# Evaluating Computer Processing Efficiency Through Matrix Decryption

**Anthony Campagna[1], Hayden Ferencz[2], Shadi Zogheib[2], Advised By: Dr. Yongjian Fu**

[1] College of Sciences and Health Professions, [2]Washkewicz College of Engineering, Cleveland State University

## Abstract

In the modern technological age, the need to develop more efficient and robust cybersecurity methods remains a primary issue. At the same time, development of faster computational hardware - especially at the commercial level - can inadvertently render certain encryption practices obsolete, leaving one's personal information at risk. The purpose of this study is to observe the efficiency at which commercial PC systems could decode messages encrypted via a columnar transposition cipher. Messages are arranged in an m x n matrix, where n is a defined keyword length and m is the number of rows needed to write out the message. Each matrix then has n! ways the columns can be permuted, creating the encryption. Decryption time was tested using messages across keywords between 2-12 characters. Findings support the hypothesis that more powerful processors decrease the overall decryption time.

## Introduction

Cryptography remains an important tool in establishing secure communications in the presence of third parties. Modern applications include e-commerce, computer passwords, military communications and the rising market of cryptocurrencies worldwide. As computing techniques become more powerful, the importance of developing and maintaining more secure encryption techniques becomes imperative. In this study, we examine the efficiency of commercially accessible processing units fitted into 3 PC systems in the time it takes for each to decode messages encrypted by means of matrix manipulation.

## Objectives

- To determine variations in the efficiency of different processors through conventional encryption/decryption techniques.
- To identify trends in the efficiency of similarly manufactured processors (Intel® Core™)
- To observe trends in number of correct decryption occurrences as repeated letters are introduced to the matrix

## Encryption/Decryption Algorithm

- Full project written in the Java programming language on the Eclipse IDE
- Encryption algorithm designed to handle execution of the columnar transposition, writing all possible permutations of a given message to an output file
  - Number of permutations determined by (keyword length)!
- Decryption algorithm reads the encrypted message file and recursively compares all possible arrangements of each line to the original message
- Number of correct decryptions and average decryption time were taken for all keyword/message length combinations for up to 10 trials

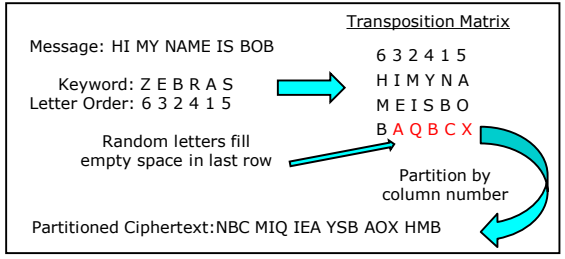


**Figure 1. Depiction of Columnar Transposition Process For A Single Permutation**

## Results

- Number of possible permutations and decryption time shared a direct relationship
- Number of correctly decrypted messages exponentially increased at the point where keyword length exceeded message length
- The Intel(R) Core(™) i7-6700K consistently outperformed the other two processors, decrypting approximately 30% faster than the Intel(R) Core (™) i5-6200U
- Decryption time differences - though present in the data across all trials - were indistinguishable on the user end of the process up until around keywords ≥ 8 characters in length (jump into tens of thousands of possible permutations)

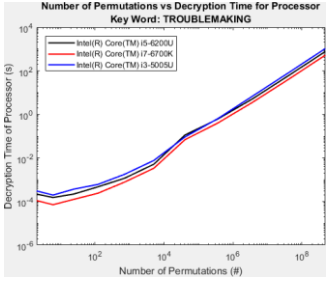


**Figure 1.1: For the key word TROUBLEMAKING, the figure shows the run time for each processor (in seconds) as the columns are increased**

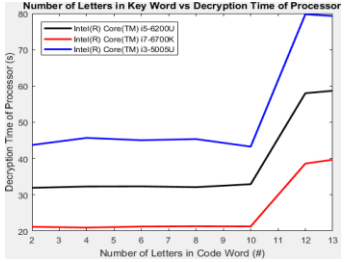


**Figure 1.2: Depicts the exponential jump when reaching a certain threshold of letters in the keyword.**

## Conclusions

Observations showed a clear dependence of decryption time on the overall complexity of the encryption, which in turn was based on the lengths of both the message and the given keyword. Each processor performed with similar efficiency on smaller message/keyword cases, with differences becoming more distinguishable at decryption times of magnitude $10^{-2}$ and greater. The arrival of distinct exponential graphs illustrated a ranking of efficiencies of different model but same brand processors. Data further revealed the impact random letters had on total number of occurrences which were greater in matrices with fewer rows.

## Future Direction

- Determine a trend of occurrence of successfully decrypted messages mathematically using linear regression
- More closely analyze how the processor is involved in the handling of random access memory (RAM) which can vary by machine
- Extend testing to different brands of processors to perform a more comprehensive analysis of commercially accessible processing units
- Examine if writing the code in another language (e.g. C) has a noticeable influence on execution time

## References/Acknowledgements

Columnar Transposition Cipher. (n.d.). Retrieved January 28, 2018, from http://practicalcryptography.com/ciphers/columnar-transposition-cipher/

Dr. Yongjian Fu, Associate Chair (BSCS/MCIS/MSSE), Dept. of Engineering

Dr. Shawn Ryan, Assistant Professor, Dept. of Mathematics

Dr. Mohammad Shirazi, Dept. of Electrical Engineering & Computer Science