Bangalie koroma, Antonette Simms, Lassine P Guindo , Lucky Uchendu , Marcus Jackson,

Tyrek Kelly, Ulises Servellon

Dr Lethia Jackson

CTEC 445

February 13 , 2025

Collaboration Phase (PigPen & Rail Fence)

Rail Fence Ciphers are transposition ciphers that rearrange the orders of letters in a message. Its purpose is to obscure the message by reordering the structure of the message in a downward, diagonal sequence. The Pigpen Cipher is a substitution cipher that replaces letters with symbols based on a geometric grid system. This cipher uses two 3x3 grids and two X shaped grids to assign symbols to letters. Both ciphers offer intriguing ways to encode messages and highlight the creativity in early cryptographic techniques.

While both the Pigpen and Rail Fence ciphers serve as good encryption techniques, they diverge significantly in their methods. One employing symbolic substitution and the other using a transposition-based pattern. For the rail fence cipher, plaintext characters are arranged in a zigzag pattern across several rails and the characters will be read by row to form the ciphertext. The encryption for pigpen is replacing each letter in the message with its corresponding symbol.

While the decryption process for the Pigpen and rail fence ciphers aim to reveal the original plaintext, they differ fundamentally in their approaches. One reversing symbolic substitution and the other reordering the transposed pattern. For the Rail fence cipher, you decrypt with the correct amount of rails, then fill in the blanks horizontally according to the rails, you will decrypt the message. For Pigpen Cipher, you use the keys to map symbols back to letters. It can be very difficult for beginners to decode, especially without the key.

Pigpen Cipher is simple and easy to understand making it practical for casual use, such as puzzles, games, or as an cryptographic exercise. However, its simplicity is also a downside in real world scenarios requiring strong security. Since it's a straightforward substitution cipher, it can be easily broken using frequency analysis or pattern recognition techniques. Therefore, while it may hold historical and educational value, its practicality in modern secure communication is limited.

Rail Fence Cipher, being a transposition cipher, offers a higher level of understanding compared to Pigpen cipher. It's practical for quick, low stakes encryption tasks where moderate security suffices. It could be used to obfuscate messages in a classroom setting or in situations where convenience is more important than high security. However, it's still vulnerable to modern cryptanalysis and would not stand up to more sophisticated attacks, making it impractical for highly sensitive data.

Pigpen Cipher is quite vulnerable to modern cryptographic attacks. Its straightforward substitution method makes it highly susceptible to frequency analysis, where the most common symbols are matched to the most common letters in the language of the plaintext. Additionally, the limited number of symbols (representing letters) allows for rapid pattern recognition by both humans and computers. Modern computing power makes it easy to analyze large amounts of text quickly, rendering simple substitution ciphers ineffective for any serious encryption purposes.

The Rail Fence cipher provides slightly better security than the Pigpen cipher, but it is still vulnerable. Since it rearranges letters rather than substituting them, it can be more challenging to break with frequency analysis alone. However, it’s still relatively weak against techniques such as pattern recognition. Modern tools can quickly brute-force the number of rails used to decrypt the message. While it involves a more complex arrangement of characters, the Rail Fence cipher still lacks the complexity needed to withstand modern cryptanalytic methods. The limited number of possible keys makes it feasible for attackers to try all possible configurations relatively quickly.

Both the Pigpen and Rail Fence ciphers are of historical interest and educational value, but neither is suitable for protecting sensitive information against modern cryptographic attacks. If you're looking for robust encryption, modern algorithms like Advanced Encryption Standard or RSA are the go-to choices, offering a significantly higher level of security and resistance to contemporary

1. Which cipher would be most suitable for encrypting a short, non-sensitive message? Why?

For a short, non-sensitive message, the Pigpen cipher is more suitable. It's a simple substitution cipher that uses symbols to represent letters, making it easy to encode and decode without requiring complex algorithms or tools. Its simplicity of use makes it ideal for casual or non-sensitive communication.

2. How could combining two or more ciphers increase the security of a message?

Combining two or more ciphers, known as cipher chaining or multi-layer encryption, can significantly increase the security of a message. This approach makes it more difficult for an attacker to decrypt the message because they would need to break multiple layers of encryption.

3. What are some real-world scenarios where classical ciphers like these might still be useful?

Classical ciphers can still be useful in scenarios such as educational purposes, puzzle games, escape rooms, and historical reenactments.

4. Why are classical ciphers no longer considered secure for modern communication?

Classical ciphers are no longer considered secure for modern communication because they are vulnerable to various cryptanalytic attacks. Advances in computational power and cryptographic techniques have made it relatively easy to break these ciphers. Modern encryption algorithms offer much stronger security by using complex mathematical principles and larger key sizes.

5. If you were tasked with designing a cipher, what features would you include to make it secure?

To design a secure cipher, I would include features such as strong encryption algorithms, large key sizes, randomized key generation and applying multiple rounds of encryption.

6. What lessons can modern cryptographers learn from studying historical ciphers?

Modern cryptographers can learn several lessons from historical ciphers, like the importance of key management, the need for complexity, and the value of redundancy.

7. How might advances in computing power (e.g., quantum computing) impact the security of ciphers?

Advances in computing power, particularly quantum computing, could impact the security of ciphers. Quantum computers have the potential to break many of the cryptographic algorithms currently in use by efficiently solving problems that are infeasible for classical computers.

8. What steps can be taken to strengthen the security of ciphers against brute-force or cryptanalytic attacks?

We can increase key sizes, rely on algorithms that have been extensively analyzed and tested, Implement multi-layer encryption, employ secure key management practices, and ensure keys are generated, stored, and exchanged securely.