key

Railfence

- Rearranges the text in a “wave”
- Squash it together
- Concatenate remaining stuff
- Takes number of “rails” (wave lines) and offset (what wave to start on)

Rotate

- Simple, just write text in rectangle grid and rotate 90 degrees left or right

go.gmu.edu/ciphers

- **Solve on your own or go play in CTF in JC Room D**
- We'll be coming around to sign for CS101