Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 4, October 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i4.13051 p-ISSN : 2541-044X

Three Pass Protocol For Key Security Using Affine Cipher Algorithm and Exclusive-OR (XOR) Combination

Muhammad Ikhwan Harahap[1)*], Suherman[2)], Rahmat W Sembiring[3)]
[1,2)] Universitas Sumatera Utara, [3)]Politeknik Negeri Medan
[1)]hrp.ikhwan@gmail.com, [2)] suherman@usu.ac.id, [3)] rahmatws@polmed.ac.id

Submitted : Sep 26, 2023 | **Accepted** : Sep 27, 2023 | **Published** : Oct 1, 2023

Abstract : Information is a very important concern in today's technological era, especially in terms of security through the exchange of information that is so fast that people can easily get various kinds of information. Information obtained easily through recording or openly disseminating data, XOR Cipher is an algorithm used to secure messages and texts but has weaknesses due to simple computation, therefore to strengthen security in XOR Cipher communication protocols can be added to secure key exchange on XOR Ciphers. Affine Cipher can be combined with Exclusive-OR (XOR) for text message security. Through the Affine Cipher algorithm with Key can change the unknown Plaintext, so that the Plaintext is kept secret. The Exclusive-OR (XOR) combination by changing each Character in each Plaintext according to the ASCII Code table can shorten the Key encoding process, so that Plaintext remains safe to send. The Affine Cipher Algorithm and the Exclusive-OR (XOR) Combination for Plaintext security levels are better because the Plaintext encryption and decryption processes are carried out twice with different cryptographic algorithms.

Keywords: Plaintext; Security; Chipertext; Afiine Cipher; XOR Chipper

INTRODUCTION

Every information is a very important concern in today's technological era, especially in terms of security through the exchange of information that is so fast that people can easily get various kinds of information (Galih, 2020). Information and messages are developing so rapidly that anyone can access them via the internet without having to interact directly (Darmayanti, Astrida, & Arius, 2018). Therefore, the security of information or messages must be truly safe and conveyed to the person who receives it. Data has become something very valuable in today's age of information technology. Especially if the data is very confidential and not just anyone can access it. The form of data that is secured in this case is digital or electronic. Treatment Specific data will be required if the data is intended only for a limited audience and if The data is sent via the Internet, while the data content may not change from sender to sender recipient. Various data security efforts have been made to ensure that data can only be accessed accessed by the right people, one way is by cryptography (encoding) data (Suhardi, 2016). Currently, a lot of research is being done on cryptography, one of which is modifying the Affine Cipher algorithm by encoding Plaintext keys by reversing the letters in the Plaintext key before the encryption process is carried out. (Babu, 2017). Next, combining the Caesar and Affine Cipher algorithms by hiding the letters in the Plaintext through the original Plaintext encryption process, while the existing

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 4, October 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i4.13051 p-ISSN : 2541-044X

Caesar Cipher encryption is encrypted with Affine Cipher, then the Ciphertext results and the same process are also carried out in the decryption process. The Affine Cipher algorithm consists of several different keys in the encryption and decryption process, as well as key transfer, so the password formed is not easy to break (Wulandari, 2020). The XOR Cipher encoding method has weaknesses due to its simple computation, so it is necessary to increase security by adding a communication protocol to secure key shifts in this method (Amalia & Rosyani, 2018). Related research in this context, the author conducted research by identifying the processes in the two algorithms between Affine Cipher and Exclusive-OR (XOR), so that what patterns or measures can be seen from the algorithm processes, especially key security.

LITERATURE REVIEW

Three Pass Protocol

A cryptographic protocol used to send secret messages is called the Three Pass Protocol. This protocol also allows two parties to exchange information safely without having to exchange keys, so that key distribution in symmetric algorithms can be handled properly. Three Pass Protocol is when each party has the encryption and decryption keys. The sender is called the Client and the recipient is called the Server using keys to encrypt and decrypt messages, so they can exchange messages without having to exchange keys. If there is no key exchange, the key cannot be tapped and the confidentiality of the message is maintained.

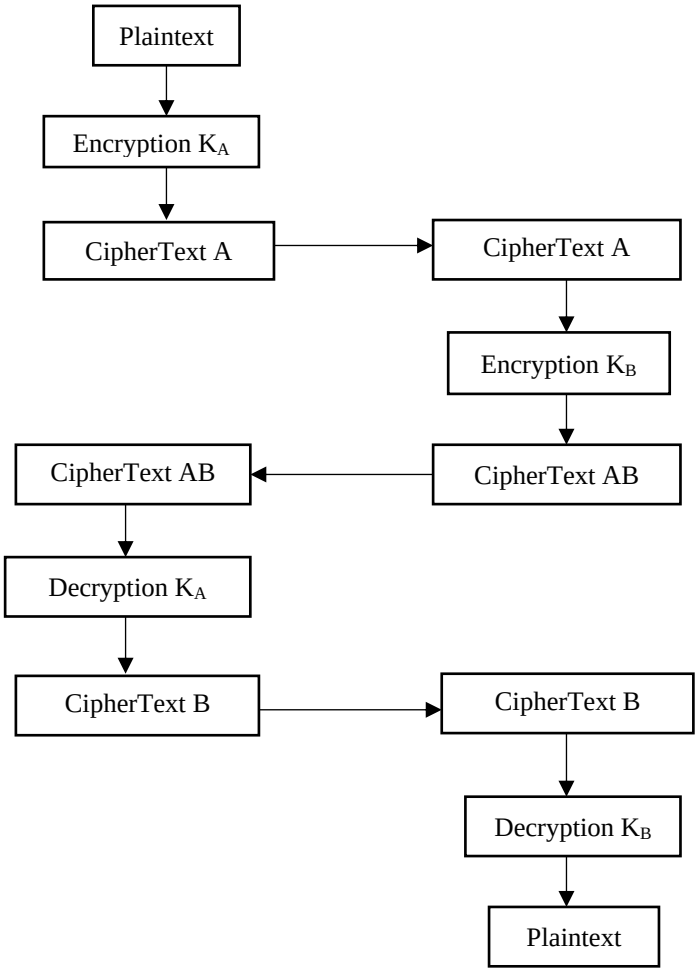


Figure 1 Three Pass Protocol Process

The description in the image above where:

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 4, October 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i4.13051 p-ISSN : 2541-044X

1. The client sends the KA secret key as an encryption and decryption process. The plaintext sent will be encrypted using the KA key. Next, the resulting Ciphertext is sent to the Server.
2. The server sends the KB secret key as an encryption and decryption process. The ciphertext received from the Client is re-encrypted using the KB key. Next, the resulting Ciphertext is sent back to the Client.
3. The ciphertext received by the Server is decrypted using the KA key, then the decryption result is a Ciphertext which is sent back to the Server. Next, the Server decrypts the Ciphertext using the KB key, so that the decryption result is a Plaintext from the Client (Oktaviana & Siahaan, 2016).

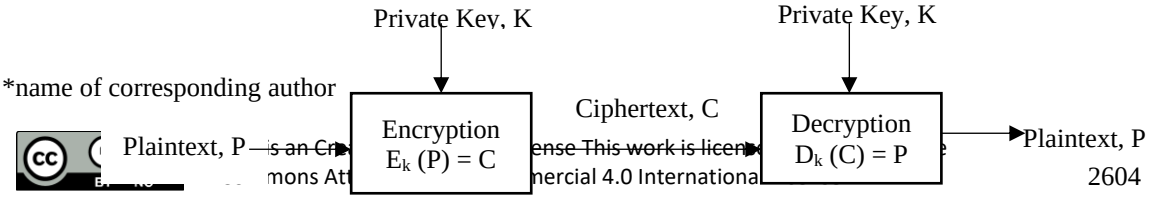
Cryptography

The science of message coding used to provide security in sending messages or data. In the current world of information technology, cryptography is very important to use to study mathematical techniques related to aspects of information security so that it remains confidential (Munir, 2006). This science also studies the process of encrypting a message which will be scrambled using an encryption key so that the message is difficult to understand by parties who do not have the key for decryption. The encryption process uses the decryption key to retrieve the original key. The key that will be sent lies in the function that will be used with the parameter provisions, in this case the decryption key that must be kept secret (Kromodimoeljo, 2010). The parameters for the message and text conversion process lie in the key and several keys (Ibisa, 2011). Cryptography is the science of encoding messages that are used to increase security in sending messages and data communications. The security of information, especially in sending cryptographic messages, provides a secure process for information to be conveyed to recipients. Cryptography aims to provide security services, as follows:

1. Confidentiality
   An attack on the confidentiality of data that is carried out by breaking access rights by entering into the system with the aim of knowing, retrieving, or changing the data.
2. Non-repudation
   Sending the message denies sending or the recipient of the message denies having received the message
3. Data Integrity
   Services that guarantee data is still in its original state or has not been changed during transmission
4. Authentification
   Services that identify the truth of the communicating parties (User Authentication or Entitu Authentication) and the truth of the message source (Data Origin Authentication) in order to ensure the authenticity of it (Munir, 2006).

Cryptography is an algorithm and key as a mathematical function that is used to encrypt and decrypt messages or data. Cryptographic algorithms are classified into two parts, including:

a. Symmetric Algorithm
   A symmetric algorithm is an algorithm that uses the same key for the encryption process as the key for the decryption process. The symmetrical algorithm is divided into 2 namely flow algorithm (Steam Cipher) and block algorithm (Block Cipher). Stream algorithm is an encoding process oriented to one bit or one byte of data. While the process block algorithm is oriented encoding on a set of bits or bytes of data (per block) for example DES (Data Encryption Standard)



*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 4, October 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i4.13051 p-ISSN : 2541-044X

Figure 2 Symmetric Algorithm Flow

b. Asymmetric Algorithm
An asymmetric algorithm is an algorithm that uses a different key for the encryption and decryption processes. This algorithm is also called a public key algorithm (Public Key Algorithm) because the key for encryption is made public (Public Key) or can be known by everyone, but the key for decryption is known only to those who have the right to know the encoded data is called a private key (Private Key). Examples are RSA and ECC.

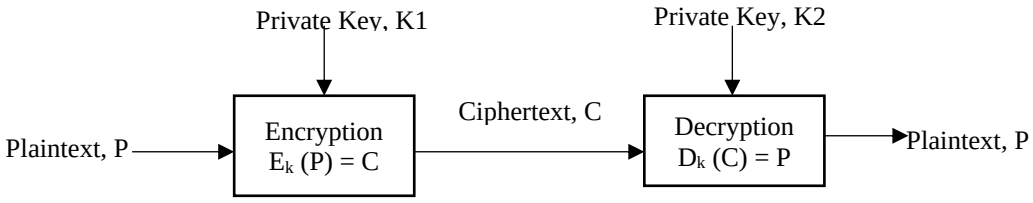


Figure 3 Asymmetric Algorithm Flow

Cryptographic Algorithms

Cryptography is an algorithm and key as a mathematical function that is used to encrypt and decrypt data or messages. The keys used in cryptographic algorithms can be differentiated on the basis of symmetric and asymmetric algorithms and their development requires ciphers and keys. Cryptographic algorithms consist of three basic functions, namely encryption, decryption and key. The security of modern cryptography is achieved by keeping the key held secret from other people. without having to keep the algorithm itself secret. Keys have the same function as passwords. If the entire security of an algorithm depends on the key used then the algorithm can be published and analyzed by others. If a published algorithm can be solved in a short time by someone else, it means the algorithm is not safe to use (Ariyus, 2008).

Chiper and Key

The cryptographic algorithm is called a cipher which can be interpreted as a rule for encrypting and decrypting. The mathematical concept of a cryptographic algorithm is the relationship between two sets consisting of cryptographic elements, namely Plaintext elements and Ciphertext elements (Pressman, 1997).

1. Plaintext is called P and Ciphertext is called C, so the encryption function E that maps P to C is E(P) = C.
2. The decryption of D that maps C to P is D(C) = P.
3. The encryption process becomes decryption to return Plaintext to Original plaintext, where D(E(P)) = P.
4. Modern cryptographic algorithms use keys that are kept secret. Keys are also called parameters that can change encryption and decryption where EK(P) = C and DK(C) = P.
5. The equation function is DK(EK(P)) = P.

Affine Cipher Algorithm

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 4, October 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i4.13051 p-ISSN : 2541-044X

Affine Cipher algorithm is an extension of Caesar Cipher which converts Plaintext with a value of n and adds with a shift as follows: In this case Plaintext encryption (P) diverts Ciphertext (C) can be expressed with the congruent function as follows: E(P) = (a.x + k) mod m.

Table 1 Equation Description

m	alphabet size
a	An integer that must be relatively prime with m but if it is not relatively prime decryption cannot be performed
k	Number of shifts with m = 1
x	Plaintext converted to integers ranging from 0 - 26 and adjusted in alphabetical order
E(P)	Ciphertext converted to integers ranging from 0 - 26 and adjusted in alphabetical order

1) In the decryption function, use the equation $D(x) = a^{-1}(x – k) \bmod m$.
2) When a^{-1} is the inverse multiplication a modulation m can be generated equation $1 = aa^{-1} \bmod m$.
3) The multiplication inverse a only exists if a and m are relatively prime integers, otherwise the algorithm process cannot be continued. The decryption function is also the opposite of the encryption function which can be seen below:

$D(E(P)) = a^{-1}(E(P) - k) \bmod m$
$= a^{-1}((a.x + b) \bmod m$
$= a^{-1}(a.x + k) \bmod m$
$= a^{-1}ax \bmod m$
$= x \bmod m$ (Juliadi, Prihandono, & Kusumastuti, 2013)

XOR Logical Operations

The XOR logical operation is a binary operator widely used in Cipher that operates in the bit model. Mathematical notation is"⊕". For operation it is divided into two bits with the rules specified in the table below:

Table 2 XOR Logical Operation Rules

A	B	A⊕B
0	0	0
0	1	1
1	0	1
1	1	0

If the input is the same $0 \oplus 0$
0

If the input is different $0 \oplus 0$
1

Exclusive-OR (XOR)

The XOR method is a cryptographic technique that uses the XOR logic operation principle in the encryption and decryption process. The encryption process by XORing Plaintext (P) with key (K) produces Ciphertext $C=P \oplus K$ while the decryption process by XORing Ciphertext (C) with key (K) produces Plaintext $P=C \oplus K$ (Sulaiman, Nasution, & Siambaton, 2020).

METHOD

Research Flowchart

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 4, October 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i4.13051 p-ISSN : 2541-044X

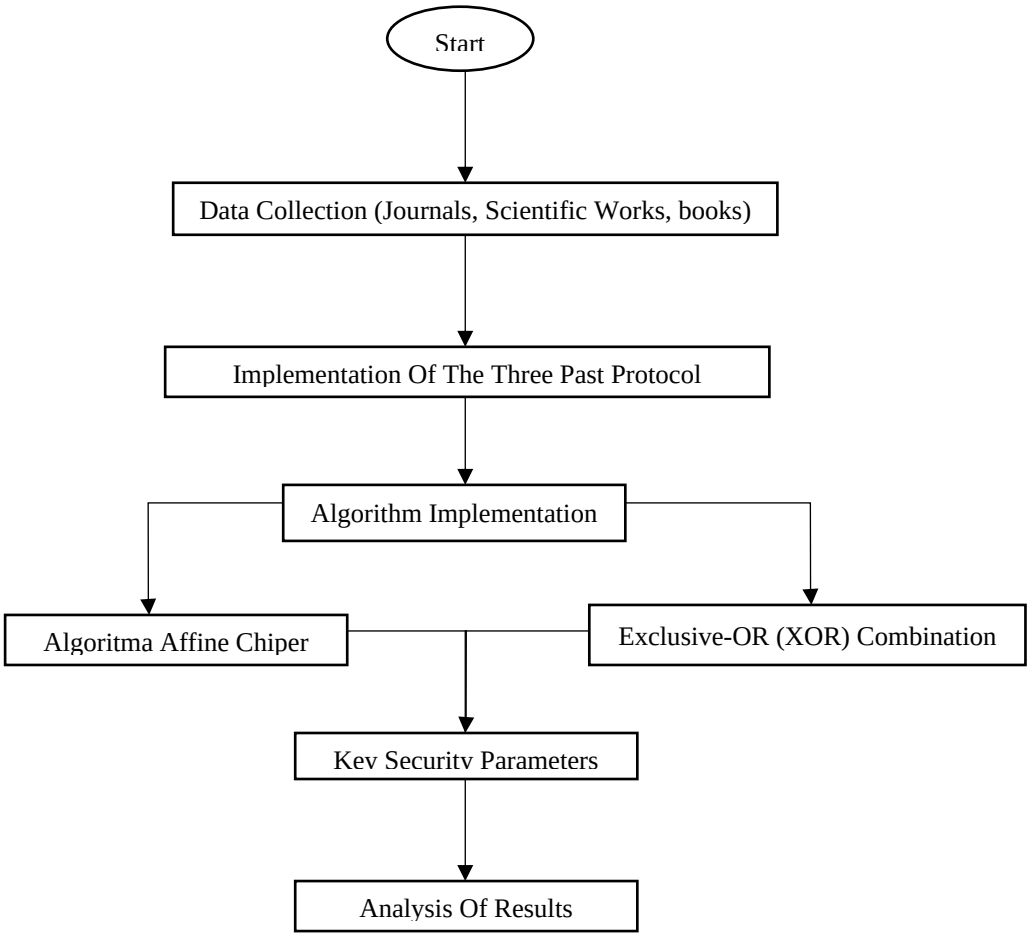


Figure 4. Research Flowchart

Parameters for Key Security

The parameters used for key security are implemented into measures as follows:

Table 3 Bit ASCII Code (Winarno & Cahyanto, 2021)

Character	ASCII Code	Binary	Character	ASCII Code	Binary
a	097	01100001	$3,6,8_A$	065	01000001
b	098	01100010	B	066	01000010
c	099	01100011	C	067	01000011
d	100	01100100	D	068	01000100
e	101	01100101	E	069	01000101
f	102	01100110	F	070	01000110
g	103	01100111	G	071	01000111
h	104	01101000	H	072	01001000
i	105	01101001	4_I	073	01001001
j	106	01101010	J	074	01001010
k	107	01101011	2_K	075	01001011
l	108	01101100	L	076	01001100
m	109	01101101	1_M	077	01001101
n	110	01101110	N	078	01001110

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 4, October 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i4.13051 p-ISSN : 2541-044X

o	111	01101111	O	079	01001111
p	112	01110000	P	080	01010000
q	113	01110001	Q	081	01010001
r	114	01110010	7_R	082	01010010
s	115	01110011	5_S	083	01010011
t	116	01110100	T	084	01010100

Limitation of Research

In order not to expand the scope of the discussion, the following limitations are given in this study:

1. Using the Affine Cipher algorithm in the Three Pass Protocol Technique
2. The Three Pass Protocol scheme is modified to allow for good key exchange through the Affine Cipher algorithm and Exclusive-OR (XOR) combinations.
3. The message used is in the form of a text message that can be read, the confidentiality and security of the key are maintained.

RESULT

Calculation of the Affine Cipher Algorithm

1. Affine Cipher Algorithm Encryption Process

Table 4 Plaintext (P)

Plaintext	MKAISARA
a	7
b	8
m	26
Alphabet Divider	4

- CAS1.1 = ((a x PAS1.1) + b) mod m
  = ((7 x I) + 8) mod 26
  = ((7 x 9) + 8) mod 26
  = (63 + 8) mod 26
  = 71 mod 26
  = 19
- CAS1.2 = ((a x PAS1.2) + b) mod m
  = ((7 x A) + 8) mod 26
  = ((7 x 0) + 8) mod 26
  = (0 + 8) mod 26
  = 8 mod 26
  = 8
- CAS1.3 = ((a x PAS1.3) + b) mod m
  = ((7 x K) + 8) mod 26
  = ((7 x 10) + 8) mod 26
  = (70 + 8) mod 26
  = 78 mod 26
  = 0
- CAS1.4 = ((a x PAS1.4) + b) mod m
  = ((7 x M) + 8) mod 26
  = ((7 x 12) + 8) mod 26
  = (84 + 8) mod 26
  = 92 mod 26
  = 14
- CAS2.5 = ((a x PAS2.5) + b) mod m
  = ((7 x A) + 8) mod 26

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 4, October 2023
DOI : https://doi.org/10.33395/sinkron.v8i4.13051
e-ISSN : 2541-2019
p-ISSN : 2541-044X

= ((7 x 0) + 8) mod 26
= (0 + 8) mod 26
= 8 mod 26
= 8

- CAS2.6 = ((a x PAS2.6) + b) mod m
  = ((7 x R) + 8) mod 26
  = ((7 x 17) + 8) mod 26
  = (119 + 8) mod 26
  = 127 mod 26
  = 23
- CAS2.7 = ((a x PAS2.6) + b) mod m
  = ((7 x A) + 8) mod 26
  = ((7 x 0) + 8) mod 26
  = (0 + 8) mod 26
  = 8 mod 26
  = 8
- CAS2.8 = ((a x PAS2.8) + b) mod m
  = ((7 x S) + 8) mod 26
  = ((7 x 18) + 8) mod 26
  = (126 + 8) mod 26
  = 134 mod 26
  = 4

Table 5 Affine Cipher Algorithm Encryption Process

Plain Text	P	$E(P_{AS?.?}) = (a.P_{AS?.?}) + b$	$C = (P_{AS?.?}) \bmod 26$	Chiper Text
I	9	71	19	T
A	0	8	8	J
K	10	78	0	A
M	12	92	14	O
A	0	8	8	J
R	17	127	23	X
A	0	8	8	J
S	18	134	4	E

Merger Section "1" and "2"

Section 1

Section 1

Ciphertext Section is "TJAO" and "JXJE
Ciphertext is "TJAOJXJE"

2. Affine Cipher Algorithm Decryption Process

Table 6 Ciphertext (Plaintext)

Ciphertext	TJAOJXJE
a	7
b	8
m	26
Alphabet Divider	4

- $P_{AS1.1} = a^{-1}(_{AS1.1} - b) \bmod m$
  $= 7^{-1} (T - 8) \bmod 26$

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 4, October 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i4.13051 p-ISSN : 2541-044X

= 15 (19 - 8) mod 26
= 15 (11) mod 26
= 165 mod 26
= 9

- $P_{AS1.2} = a^{-1}(_{AS1.2} - b) \bmod m$
  $= 7^{-1}$ (J - 8) mod 26
  = 15 (8 - 8) mod 26
  = 15 (0) mod 26
  = 0 mod 26
  = 0
- $P_{AS1.3} = a^{-1}(_{AS1.3} - b) \bmod m$
  $= 7^{-1}$ (A - 8) mod 26
  = 15 (0 - 8) mod 26
  = 15 (-8) mod 26
  = -120 + 26 mod 26
  = -94 + 26 mod 26
  = -94 mod 26
  = -94 +26 mod 26
  = -68 mod 26
  = -68 + 26 mod 26
  = -42 mod 26
  = -42 +26 mod 26
  = -16 mod 26
  = -16 + 26 mod 26
  = 10
- $P_{AS1.4} = a^{-1}(_{AS1.4} - b) \bmod m$
  $= 7^{-1}$ (O - 8) mod 26
  = 15 (14 - 8) mod 26
  = 15 (6) mod 26
  = 90 mod 26
  = 12
- $P_{AS2.5} = a^{-1}(_{AS2.6} - b) \bmod m$
  $= 7^{-1}$ (J - 8) mod 26
  = 15 (8 - 8) mod 26
  = 15 (0) mod 26
  = 0 mod 26
  = 0
- $P_{AS2.6} = a^{-1}(_{AS2.6} - b) \bmod m$
  $= 7^{-1}$ (X - 8) mod 26
  = 15 (23 - 8) mod 26
  = 15 (15) mod 26
  = 225 mod 26
  = 17
- $P_{AS2.7} = a^{-1}(_{AS2.7} - b) \bmod m$
  $= 7^{-1}$ (J - 8) mod 26
  = 15 (8 - 8) mod 26
  = 15 (0) mod 26
  = 0 mod 26
  = 0
- $P_{AS2.8} = a^{-1}(_{AS2.8} - b) \bmod m$
  $= 7^{-1}$ (E - 8) mod 26
  = 15 (4 - 8) mod 26
  = 15 (-4) mod 26

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 4, October 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i4.13051 p-ISSN : 2541-044X

= -60 mod 26
= -60 + 26 mod 26
= -34 mod 26
= -34 + 26 mod 26
= -8 mod 26
= -8 + 26 mod 26
= 18

Table 7 Affine Cipher Algorithm Decryption Process

Chiper Text	C	$D(C_{AS?.?}) = a^{-1}(AS?.? - b)$	$P_{AS?.?} = D(C_{AS?.?}) \bmod 26$	Plain Text
T	19	165	9	I
J	8	0	0	A
A	0	-120	10	K
O	14	90	12	M
J	8	0	0	A
X	23	225	17	R
J	8	8	0	A
E	4	-60	18	S

Combine Section "1" and "2"

Section 1

Section 2

Plaintext Section is "IAKM" and "ARAS"
Plaintext Merger is "IAKMARAS" Reverse is "MKAISARA"
Plaintext is "MKAISARA"

Affine Cipher Algorithm Message Cryptographic Program Design

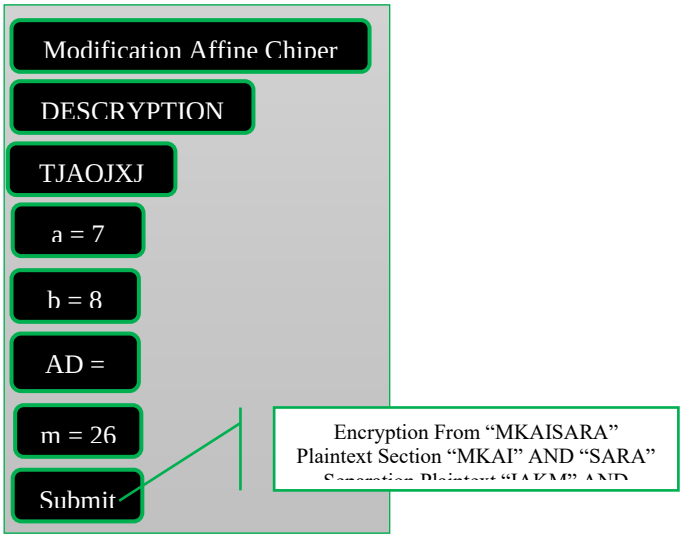


Figure 5 Display of Affine Cipher Algorithm Encryption

*name of corresponding au

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 4, October 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i4.13051 p-ISSN : 2541-044X

Figure 6 Display of Affine Cipher Algorithm Decryption

Calculation of Exclusive-OR (XOR) Combination Encryption and Decryption

Table 8 Plaintext (Message) with Key

Plaintext	MKAISARA
Key	8

Cryptographic Design Exclusive-OR (XOR) Combination Message

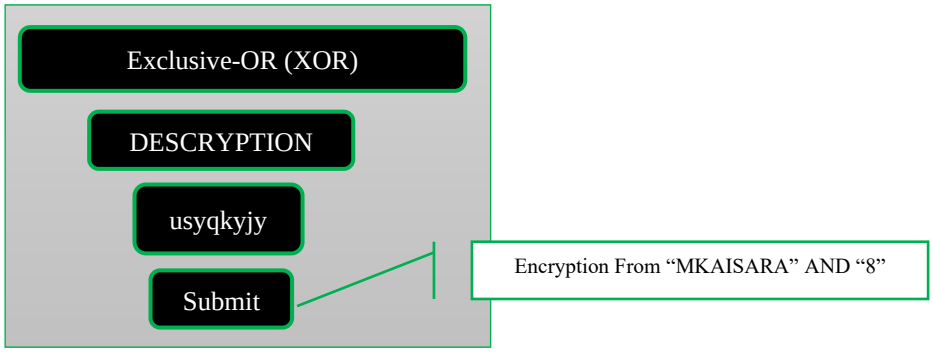


Figure 7 Display Exclusive-OR (XOR) Combination Encryption

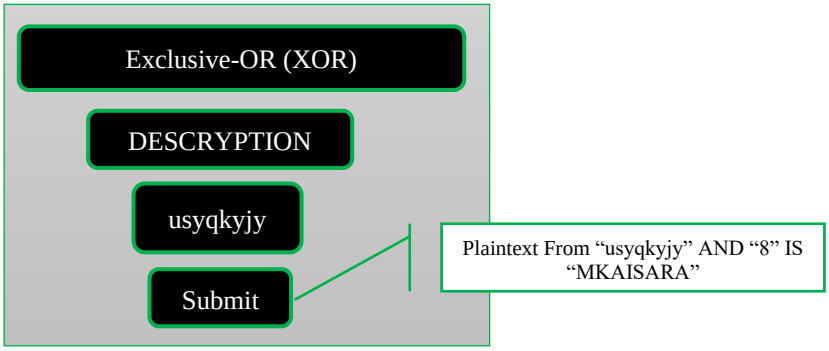


Figure 8 Display Exclusive-OR (XOR) Combination Decryption

DISCUSSIONS

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 4, October 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i4.13051 p-ISSN : 2541-044X

The stages of this research, the process of calculating the Affine Cipher algorithm, are divided into two processes, including process. encryption. And. process. decryption. Which. calculations will be carried out.

The encryption process creates a way to secure a message by changing or replacing the Plaintext P message into a message that cannot be read Ciphertext C through a predetermined formulation. If Plaintext is written in alphabetical form.

a. Look for the value of the Greatest Common Factor (FPB/PBT) from the table above, a = 7, m = 26, the FPB result of (7.26) is equal to 1. The factor of 7 = (1.7) and the factor of 26 = (1, 2, 13, 26). So the greatest common factor of a set of the same value, then the GCF of (7, 26) = 1
b. Plaintext (MKAISARA) is divided into 4 letters in 2 sections
c. Shifting the alphabet from Plaintext to 2 Sections
d. Convert the alphabets from plaintext in the 2 sections above into numerical form
e. Make calculations with the CAS function?.? = ((a x PAS?.?) + b) mod m and adjust the numbers from the Plaintext alphabet.
f. The results of calculating the numbers above are converted into alphabetical form
g. The conversion above shows that the result of Ciphertext Section 1 of Plaintext "MKAI is "TJAO" and the result of Ciphertext Section 2 of Plaintext "SARA" is "JXJE", so that the result of combining 2 Ciphertexts from Plaintext "MKAISARA" is "TJAOJXJE"

This process creates a way to change or replace a message whose meaning cannot be read (Ciphertext) into a message that can be read (Plaintext) through a predetermined formulation. If the Ciphertext results from Plaintext are written in alphabetical form, it is difficult to understand.\

a. Look for the value of the Greatest Common Factor (FPB/PBT) from the table above, a = 7, m = 26, the FPB result of (7.26) is equal to 1. The factor of 7 = (1.7) and the factor of 26 = (1, 2, 13, 26). So the greatest common factor of a set of the same value, then the GCF of (7, 26) = 1
b. Next, how to get the Inverse Modulo results where a.n mod m = 1. In this case, by calculating 7-^{1} x? = ? if mod 26 = 1. The value of n has been found n =15 then: $a\text{-}^{1}$ = a.n mod m = 7-1. 15 mod 26 = 105 mod 26 = 1 So, n = 15 produces Modulo 1, then the Inverse Modulo 7-1 is 15
c. Ciphertext C results from Plaintext (TJAOJXJE) divided into 4 alphabets 2 Sections
d. Convert the letters from the Plaintext above into numbers
e. Calculation of Plaintext where PAS?.? = a-1(AS?? - b) mod m. If the calculation result is negative (-), then add 26 until you get a positive result (+).
f. The results of the calculations above are converted into alphabetical form
g. The conversion above shows that the Plaintext result of part 1 of the Ciphertext "TJAO" is "IAKM" and the Plaintext result of part 2 of the Ciphertext "JXJE" is "ARAS", so that the result of combining the Plaintext of the Ciphertext is "IAKMARAS".
h. Next, reversing the results of the Plaintext alphabet "IAKMARAS" to "MKAISARA", then the Plaintext result of the Ciphertext "TJAOJXJE" is "MKAISARA"

Calculation of Exclusive-OR (XOR) Combination encryption and Decryption

a. This encryption process makes how to XOR Plaintext P with Key K to produce Ciphertext C with the function that can be seen below: C = P⊕K. So from the above table a Plaintext "MKAISARA" with Key "8" will be calculated through the steps and functions that have been determined. F. Then the Ciphertext result from Plaintext "MKAISARA" with Key "8" is "usyqkyjy".
b. This decryption process how to XOR Ciphertext C with Key K produces Plaintext P with a function that can be seen as follows: P = C ⊕ K. The results of Ciphertext C from Plainteks "usyqkyjy" Key "8" are calculated using a predetermined function. Then the Plaintext result of the Ciphertext "usyqkyjy" with Key "8" is "MKAISARA.

*name of corresponding author

CONCLUSION

Through the Affine Cipher algorithm with a key, you can change the unknown Plaintext, so that the secret of the Plaintext is maintained. The Exclusive-OR (XOR) combination by changing each Character in each Plaintext according to the ASCII Code table can shorten the Key encoding process, so that Plaintext remains safe to send. The process of encryption and decryption of the Affine Cipher algorithm is carried out by dividing the Plaintext into 4 alphabets 2 Sections while the Exclusive-OR (XOR) for the encryption and decryption process is only Plaintext. The Affine Cipher Algorithm and the Exclusive-OR (XOR) Combination for a better level of Plaintext security because the Plaintext encryption and decryption process is done twice with different cryptographic algorithms.

REFERENCES

Amalia, R., & Rosyani, P. (2018). Implementasi Algoritma AES dan Algoritma XOR pada Aplikasi Pengaman Teks Berbasis Mobile. *Faktor Exacta*, 369-378.

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi.* Yogyakarta: Penerbit Andi.

Babu, S. A. (2017). Modification Affine Chipers Algorithm For Cryptography Password. *International Journal of Research In Science & Engineering*, 346-351.

Darmayanti, I., Astrida, D. N., & Arius, D. (2018). Penerapan Keamanan Pesan Teks Menggunakan Modifikasi Algoritma Caisar Chiper Kedalam Bentuk Sandi Morse. *Jurnal IT CIDA*, 39-40.

Galih, A. P. (2020). Keamanan Informasi (Information Security) Pada Aplikasi Perpustakaan IPusnas. *AL Maktabah*, 2-3.

Ibisa. (2011). *Keamanan Sistem Informasi.* Yogyakarta.: Penerbit Andi.

Juliadi, Prihandono, B., & Kusumastuti, N. (2013). Kriptografi Klasik Dengan Metode Modifikasi Affine Cipher Yang Diperkuat Dengan Vigenere Cipher. *Buletin Ilmiah Mat. Stat. dan Terapannya (Bimaster)*, 87-92.

Kromodimoeljo, S. (2010). *Teori dan Aplikasi Kriptografi. SPK IT Consulting.* Penerbit SPK IT Consulting.

Munir, R. (2006). *Kriptografi Cetakan Pertama.* Bandung: Penerbit Informatika.

Oktaviana, B., & Siahaan, A. P. (2016). Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 26-29.

Pressman, R. S. (1997). *Software Engineering a Practitioner's Approach, 4th edition.* New York: McGraw-Hill International Editions.

Suhardi. (2016). Aplikasi Kriptografi Data Sederhana Dengan Metode Exclusive-OR (XOR). *Jurnal Teknovasi*, 23.

Sulaiman, O. K., Nasution, K., & Siambaton, M. Z. (2020). Three Pass Protocol untuk Keamanan Kunci. *Jurnal Sains Komputer & Informatika (J-SAKTI)*, 721-727.

Winarno, N. P., & Cahyanto, T. A. (2021, September 27). Penggunaan Karakter Kontrol ASCII Untuk Integrasi Data Pada Hasil EnkripsiAlgoritma Caesar Cipher. *Informatics Journal*, 197-204. Retrieved from https://www.ascii-code.com/: https://www.ascii-code.com/

Wulandari, S. Y. (2020). Cryptography: A Combination of Caesar and Affine Cipher to Conceal the Message. *Proceeding International Conference on Science and Engineering*, 741-744.

*name of corresponding author