History of Encryption

Reading

25m - 40m

Status | Incomplete

Introduction

The technical definition of **encryption** is the process of converting human-readable plain text to incomprehensible text, also known as **ciphertext**. In simpler terms, it is a process of scrambling readable data and altering it so that it appears random. Encryption requires the use of a cryptographic key: a set of mathematical values that both the sender and the recipient of an encrypted message agree on.

A **cryptographic key** is a string of characters used within an encryption algorithm for altering data so that it appears random. Think of it as you would a physical key. It locks (encrypts) data so that only someone with the right key can unlock (decrypt) it.

> The type of data shared on the internet today can be confidential and sensitive, leading individuals and organizations to protect their ideas and information they share. Think about the volume of data shared over the Internet today. From private messages, photos, banking information, confidential conversations, digital signatures, passwords, contracts, and private emails, just to name a few.

> Reflection Question: What methods of encryption can you think about that may have been used in ancient times?

History of Encryption

Encryption has been used for centuries and is sometimes associated with military practices. From as far back as circa 600 BC, the ancient Spartans used a scytale device to send secret messages during battle. The Romans around 60 BC used a simple and effective encoding method at that time that proved to be very effective. The first encrypted messages consisted of replacing simple characters in a message or, in a certain way, changing the characters' positions so that it was almost impossible to read the text without reordering it in a given way. In this reading you will explore some of the most important encryption techniques used in history.

Today, many communication technologies, including phones, digital television, and ATMs, rely on ciphers to maintain security and privacy.

Cipher

To fully understand the methods discussed in this reading, you need to know what a cipher is. A **cipher** is an algorithm for encrypting and decrypting data.

Traditionally, ciphers used these two main types of transformation:

- Transposition ciphers keep all the original bits of data in a byte but mix their order.
- Substitution ciphers replace specific data sequences with other data sequences.

For example, one type of substitution would be to transform all bits with a value of 1 to a value of 0, and vice versa.

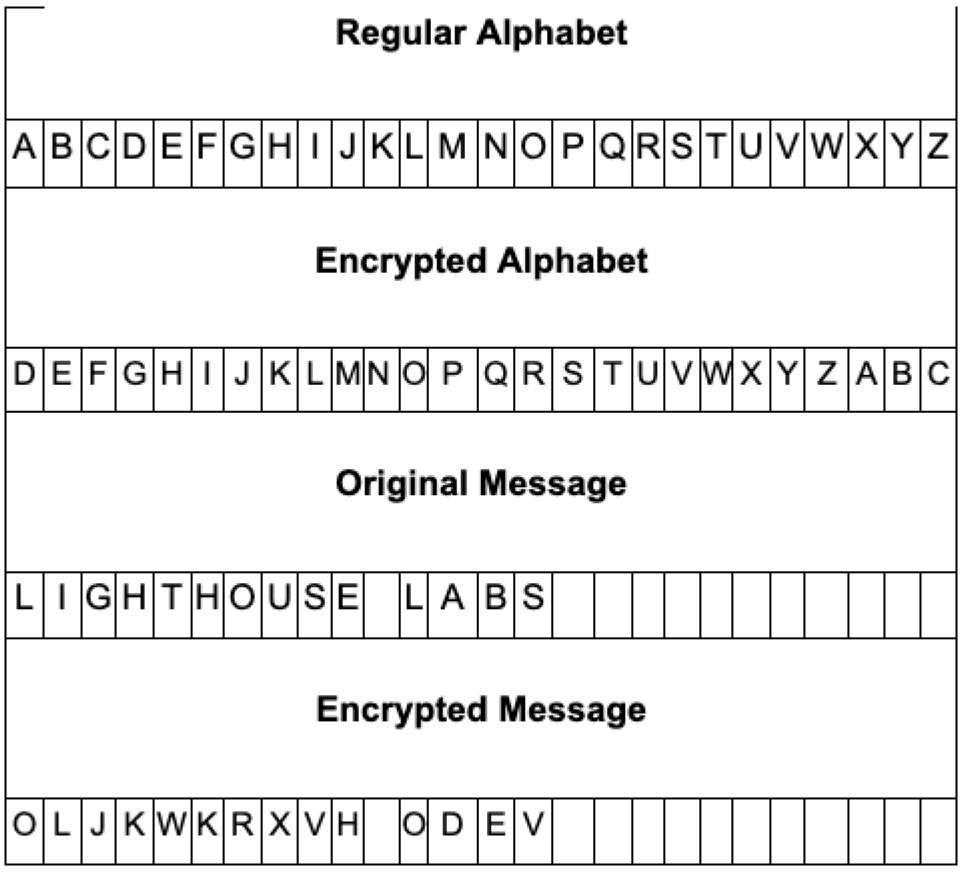
Classic Encryption

This is the oldest cryptography known. This technique went hand in hand with military activities, and its strength against possible attacks depended solely on secrecy and knowing the algorithm needed to decrypt the message.

One of the oldest known cipher algorithms and perhaps also the simplest to understand in this work is the **Caesar Cipher**, which was named after the Roman emperor who ruled at the time. The algorithm was simple: a three-character shift to the right to encrypt, and then a three-character shift to the left to decrypt.

The example below shows four categories:

- The regular alphabet
- The encrypted alphabet
- The original message
- The encrypted message



Regular Alphabet																									
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
Encrypted Alphabet																									
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
Original Message																									
L	I	G	H	T	H	O	U	S	E		L	A	B	S											
Encrypted Message																									
O	L	J	K	W	K	R	X	V	H		O	D	E	V											

> To encrypt the original message “LIGHTHOUSE LABS”, use the encrypted alphabet row to count three characters to the right for each letter.

Example: the letter “L” in the encrypted alphabet row, becomes “O” when you shift three characters to the right and so on.

The encrypted message when completed will read as: `OLJKWKRXVH ODEV`

At first, this might seem like a secure way to protect messages, however, once the encryption and decryption algorithms are known, it becomes easier to read the message.

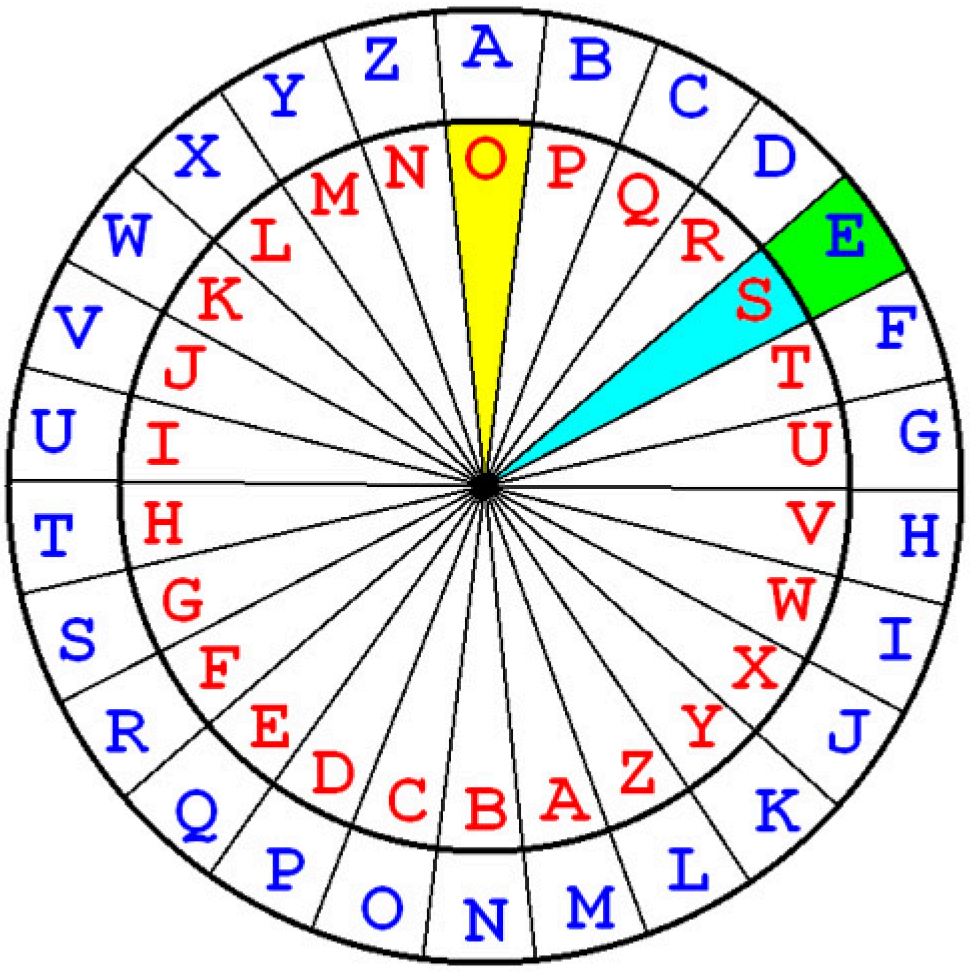
> Reflection Question: Reflect on how secure this technique would be in today’s modern world. Would you use this technique to secure financial data?

Alberti-Vigenère Cipher

The Alberti-Vigenère cipher, also known as the **Vigenère cipher**, is an encryption method that uses a series of different Caesar ciphers based on letters in a password. This is a simplified version of a more general polyalphabetic substitution cipher invented by Leon Battista Alberti around 1465.

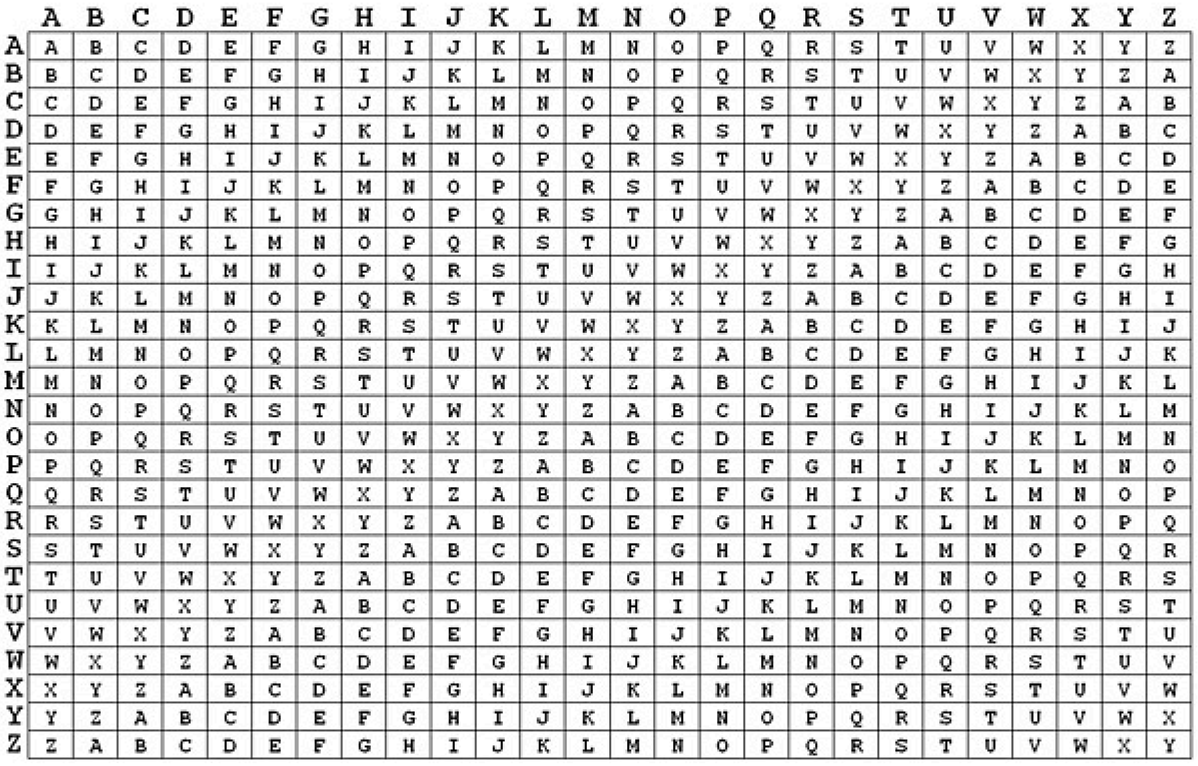
This cipher is well known because it is easy to understand and said to be unbreakable or indecipherable. Consequently, many programmers have implemented cryptographic schemes in their applications that are essentially Vigenère ciphers and easily cracked by any cryptanalyst.

In the image below, you can see an example of one of the Vigenère devices:


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
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

As you may recall, in a Caesar cipher, each letter of the alphabet is shifted from its position a fixed number of places; for example, if it has an offset of three, "A" becomes "D", "B" becomes "E", etc. The Vigenère cipher uses several Caesar ciphers in sequence, with different shift values dictated by a "keyword".

For encryption, an alphabet table consists of the alphabet written 26 times on different lines, each shifted from the previous one by one position. The 26 lines correspond to the 26 possible Caesar ciphers. After choosing the "keyword", each letter of this word will indicate the line to be used to encrypt or decrypt a letter of the message.



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

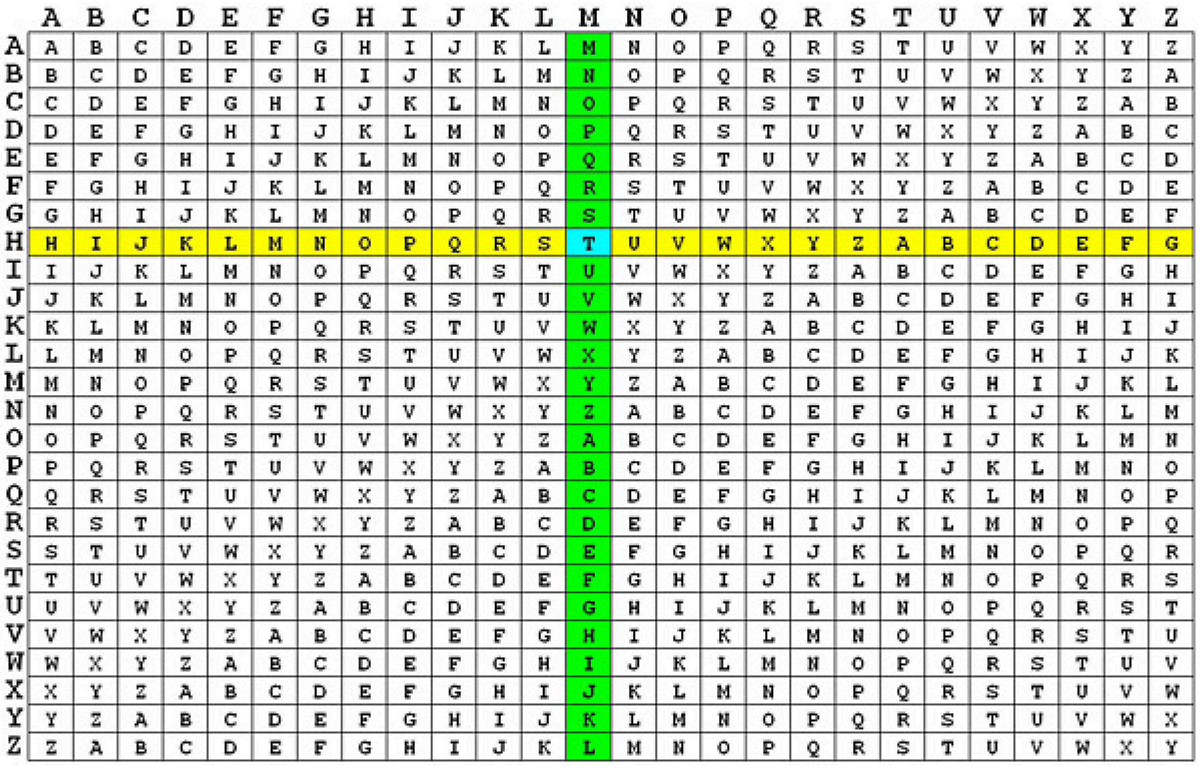
Watch the following video demonstration before trying the exercise. It shows a short demonstration of a similar example using the Vigenère cipher. Than try it using the instructions in the example below.

To understand how to encrypt a message, follow the steps below:

1. Pick a letter in the plain text and its corresponding letter in the keyword.
2. Use the keyword letter and the plain text letter as the row index and column index, respectively.

The entry at the row-column intersection is the letter in the ciphertext.

The image below shows an example using the matrix of letters, where the first letter in the plaintext is M, and its corresponding keyword is H. This means that the row of H and the column of M are used, and the entry T at the intersection is the encrypted result.



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

In addition to the plain text, the Vigenère cipher also requires a keyword, which is repeated so that the total length is equal to that of the plain text.

For example, suppose the plain text is `LIGHTHOUSE LABS IS THE BEST BOOTCAMP`, and the keyword is `PYTHON`.

Then, the keyword must be repeated as follows:

Plain text: lighthouse labs is the best bootcamp

Keyword: python python python python python p

We follow the tradition by removing all spaces and punctuation, converting all letters to uppercase, and dividing the result into five-letter blocks. As a result, the above plain text and keyword become the following:

Plain text: LIGHT HOUSE LABSI STHEB ESTBO OTCAM P

Keyword: PYTHO NPYTH ONPYT HONPY THONP YTHON P

Ciphertext: AGZOHGWMNZSGAYUZHVHRMOSGQCLAHODMMJOZE

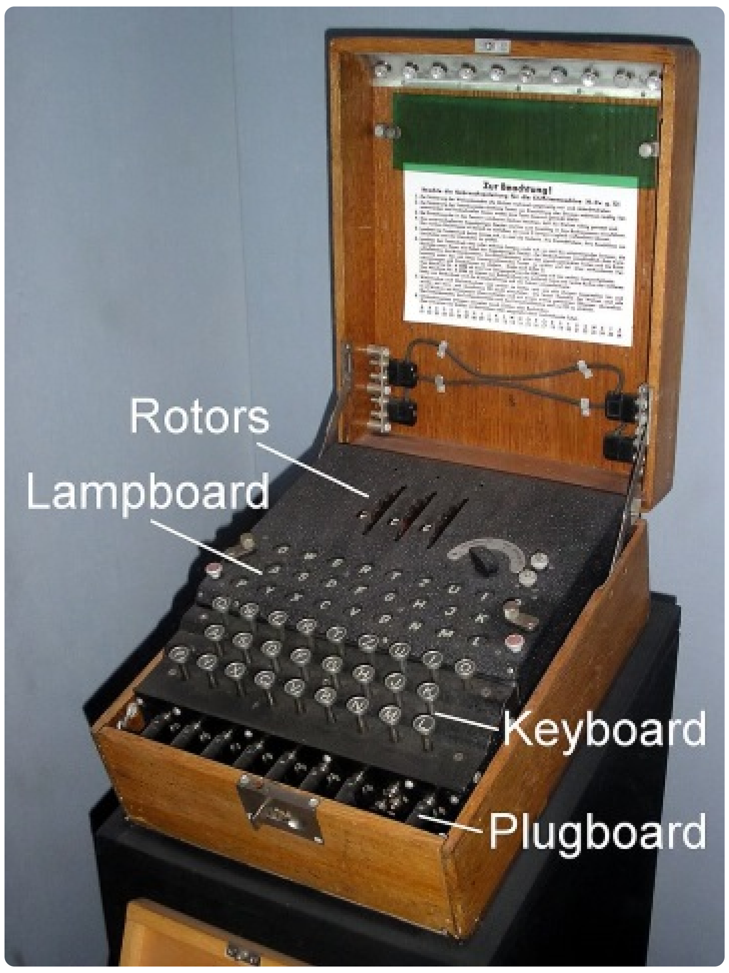
> To understand how to decrypt the message, follow the steps below:

1. Pick a letter in the ciphertext and its corresponding letter in the keyword.
2. Use the keyword letter to find the corresponding row, and the letter heading of the column that contains the ciphertext letter is the needed plain text letter.
3. Repeat the action until the end of the message.

Modern Encryption

Until the beginning of the 20th century, older ciphers developed could be solved without needing a machine, and all it took was time and dedication. But with evolving modern techniques, some machines were developed to accelerate the encryption/decryption process and make the cryptanalysis of encrypted messages more difficult.

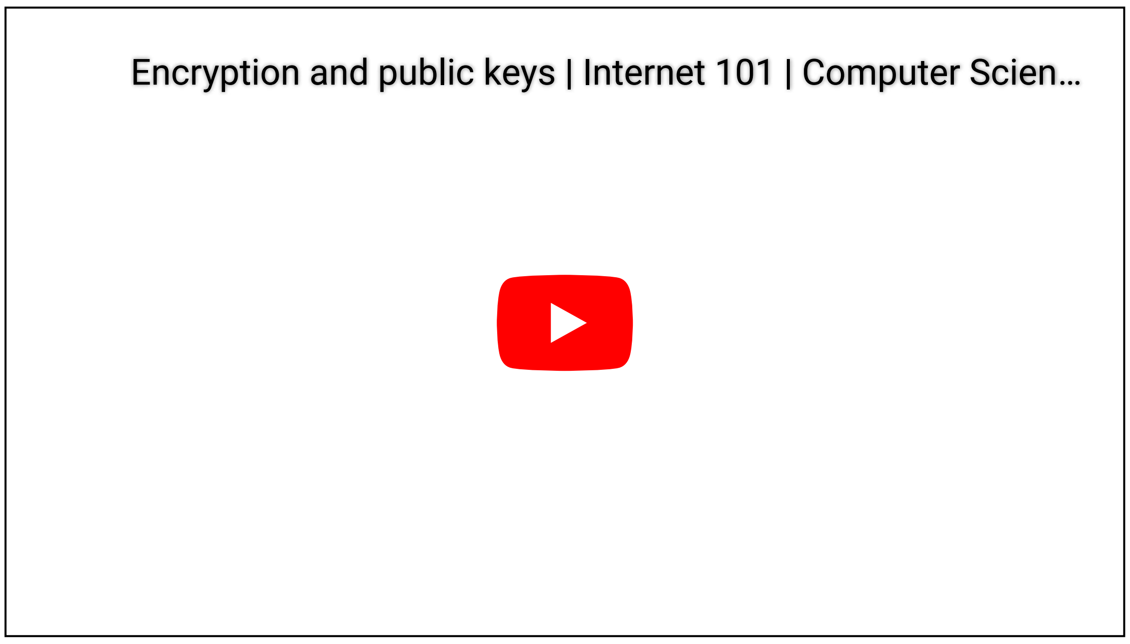
Among these machines, the most popular is the Enigma machine, used by the Germans during World War II. Enigma is somewhat reminiscent of a typewriter. Instead of putting the result on paper, it was shown on a luminous panel with the alphabet's characters. The key used to encrypt/decrypt a message was configured using electromechanical rotors (three or more) that could change to form the key.



At that time, it was considered impossible to decipher a message encrypted with Enigma, as the Germans increased its security by changing the cipher code daily. Eventually, famous mathematician Alan Turing and his team were able to break the Enigma cipher; they created the basic structure for the actual computing system, where the operations of reading, writing, and deleting binary symbols correspond to a defined method or algorithm.

Watch the following video.

> While watching this video, take note of the oldest form of encryption and the time it took to decrypt messages manually.



Encryption and public keys | Internet 101 | Computer Scien...

> Reflection Question: Reflect on modern encryption and decryption techniques and the time and resources it takes to break modern encryption today.

Reading (Optional)

Interested in learning more about the Enigma cipher and the historical milestone of how it was cracked? Read the article below from the The U.S. National Archives and Records Administration:

- Alan Turing, Enigma, and the Breaking of the German Machin Ciphers in World War II

Safeguarding Today's Information - What Can We Learn From History?

Modern cipher implementations depend on the algorithm and a secret key, which is used by the encryption algorithm to modify data as it is encrypted. Ciphers that use longer keys, measured in bits, are more effective against brute-force attacks. The longer the key length, the more brute-force attempts are necessary to expose the plain text. While cipher strength is not always dependent on the length of the key, experts recommend modern ciphers be configured to use keys of at least 128 bits or more, depending on the algorithm and the use case.

> ℹ A key is an essential part of an encryption algorithm, so much so that, in real-world ciphering, the key is kept secret, not the algorithm.

Strong encryption algorithms are designed so that, even if someone knows the algorithm, it should be impossible to decipher ciphertext without knowing the appropriate key. Consequently, before a cipher can work, both the sender and receiver must have a key or a set of keys.

Conclusion

Encryption is just one of many techniques used to secure information. Cryptography, which is considered to be a science of writing a text which can't be perceived by the adversary, uses a combination of techniques, like encryption and decryption, to secure information and communicate them based on mathematical concepts and algorithms.

Next, you'll have a hand-on expereince with Encryption by playing a game!

✓ Mark Completed

← Previous History of Cryptography

Next Encryption Exercise →

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W06D4

Thu Aug 1

- Outline & Notes (1)
- Lectures (1)
- Work (8)

6 hrs

- Project: IR Plan, Playbook and Policy
- Course Reflection
- Overview - Encryption
- History of Cryptography
- History of Encryption
- Encryption Exercise
- Symmetric Key Encryption
- Asymmetric Key Encryption

› Other (1)

W06D4 Schedule »