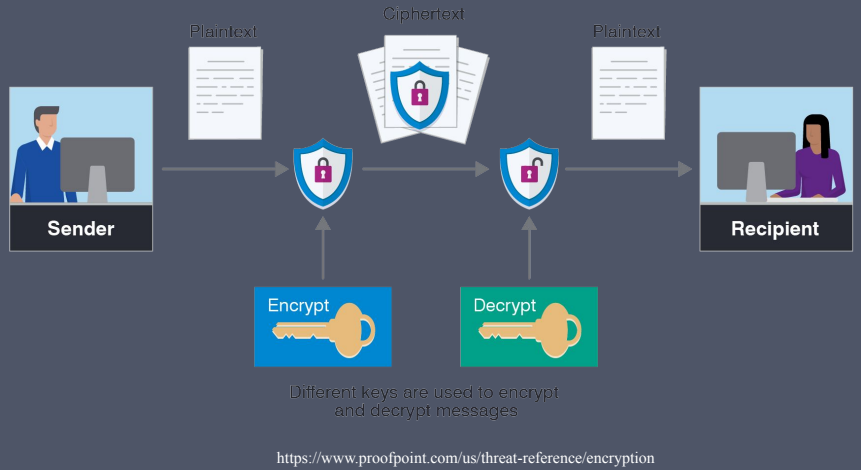
The Evolution of Encryption

A Presentation by Drake Sims

What is Encryption

- Encryption and decryption are all apart of cryptology
- “encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext.” (https://en.wikipedia.org/wiki/Encryption). This ciphertext is then subject to decoding, which is apart of the decryption process.
- Typically for a party to decrypt ciphertext, some sort of key is needed to decipher the original message



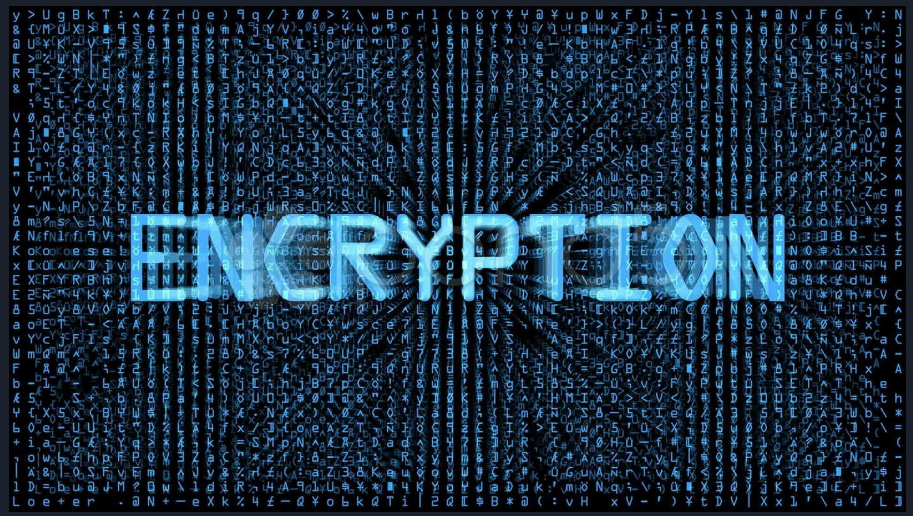
https://www.proofpoint.com/us/threat-reference/encryption

How Does Encryption Work?

- There are two types of encryption today
  - Asymmetric Encryption
    - “uses a public key-private key pairing: data encrypted with the public key can only be decrypted with the private key.” (https://www.cloudflare.com/learning/ssl/what-is-asymmetric-encryption/)
    - Examples include:
      - Rivest-Shamir-Adleman (RSA)
      - Digital Signature Standards (DSS)
      - Transport Layer Security (TLS)
      - Secure Sockets Layer (SSL)
  - Symmetric Encryption
    - Symmetric encryption uses the same key to encrypt and decrypt data. This means the key must be known by both parties.
    - Examples include:
      - Advanced Encryption Standard (AES)
      - Data Encryption Standard (DES)
      - Blowfish

My Project

- My project plans to show the evolution of encryption algorithms, starting from one of the earliest known encryption algorithms to a modern day encryption algorithm known as RSA
- Encryption Algorithms discussed in my project:
  - Caesar Cipher
  - Enigma Machine
  - RSA



https://randerson112358.medium.com/programming-encryption-algorithms-520cb98c039d

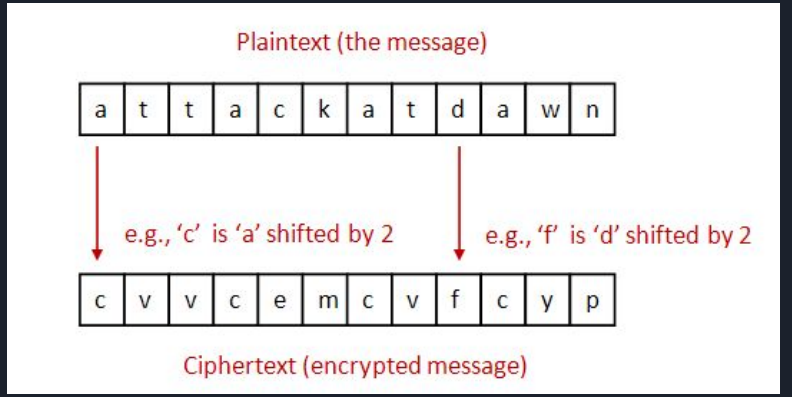
Caesar Cipher

- One of the earliest known ciphers dating back to 100 BC
- Used by Julius Caesar to send messages to generals
- Although it is seen as extremely trivial today, due to the cipher not being widely known, if a message was intercepted by another army, the encoded messages could not be read

https://sites.dartmouth.edu/jacko/2019/11/18/history-department-uncovers-concrete-evidence-that-julius-caesar-was-in-fact-not-a-dartmouth-alumnus/

How Did the Caesar Cipher Work?

- The Caesar Cipher was a substitution cypher
- To encode a message:
  - Fixed set of characters, alphabet
  - A shift value would be decided
    - Caesar was known to use 3 as a common shift value
  - This shift value would then be applied to every character in a message
- To decrypt a message:
  - Subtract the shift value from every character in the current message
- If the shift value given made you reach the end of the fixed list, you would then wrap around to the beginning or end of the list depending on the shift value.
- The Caesar Cipher is a form of symmetric encryption



https://www2.seas.gwu.edu/~simhaweb/cs1111/classwork/module14/module14.html

The History of the Enigma Machine

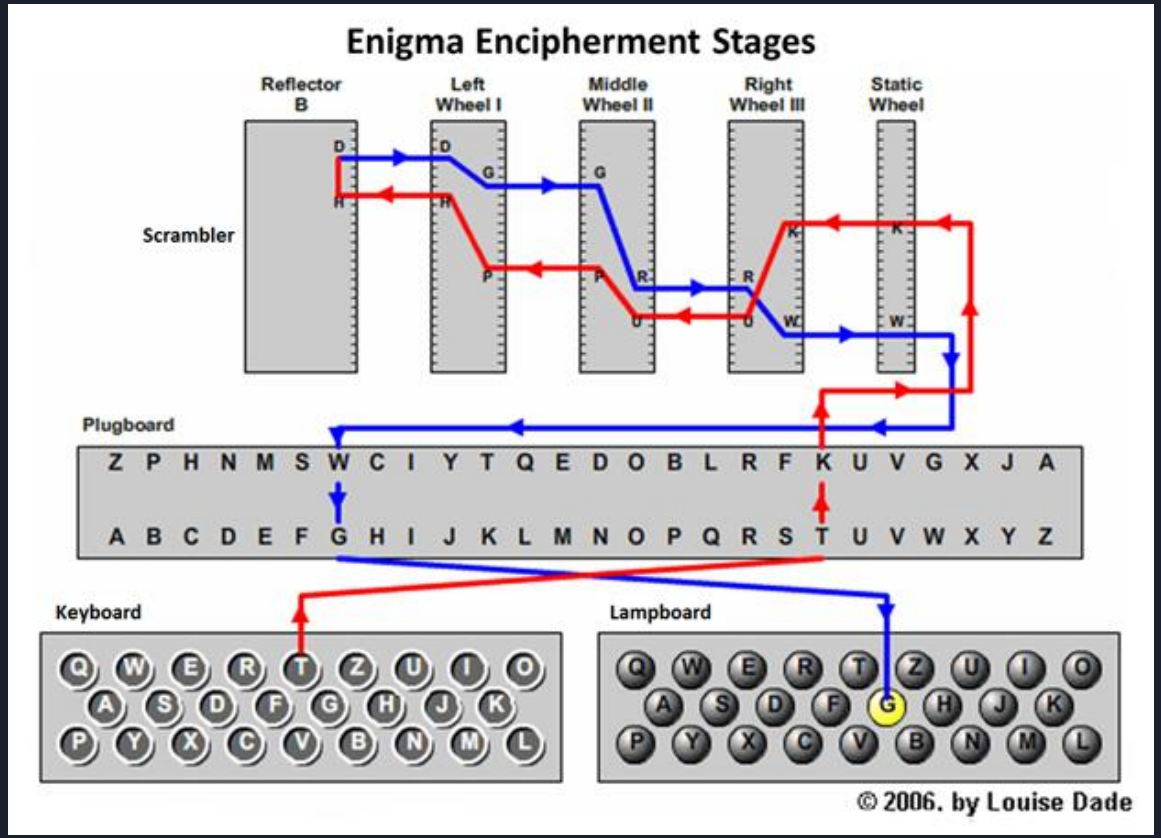
- Developed in 1923
- Primarily used by Nazi Germany during World War 2
- Was known for very secure/unbreakable codes
    - “The Enigma’s settings offered 150,000,000,000,000,000,000 possible solutions” (https://www.cia.gov/legacy/museum/artifact/enigma-machine/)
- The Enigma Machine saw several developments through its use to try and slow down decryption efforts
- The Enigma Machine’s internal wiring had initially been broken by a team of Polish cryptanalysts in 1932, but Alan Turing is credited with devising a code breaking machine called the Bombe.
- The Bombe was able to intercept and decrypt thousands of messages a month, providing the allies with a large advantage against Germany.

https://www.tnmoc.org/bh-2-the-enigma-machine

How Did the Enigma Machine Work?

- The Enigma Machine featured mechanical and electrical components to work
  - Mechanical Features
    - Keyboard
    - Rotors
    - Reflector
  - Electrical Features
    - Wires to carry a current
    - Plugboard
- The rotors in the Enigma Machine typically had 26 electrical contacts representing the alphabet on each
- The reflector was typically the last rotor in the Enigma Machine, and used pairs.
  - The reflector would then redirect the electrical current through the rotors.
- The plugboard was later introduced to the Enigma Machine to make it harder to crack.
  - The plugboard allowed for 150 trillion possible settings and did this by placing a cable connected to a pair of letters with the purpose of swapping them before and after being ran through the Enigma Machine.
- To properly decode a message using the Enigma Machine it was important to know the settings of the rotors on the enigma machine when encrypting
  - These settings would be changed by Germany at least once a day, and sometimes more

How Did the Enigma Machine Work? cont.



https://www.mpoweruk.com/enigma.htm

History of Rivest-Shamir-Adleman (RSA)

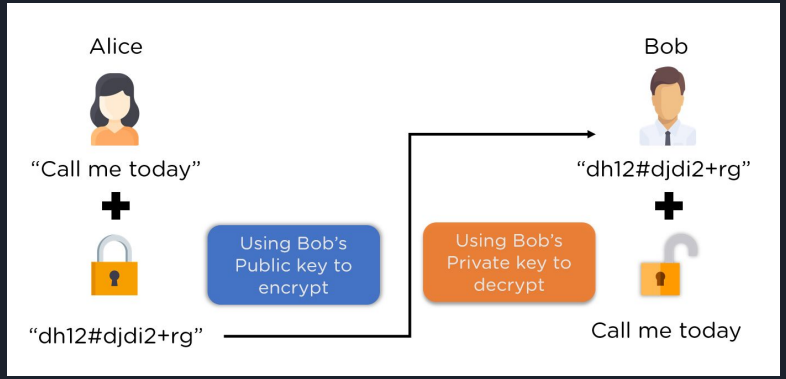
- Asymmetric Encryption algorithm
- Introduced in 1977
- The name derives from the 3 MIT colleagues who developed the algorithm
  - Ron Rivest
  - Adi Shamir
  - Leonard Adleman
- The purpose of RSA was to allow for data to be exchanged between two parties without the need for a shared key.

How RSA Works

- RSA uses two keys
  - Public Key
    - The public key is used to encrypt data being sent by a user
  - Private Key
    - The private key is needed to decrypt data encrypted by the public key
  - These keys are generated using a mathematical equation
- The RSA Algorithm
  - First, two prime numbers must be selected. (P, Q)
  - You then multiply your two prime numbers. (P*Q)
  - After multiplying P & Q you get your product. (P*Q) = N
  - Next, calculate the totient. (P-1)*(Q-1) = T
  - You can now select your public key. (E)
    - Must be prime
    - Must be less than the totient
    - Must not be a factor of the totient
  - You can now select your private key (D), but must meet these conditions.
    - Product of D and E, divided by T must result in a remainder of 1. (D*E) MOD T = 1

How RSA Works cont.

- After selection of your public and private key you must know the algorithms for encrypting and decrypting
  - Encryption
    - Message^E MOD N = CipherText
  - Decryption
    - CipherText^D MOD N = Message
- In modern RSA algorithms we see large prime numbers being used ranging from 1024 bits to 2048 bits.
- RSA is not commonly used for encoding messages due to the amount of resources it takes up on a computer, however, RSA is extremely common on web browsers and VPNs.



Live Demo!

My Difficulties and What I Would Change

- Caesar Cipher
  - The Caesar Cipher was very trivial in terms of coding, and I did not face much issue.
- Enigma Machine
  - Due to having never heard of this machine before I had some trouble trying to implement it in my code. I wish I had some more time to understand the inner workings of the machine.
  - Due to my program being a text based program that resets when it is ran, I was not able to do the rotors properly. In my program I had to set the rotor settings to a constant, so that any message encrypted on my program could still be decrypted. If I had more time I would love to find a solution to have the rotors work and do what they are supposed to on their own.
- RSA
  - The RSA done in my project is a very simplistic version of RSA that if I had more time I would love to improve, and make more like the modern version.
- Overall
  - I would like to clean up the code a little more and increase the complexity of everything to make a more polished project.

Works Cited

Caesar cipher in cryptography. GeeksforGeeks. (2023, May 11). https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/#

Central Intelligence Agency. (n.d.). Central Intelligence Agency. https://www.cia.gov/legacy/museum/artifact/enigma-machine/

Encyclopædia Britannica, inc. (2024, April 12). *Alan Turing*. Encyclopædia Britannica. https://www.britannica.com/biography/Alan-Turing

Jacko, P. B. (2019, November 18). *History department uncovers concrete evidence that Julius Caesar was, in fact, not a Dartmouth alumnus*. o. https://sites.dartmouth.edu/jacko/2019/11/18/history-department-uncovers-concrete-evidence-that-julius-caesar-was-in-fact-not-a-dartmouth-alumnus/

The language's impact on the Enigma machine. (n.d.-a). https://eprint.iacr.org/2021/1434.pdf

Module 14: Science & Engineering Applications III - Cryptography and computational biology. Introduction to Software Development. (n.d.). https://www2.seas.gwu.edu/~simhaweb/cs1111/classwork/module14/module14.html

randerson112358. (2020, July 10). *Programming Encryption Algorithms*. Medium. https://randerson112358.medium.com/programming-encryption-algorithms-520cb98c039d

The RSA cryptosystem: History, algorithm, primes. (n.d.-b). https://math.uchicago.edu/~may/VIGRE/VIGRE2007/REUPapers/FINALAPP/Calderbank.pdf

Simplilearn. (2023, February 13). *What is RSA algorithm in cryptography?: Simplilearn*. Simplilearn.com. https://www.simplilearn.com/tutorials/cryptography-tutorial/rsa-algorithm

What is asymmetric encryption? | asymmetric vs. Symmetric Encryption | Cloudflare. (n.d.-c). https://www.cloudflare.com/learning/ssl/what-is-asymmetric-encryption/

What is encryption? - definition, types & more: Proofpoint us. Proofpoint. (2024, February 12). https://www.proofpoint.com/us/threat-reference/encryption

Wikimedia Foundation. (2024a, April 19). *Enigma machine*. Wikipedia. https://en.wikipedia.org/wiki/Enigma_machine

Wikimedia Foundation. (2024b, April 24). *Encryption*. Wikipedia. https://en.wikipedia.org/wiki/Encryption

YouTube. (2021, November 8). *RSA algorithm - how does it work? - I'll prove it with an example! -- cryptography - practical TLS*. YouTube. https://www.youtube.com/watch?v=Pq8gNbvfaoM&ab_channel=PracticalNetworking