2021 Freshers Crypto

Bot

- Bot used to accept flags
- Logging timestamps of flag entries
- Dm next step
- Leaderboard
- Flag: DEV{text}
    - IMPORTANT: Bot can accept any uppercase or lowercase variant of flags (simple .toLower() of input) due to hex implications

Main Ideas

- Spaghetti code
- Hiding data in images (metadata and visually)
- Piet (need obvious clues) (https://github.com/robyntiger/FSym)
- Connecting socials
    - Socials header images
    - Clues in bios
- Collaboration with other societies e.g. gamersoc
    - Clues scattered about (and/or theme hints) in cross-promotional messages
- Clues in channel headers
- Monk’s cipher
- Cookies in header data
- Maze that when solved shows text
- Let’s say you have a grid, say, 10x10, and each cell has a number, 1 or 0 in it (or others for other colours). Hide a key in a clue somewhere. Get people to “colour in” the squares using the key that shows something. What if, on the SAME grid, you also had it indexed and used grid coordinates to expose more squares. That way, you can’t tell what is going to be shown just from the numbers already on it

Rough Idea of the Stages

(Refer to ideas above)

Introduction

- Html thing

Stage 1

- Clue in discord

Stage 2

- Spaghetti code

Stage 3

- Hiding data in images

Stage 4

- Web crawler with hint

Stage 5

- Txt file on github with hint instructions to remove letters

Puzzles

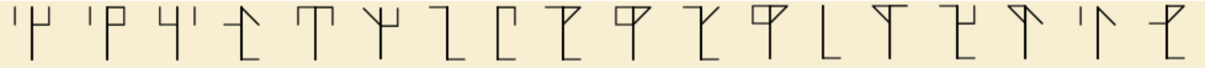
Monk's Cipher

Example Flag: DEV{M0nks_r_d3v5?}

Encode into decimal: 68 69 86 123 77 48 110 107 115 95 114 95 100 51 118 53 63 125

Encode dec into Monk's cipher:

Note from Bobby: I got a friend to test this and I watched them try 4 different anagram solver websites with "Chrome Pink" like myself, and none of them came out with "Monk Cipher" or any variation. Although as Jay showed, at least 1 website does show it, but a 1 in 4 or lower is not good enough chances for someone to see it for the first time without just thinking that it can't be an anagram. Going to have to find another way of showing that it's a monk cipher.

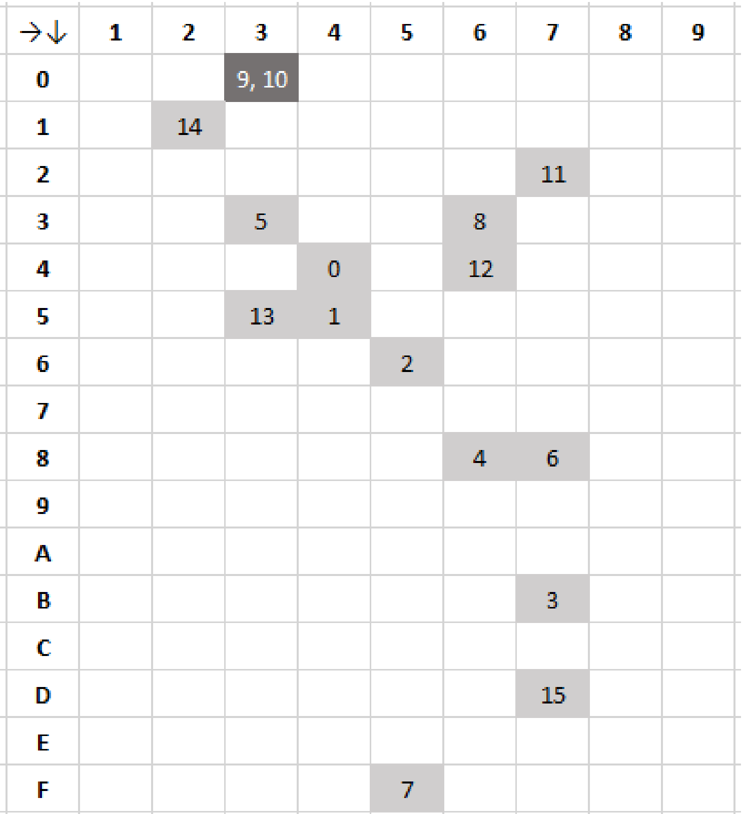


Indexed Grid (Tested)

Example Flag: DEV{h3x_c00rd5!}

Encode into hex: 44 45 56 7B 68 33 78 5F 63 30 30 72 64 35 21 7D

Encode into grid (file available for DL in drive):



→↓	1	2	3	4	5	6	7	8	9
0			9, 10						
1		14							
2							11		
3			5			8			
4				0		12			
5			13	1					
6					2				
7									
8						4	6		
9									
A									
B							3		
C									
D							15		
E									
F					7				

ASCII to Date

Example flag: DEV{d4y5_w3_5t34l}

Convert ASCII to base 7 then to date:

125 126 152 234 202 103 232 104 164 230 102 164 104 224 102 103 213 236

Convert from decimal to day:

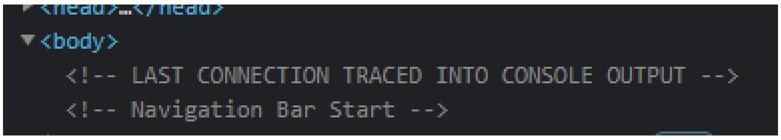
TueWedSat
TueWedSun
TueSatWed
WedThuFri
WedMonWed
TueMonThu
WedThuWed
TueMonFri
TueSunFri
WedThuMon
TueMonWed
TueSunFri
TueMonFri
WedWedFri
TueMonWed
TueMonThu
WedTueThu
WedThuSun

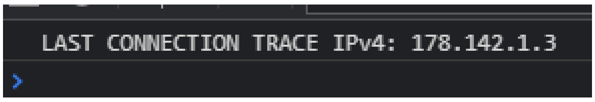
Themes:

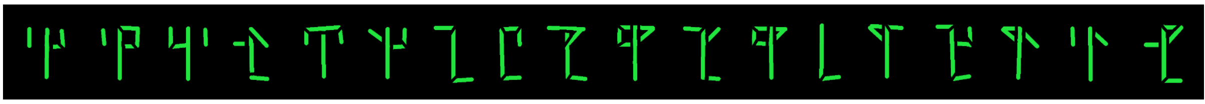
We badly need to brainstorm themes, because creating flags and clues is basically impossible without any idea of a theme. Here's what I'm thinking:

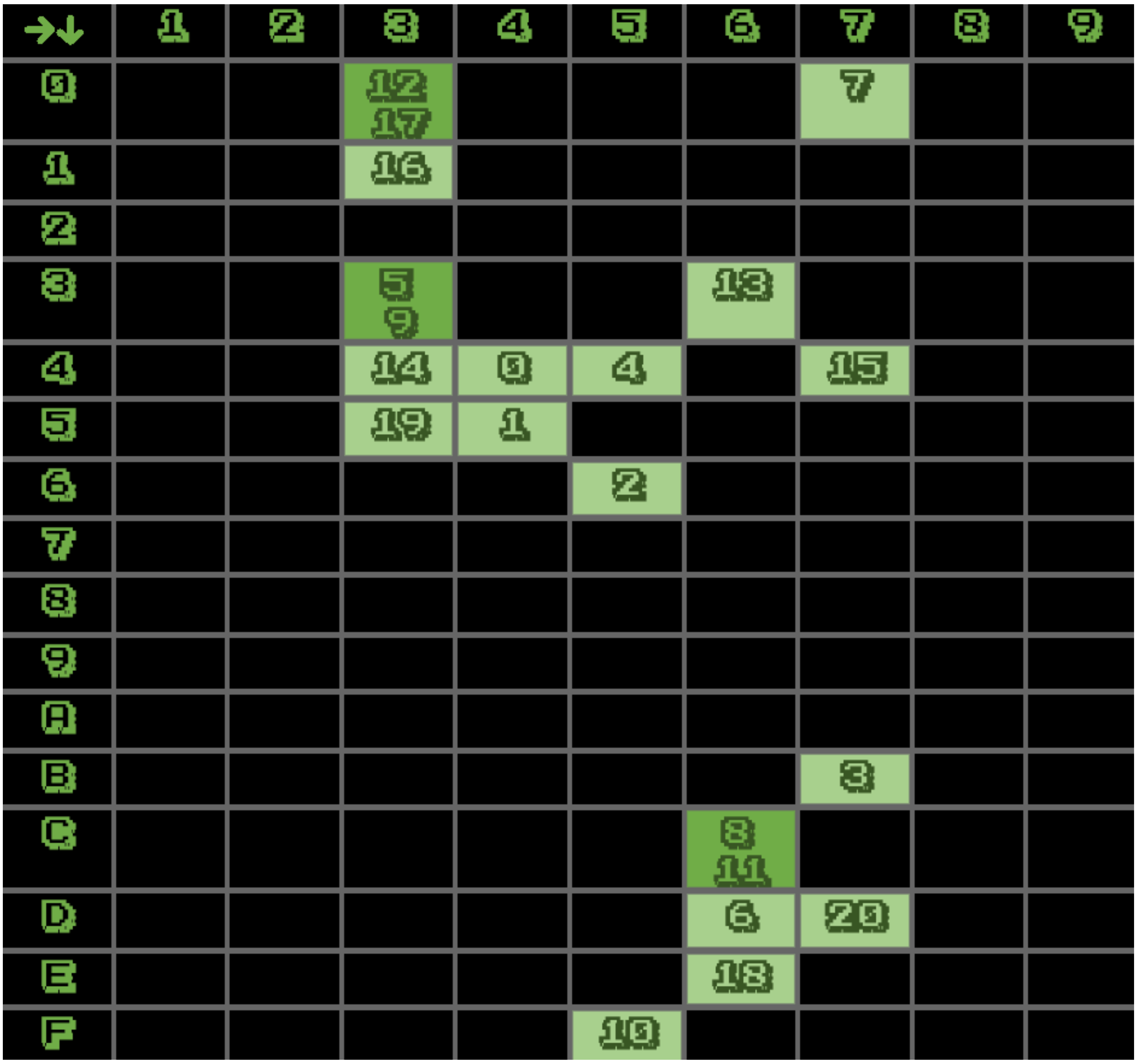
- Hacker has stolen data from DevCorp and he's on the run!
    - He's left a trail of breadcrumbs behind, in the form of puzzles/clues
    - The player (DevCorp employee) is tasked with solving these breadcrumb clues in order to unlock the final passcode to his computer or something (since you found that in the prelog to the story perhaps)
    - Maybe you play the role of the hacker instead and are trying to get vital information from DevCorp for the greater good?
    - DevCorp idea introduces new members to the entire "meme" of the society in a subtle way - this allows us to put fun little easter eggs of devsoc dino, beans, raccoons, octogarf etc, if we can
    - Maybe each flag "unlocks" a new part of the hackers' computer, as in it gives us some image/textfile/whatever or something, or maybe these are just part of the trail

Puzzle Creation/Story Notes:

- In the crypto discord channel, introduce the story.
- Something along the lines of devcorp has been hacked, we need to follow the trail of signatures that the hacker has left behind. The first obvious place to check is the devcorp website where the hacker must have gone to scout for socials/vulnerabilities.
- **Puzzle 1:**
    - Hint: Have you inspected the element comments on our website recently? If not I suggest you do.
    - Subtle hints around the devcorp website to look at the HTML if they haven't already.
    - Inside the HTML, there is the following comment:
    - 

      ```
      ▸<head>…</head>
      ▾<body>
          <!-- LAST CONNECTION TRACED INTO CONSOLE OUTPUT -->
          <!-- Navigation Bar Start -->
      ```
    - In the console is:
    - 

      ```
        LAST CONNECTION TRACE IPv4: 178.142.1.3
      >
      ```
    - Puzzle could potentially be made harder by requiring them to look in javascript.js and looking at hexadress const for the address and converting to ints and using the function to get the output format (or just using ipv4 format) - but this seems too far as it would include code reading that we should avoid
    - Maybe IP could lead to an actual server which gives the flag, maybe IP address in the format or whatever
    - Flag: DEV{178.142.1.3}
- **ELLIE:** Bot hint for next stage - hinting at monk cipher (NOT "Chrome Pink" anagram for reasons I explained previously)
    - Check the banner in the blue-bird app and use the knowledge of the friar to decode it.
- **Puzzle 2:**
    - 
    - 68 69 86 123 77 48 110 107 115 95 114 95 100 51 118 53 63 125
    - Flag: DEV{M0nks_r_d3v5?}
    - Twitter banner
    - DevCorp begins to suspect that the hacker is a monk and that it makes sense because they have been stealing from ancient monk temples to sell for large amounts of money on the black market
- **ELLIE:** Bot hint from next stage some riddle to do with "hex grid"
    - The number IG is useful here, going across then down and into ascii will give you the flag.

- **Puzzle 3:**
  - Flag: DEV{T3mpl3_l0c4t10n5}
  - 44 45 56 7b 54 33 6d 70 6c 33 5f 6c 30 63 34 74 31 30 6e 35 7d
  - 

→↓	1	2	3	4	5	6	7	8	9
0			12 17				7		
1			16						
2									
3			5 9			13			
4			14	0	4		15		
5			19	1					
6					2				
7									
8									
9									
A									
B							3		
C						8 11			
D						6	20		
E						18			
F					10				

  - Image name is “Acr055_th3n_d0wn”
  - Instagram
  - The flag shows that this grid is the locations of all the monk temples that they stole artefacts from
- **ELLIE:** Bot hint for next stage - something about converting ascii to base 7
  - The events channel in the discord server is your friend here, once you see the base 7 pattern you’re halfway there, now use the American Standard Code for Information Interchange to get the flag.
- **Puzzle 4:**
  - Flag: DEV{d4y5_w3_5t34l}
  - 125 126 152 234 202 103 232 104 164 230 102 164 104 224 102 103 213 236
  - TueWedSat TueWedSun TueSatWed WedThuFri WedMonWed TueMonThu WedThuWed TueMonFri TueSunFri WedThuMon

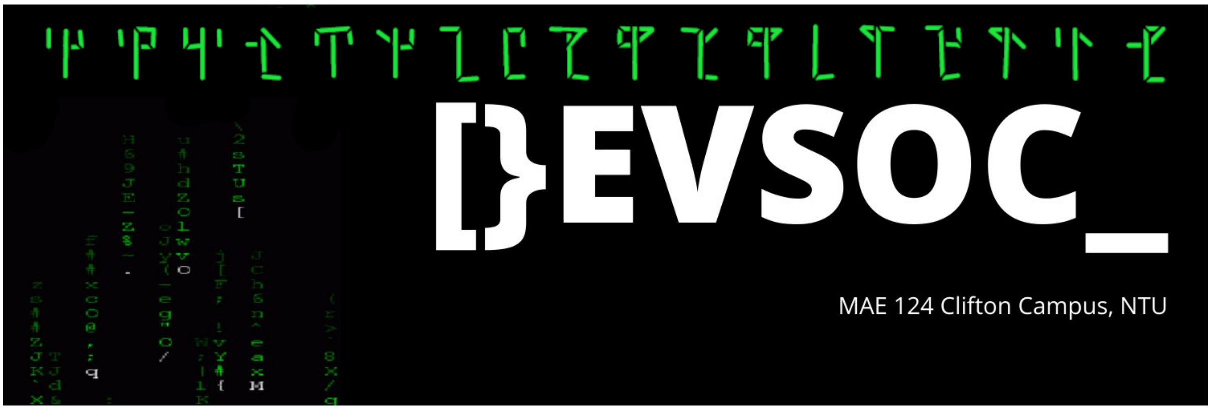
    TueMonWed TueSunFri TueMonFri WedWedFri TueMonWed TueMonThu WedTueThu WedThuSun
  - **ROBYN:** You have free reign on this one, do whatever that fits the aesthetic (although keep the spacings correct). As long as no extra hidden “patterns” emerge from the aesthetics that people may try to go down the path of, I’m excited to see what you come up with :)
  - Discord events channel

Stuff to post/do on Monday morning:

Discord:

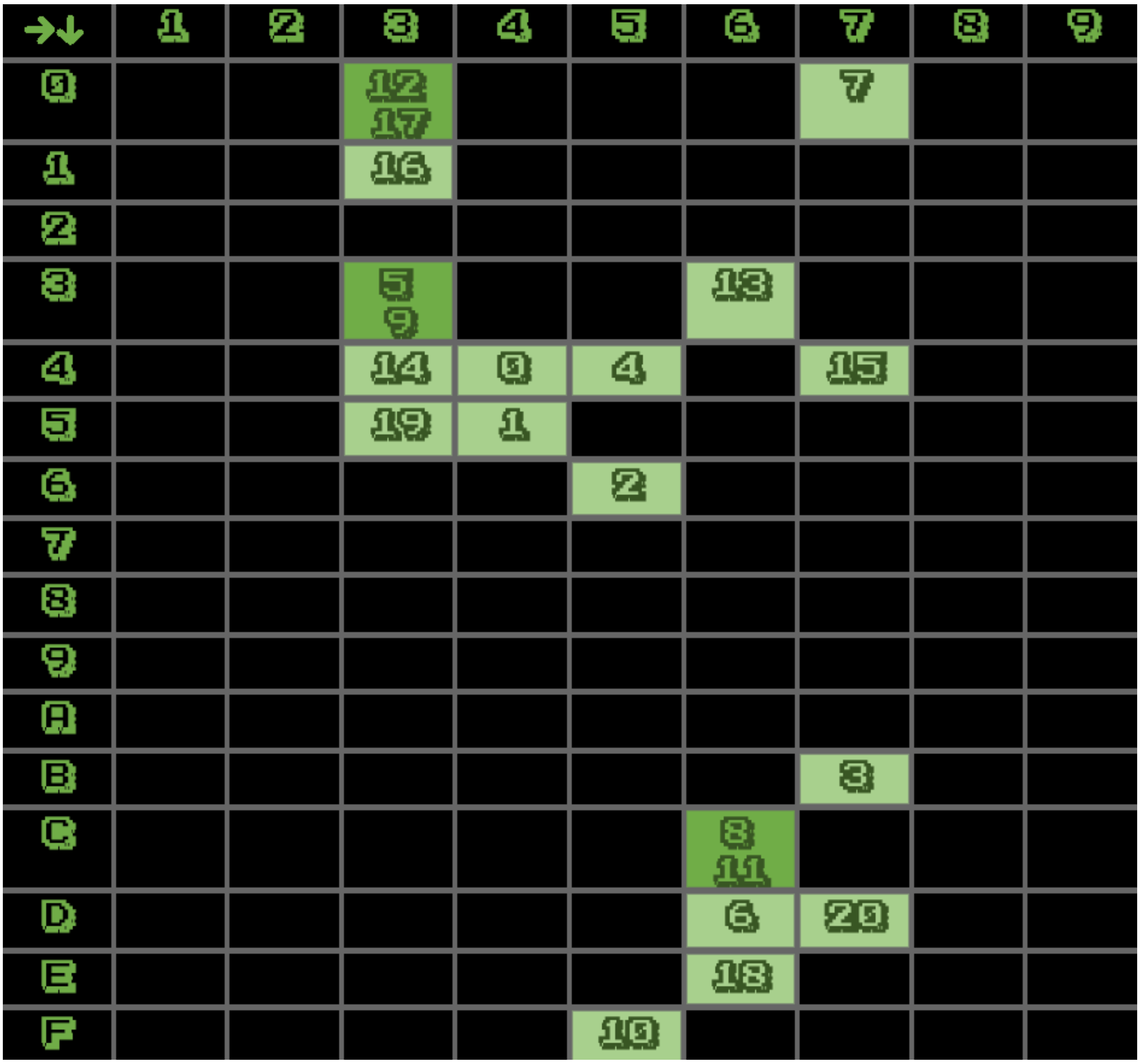
- Announcement in events channel (Bobby has message)
  - Upload the crypto poster + animated crypto logo
- Put the calendar puzzle into events channel (Bobby has message)
- Unlock project-revil channel

Twitter:

- Put this new image into the new banner
- 

Instagram:

- Upload puzzle 3 grid onto instagram - make sure it’s called Acr0ss_th3n_d0wn

- 

→↓	1	2	3	4	5	6	7	8	9
0			12 17				7		
1			16						
2									
3			5 9			13			
4			14	0	4		15		
5			19	1					
6					2				
7									
8									
9									
A									
B							3		
C						8 11			
D						6	20		
E						18			
F					10				