An approach to Improving Columnar Permutation Cipher for Wills in Distributed Systems of Law Firms

Nwokedi, E. P
Department of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria
nwokedie@gmail.com

Oluwaseun, A. Ojerinde
Department of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria
o.ojerinde@futminna.edu.ng

Ojeniyi, A. J.
Department of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria
ojeniyija@futminna.edu.com

Adepoju, A. S.
Department of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria
solo.adepoju@futminna.edu.ng

ABSTRACT

With the evolution of cryptography in the twentieth century, classical ciphers (transposition ciphers) are gradually being pushed out because it now possesses low security ratings, however we can still salvage them, as they have other desirable and admirable qualities which include: easy of design, medium technical know-how and low computational power and it is to achieve this that this study; "A three layer permutation Cryptosystem using a modification of Transposition cipher and two layers content permutation for Wills" was carried out . The aim of this study is to make columnar transposition more secure and relevant so that companies with low technology budget and know-how be secured from known cryptosystem attack. The method used to achieve the above aim is adding to columnar transposition the technique of rail cipher, this affected the sequence of transposition, and lead to a new encryption equation and function. Cryptanalysis was carried out using various tools (Cryptool 2, Dcode and Countwordsfree) and parameters, using a transposition decoder the cipher text gotten using the traditional transposition cryptosystem decrypted with a hundred percent word and character accuracy whilst using the improved system gave a thirty percent accuracy.

KEYWORDS

Index Terms: Cryptography, encryption, permutation, transposition

ACM Reference Format:
Nwokedi, E. P, Oluwaseun, A. Ojerinde, Ojeniyi, A. J., and Adepoju, A. S.. 2021. An approach to Improving Columnar Permutation Cipher for Wills in Distributed Systems of Law Firms. In *The 5th International Conference on Future Networks & Distributed Systems (ICFNDS 2021), December 15, 16, 2021, Dubai, United Arab Emirates.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3508072.3512287

1 INTRODUCTION

Information is very vital and should be kept secured through networks [1], however the threats to devices in a networked environment keeps on metamorphosing because of the variety in network devices, protocols, and configuration [2]. This is particularly more difficult for industries who are not in the technology industry but make use of electronic data.

Cryptographic algorithms play an important role in the security architecture of any communication network [3]. With the rapid growth of Internet, global information tide expends the application of information network technology. It also brings about great economic and social benefit along with the extensive use of this technology. However, because Internet is an open system which faces to public, it must confront many safe problems. The problems include network attack, hacker intruding, interception and tampering of network information which lead huge threat to Internet [4]. Information encryption and decryption systems are used to move information security forward making data secured from external attacks, this provides a higher level of guarantee, such that the data that are encrypted cannot be gotten and altered by unauthorized parties in the event of theft, loss or interception.

Cryptography, which is the broad terminology that houses encryption and decryption, is the science and art of making communication systems secured from attacks. The term is gotten from the Greek words: 'kryptos' means "hidden" and 'graphos' [5], [6]. There are two common approaches used to create ciphers systems, they are; substitution and permutation. Substitution substitutes plaintext characters or strings of letters by letters or numbers or symbols. Permutation uses the plaintext message letters but repositions their order [7] therefore the characters in the ciphertext are the same amount with those in the plain text, they are just put in different positions .

In cryptography, a transposition or permutation cipher is a cipher in which the order of the letters are altered, some sort of permutation, therefore instead of replacing the letters with other symbols as in substitution ciphers [8], [9]. Permutation cipher works by dividing a message into a fixed size blocks, and then reordering the letters within each block based on a fixed permutation, say P. The key to the transposition cipher is simply the permutation P. So, the transposition cipher has the property that the encrypted message, that is to say that the, ciphertext contains all the characters that

ICFNDS 2021, December 15, 16, 2021, Dubai, United Arab Emirates

ACM ISBN 978-1-4503-8734-7/21/12…$15.00
https://doi.org/10.1145/3508072.3512287