

# 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. Caesar cipher
- make visualization showing brute force
- Suggest books, movies, articles, etc.

## Target Audience:

- People new to ciphers
- Me & for more learning

## Scope:

- Shift Ciphers:
  - Caesar: default by 1, turn to 2013, allow user to choose
  - Vigenère
- Substitution Ciphers:
  - Simple/Monalphabetic
  - 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

  
response

Drop down  
to do cipher  
in different  
ways

goes  
away  
if  
not chg

If user  
automatically  
substituting  
the cipher  
then  
allow every  
user to  
break it

Board  
on cipher  
and length  
of plain text

Caesar Shift      # Shift

Decryption of cipher

Plain Text	Index	Plain Index	Cipher Index
A	0	0	
B	1	1	
C	2	2	
D	3	3	
E	4	4	
F	5	5	
G	6	6	
H	7	7	
I	8	8	
J	9	9	
K	10	10	
L	11	11	
M	12	12	
N	13	13	
O	14	14	
P	15	15	
Q	16	16	
R	17	17	
S	18	18	
T	19	19	
U	20	20	
V	21	21	
W	22	22	
X	23	23	
Y	24	24	
Z	25	25	

Responsive Text Box: Estimated time to break

Cipher

About Ciphers | Create | Break | Passwords

Break Cipher

Answer we don't know what cipher was used.

  
Enter cipher text

Calculate

  
Plain Text

response

Time Spent:

have this  
in one column

## Design (2/2)

Cipher      About Ciphers | Create | Break | Passwords

Commonly suggested passwords

1+	special characters
1+	upper case
1+	lower case
1+	numerical character
6	character password

Password	Num Characters	Num Special Chs	Time to crack
LabLCD+	6	1	
	8	4	
	12	2	
	14	4	

Other tools used by hackers

- Whitelists
- Sha cracking

Defenses:

- Usually 3 attempts before lock out
- 2 auth (i.e. password and pin set to phone)

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

{ scroll