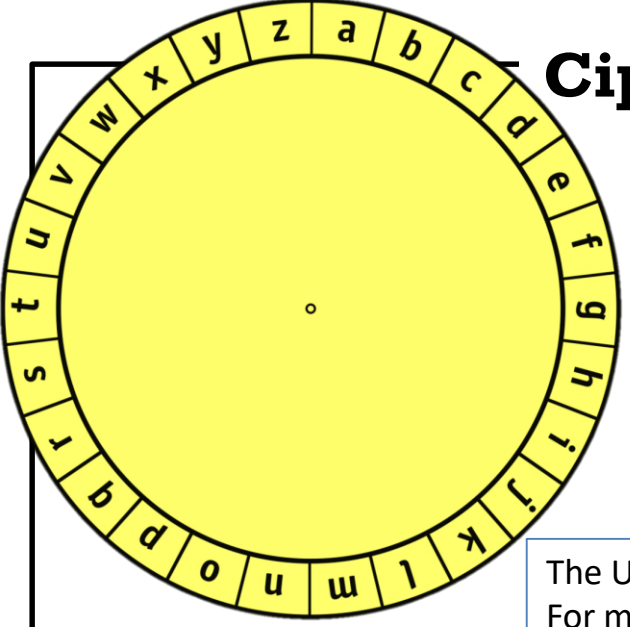
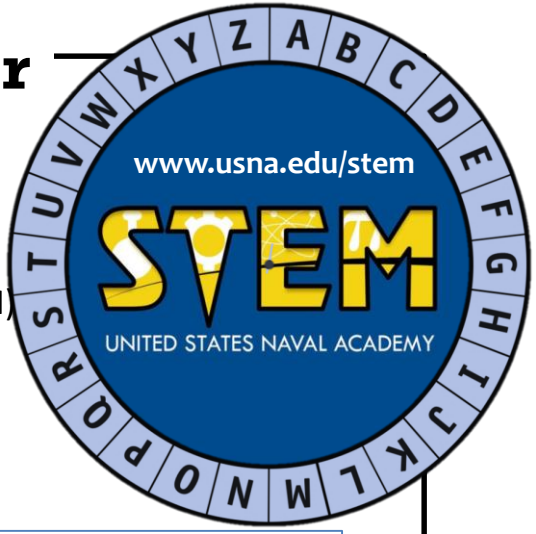
Cipher Disk/Caesar Cipher



In the times of Julius Caesar, a shift cipher was adequate to conceal information because Latin grammar was complicated and the populace was illiterate. The recent inventions of the rotor cipher machines (WW I) and of computers (WW II) have required increased complexity in encryption techniques that rely heavily on computer science principles andcomplex mathematical algorithms.



NAVY NOTES

The US Navy has been the world's leader in cryptography For more than 80 years. From the ON THE ROOF GANG who intercepted enemy messages from a rooftop in Washington DC in the 1920s to the Navajo Code Talkers who encrypted, transmitted and decrypted messages during WWII to the high-tech data links, connectivity and surveillance/reconnaissance techniques of today, the Navy seeks to maintain its information dominance as the battlespace of information shifts to the electromagnetic spectrum.

1. **Cut** out the two cipher disks.
2. **Place** the smaller disk on top of the larger disk.
3. **Attach** the disks using a paper fastener.
4. **Create** a key by choosing a letter on the small disk (encryption) and lining it up with a different letter on the large disk (decryption).
5. **Think** of a secret message. Find each letter on the large disk (message), and write down the corresponding letter on the small disk (code). Ask a partner to crack the code using your key.

Try it out!

Key: Large Disk = P
Small Disk = S

Encryption: **VWHP LV DZHVRPH**
(small disk, code)

Decryption: **STEM** ____ _____
(large disk, message)

https://www.naval-technology.com/features/featureeighty-years-of-navy-cryptography-where-to-next-4922639/