Int. J. Sci. R. Tech., 2025 2(5)
A Multidisciplinary peer-reviewed Journal
www.ijsrtjournal.com [ISSN: 2394-7063]

Original Article

Modification of Vernam Cipher

Jehan Tamna, Manthan Prajapati*, Raviranjan Jha, Yugkumar Bhanderi, Vishal Kar, Twinkle Patel

IT, Sal College of Engineering

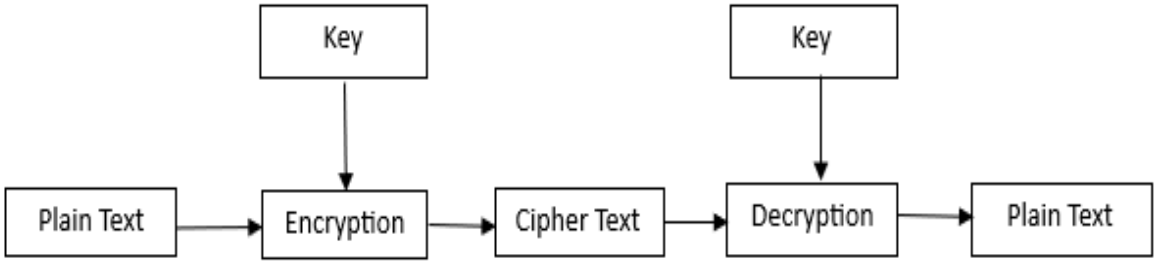
ABSTRACT

In this age of ever-expanding digital world, Communication plays a very important role which helps in growth of new technology. Naturally security of communication services is also essential. To achieve it we use Encryption. Cryptography plays huge role in Encryption of data, Cryptography comes from two Greek words, "krypos" which means "Hidden or Secret" and "graphein" which means "to write". In this research, we create extension of vernam cipher using square matrix as key matrix.

Keywords: Encryption, Xor (⊕), Square Matrix, Byte Extraction, Size of Variable

INTRODUCTION

Cryptography is the strongest tool used for secret writing which is controlling against the security threats [1]. Cryptography is study of encryption and decryption of plain text and cipher text respectively. In cryptography, cipher is an algorithm of well-defined steps for performing encryption and decryption. In encryption process, the original plain text is converted into cipher text using a key and in decryption process, plaintext is restored from cipher text using key. We need a strong encryption algorithm in order to encrypt plain text to cipher text [2]. The sender and receiver both must have key and key must be kept private. The process of encryption and decryption is shown below



Traditional ciphers consist of substitution or transposition techniques. In substitution cipher, we replace letters in plain text with other letters or symbols keeping the order of letters same. It Transposition ciphers, we keep all letters in their original form but change the position of letters. Transposition cipher hides the message by rearranging the order [3]. A character in the 1st position of plaintext may appear at 10th position in cipher text, and a character at 7th position in the plaintext may appear at 25th position in cipher text. Vernam Cipher is not used a lot in today's age, due to it having drawbacks related to its key. If the key is smaller than plaintext, it loses its security as it becomes vulnerable to attacks like known-plaintext attack or ciphertext-only attack. While if we use its One-Time Pad version, which says use randomly generated key equal to length of plaintext we run into issue of storing and distributing key securely which makes it hard to use even though it exhibits property of perfect secrecy. To try overcome issue of small key size we propose this modified version of vernam cipher.

Proposed Modified Vernam Cipher:

This modification of vernam cipher changes how key is used in cipher, here we first assume what size will

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

our square matrix will be, size of matrix will tell us how many letters it will encrypt before key cycles back to 1st element, which is (size of matrix)^2. After size of matrix is decided, we will generate integers and store it in matrix, once matrix is full, we generate determinant of that matrix, determinant is then wrapped based on size of variable so that it comes in range of size of variable. If determinant is zero, we generate new matrix. After above key generation procedure is done, we start encryption process, our encryption process will depend on byte size of integer variable and char set. Here we will assume variable size to be 4 and charset to be extended ascii which is 1 byte.

Encryption:

Here we will take first letter of plain text, and take 1st element of key matrix, determinant of matrix and divide both of them into bytes such that it will give us 4 bytes for each, for key element assume bytes named k_i and for determinant assume bytes named d_i where i is ith byte of key element or determinant. after dividing keys and determinant into bytes we apply xor operator in following format

For i = (size_of_variable) to 1 {
CT = CT ^ k_i;
CT = CT ^ d_i;
}
From above codelet we can see that in first iteration, last byte of key element is xor with plain text and then last byte of determinant is xor with result of previous operation. Once loop terminates our letter is converted to its cipher equivalent, assuming CT first stored plaintext when loop was initiated.

Decryption:

The process is similar to Encryption except operations performed are reversed.

For i = (size_of_variable) to 1 {
PT = PT ^ d_i;
PT = PT ^ k_i;
}

Since we perform operations in reverse, we get plain text back from cipher text, assuming cipher text was stored in PT when loop was initiated.

Advantages:

This proposed vernam cipher makes it harder to perform analysis attack or makes it hard to perform brute-force attack.

CONCLUSION:

Here, we point out merits and demerits of vernam cipher in both mode of operation (with small key than plaintext and with key equal to plaintext). In order to overcome demerits of vernam cipher with small key, we proposed modified version of vernam cipher which can be used to make ciphertext more secured from attacks.

REFERENCE

1. William Stalling: Network Security Essentials (Application and Standards). Pearson Education, 6th Edition 2004.
2. Atul Kahate: Cryptography and Network Security. McGraw-Hill Education, 2nd Edition 2009.
3. William Stalling: Cryptography and Network Security, Pearson Education, 5th Edition 2008.

HOW TO CITE: Jehan Tamna, Manthan Prajapati*, Raviranjan Jha, Yugkumar Bhanderi, Vishal Kar, Twinkle Patel, Modification of Vernam Cipher, Int. J. Sci. R. Tech., 2025, 2 (5), 50-51. https://doi.org/10.5281/zenodo.15322589