Cipher Learning Tool

Goal:

- Get people interested in ciphers and encryption
- Improve knowledge on password security (showing how quickly a password can get cracked)
- Describe history and usage (i.e. WWII, now, etc.)

Functionality:

- Show how long it would take to break a cipher and what it'd look like.
  - i.e. Ceaser cipher
- make visualization showing brute force
- Suggest books, movies, articles, etc.

Target Audience:

- People new to ciphers
- Menu for more learning

Scope:

- Shift Ciphers:
  - Caesar: default by 1, turn do ROT13, allow user to choose
  - Vigenère
- Substitution Ciphers:
  - Simple/Monoalphabetical
  - Nomenclator
  - Beale
- Transposition Cipher

Planned Implementation:

- Cipher creation, breaking, & timing: python3
- UI: Node JS
- Distribution: Docker

Design (1/2)

Cipher | About Ciphers | Create | Break | Passwords

Explanation of Ciphers.
Why people care.
What this tool is meant to do.

Cipher | About Ciphers | Create | Break | Passwords

About Ciphers

What is a Cipher?

Where did they come from?

What different types of Ciphers are there?

How are they used now?

Additional information:
- Movies
- Books

Cipher | About Ciphers | Create | Break | Passwords

Create Cipher

Plain Text

Cipher Text

response

Caesar Shift

Shift

Description of cipher

Plain	Index	Cipher	Index
A	0	B	0
B	1	C	1
C	2	D	2
⋮	⋮	⋮	⋮
Y	25	Z	25
Z	26	A	26

Responsive Text Box: Estimated time to crack

drop down to do cipher in different ways

goes away if not shift

automatically adjust upper and lower case for substitution cipher

based on cipher and length of plain text

have this in one column

Cipher | About Ciphers | Create | Break | Passwords

Break Cipher

Assumes we don't know what cipher was used.

Enter cipher text

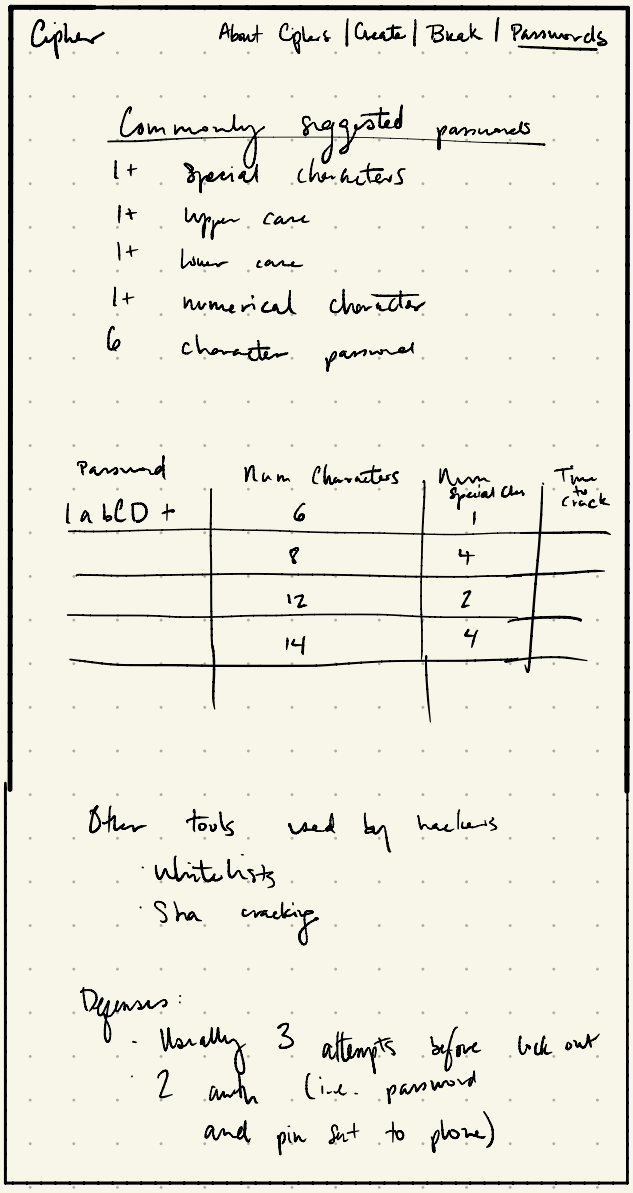
Calculate

Plain Text

responsive

Time Spent

Design (2/2)



Drive point home that non-alphabetical doesn't always mean more time to crack

Scroll