Ju-ti : Jurnal Teknik Indonesia
ISSN : 2964-0490 (online)
Vol. 3, No. 02, 2024, pp. 54-60
https://jurnal.seaninstitute.or.id/index.php/juti

Cryptography With One-Time Pad (OTP) Algorithm Xor Based

Reymond[1], Johanes Manullang[2], Jhoische Tamba[3], Farel Parasian Sitohang[4], Eikel Nioisha Ginting[5]
Teknik Informatika,Universitas Santo Thomas Medan

Article Info

Keywords:
One-Time Pad (OTP),
decryption,
Cryptography.

ABSTRACT

The One-Time Pad (OTP) algorithm is a symmetric cryptographic method that is recognized as one of the most secure methods for encrypting data. In this study, OTP utilizes a unique random key that has the same length as the original message (plaintext). The encryption and decryption processes are carried out using the XOR (Exclusive OR) operation, which ensures that the resulting ciphertext does not provide information about the plaintext without knowing the key used. This document explains the basic theory of OTP, including the encryption process that produces ciphertext from plaintext and key, and the decryption process that returns ciphertext to plaintext. Through a manual example, this document shows how the characters in the plaintext and key are converted into binary format and operated with XOR to produce ciphertext. Testing using Python is also explained to provide a practical overview of the implementation of this algorithm. Although OTP offers a high level of security due to the random and disposable nature of the key, challenges in key distribution and management often limit its use in practice. The conclusion of this study confirms that although OTP is secure in theory, its real-world application requires special attention to key management to maintain data integrity and confidentiality.

Corresponding Author:
Reymond
Universitas Katolik Santo Thomas
ssreymon78@gmail.com

1. INTRODUCTION

Information technology security has a crucial role in an agency or institution to protect valuable assets, such as data and communication systems, from various potential threats. One way to secure communication is to apply encryption methods.(Haq et al., 2024).

Cryptography is a field of science that focuses on protecting the confidentiality of messages (data or information) by converting them into codes that are difficult to understand.(Clawdia et al.,2017.). Therefore, a data protection system is needed that can guarantee information security. One of the security methods that can be applied is one-time pad cryptography, which has proven to be very difficult to hack (see Claude Shannon in "Communication Theory of Secrecy Systems") (Claude Shannon, 2012). The OTP encoding technique was first introduced by Gilbert Vernam during World War I.

In cryptography, there are two basic concepts, namely encryption and decryption. Encryption is the process of securing information by changing its form or format using a certain algorithm, so that only the sender and recipient are entitled to understand the contents of the message.(Akbar et al., nd). In contrast, decryption is the process of returning an encrypted message to its original form.

Previous research results Implementation of Modified OTP Cryptography for File Encryption This research modifies the OTP algorithm so that it can be used for file encryption, solving the problem of key usage in the encryption and decryption process. This system creates variables based on plaintext, ciphertext, and key, and uses a matrix to strengthen the encryption process(Christy Winaryo et al., 2014). Development of Split-Merge One Time Algorithm In this research, the OTP algorithm is developed using the Split-Merge method, where the plaintext and key are separated into several parts before the XOR process is carried out. The results show that this method can increase the amount of ciphertext generated up to four times, thus strengthening data security. (Utomo & Zarlis, 2017).

Cryptography itself is a discipline that focuses on maintaining the security of a message (plaintext). Its main goal is to protect the message or encryption key to keep it confidential from unauthorized parties (eavesdroppers). An eavesdropper is considered to have full access to the communication channel between the sender and recipient of the message.

2. METHOD

This study uses an experimental method by implementing the One-Time Pad (OTP) algorithm to encrypt and decrypt messages. The research steps are carried out systematically to test the effectiveness and security of this method in securing data.

Encryption Process

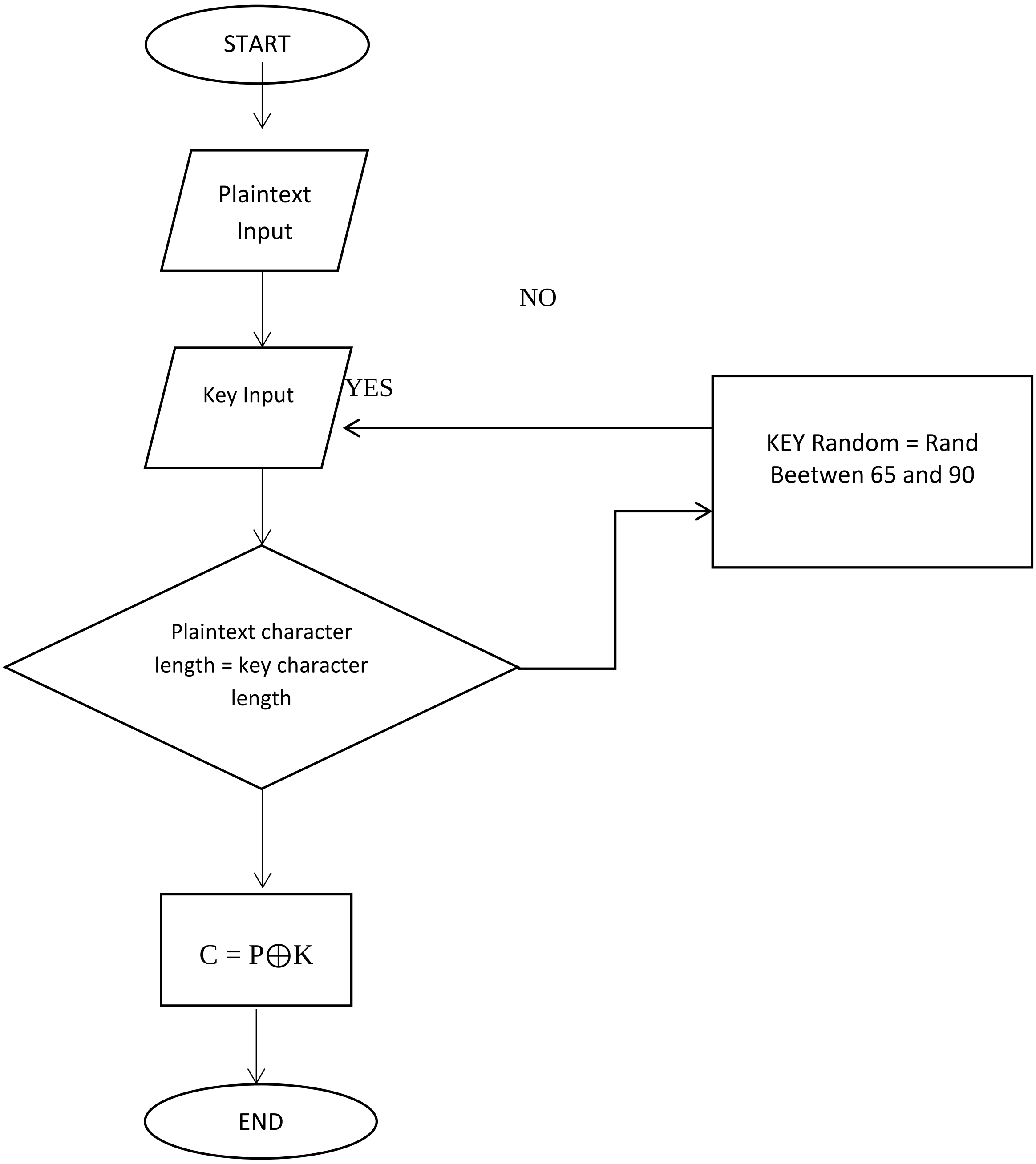

figure 1. Encryption process

Ciphertext (C) is generated by performing XOR between plaintext (P) and random key (K):

$$C = P \oplus K$$

Information
P = Bits or bytes of the original message (plaintext).
K = Bits or bytes of a unique random key, with the same length as the plaintext.
C = Bits or bytes of the resulting ciphertext.

Decryption Process

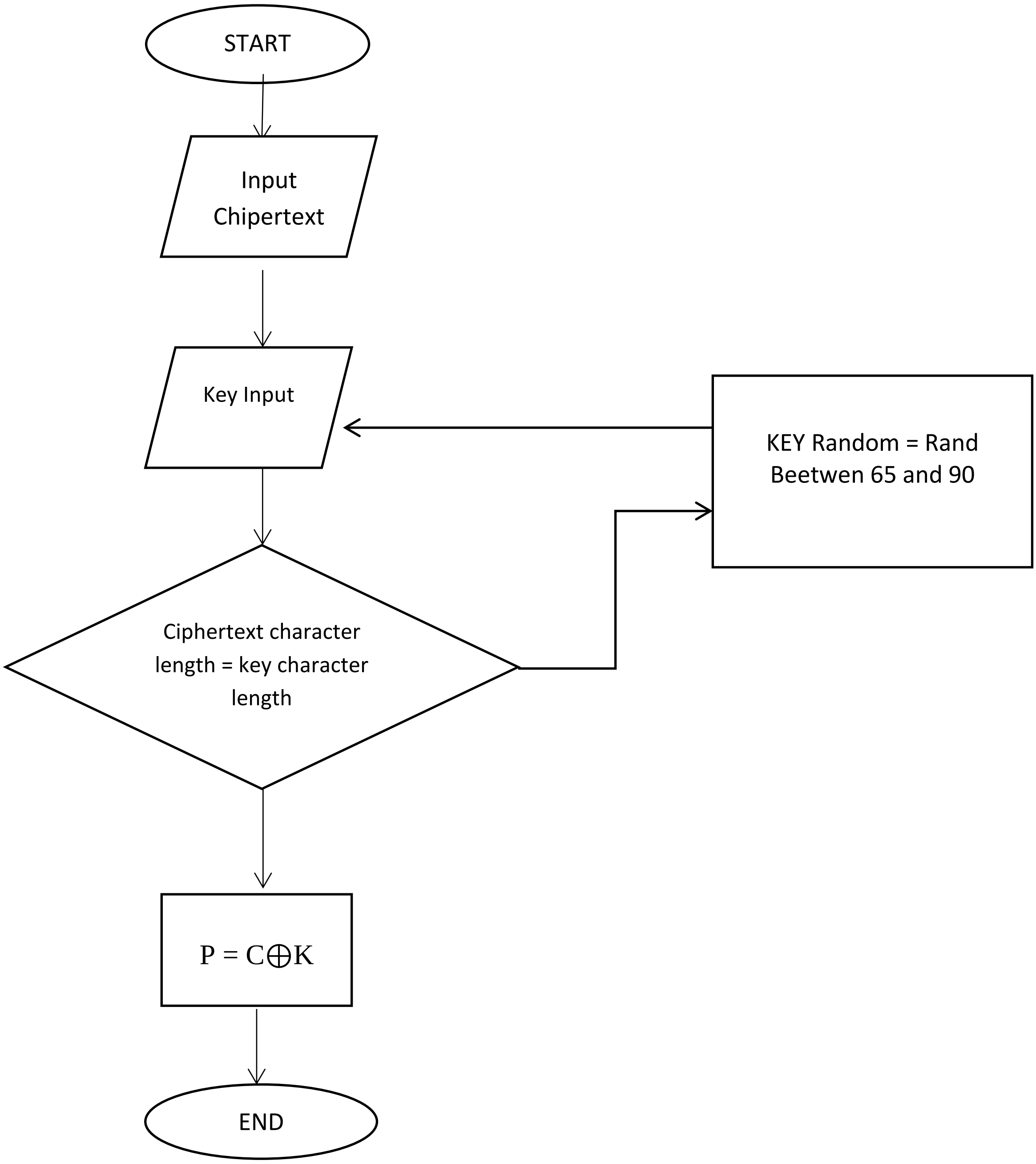

Table 2. Decryption process diagram

Plaintext (P) is restored by performing XOR between ciphertext (C) and key (K):

$$P = C \oplus K$$

3. RESULTS AND DISCUSSION

In designing an unbreakable cipher, there are two important requirements that must be met. First, the key selection must be done randomly, and second,longThe key must be the same length as the plaintext to be encrypted. Both are very influential, because even though the same plaintext can be encrypted, the resulting ciphertext will not necessarily be the same.

For example, if the plaintext is "JHOISCHE" and the key is "GROUP", keep in mind that the length of the key and the plaintext must be identical. First, we need to get the ASCII code for the plaintext, and then convert it to binary, as shown in table 1.

Table 3. Plaintext Binary Notation

Character	Plaintext (ASCII)	Binary
J	74	01001010
H	72	01001000
O	79	01001111
I	73	01001001
S	83	01010011
C	67	01000011
H	72	01001000
E	69	01000101

From table 3 above, the ASCII code for Plaintext Binary Notes is produced, and this also needs to be implemented on the selected key.

Table 4. Key Binary Notation

Character	Plaintext (ASCII)	Binary
K	75	01001011
E	69	01000101
L	76	01001100
O	79	01001111
M	77	01001101
P	80	01010000
O	79	01001111
K	75	01001011

Encryption and Decryption Process

Encryption

Ciphertext (C) is generated by performing XOR between plaintext (P) and random key (K): $C = P \oplus K$

Table 5. XOR Result of Plaintext with Key

Binary	Decimal
00000001	1
00001101	13
00000011	3
00000110	6
00011110	30
00010011	19
00000111	7
00001110	14

The encryption process in the One-Time Pad (OTP) algorithm is carried out by the XOR operation between the plaintext and a random key that has the same length. Each character in the plaintext is converted into binary format, as is the key used. Furthermore, each bit of the plaintext is operated with the corresponding bit of the key using the XOR operation. XOR works with the rule that if two bits are the same ($0 \oplus 0$ or $1 \oplus 1$), the result is 0, whereas if the two bits are different ($0 \oplus 1$ or $1 \oplus 0$), the result is 1. In this example, the plaintext "JHOISCHE" represented in binary is combined with the key "GROUP" using XOR, resulting in a unique ciphertext. The XOR result for each pair of bits forms the ciphertext in binary form, which overall becomes "00000001 00001101 00000011 00000110 00011110 00010011 00000111 00001110". This ciphertext cannot be restored to its original form without knowing the key used, which shows the high security of the OTP method. Due to its nature of using a single-use and completely random key, this method guarantees unhackable security if the key is managed properly.

Decryption Process

Plaintext (P) is restored by performing XOR between ciphertext (C) and key (K):

$$P = C \oplus K$$

Table 6. Result Description

Binary	Decimal	Text
01001010	74	J
01001000	72	H
01001111	79	O
01001001	73	I
01010011	83	S
01000011	67	C
01001000	72	H
01000101	69	E

The decryption process in the One-Time Pad (OTP) algorithm is carried out by the XOR operation between the ciphertext and the key used in encryption. Because of the reversible nature of XOR ($C \oplus K = P$ and $C \oplus P = K$), then by knowing the same ciphertext and key, the plaintext can be restored to its original form. In this example, the ciphertext generated from the previous encryption process is recombined with the same key using the XOR operation. Each bit of the ciphertext is operated on with the corresponding bit of the key, producing the plaintext back in binary form, namely "01001010 01001000 01001111 01001001 01010011 01000011 01001000 01000101". This result shows that the original message can be perfectly recovered as long as the key used in the decryption process is the same as the key used during encryption. This confirms the security of the OTP algorithm, where without knowing the correct key, the decryption process cannot be carried out correctly, thus maintaining the confidentiality of the data sent.

Testing With Python

Encryption Process

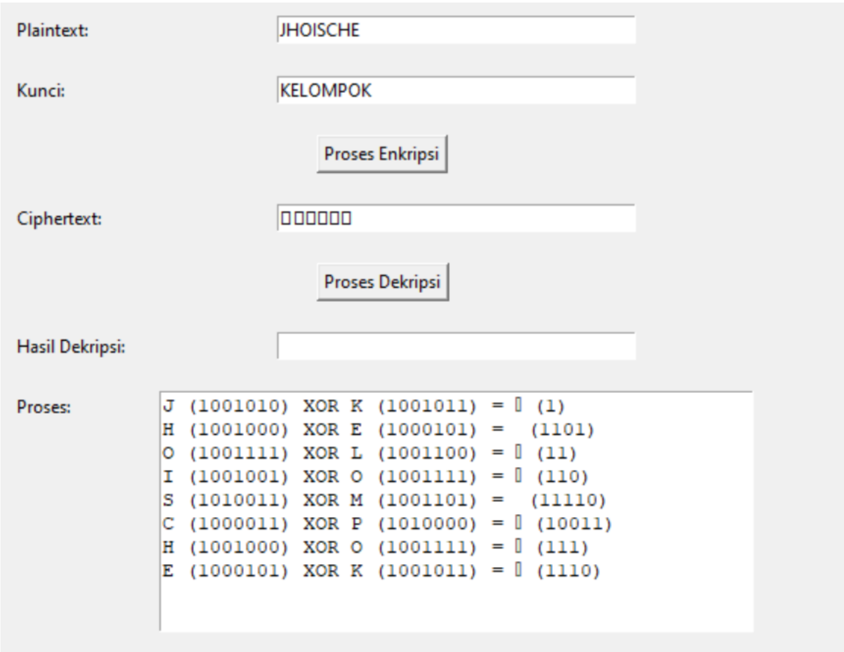

Figure 1. Encryption Process

This figure shows the encryption and decryption process using the key "GROUP". The plaintext "JHOISCHE" is encrypted into ciphertext with the XOR operation. Decryption uses the same key to restore the original text. This process ensures that the data can be disguised and recovered.

Decryption Process

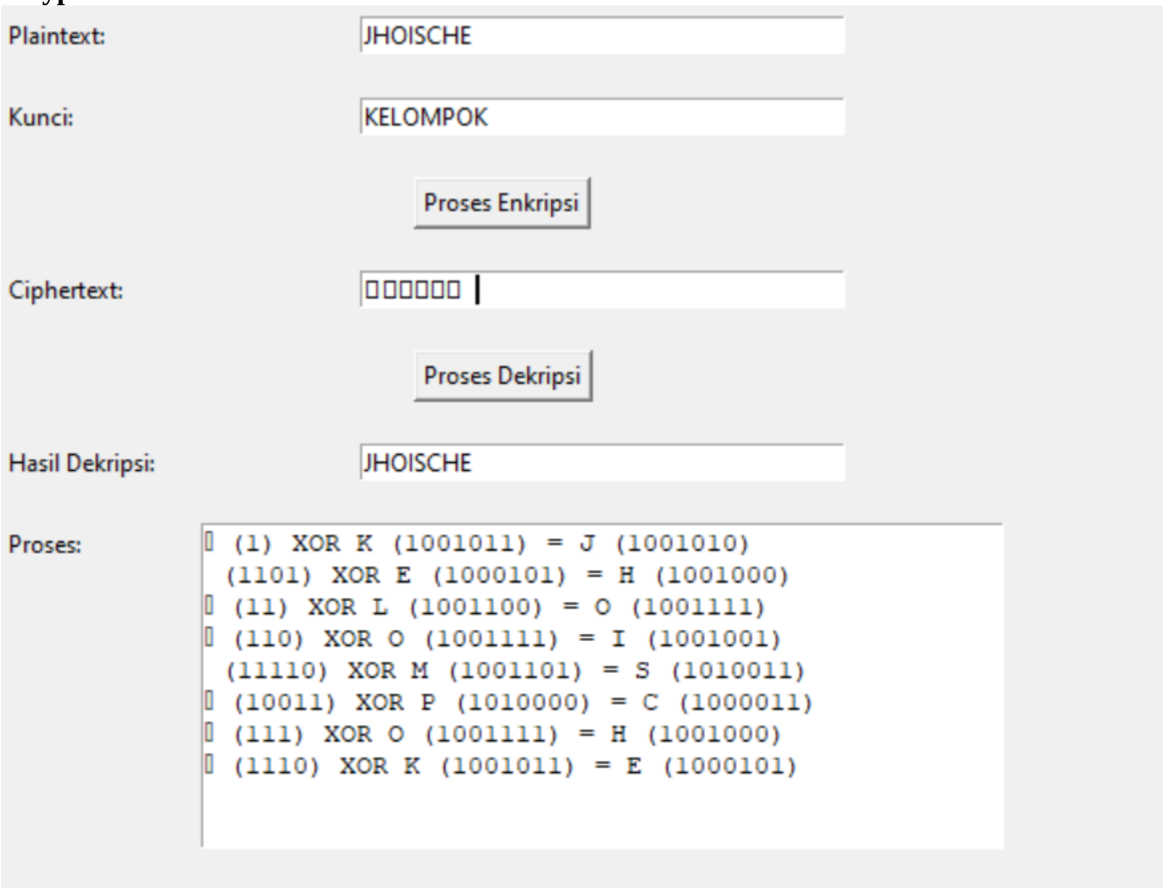

Figure 2. Decryption Process

This figure shows the process of encrypting and decrypting text using a key-based method, possibly the XOR cipher.Plaintext"JHOISCHE" is combined with the key "GROUP" to produce the ciphertext. The decryption process then returns the text to its original form. The "Process" section shows the encryption and decryption steps per character, ensuring that the method works properly.

4. CONCLUSION

One-Time Pad (OTP) is a very secure encryption algorithm because it uses a unique random key with the same length as the plaintext. The encryption process is carried out by XOR operation between the plaintext and the key, producing ciphertext that cannot be cracked without knowing the key. In this manual calculation, each character in the plaintext and key is converted to binary, then operated with XOR to obtain the ciphertext. For decryption, the ciphertext is again XORed with the key, producing the original plaintext. The security of OTP lies in the nature of its key which is completely random and only used once. If the key is reused or is not completely random, then security can be compromised. Therefore, although OTP is very secure in theory, its application in practice is often limited due to difficulties in key distribution and management.

REFERENCES

Akbar, I., Sari, A. K., Si, S., & Kom, M. (n.d.). *Implementasi Enkripsi Homomorfik RSA Termodifikasi Untuk Sistem Electronic Voting*. http://etd.repository.ugm.ac.id/

Christy Winaryo, F., Danny Wowor, A., & Indrastanti Widiasari, Mc. R. (2014). *Implementasi Modifikasi Kriptografi One Time Pad (OTP) untuk Pengamanan Data File Artikel Ilmiah Peneliti*.

Clawdia, J., Khairina, N., & Harahap, M. K. (n.d.). *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*. http://ejurnal.stmik-budidarma.ac.id/index.php/komik

Haq, S. H., Fauzi, A., Thamrin, D., Maulana, P., Hidayat, A. N., Muslih, S. A., & Fernando, A. (2024). *Peran Manajemen Sekuriti Dalam Meningkatkan Kesadaran Keamanan Data Mahasiswa Pada Sistem Informasi Akademik Ubhara Jaya* (Vol. 1, Issue 2). https://inovanpublisher.org/orbit,

Utomo, P., & Zarlis, M. (2017). *Seminar Nasional Teknologi Informatika*.

Stallings, W. (2011). *Cryptography and Network Security: Principles and Practice* (5th ed.). Pearson Education.

Shannon, C. E. (1949). *Communication Theory of Secrecy Systems*. *Bell System Technical Journal*, 28(4), 656-715.

Vernam, G. S. (1926). *Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications*. *Journal of the American Institute of Electrical Engineers*, 45(2), 109-115.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (2nd ed.). John Wiley & Sons.

Diffie, W., & Hellman, M. E. (1976). *New Directions in Cryptography*. *IEEE Transactions on Information Theory*, 22(6), 644-654.

Shannon, C. E. (2012). *Teori Komunikasi dari Sistem Kerahasiaan*. (Reprint dari karya asli tahun 1949).