CRYPTOGRAPHY

THE SCIENCE OF SECURE INFORMATION

By: Hajar, Becky, and Grace
Artemis 2021

VOCAB TERMS

CIPHER

A secret or disguised way of writing code.

PLAINTEXT

A text that is not specially formatted or written in code.

ENCODE

To convert a message from one system of communication to another

DECODE

To convert a coded message back to its plaintext

ENCIPHER

To convert a message into cipher

DECIPHER

To convert an enciphered message to it original text

WHAT IS CRYPTOGRAPHY

Cryptography is a process in which the letters of each word are “scrambled”, so that certain pieces of information are hidden.

In fact, this word gives us this definition if we simply break down the word…

Crypt-o-graphy

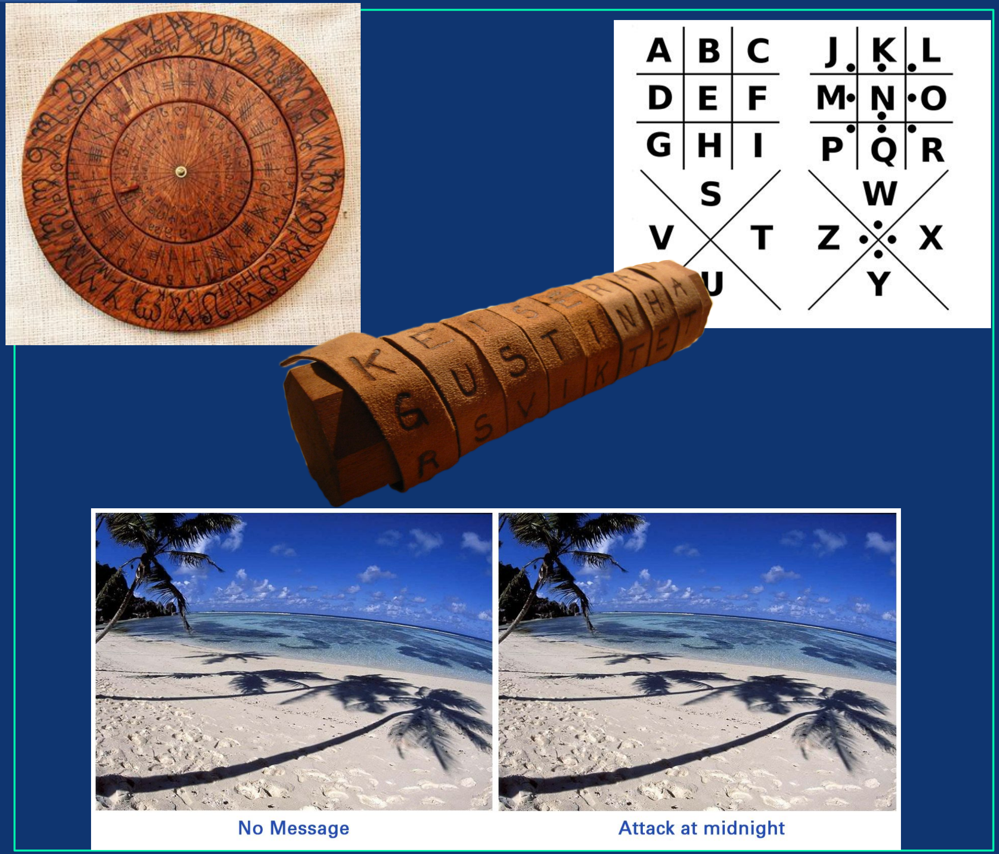
The prefix “crypt-” means hidden and the suffix “-graphy” means writing. So, all together it says hidden writing

ASYMMETRIC VS. SYMMETRIC CRYPTOGRAPHY

Symmetric encryption is when you only have to figure out one “key” to encrypt and decrypt the ciphered text. Asymmetric encryption is the newer method of the two. Unlike symmetrical encryption, there are two different “keys” or ways to encrypt and decrypt. Then through the internet, “secret” keys are exchanged that only a select few get in order to decrypt the text. Then theres a public key that encrypts the plain text back to the ciphered text.

FUN FACTS ABOUT CRYPTOGRAPHY

- In the days of the Roman Empire, encryption was used by Julius Caesar and the Roman Army to cipher text.
- Encryption is known to be the easiest and most practical way to protect electronically stored data.
- The most popular Cryptographic Techniques include:
  - The Caesar Cipher
  - Scytale
  - Steganography
  - The Pigpen Cipher



No Message

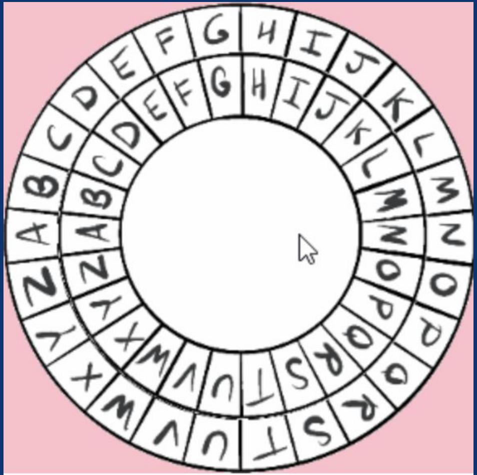
Attack at midnight

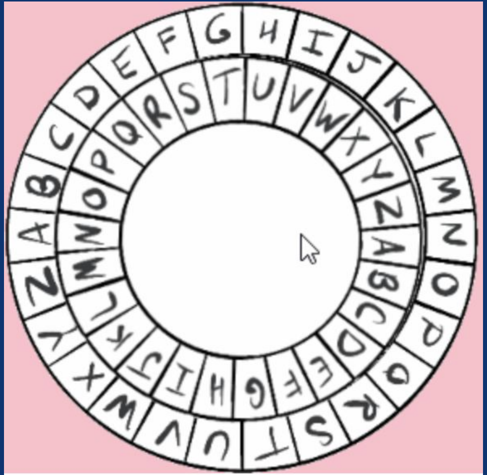
WHAT IS THE CAESAR CIPHER?

Caesar Cipher is standard example of ancient cryptography that is said to have been used by Julius Caesar himself. Surprisingly enough, Caesar Cipher is known by many names including the shift cipher, Caesar's code, and even Caesar shift.

HOW TO USE THE CAESAR CIPHER

This wheel to the right is how we decipher the code. Each letter represents a different number, for example a=0 and then all the way to z which equals 25. These numbers will tell us the shift of the wheel. When you input a certain shift it will take the inner wheel and turn it clockwise in the number of shifts. In the top picture there is no shift, but as we can see in the second picture there is a shift of 11.


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

ANCIENT CRYPTOGRAPHY VS. CURRENT CRYPTOGRAPHY

ANCIENT EGYPT

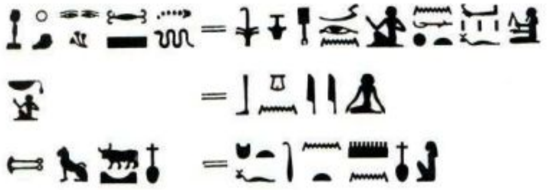
In about 1900 B.C., hieroglyphics were introduced to Ancient Egypt. Numbers of unusual symbols obscure the meaning of the symbols, Egyptians did this because they were likely that they wished to preserve the sacred nature of their religious rituals from common people.

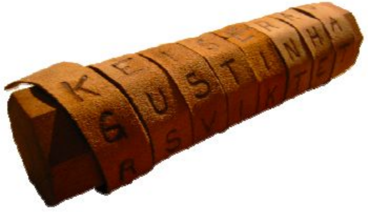
As the Egyptain Culture evolved, hieroglyphic cryptography became more common, this method was relatively easy to translate for those who can read and write. Egyptain Cryptography was used for scribes to impress others by showing that he could write at a higher level.

ANCIENT GREECE AND ROME

In about 500 B.C., the Spartans developed a device called Scytale, which was used to send and receive secret messages. In today's standards, the Scytale would be very easy to decipher, but 2,500 years ago the percent of people who could read and write was relatively small.

Julius Caesar, who was the commander of the Roman army, solved the problem of secure communication 2000 years ago. Caesar developed a method in which he would substitute letter for different letters. Only those who knew the substitutions could decipher the secret messages, which gave the Roman army a big advantage during war.





ANCIENT CRYPTOGRAPHY VS CURRENT CRYPTOGRAPHY

Modern cryptography is the cornerstone of computer and communications security. Its foundation is based on various concepts of mathematics such as number theory and probability theory. Cryptography isn't used for secret messages anymore, it is used as a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication(basically identity theft or theft of relevant and sensitive information).

From the simple substitution methods of the ancient Greeks to today's computerized algorithms, various codes and ciphers have been used by both individuals and governments to send secure messages. As an increasing amount of our personal communications and data have moved online, understanding the underlying ideas of internet security has become increasingly important.

Ancient Cryptography	Modern Cryptography
More Complicated Letter Scrambling	Based on Computational Complexity-the study of what Computer can and can't do efficiently
Military	All you need is a working device
Secrecy of protocol algorithm	Provable security based on mathematics
Requires cryptosystem(aset of algorithms to encode or decode messages securely) for communicating confidentially	Only requires substitute letter(shift)

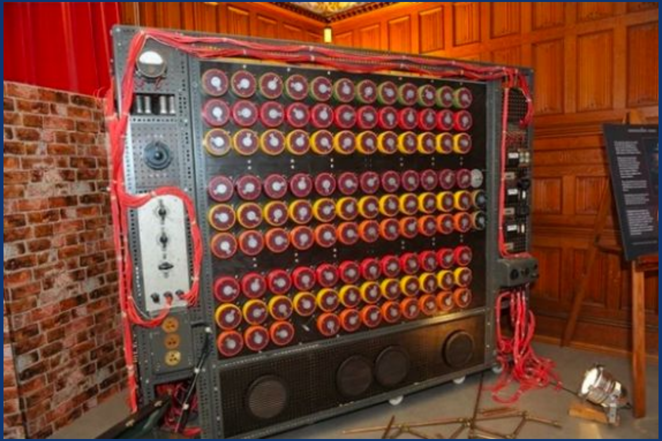
CRYPTOGRAPHY USED IN WORLD WAR II

At the end of World War 1, the Enigma was created, an electro-mechanical machine that was used for encryption and decryption of secret messages. An Enigma machine allows for billions and billions of ways to encode a message, making it incredibly difficult for other nations to crack German codes during the war — for a time the code seemed unbreakable.

Cracking the Enigma was the single most important victory by the Allied powers during WWII. The allies prevented some attacks, but had to allow some attacks to be carried out to avoid Nazi suspicion they had insight to German communication despite the fact they they had knowledge to stop them.

ALAN TURING AND THE BOMBE MACHINE

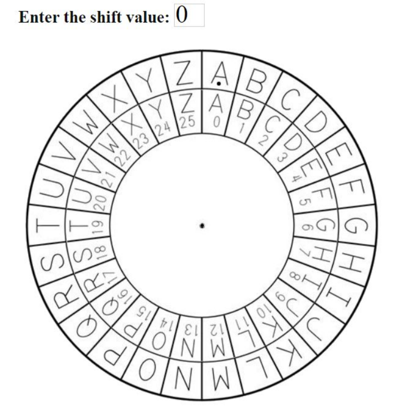
Alan Turing designed a machine called the Bombe machine(Gordon Welchman included improvements to the machine) which used electric circuits to solve an Enigma encoded message. The Bombe machine would try to determine the settings of the rotors and the plugboard of the Enigma machine used to send a given coded message.

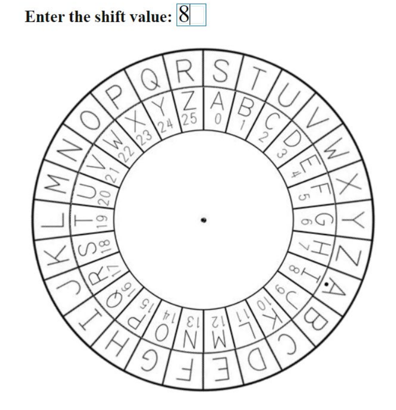


Enigma machines typically changed settings every 24 hours. Every day, there were many billions of possible combinations. The Bombe helped Codebreakers discover part of an Enigma key – the settings of the Enigma machine used to encipher a message. Enigma's rotors and plugboard meant the Germans could use one of many millions of different encryption settings to send their messages.

CAESAR CIPHER CHALLENGE

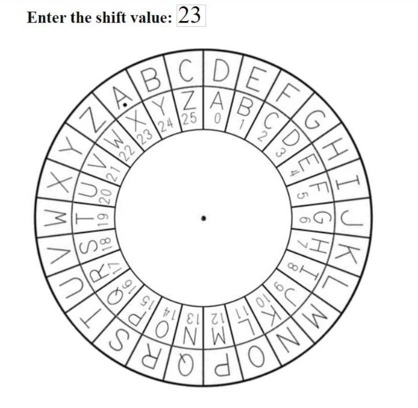
Encipher Challenge
Word - Food


Enter the shift value: 0


Enter the shift value: 8

Answer - NWWL

Decipher Challenge
Word - DROI


Enter the shift value: 23

Answer - Gurl

WORK CITED

- https://blog.pwere-sure-you-dont-know-these-10-interesting-facts-about-encryptioncloud.com/
- https://interestingengineering.com/11-cryptographic-methods-that-marked-history-from-the-caesar-cipher-to-enigma-code-and-beyod
- https://languages.oup.com/google-dictionary-en/
- https://www.merriam-webster.com/dictionary/
- http://www.faqs.org/espionage/Cou-De/Cryptology-History.html
- https://www.tutorialspoint.com/cryptography/modern_cryptography.htm
- https://my.eng.utah.edu/~nmcdonal/Tutorials/EncryptionResearchReview.pdf
- https://brilliant.org/wiki/enigma-machine/
- https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences
- https://searchsecurity.techtarget.com/definition/cryptography
- https://www.tnmoc.org/bombe