

Spy Decoder

Nate Higgs*

April 7, 2020

*for K&A

1 Assembly

The decoder consists of three parts:

Cap

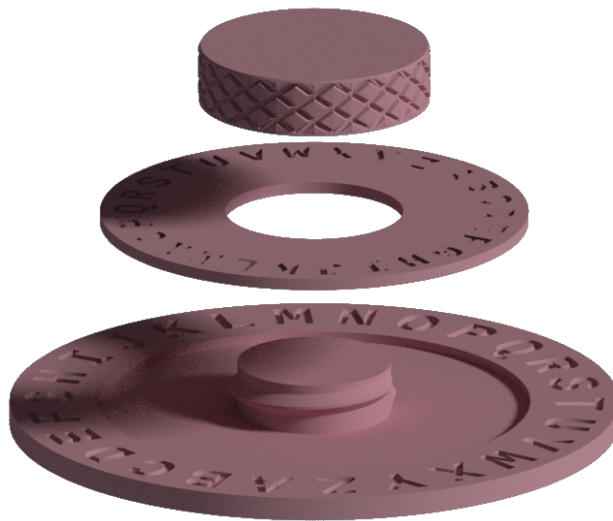
Holds everything together and prevents the inner ring from turning when tightened.

Inner Ring

Contains all the letters of the alphabet. This is used with the **encoded** part of the message.

Base

Holds the inner ring and contains all letters of the alphabet. This is used with the **decoded** part of the message.



2 Decode A Message

This section shows how to decode a message. You will need a message and the encryption key for the message.

Sample Message and Key

R O V V Y

$$Key = \frac{A}{K}$$

Set the Encryption Key

Set your wheel to match the encryption key for your message.



2.1 Decode Your Message

Locate the first letter of your message on the **inner wheel** and write down the matching letter from the outer wheel above this letter. Repeat this step for all letters of your message.

H E L L O
R O V V Y

HELLO is your decoded message!

3 Encode A Message

This section shows to to encode a message. Once encoded you will need to give the recipient the message **and** key.

Choose an Encryption Key

Set the inner wheel to so that the letters do not match the outer wheel. Write down a matching pair of letters from the outer and inner wheel.



$$Key = \frac{A}{K}$$

Write down you message

H E L L O

Encode Your Message

Locate the first letter of your message on the **outer wheel** and write down the matching letter from the inner wheel below this letter. Repeat this step for all letters of your message.

H E L L O
R O V V Y

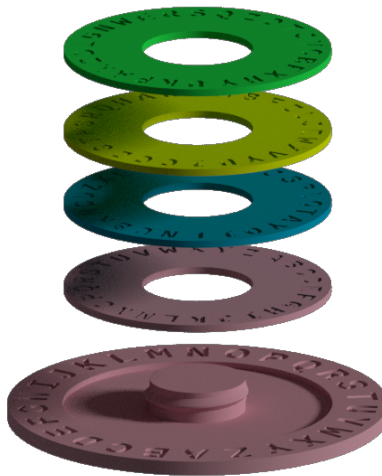
ROVVY is your encoded message!

4 Cheat Sheet

1. Set the encryption key
2. Encode/Decode your message
 - To encode (*lock*) your message go from the outer wheel to the inner wheel
 - To decode (*unlock*) your message go from the inner wheel to the outer wheel

Tips

- Don't keep the encryption key with the message!
- Use different wheels and keys to keep different recipients from reading each others messages



- When encoding or decoding a message don't lookup the same letter more than once. i.e. If you lookup the letter "E" write down all the matches for "E" at that time.

5 Appendix

5.1 Crypto

This type of encryption is called a shift cipher, Caesar cipher, or ROT cipher. For more information on this type of encryption check out the resources below.

[Shift cipher](#)

[ROT cipher](#)

5.2 Advanced Concepts

The replaceable inner rings were created to help teach the concept of salts. Salts are random characters used to make encryption stronger. Salts are approximated here by the random order of the alphabet.

[Salts](#)

5.3 Historical Tie In

This type of encryption was the basis for the German enigma machine. The breaking of the enigma code was one of the biggest factors in the outcome of WWII.

[Enigma](#)