University of Stavanger

Security and Vulnerability in Networks

Assignment 1

The Avalanche Effect in Encryption: A Study on Combined Cipher Techniques

---

Marco Bologna

A.Y. 2024-2025

Abstract

The presented study investigate the avalanche effect in cryptographic algorithms by combining substitution ciphers, such as *Caesar* and *Vigenère*, with a transposition cipher (*Row Transposition*). The avalanche effect is a cryptographic phenomenon where a small change in the input of a cypher (for example flipping a single bit) results in a significant and unpredictable change in the output, so in the cyphertext. The effect was evaluated after a single round of encryption and after multiple rounds.

The results indicated that the combination of Caesar and transposition cipher generates a weak avalanche effect, but the combination of Vigenère and transposition cipher, particularly when utilizing Vigenère's Autokey feature, demonstrated a significantly stronger avalanche effect.
In this work is also been proved that some keys for the transposition cipher (for example symmetric ones) can lead to a deadlock of the avalanche effect, even with multiple rounds of encryption.
Additionally, the study explored a block cipher mode similar to CBC (*Cipher Block Chaining*) using Vigenòre and transposition ciphers. This experiment showed that while the overall effectiveness was consistent with previous results, there was a more rapid increase in the avalanche effect as the number of encryption rounds increased. A considerable effect was observed even after the first round, indicating the potential for a highly secure encryption method.

Code developed, including presentation, is already available on following GitHub page:

GitHub link

Contents

1 Introduction

The main objective of this project is to evaluate the avalanche effect in cryptographic systems that combine substitution and transposition ciphers. The avalanche effect is a critical property in secure encryption algorithms, where a small change in the input (for example flipping a single bit) leads to a significant and unpredictable change in the output. This property is essential for ensuring that encrypted messages cannot be easily deciphered if only partial information is known.

The main challenge of this study is to reach a good level of avalanche effect using some classical and well known encryption algorithms like substitution and transposition ones.
The substitution ciphers used include:

- **Caesar** cipher is a simple algorithm where each letter in the plaintext is shifted by a fixed number of positions in the alphabet.
- **Vigenère** cipher is a more complex algorithm that uses a repeating key to determine the shift for each character.

In this project also a transposition cipher were used, specifically a **Row Transposition** method, where the plaintext is arranged into a matrix and then transposed, reading by columns according to a key.

In the final part of the study, in order to achieve a better encryption , the project further explores the effectiveness of these ciphers when used in a block cipher mode similar to *Cipher Block Chaining* (**CBC**): in this mode, the encryption of each block of plaintext is dependent on the encryption of the previous block, which enhances the diffusion properties of the cipher.

2 Design and Implementation

This section provides a detailed explanation of the project's design, the procedures followed, and the implementation of the encryption techniques and the evaluation of the avalanche effect.

2.1 Apply Encryption

The encryption process was initiated by applying different combinations of substitution and transposition ciphers.
The fist combination used was *Caesar + Transposition* and the first problem to solve was to understand the best order of encryption for the 2 ciphers:

- **Plaintext**: Marco Bologna Security and Vulnerability in Networks
- **Caesar shift** = 2; **Transposition key** = 45312
- **Caesar first**: eqgvxtkptxqieawcvgmxtnukfgnpqxodpwcndavucqctppkkyx
- **Transpose first**: eqgvxtkptzqieawcvgmztnukfgnpqzodpwcndavucqctppkkyz

The only difference between the 2 modalities are the padding characters[1] added at the end of the text (by the transposition cipher); in the first case these characters remains the same, in the second case they are changed by the Caesar cipher.
In Any case, these characters are not part of the original text, so there is no difference in the final result.

2.2 Evaluate the Avalanche Effect

The avalanche effect was evaluated by flipping a single bit in the plaintext before encryption and the encrypted outputs were then compared to quantify how much the small change in input affected the ciphertext. In order to do this, at each round of encryption, the percentage of differing characters and bits between the original and altered ciphertexts was measured, along with the computation time.

[1] Padding characters are added at the end of the text beacuse the text lenght nedds to be multiple of the transposition key lenght; in this case, to better undertand and evaluate ciphers diffences and avalanche effect, padding character are 'x', in real scenarios they should be random characters.

Using *Caesar + Trasposition* reveals to be a bad choice in term of avalanche effect, as shown in the graphs below:

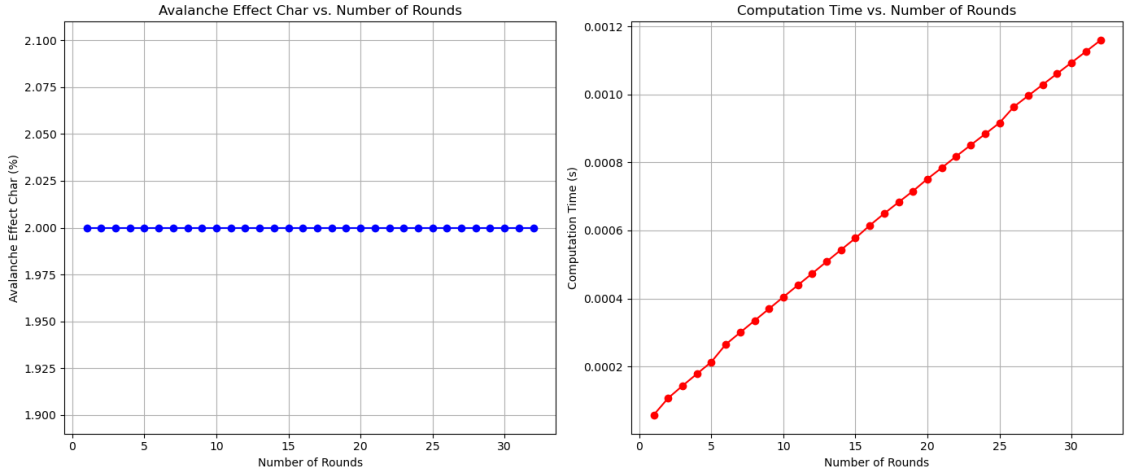


Figure 1: Avalanche Effect of Transposition + Caesar

2.3 Analyze the Avalanche effect

As shown in the graphs, with multiple rounds of encryption the character difference remains the same, this is due to the fact that Caesar and Trasposition ciphers are always shifting and moving letters in the same way, so the only difference between the 2 ciphertext remains of only one character, introduced manually before the first round.
Talking about execution time, it seems to increase linearly with the number of rounds (as expected, beacause the cipher is repeating the same exacts operations more times), so in term of avalanche effect is usless ciphering more than one time with this configuration.
To solve this problem, the solution adopted in this study was to use a more complex substitution cipher: the **Vigenère Cipher**.

Using this new cipher (in combination with the transposition one) significantly enhances the avalanche effect due to the Vigenère **Autokey** feature, where the plaintext is concatenated with the key to create a complex key of the same length as the plaintext. In each round of encryption, the autokey changes, for example in the second round the key is generated by concatenating the original key with the ciphertext from the previous round. This dynamic process amplifies the avalanche effect because altering even a single letter in the plaintext modifies not only the ciphertext but also the key itself. As rounds progress, this cascading change results in a rapidly increasing avalanche effect, making the encryption more secure and unpredictable.

The result obtained is shown in the following graphs:

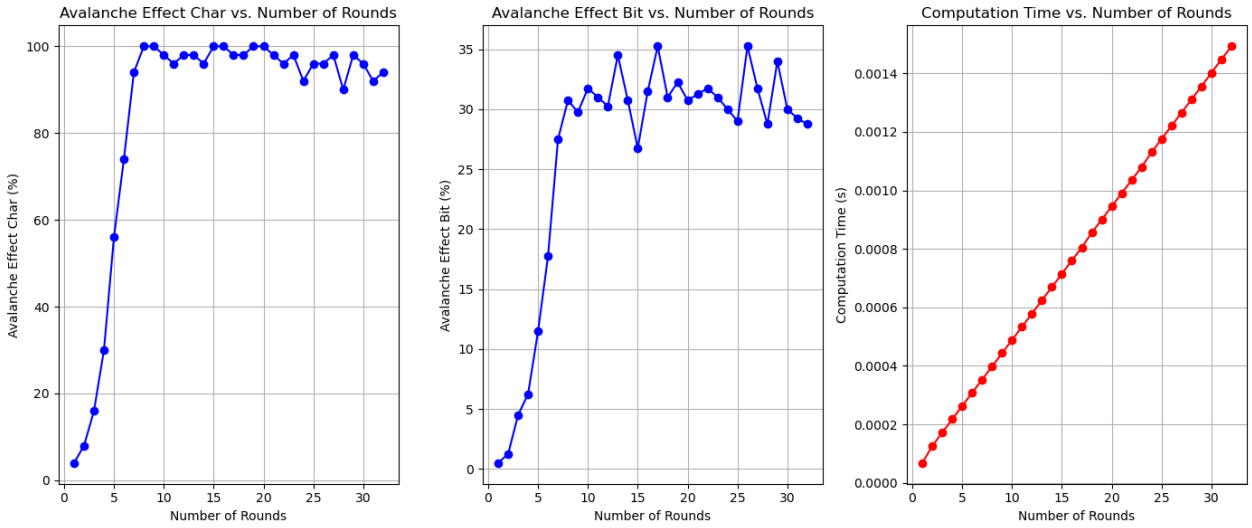


Figure 2: Avalanche Effect of Transposition + Vigenère

2.4 Optimize Avalanche Effect with Reasonable Computation

The graph above shows a huge improvement in term of avalanche affect: after 7 rounds of encryption the percentage of different characters is over **90%** and remains stable, while the percentage of different bits fluctuates around **30%**. This lower difference is due to the fact that characters in standard text are often lower ASCII values, so their binary representations start in the same way.
So, even when characters change significantly through encryption, the bit-level differences may not fully capture this, due to the similarity in higher-order bits.

To boost the performance further, was implemented a Vigenère cipher that operates across the entire 256-character set, which is referred to as the *extended ASCII alphabet*. Using this upgraded cipher, the encryption process would introduce more variability at the bit level, potentially increasing the percentage of different bits and providing a more robust avalanche effect.

This modification has been implemented, and the results are visible in the following graph:

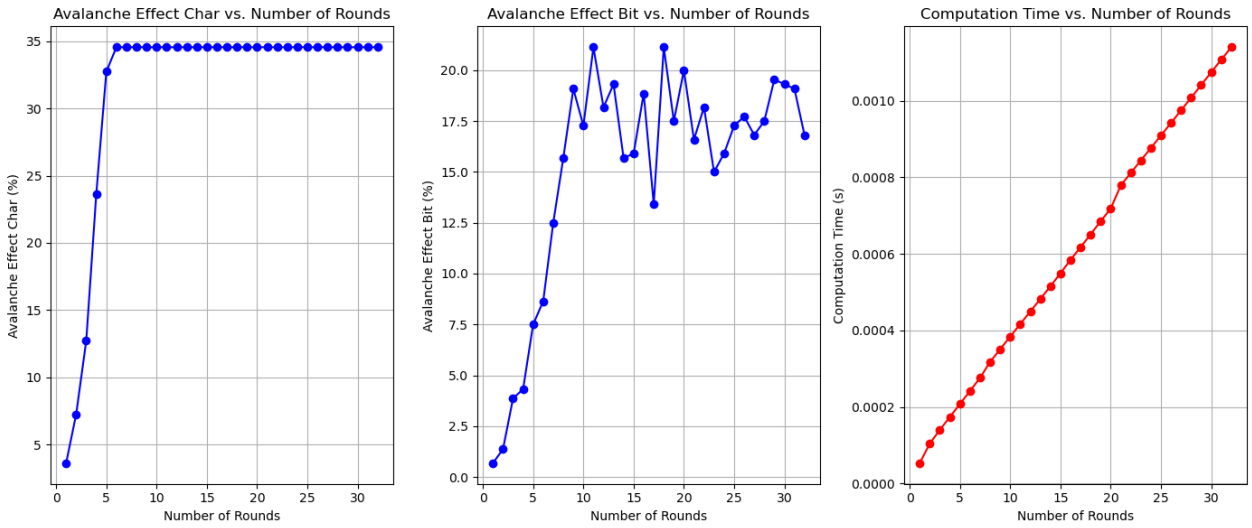


Figure 3: Avalanche Effect of Transposition + Vigenère extended

Surprisingly, using this updated cipher the result are really poor and present a strange behaviour, the avalanche effect rise till around 35% and then remains constant, this behaviour is due to the key used for the transposition cipher that in this case is a symmetric key ("45312"), so the avalanche effect is limited by the key itself beacuse ciphering 2 times with this key is the same as ciphering and then deciphering.
After this discovery, the experiment was repated with a new transposition key: "45321".

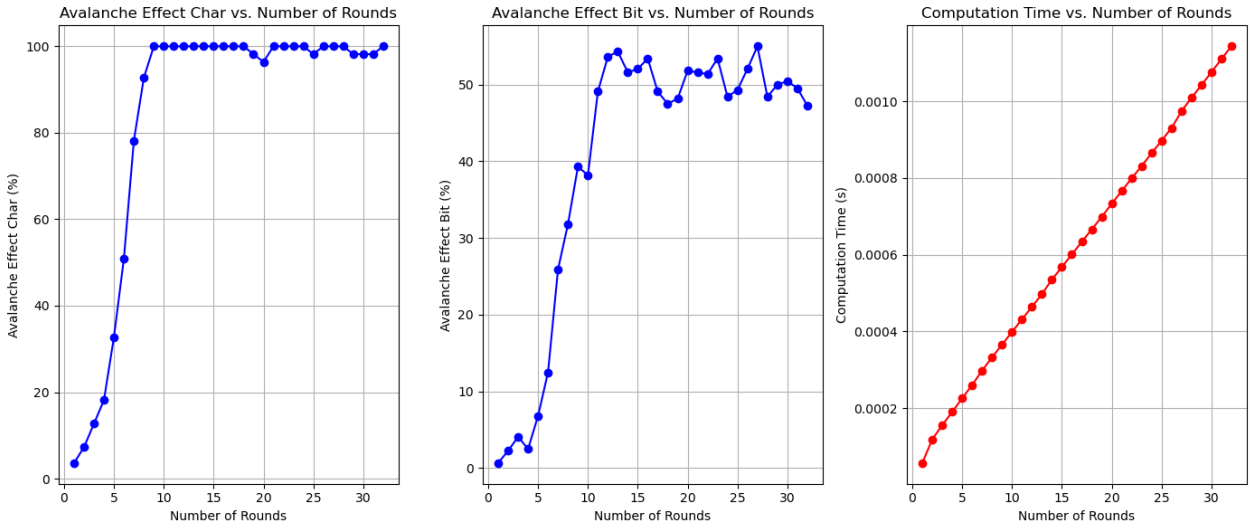


Figure 4: Fixed Avalanche Effect of Transposition + Vigenère extended

As shown in the graphs, the problem is solved and the percentage of different bits reaches a new stability at around 50%, instead of 30% reached using the standard alphabet.

Looking at the time of execution, the time increase linearly with the increase of the rounds of encryption, this is simply because at each round the same operations are repeated. Even with the increase of the rounds, the cost in term of time remains low, on the order f 10^{-4} seconds, so the best solution is to use the number of rounds that first achieves the maximum avalanche effect.
In this scenario, at round 9 the percentage of different characters reach the 100% and remains stable, while the percentage of different bits reaches his higher stable value at round 11 with a really low difference in time of the execution, this makes 11 rounds of encryption the most secure choice.

The observed behavior in the interaction between transposition and substitution ciphers, particularly in terms of the avalanche effect, highlights the complementary strengths of these techniques in encryption.

- **Substitution Ciphers** (Vigenère): This type of ciphers replace each character based on a key. When using the autokey method of the Vigenère cipher, the key evolves with each round, influenced by both the original key and previous ciphertext. The avalanche effect is increased because the change affects not just the corresponding character but also the key, this ensures that the number of differences increases with the number of rounds.

- **Transposition Ciphers** (Row transposition cipher): Transposition ciphers move characters according to the key, for example in row transposition cipher the text is written in a matrix filling each row, and then is extracted reading the matrix by columns, in the order that the key specifies. When used before substitution, transposition increase the complexity of the autokey in the Vigenère cipher, as the input for substitution becomes more randomized.

The combination of transposition followed by substitution increases the avalanche effect. Transposition redistributes the characters making the subsequent Vigenère autokey more complex, this approach ensures that small differences in the plaintext lead to substantial and widespread differences in the ciphertext, significantly improving security and making cryptanalysis more difficult.

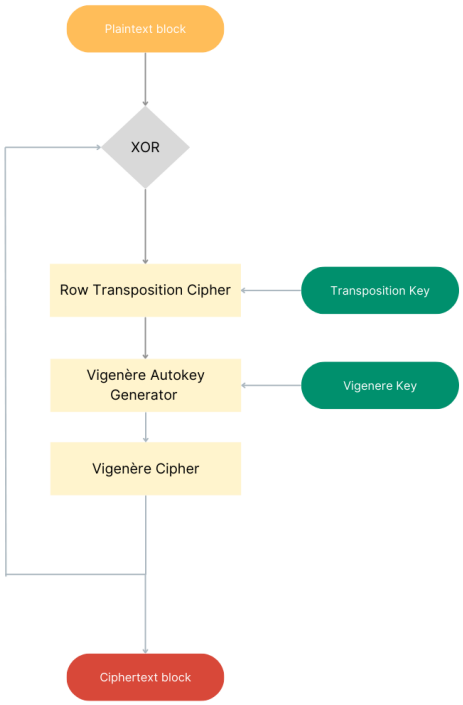
2.5 Enhance Security with Block Ciphers

The final experiment in this study aimed to increase the security of this combination of ciphers implementing a block cipher mode; this approach was explored to measure its impact on the avalanche effect and to determine if it could improve the overall robustness and complexity of the encryption system.
Block ciphers are a more secure cipher's category in which the plaintext is divided into fixed-size blocks[2], which are then encrypted individually.
After the first block is encrypted, its ciphertext is used to modify the next block through an XOR operation, this technique is known as Cipher Block Chaining (CBC).
The above process is repeated for all the blocks in the plaintext.

Block Cipher Process:

- **Division into Blocks**: The plaintext is divided into fixed-size blocks (10 characters each in this study).
- **Initial Block Encryption**: The first block is encrypted using a combination of transposition and Vigenère cipher.
- **Cipher Block Chaining (CBC)**: The resulting ciphertext of the first block is XORed with the second plaintext block before the second block is encrypted. This chaining process goes on for each subsequent block.

Thus, the encryption of each block has been made to be dependent on the others in order to ensure that no single block is easily accessible to the attacker.



[2]In this study, the plaintext is split into blocks of 10 characters each.

Employing a block cipher mode such as CBC greatly improves both the avalanche effect and the general security of the encryption process.
The key benefits are:

- **Increased Avalanche Effect**: In CBC mode, any change in a single character of the plaintext is propagated to all subsequent blocks, this leads to a rapid and widespread propagation of changes, resulting in a strong avalanche effect.
  This happens even after one round if the change occours in the initials blocks, this is beacuse more blocks are affecteted by the change if that change is in one of the firsts blocks.

- **Mitigation of Cipher Weaknesses**: CBC mitigates the weaknesses of simple transposition and substitution ciphers, introducing dependency between blocks. This dependency makes sure that the same plaintext blocks do not generate same ciphertexts, thus offsetting patterns that could be used in cryptanalysis; this makes it much more difficult for the attackers to decrypt the plaintext from the ciphertext since the encryption of each block is interrelated.

The results achieved in term of avalanche effect are presented in the following graphs:

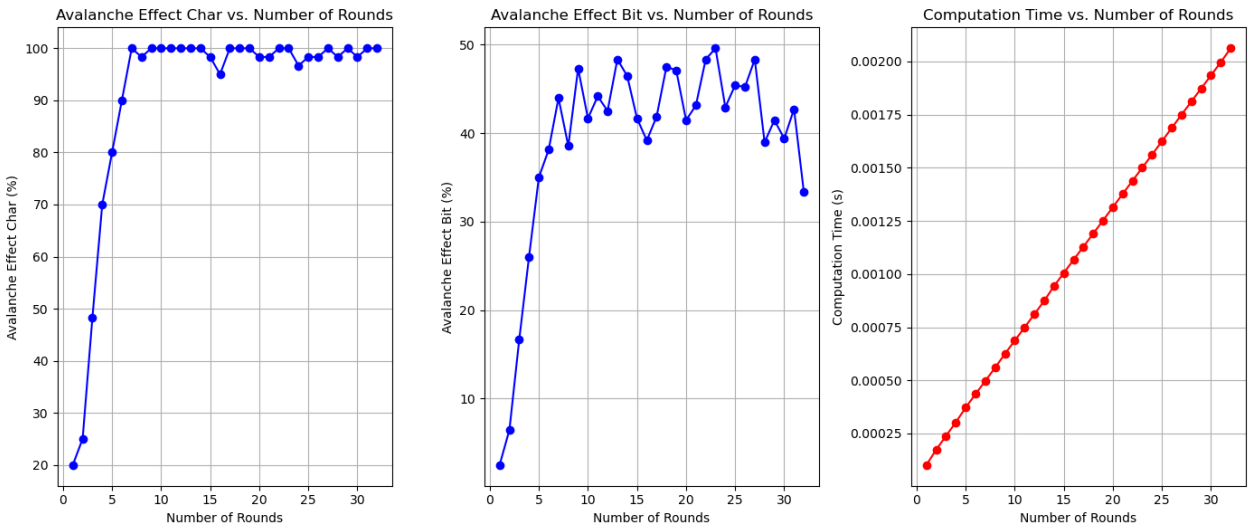


Figure 5: Avalanche Effect of CBC cipher

From the CBC graph, it is evident that the bit difference stabilizes around 40%, which is slightly lower than the version without CBC.
However, there is a much faster growth in the avalanche effect: stability is reached after 7 rounds of encryption. Notably, after just one round, 20% of the characters are already different.

3 Discussion

In this work, the combined behavior of the substitution and transposition ciphers was investigated with the purpose of assessing the avalanche effect in various configurations and after several rounds of the encryption process. The analysis of the results indicated that the use of ciphers like Caesar or Vigenère together with transposition resulted in different behaviour in the propagation of differences between the plaintext and ciphertext.

In the case of Caesar cipher combined with transposition, the avalanche effect was not so significant, low percentage of different characters and bits even after several rounds of encryption. This is because Caesar's cipher is fixed and does not allow much of the differences to propagate forward.

On the other hand, the Vigenère and transposition cipher gave much better results because of Vigenère's auto-key approach. The process of joining the plaintext to the key added more complexity to the system which in turn increased the number of different characters and bits in each round. This led to a very rapid growth of the avalanche effect, particularly because a change in the plaintext also impacts the key and, therefore, the rest of the ciphertext.

The last of these was the application of block ciphering, in the Cipher Block Chaining (CBC) mode, which added to the effectiveness of the avalanche effect. Because of the dependency between the blocks, the avalanche effect was increased from the first round with significant differences in characters and bits and low computational complexity. Stability was achieved in only 7 rounds, and other security benefits are associated with the block structure that is more challenging for an attacker to decipher.

4 Conclusion

In conclusion, this study established that the interaction between the substitution and transposition ciphers has a great impact on the avalanche effect. The use of both Vigenère and transposition, especially with the use of autokey gave the best results. As seen in the above experiment, even a slight variation of the plaintext resulted in a massive avalanche effect after a few rounds of the autokey changing the encryption mechanism. Regarding transposition cipher, symmetric keys must to be avoided, because they can really deteriorate the performance of the cipher.
The results were further improved when block cipher encryption was implemented using the CBC (Cipher Block Chaining) mode. This method not only enhanced the security by making a connection between each block with the previous one but also enhanced the avalanche effect more rapidly, that is, the diffusion was higher after one round. However, these improvements were not at the cost of computational efficiency which remained high, thus proving that CBC can be a good solution for enhancing the encryption without much impact on the computation front.

In general, the results indicate that the employment of both the substitution and transposition ciphers, with the block cipher techniques such as CBC, provides a more secure encryption system. It increases the avalanche effect, which means that the encryption is much more dependent on the changes in the plaintext, and therefore it is more difficult to break by using cryptanalysis attacks.

Difference between plaintext and modified plaintext after **1 round** of encryption, using *Transposition+Vigenère* in *CBC mode*:

```
Plaintext: Marco Bologna Security and Vulnerability in Networks
Cyphertext: °´¼ÛáÒ¹ØÐØ$ØÅØ+G`T3EØ«Øý§ðØÐüÑ0ØÅ+L:kØ2Ø©¢¼Ø¬-äØÒØÂÇÅÖìíoØAØ

Modified Plaintext: Larco Bologna Security and Vulnerability in Networks
Modified Cyphertext: °´¼ÛáÒ¸ØÐØ$ØÅØ+GaT3DØ«Øý§ðØÐüÐ0ØÅ+L:jØ2
©¢¼Ø¬-åØÒØÂÇÅÖiínØAØ
```

Difference between plaintext and modified plaintext after **7 rounds** of encryption, using *Transposition+Vigenère* in *CBC mode*:

```
Plaintext: Marco Bologna Security and Vulnerability in Networks
Cyphertext: ØÑØ«Ø\zyB=wé¨Øi <ØØþBNlRØd;ä#:ØØéØØðÙØ%:QJxKKØÉØÔíØj]9ØØHØâ2

Modified Plaintext: Larco Bologna Security and Vulnerability in Networks
Modified Cyphertext: ØÏØ¡ØPnq<3'-^Û¥bÆO1¼Ø0â"Ú°§DØRLØÂ²¨iÏØØx¯²Lm«ßá+Vç|iµµØØZLØ°
```

References

1. W. Stallings: "Cryptography and Network Security" 8th Ed., Prentice Hall

2. Paul et al.: Data based Transposition to Enhance Data Avalanche and Differential Data Propagation in Advanced Encryption Standard

3. Bhargava et al.: A new algorithm combining substitution & transposition cipher techniques for secure communication

4. Ramanujam et al.: Designing an algorithm with high Avalanche Effect

5. Astuti et al.: Analysis of the security level of modified CBC algorithm cryptography using avalanche effect