Euler Circle Cryptography Paper – Classical Ciphers

Isabella Soriano

August 12, 2024

Abstract

If Alice and Bob wish to send securely encrypted messages to each other, they might want to turn to the world of classical ciphers. Varying in levels of security, classical ciphers provide protection against Eve- who wishes to decipher their messages. While several examples of important classical ciphers are covered in this Euler Circle Cryptography class, this paper will discuss others. The three main classical ciphers I will highlight in this paper are: The Affine Cipher, The Playfair Cipher, and the VIC Cipher.

1 The Affine Cipher

The Affine Cipher is a type of substitution cipher used in cryptography where each letter in the plaintext is mapped to a corresponding letter in the ciphertext through a linear mathematical transformation. It is a combination of the Caesar Cipher and the Multiplicative Cipher.

1. **A Linear Mathematical Formula**

   The Affine Cipher encrypts every letter using the formula:

   $$E(x)= (ax+b) \text{ mod } m$$

   - x is the numerical equivalent of the plaintext letter (a = 0, b=1, etc.)
   - $E(x)$ is the resulting ciphertext letter
   - a and b are keys of the cipher. a is the multiplicative key and b is the additive key.
   - m is the size of the alphabet (m=26)

   Example: Say that Alice will encrypt the letter 'C' given that a=5 and b=8. Also remember that 'C' corresponds to x=2 as 'C' is the 3rd letter of the alphabet.

   $$E(x)=((5*2)+8) \text{ mod } 26 = (10+8) \text{ mod } 26 = 18 \text{ mod } 26$$

   The 18th letter of the alphabet is 'S', so 'C' is encrypted as 'S'. This is what Bob will recieve.

2. **Decryption**

   For Bob to decrypt the ciphertext, he needs to reverse the encryption. The decryption formula is:

   $$D(y)=a^{-1}(y\text{-}b) \text{ mod } m$$

   - y is the numerical equivalent of the ciphertext letter
   - $D(y)$ is the resulting plaintext letter
   - a^{-1} is the modular multiplicative inverse of a modulo m. (This means that $a{*}a^{-1} \equiv 1 \text{ mod } m$)

   Example: Decrypt the ciphertext letter 'S' into plaintext by finding the modular inverse of a modulo 26. Reminder that a=5 and b=8.

   The modular inverse of 5 modulo 26 is 21: 5*21≡ 1 mod 26

$$D(y)\text{=21*(18-8) mod 26 = (21*10) mod 26 = 210 mod 26 = 2}$$

The letter corresponding to 2 is 'C', so 'S' decrypts to 'C'.

3. **Security Analysis**

   Definition 1.1 *Coprime* numbers are two integers that have no common positive integer divisors other than 1. Their greatest common divisor (GCD) is 1.

   The security of the Affine Cipher is relatively weak by modern standards. The keyspace is small due to the limited number of choices for a and b. Specifically because a must be coprime with 26 (which limits the number of possible values for a) and b can be any integer between 0-25. Because of this small keyspace, the Affine Cipher is vulnerable to attack. Eve can use frequency analysis to break the cipher.

4. **Conclusion**

   The Affine Cipher is a simple and historical cryptographic cryptographic technique. Although it is not very secure against Eve's attacks which employ modern crytopo-technology, it is an example of the fundamental classical ciphers.

2 The Playfair Cipher

The Playfair Cipher is a manual symmetric encryption technique and was the first literal digraph substituion cipher. It was invented in 1854 by Charles Wheatstone but was named after Lord Playfair who promoted its use. The cipher encyrpts pairs of letters (known as digraphs) instead of single letters. This makes it more secure than a simple substituion cipher. Eve will therefore have more trouble in her quest to decipher the message.

1. **How the Playfair Cipher Works**

   1. The Key Square

   The Playfair Cipher uses a 5x5 matrix of letters constructed using a keyword. The keyword is written into the matrix (without repeating any letters), followed by the remaining letters of the alphabet in order (also without repeating). Since the English alphabet has 26 letters, one letter is omitted (typically 'J' is combined with 'I').

   For example, if Alice wanted to send the message "monarchy" to Bob, the matrix would be:

$$\begin{array}{ccccc} M & O & N & A & R \\ C & H & Y & B & D \\ E & F & G & I/J & K \\ L & P & Q & S & T \\ U & V & W & X & Z \end{array}$$

2. **Encryption and Decryption**

   Definition 2.1 *Digraphs* are a pair of letters that are encrypted together as a unit. The Playfair cipher is a type of polygraphic substitution cipher, meaning it encrypts groups of letters instead of single letters.

   To encrypt a message, the text is divided into digraphs. If the message has an odd number of letters, an extra letter (usually 'X') is added to the end. If a digraph consists of the same letter twice (like "LL"), an 'X' is usually inserted between them.

Rules for Encryption:

• Same Row: If both letters of the digraph appear in the same row of the matrix, Alice must replace them with the letters immediately to their right, wrapping around to the left side of the row if needed.

• Same Column: If both letters of the digraph are in the same column, Alice should replace them with the letters immediately below them, wrapping around to the top of the column if needed.

• Rectangle: If the letters are not in the same row or column, Alice has to form a rectangle with the two letters as opposite corners. Replace each letters with the one in the same row but at the other corner of the rectangle.

Encrypting the plaintext example

Alice will apply these encyrption rules to the pairs of letters in the plaintext word 'monarcy'

• mo: Both m and o are in the same row. Alice will replace m with O and o with N → ON.

• na: Both n and a are in the same row. Replace n with A and a with R → AR.

• rc: r and c form a rectangle. Replace r with M and c with D → MD.

• hy: Both h and y are in the same row. Replace h with Y and y with B → YB.

The plaintext 'monarchy' becomes the ciphertext 'ONARMDYB'.

Rules for Decryption:

• Same Row: Bob will work backwards and replace each letter with the one immediately to its left, wrapping around to the right side of the row if needed.

• Same Column: Bob will work backwards and replace each letter with the one immediately above it, wrapping around to the bottom of the column if needed.

• Rectangle: Bob will work backwards and replace each letter with the one in the same row but at the other corner of the rectangle.

3. **The Math behind the Playfair Cipher**

The keyspace of the Playfair Cipher is determined by the number of possible 5x5 matrices. The keyword can be any combination of the 25 letters (omitting 'J'), and the remaining letters are filled in to complete the matrix. The total number of possible matrices can be calculated as:

$$\text{Keyspace} = \frac{25!}{(25-\text{length of keyword})!}$$

For example, if the keyspace of 'monarchy' is 8 letters long the the amount of possible matrices is:

$$\text{Keyspace} = \frac{25!}{17!}$$

4. **Security Analysis**

The Playfair Cipher is more secure than most ciphers because it encrypts digraphs instead of single letters. This means that Eve will not be able to use frequency analysis like she could with other classical ciphers. However, it is still vulnerable to more sophisticated techniques such as digraph frequency analysis, and with modern computational power (which Eve has), it can be broken relatively easily.

5. **Conclusion**

The security of the Playfair Cipher relies on the mathematical complexity of digraph substitution. Since there are 600 possible digraphs (25*24), the cipher has a much larger potential for security compared to monoalphabetic ciphers, which only have 26 possible substitutions. However, because the Playfair Cipher does not use a truly random substitution for each digraph but instead follows structured rules based on the key square, patterns can still emerge.

The Playfair Cipher was an important step in the evolution of cryptography, offering greater security than simpler substitution ciphers. Its reliance on digraphs adds mathematical complexity, making it more resistant to basic frequency analysis. However, with advances in cryptanalysis and computing, the Playfair Cipher is now considered insecure by modern standards, but it remains an interesting example of historical encryption techniques

3 The VIC Cipher

The VIC cipher (Victor cipher) is a cipher system developed by Soviet spy Reino Häyhänen, also known as ”Victor”. It is considered one of the most complex hand ciphers ever used and remained unbroken during its use in the Cold War. The VIC cipher combines several cryptographic techniques, including a modified Polybius square, a straddling checkerboard, and a disrupted double transposition, making it extremely secure for a pen-and-paper cipher. This will be the most secure cipher in this paper that Alice can use to send a messsage to Bob, as Eve will have great difficulty decoding this.

1. **Steps to Perform the VIC Cipher**

   Imagine that Alice wants to send the plaintext 'meet me at dawn' to Bob using the VIC Cipher.

   Generate a Random Number Key: 1,2,3,4,5,6,7,8,0

   Create a straddling checkerboard

   Definition 3.1 A *Straddling checkerboard* is used in the VIC cipher to efficiently encode text into digits. This board is a two-row grid with numbered columns, where each letter of the alphabet is assigned a single number.

   This checkerboard uses the key digits to map letters. The letters are mapped in a similar way Alice did in the Playfair cipher. But in this case individual letters they will be directly translated into numbers. Here is an example:

0	1	2	3	4	5	6	7	8
0	0	*M*	*E*	*T*	0	0	0	0
1	*A*	*B*	*C*	*D*	*F*	*G*	*H*	*I*
2	*J*	*K*	*L*	*N*	*O*	*P*	*Q*	*R*
3	*S*	*U*	*V*	*W*	*X*	*Y*	*Z*	

   Encode the message Using the checkerboard encode the plaintext 'meet me at dawn':

   • m=2, • e=3, • e=3, • t=4, • m=2, • e=3, • a=10, • t=4, • d=14, • a=10, • w=34, • n=24

   Perform a Double Transposition to upgrade security

   Definition 3.2 *Double Transposition* involves using two separate transposition processes to rearrange a message's characters, increasing the complexity and security of the encryption. The plaintext is written into a grid, and then the columns are rearranged according to two different numeric keys, first by rows and then by columns. This method makes it significantly more challenging for unauthorized parties to decipher the message without knowing both keys.

   This transposition further scrambles the message by using another key in the encryption. Alice will choose the additional key **3124** in this scenario.

3	**1**	**2**	**4**
2	3	3	4
2	3	10	4
14	10	34	24

Use the key that is the first line and rearrange that into numerical order → **1234**. Rearrange every number that fell into each column in this new order. As such:

1	**2**	**3**	**4**
3	3	2	4
3	10	2	4
10	34	14	24

After this transposition, read the rows in descending order to find the ciphertext: **33243102410341424**

2. **Alice's Security Measures in the VIC Cipher**

   1. The Straddling Checkerboard By using the checkerboard, Alice can rely on positional mappings to convert letters into numbers. This compresses frequent letters into fewer digits. This optimizes the digit sequence's length.

   2. The Double Transposition This is a permutation-based method, mathematically representing a mapping of positions, adding complexity by disrupting the original sequence twice. This is what makes it very difficult for Eve to interpret.

   3. The Random Key Generation The security of the VIC cipher significantly depends on the randomness of the keys, which dictate the mapping and transposition order, adding layers of entropy.

3. **Conclusion** The VIC cipher stands out as a sophisticated cryptographic system, blending multiple encryption techniques to achieve robust security. Despite its complexity, the VIC cipher was never successfully broken during its operational period, reflecting its effectiveness.

   The mathematical principles behind the VIC cipher—specifically, the use of positional mappings and permutations—demonstrate how encryption techniques can create layers of complexity, safeguarding messages against unauthorized access. Its design highlights the importance of combining different cryptographic methods to enhance security, a practice that continues to influence modern encryption strategies.