Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 2 Issue 1 June, 2025, pp. 11-20
https://idjams.com/index.php/jms/index

Implementation of Combination RSA, Vigenere Cipher, and Permutation Cipher in Digital Communication

M. Fariel Fahriza Tielung[1], Edi Kurniadi[2], Sisilia Sylviani[3,*]

[1, 2, 3] *Universitas Padjadjaran, Jl. Soekarno Km 21 Jatinangor, Kab. Sumedang, 45363, Indonesia*

[*] *Corresponding author: sisilia.sylviani@unpad.ac.id*

Copyright: ©2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution-ShareAlike 4.0 International License-(CC-BY-SA) (https://creativecommons.org/licenses/by-sa/4.0/)

Article Info

Article history:
Received: October 30, 2024
Revised: December 19, 2024
Accepted: December 29, 2024
Available online: June 1, 2025

DOI:
https://doi.org/10.71385/idjams.v2i1.18

Abstract

In the digital era, data security is essential for preventing unwanted access to information. To improve message security, this study intends to apply a mixture of three cryptographic algorithms: RSA, Vigenere cipher, and permutation cipher. The Vigenere and permutation ciphers are used to the message content to add an extra degree of security, while the RSA technique is utilized for asymmetric key encryption. In this system, the Vigenere cipher and permutation cipher, is used to encrypt the message, followed by RSA is used to encrypt the Vigenere process key. According to test results, combining these three techniques strengthens the cryptographic defenses against frequency analysis and brute force assaults by increasing their complexity. Although the combination lengthens the processing time, the resulting security is higher than the application of a single method. This system is expected to be applied to applications that require the protection of sensitive data with a high level of security.

Keywords: Permutation; RSA; Vigenere

I. Introduction

Egyptians used hieroglyphics that is an application of cryptography at around 3000 BCE according to ancient historical records. Around 400 BCE during the golden age of greece, it developed thorugh the Spartans. At that time, the tool used to create hidden messages was called the Scytale. The Scytale was a cylindrical rod combined with 18 letters and a long strip of papyrus. The message could be read by wrapping the strip around the rod. The Chinese and Japanese began recognizing cryptography in the 15th century CE [1].

Cryptography is a method for securing the authenticity of data. In the process of cryptography require 2 steps which are encryption and decryption [2]. Encryption process is supposed to change the original data into encoded data which makes the data highly confidential so that unauthorized parties don't know the original data since the data already encrypted. Meanwhile, decryption process is supposed to change encoded data into original data.The original and the encoded data is respectively called plaintext and ciphertext. By keeping unauthorized people from accessing data, cryptography serves to safeguard the secrecy of that data.Those who develop cryptographic algorithms are known as cryptographers [3].

The decryption and encryption process are two crucial steps in the field of cryptography. Encryption process changes the original data using specific algorithms into an unkown format. If the encryption process takes more time, then the encoded data that already been transmitted is more highly confidential than the process that takes not much time. In contrast, the decryption process returns previously altered data or information to its original form once it has been transformed into an unknown form. Data security can be implemented using a variety of cryptographic algorithms.

Cryptography is divided into classical cryptography and modern cryptography based on its historical context. Classical cryptography can be completed by hand with simple computation. Meanwhile,

modern cryptography needs a complicated computation that will be take more time to solve by hand. Modern cryptography usually compute by computer assistance [4].

There is also two types of cryptographic algorith which are the symmetric and the asymmetric algorithm. The difference between symmetric and asymmetric is the key. Symmetric algorithm use public key for encryption and private key for decryption. Meanwhile, Asymmetric algorithms use different keys for the encryption and the decryption. Both of it are inversely proportional, which uses the same key for the encryption and decryption process. [5]. The weaknesses of the two types of cryptography can be overcome by combine those type of cryptography which is called a hybrid cyptosystem coding method. A hybrid cryptosystem is a method that combines multiple ciphers to benefit from each one's unique features. It uses two different key called public and symmtric key. In a hybrid cryptosystem, files are secured using a symmetric algorithm and symmetric keys are secured using an asymmetric algorithm [6].

Cryptography has evolved into digital era. For example, chatGPT is already using cryptography algorithm to its program [7]. Cryptography has a lot of type since it was discovered. Some of its type that will be discussed are the Permutation Cipher, the Vigenère Cipher, and the RSA Algorithm. In the permutation cipher, the order of characters is swapped according to specific rules without altering the characters themselves [8]. This swapped show how complex the process, making it challenging for recipient to compute the decryption process that will result the original content without knowledge of the specific permutation key [9]. Meanwhile, the Vigenère cipher requires a key to transform a character into a new one, using the key for both the encryption and decryption processes [10]. Vigenere is one of the classic cryptographic algorithms introduced in the 16th century or roughly in 1986 [11]. Then, RSA algorithm is used to change a character into a numerical code using 2 types of key which is public key for the encryption process and private key for the decryption process [12]. The RSA algorithm was found in 1977 by three people which is Ron Rivest, Adi Shamir and Len Adleman from the Massachusetts Institute of Technology. The letters RSA is from the initials of their names R, S, and A. The security of the RSA algorithm based on the difficulty of factoring large numbers into prime factors. Factoring is done to obtain a private key. As long as the factoring of large numbers into prime factors has not been found, then the security of the RSA algorithm is guaranteed.

So that, we can conclude that study is needed by combining multiple types of cryptography. For example, combining vigenere cipher, which is a symmetric key with RSA, which is an asymmetric key with hybrid cryptosystem method. Thus, it is envisaged that combining the two forms of cryptography will produce a high level of security while enabling quick encryption and decoding. A similar approach has been applied in previous studies by combining the Vigenere cipher and RSA algorithm [3]. However, message security can still be enhanced by incorporating additional algorithms into the encryption and decryption process.

Therefore, the goal of this study is to create and assess an encryption scheme that combines the permutation cipher, the Vigenère cipher, and the RSA algorithm. It is anticipated that the suggested method will offer extra security layers for data protection during digital communication by leveraging the advantages of each algorithm. The study will make significant contributions to the domains of data security and cryptography by thoroughly examining the efficacy and efficiency of this strategy.

II. Materials and Method

In this study, the encryption and decryption process will be carried out involving the Vigenere cipher, permutation cipher, and RSA algorithm. The method for the encryption process is as follows:

1. Encrypt the plaintext with the vigenere key resulting in ciphertext-1.
2. Encrypt the vigenere key with RSA Algorithm, generating ciphertext-2
3. Encrypt ciphertext-1 with permutation to produce ciphertext-3.
4. Ciphertext-2 and ciphertext-3 are given to the recipient of the message.

Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 2 Issue 1 June, 2025, pp. 11-20
https://idjams.com/index.php/jms/index

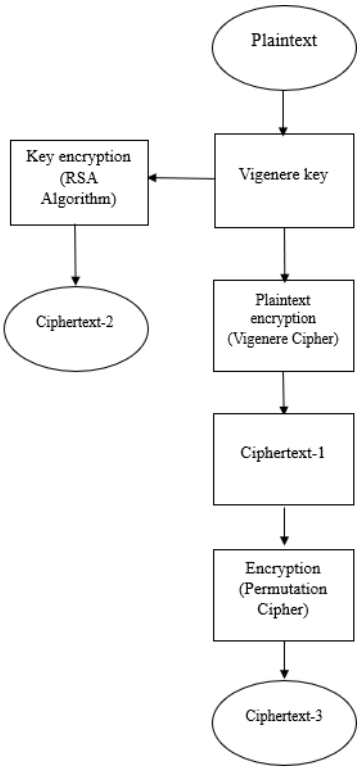


Figure 1. Encryption Process

The method for the decryption process is as follows:

1. Ciphertext-2 and Ciphertext-3 are given.
2. Decrypt ciphertext-2 using RSA Algorithm. This produces the original vigenere key.
3. Decrypt ciphertext-3 with permutation to produce Ciphertext-1.
4. Decrypt ciphertext-1 using vigenere cipher with the original key to produce plaintext.

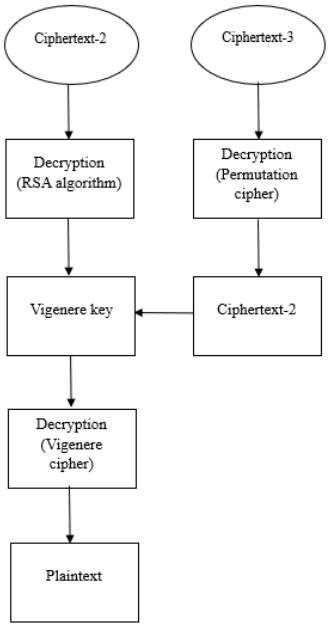


Figure 2. Decryption Process

Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 2 Issue 1 June, 2025, pp. 11-20
https://idjams.com/index.php/jms/index

In general, the encryption and decryption processes carried out only go through 4 stages. Each stage has more detailed steps that will be explained in this chapter.

A. RSA Algorithm (Rivest-Shamir-Adleman)

RSA is one of cryptographic technique to protect data. RSA is used for encryption, key exchange (private and public key), and digital signature. RSA algorithm is very commonly used in data encryption and digital signature applications [13]. The essence of RSA is to generate two keys, namely the public key and the private key. The public key will be shared to encrypt information. Messages encrypted with the public key can only be deciphered with the private key.

1. Generate public and private keys

   There are several steps to generate a public and private key. Those steps are as follows [12]:

   a. Randomly select two prime numbers p and q. To make it difficult to solve, p and q must be large prime numbers.
   b. Compute a number $n = pq$. Where n is computed as the modulo for both the public and private keys.
   c. The Euler's function $\phi()$ should be computed as, $\phi(n) = (p-1)(q-1)$, where ϕ function is the integer number.
   d. Choose a new number, say e that satisfies $1 < e < \phi(n)$ and the $\gcd(e, \phi(n)) = 1$. e will be published as a public key.
   e. Find the value of d so that $de \equiv 1(mod\ r)$ or in other words d is the inverse of $e\ mod\ r$. d will be saved as a private key and not shared.

   In the following, we offer an applied example of RSA encryption/decryption [14]. The parameters used here are small to clarify the procedure.

   - Enter the prime integer for $p = 59$ and $q = 41$.
   - Compute $n = pq = 59 * 41 = 2419$.
   - Compute the function $\phi(n) = (59-1)(41-1) = 2320$
   - Compute the public key for exponent e such that $1 < e < \phi(n)$ and so that greatest common divisor $\gcd(e, \phi(n)) = 1$. $e = 1381$.
   - Compute the private key d as
   -

$$de \equiv 1(mod\ \phi(n))$$
$$d * 1381 \equiv 1(mod\ 2320)$$
$$d = 1181$$

   To prove that public and private keys whether to satisfy the above relation:

$$de\ (mod\ \phi(n)) = 1181 * 1381\ (mod\ 2320)$$
$$= 1630961\ (mod\ 2320)$$
$$= 1$$

   So, the public and private keys respectively are (1381, 2419) and (1181, 2419).

2. Message Encryption

   Suppose the message is an integer m that $m < n$, so the way to encrypt m is to raise e (public key) to the power of m. Let say c is the ciphertext so

$$c = m^e (mod\ n).$$

   c can be visible to the public but without the private key the real information of this message cannot be obtained.

3. Message Decryption

   To decrypt the message is to raise d (private key) to the power of c (ciphertext). For example, it's f so

Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 2 Issue 1 June, 2025, pp. 11-20
https://idjams.com/index.php/jms/index

$$f = c^d (mod\ n)$$
$$f = m^{ed} (mod\ n).$$

Note that f must be equal to m.

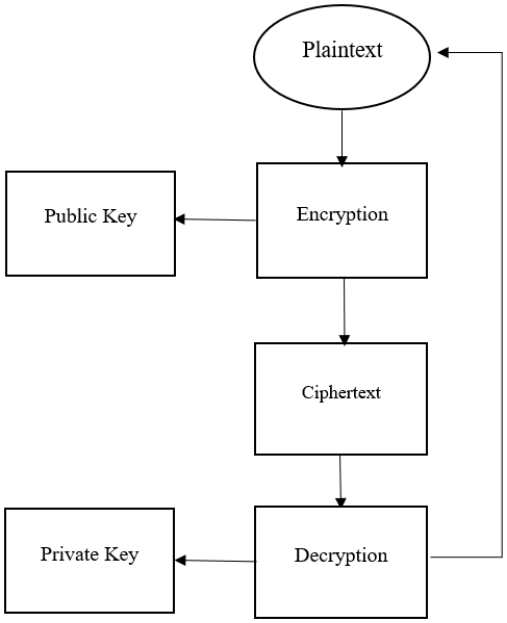


Figure 3. RSA Algorithm Process

B. Vigenere Cipher

Using a matrix of 26 Caesar cipher shifts, the Vigenere cipher is a polyalphabetic substitution cipher. It is composed of a set of Caesar cipher substitution rules that are monoalphabetic and with shifts ranging from 0 to 25. Using the Vigenere square (sometimes called the Vigenere tableau), Vigenere encryption is implemented by appending each plaintext character's index to the password character's index. [15].

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 4. Vigenere Square Table

Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 2 Issue 1 June, 2025, pp. 11-20
https://idjams.com/index.php/jms/index

The encryption and decryption process of the vigenere cipher can also be represented mathematically as:

$$C_i = E(P_i + K_i)(mod\ 26)$$
$$P_i = D(C_i - K_i)(mod\ 26),$$

where C, P, K, E, and D respectively represent ciphertext, Plaintext, Key, Encryption function, and Decryption function. If for example, we have a plaintext "DEPARTEMEN", and a keyword "DEPMAT". The vigenere cipher is done by aligning the keyword below the plaintext.

Plaintext: DEPARTEMEN
Keyword: DEPMATDEPM

$$C_1 = E(P_1 + K_1) = 3 + 3\ (mod\ 26) = 6 \rightarrow G$$
$$C_2 = E(P_2 + K_2) = 4 + 4\ (mod\ 26) = 8 \rightarrow I$$
$$C_3 = E(P_3 + K_3) = 15 + 15\ (mod\ 26) = 4 \rightarrow E$$
$$C_4 = E(P_4 + K_4) = 0 + 12\ (mod\ 26) = 12 \rightarrow M$$
$$C_5 = E(P_5 + K_5) = 17 + 0\ (mod\ 26) = 17 \rightarrow R$$
$$C_6 = E(P_6 + K_6) = 19 + 19\ (mod\ 26) = 12 \rightarrow M$$
$$C_7 = E(P_7 + K_7) = 4 + 3\ (mod\ 26) = 7 \rightarrow H$$
$$C_8 = E(P_8 + K_8) = 12 + 4\ (mod\ 26) = 16 \rightarrow Q$$
$$C_9 = E(P_9 + K_9) = 4 + 15\ (mod\ 26) = 19 \rightarrow T$$
$$C_{10} = E(P_{10} + K_{10}) = 13 + 12\ (mod\ 26) = 25 \rightarrow Z$$

So, we can conlude that the ciphertext is: "GIEMRMHQTZ".

Further we wil decrypt a ciphertext "GIEMRMHQTZ". We are still using the same keyword "DEPMAT". The vigenere cipher is done by aligning the keyword below the ciphertext.

Ciphertext: GIEMRMHQTZ
Keyword: DEPMATDEPM

Using the same method for the decryption, we will have the plaintext: "DEPARTEMEN".

C. Permutation Cipher

Permutation cipher is a technique to move or rotate each character in the text with certain models. The principle of transposition is opposite to substitution where the position of the character remains only replaced by another character, while transposition itself does not replace the character but changes its position [16].

For example, let's assume a block size of 5 and the permutation pattern is (3 1 4 5 2). We will encrypt a plaintext "DEPARTEMEN". Since the block size is 5, we divide the plaintext blocks of size 5.

Plaintext: DEPAR TEMEN.
Position of plaintext: 12345 12345.
Permutation: 31452 31452.
Ciphertext: ERDPA ENTME.
From above text we got ciphertext "ERDPAENTME".

Further, we will decrypt a ciphertext "ERDPAENTME". Firstly, we have to find the inverse permutation. If the permutation pattern is (3 1 4 5 2) then the inverse is (2 5 1 3 4). Next, we divide the ciphertext blocks of size 5.

Ciphertext: ERDPA ENTME.
Position of ciphertext: 12345 12345.
Inverse permutation: 25134 25134.
Plaintext: DEPAR TEMEN.
From above text, the plaintext becomes "DEPARTEMEN".

Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 2 Issue 1 June, 2025, pp. 11-20
https://idjams.com/index.php/jms/index

D. American Standard Code for Information Interchange (ASCII)

ASCII is a table of printable and non-printable characters [17]. ASCII codes were standardized in 1982 as a source of storing and transmitting data like English texts [18]. ASCII is an international standard for letter and symbol codes like Hex and Unicode, but ASCII is more universal, for example 124 is for the character "|" [19]. It is always used by computers and other communication devices to indicate text. The ASCII code actually has a 7-bit composition of binary numbers. However, ASCII is stored as an 8-bit cipher by adding a 0 as the highest significant bit. The number of ASCII characters is 255, where characters of order 0 to 127 are characters for text manipulation, ASCII characters of order 128 to 255 are characters for graphic manipulation. ASCII has control characters that are divided into 5 groups according to consecutive usage, namely Logical Communication, Device Control, Information Separator, Code Extension, and Physical Communication [20]. These characters will be integrated with the key that will be used in the encryption and decryption process of the Vigenere cipher.

Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
32	20	040		Space	64	40	100	@	@	96	60	140	`	`
33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Figure 5. ASCII Table

III. Results and Discussion

Suppose given a message "CRYPTOGRAPHY" and the key for Vigenere Cipher is "MATH" then, the steps that will be carried out according to the method determined in this article will be explained in this chapter.

A. Encryption

1. Encrypt the plaintext with vigenere key
   First, convert the plaintext and keyword into numbers by using the mapping where $A = 0, B = 1, \dots, Z = 25$. Based on the formula of vigenere key, we have:

$$C_1 = E(P_1 + K_1) = 2 + 12 \ (mod\ 26) = 14 \rightarrow O$$
$$C_2 = E(P_2 + K_2) = 17 + 0 \ (mod\ 26) = 17 \rightarrow R$$
$$C_3 = E(P_3 + K_3) = 24 + 19 \ (mod\ 26) = 17 \rightarrow R$$
$$C_4 = E(P_4 + K_4) = 15 + 7 \ (mod\ 26) = 22 \rightarrow W$$
$$C_5 = E(P_5 + K_5) = 19 + 12 \ (mod\ 26) = 5 \rightarrow F$$

Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 2 Issue 1 June, 2025, pp. 11-20
https://idjams.com/index.php/jms/index

$$C_6 = E(P_6 + K_6) = 14 + 0\ (mod\ 26) = 14 \rightarrow O$$
$$C_7 = E(P_7 + K_7) = 6 + 19\ (mod\ 26) = 25 \rightarrow Z$$
$$C_8 = E(P_8 + K_8) = 17 + 7\ (mod\ 26) = 24 \rightarrow Y$$
$$C_9 = E(P_9 + K_9) = 0 + 12\ (mod\ 26) = 12 \rightarrow M$$
$$C_{10} = E(P_{10} + K_{10}) = 15 + 0\ (mod\ 26) = 15 \rightarrow P$$
$$C_{11} = E(P_{11} + K_{11}) = 7 + 19\ (mod\ 26) = 0 \rightarrow A$$
$$C_{12} = E(P_{12} + K_{12}) = 24 + 7\ (mod\ 26) = 5 \rightarrow F$$

Thus, **ciphertext-1** is "ORRWFOZYMPAF"

2. Encrypt the vigenere key with RSA Algorithm

Each character of "MATH" will be converted to its ASCII code where $M = 77, A = 65, T = 84, H = 72$. For prime numbers $p = 17$ and $q = 11$ we have

$$n = 17 * 11 = 187$$
$$\phi(n) = (17 - 1)(11 - 1) = 160$$

We choose $e = 7$, which is relatively prime to 160. Based on the encryption formula for RSA, we get:

$$C_1 = 77^7\ (mod\ 187) = 114$$
$$C_2 = 65^7\ (mod\ 187) = 92$$
$$C_3 = 84^7\ (mod\ 187) = 25$$
$$C_4 = 72^7\ (mod\ 187) = 54$$

So, **ciphertext-2** is "114 92 25 54"

3. Encrypt the ciphertext-1 using permutation cipher

Let's assume a block size of 6 with permutation pattern is (4 3 6 5 2 1). We will encrypt a plaintext "ORRWFOZYMPAF". Since the block size is 6, the plaintext will be divided into blocks of size 6.

Plaintext: ORRWFO ZYMPAF
Permutation Pattern: 436521 436521
The resultant plaintext from the above text becomes "WORFOR PMAFYZ".
So, **ciphertext-3** is "WORFORPMAFYZ"

The encryption process is ended and e, ciphertext-2, permutation pattern, and ciphertext-3 are given to the public. Next, the decryption process is carried out according to the method.

Based on the encryption process, the steps required are lengthy and complex. This method uses three approaches, which if used separately would be easy, but would be difficult when combined. Therefore, classical cryptography is still useful in the modern era if used in conjunction with other cryptography to form multiple layers that are difficult to crack.

Therefore, this method has several advantages. First, it takes a long time to decrypt the ciphertext if done manually. Secondly, it is easy for the message sender to perform encryption because the type of cryptography used is classical cryptography. Third, the level of confidentiality of the message increases due to the layered process. However, this method still has some drawbacks. First, it is quite easy to crack if using a program. Secondly, the sender is vulnerable to producing a wrong ciphertext due to the layered process.

The algorithm in this study relies solely on the ASCII table, requiring both the sender and receiver to understand its contents. This could become an issue if the receiver is unfamiliar with the table or lacks access to it. Therefore, the algorithm can be expanded to utilize other types of codes beyond the ASCII table.

IV. Conclusion

The method of combining several types of basic cryptography is one way to increase the confidentiality of a message. Although it makes the encryption and decryption process layered and prone to errors in the process. However, if done carefully, it will produce a strong ciphertext that is difficult to crack.

References

[1] N. A. Nanda, S. M. S. Silalahi, D. Fatricia Nasution, M. Sari, and I. Gunawan, "Cryptography and Its Application in Data Security Systems," *J. Media Inform.*, vol. 4, no. 2, pp. 90–93, 2023, DOI: 10.55338/jumin.v4i2.428.

[2] D. Rachmawati, A. Sharif, Jaysilen, and M. A. Budiman, "Hybrid Cryptosystem Using Tiny Encryption Algorithm and LUC Algorithm," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 300, no. 1, 2018, DOI: 10.1088/1757-899X/300/1/012042.

[3] R. Romindo and J. Jamaludin, "Decision Support System Using ANP Method for Selecting the Best Online Store at Ganesha Polytechnic," *REMIK (Riset dan E-Jurnal Manaj. Inform. Komputer)*, vol. 4, no. 1, p. 83, 2019, DOI: 10.33395/remik.v4i1.10231.

[4] B. S. Hasigian, "The Role of Cryptography as Information System Security in Small and Medium Enterprises," *J. War.*, vol. 53, no. 9, p. 2, 2017.

[5] M. O. Safira and I. K. Ari Mogi, "Design of Hybrid Cryptography with Vigenere Cipher and RSA Algorithm on IOT Data Security," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 8, no. 4, p. 475, 2020, DOI: 10.24843/jlk.2020.v08.i04.p14.

[6] Jamaludin and Romindo, "Implementation of Combination Vigenere Cipher and RSA in Hybrid Cryptosystem for Text Security," *Int. J. Inf. Syst. Technol. Akreditasi*, vol. 4, no. 1, pp. 471–481, 2020.

[7] H. Kwon, M. Sim, G. Song, M. Lee, and H. Seo, "Novel approach to cryptography implementation using ChatGPT," *Cryptol. ePrint Arch.*, 2023, [Online]. Available: https://eprint.iacr.org/2023/606%0Ahttps://eprint.iacr.org/2023/606.pdf

[8] A. Deepshika, J. Kannan, M. Mahalakshmi, and K. Kaleeswari, "Mathematics and Its Applications Cryptographic Algorithm Based on Permutation Ciphers," vol. 11, no. 4, pp. 1–7, 2023.

[9] M. N. John, U. Otobong, and G. A. Musa, "Symmetric Bilinear Cryptography on Elliptic Curve and lie algebra," GPH-Int. J. Math., vol. 6, no. 10, pp. 1-10, 2023, DOI: 10.5281/zenodo.10209885.

[10] E. Bahtiar and A. Nilogiri, "Combination of Vigenere Cipher and Permutation Cipher with Dynamic Key Modification in Text-Based Cryptography," *Seminar Hasil Tugas Akhir*, pp. 1–9, 2015.

[11] N. B. Putra, B. C. Andika, A. D. P. Bagas, and M. Ridwan, "Implementation of Vigenere Cipher in Encrypting Messages," *JOCITIS-J. Sci. Infom. Robot.*, vol. 1, no. 1, pp. 42–50, 2023.

[12] R. I. Parama, "Application of Number Theory in Cryptography for Information Technology Security in the Form of RSA Algorithm," *Makal. IF2120 Mat. Disk.*, 2016.

[13] S. A. Sholikhatin, A. P. Kuncoro, A. L. Munawaroh, and G. A. Setiawan, "Comparative Study of RSA Asymmetric Algorithm and AES Algorithm for Data Security," *Edu Komputika J.*, vol. 9, no. 1, pp. 60–67, 2022, DOI: 10.15294/edukomputika.v9i1.57389.

[14] T. S. Obaid, "Study A Public Key in RSA Algorithm," *Eur. J. Eng. Res. Sci.*, vol. 5, no. 4, pp. 395–398, 2020, DOI: 10.24018/ejers.2020.5.4.1843.

[15] A.-A. Mohammed and A. Olaniyan, "Vigenere Cipher: Trends, Review and Possible Modifications," *Int. J. Comput. Appl.*, vol. 135, no. 11, pp. 46–50, 2016, DOI: 10.5120/ijca2016908549.

[16] R. Feraldi, A. Khairuna, M. A. Hasan, R. Rezky, and H. Ramadhan, "Combination of Caesar Cipher and Permutation Cipher Cryptographic Algorithms for Text Messages Using Python,"

Riau J. Comput. Sci., vol. 7, no. 1, pp. 76–86, 2021.

[17] N. P. S. Winarno and T. A. Cahyanto, "Use of ASCII Control Characters for Data Integration in Caesar Cipher Algorithm Encryption Results," *INFORMAL- Inform. J.*, vol. 6, no. 3, p. 197, 2021, DOI: 10.19184/isj.v6i3.21091.

[18] A. Sultan, Y. Lin, and A. Mushtaq, "A Survey Paper on ASCII-Based Cryptographic Techniques," *Int. J. Innov. Sci. Technol.*, vol. 4, no. 4, pp. 1087–1098, 2022, DOI: 10.33411/ijist/2022040411.

[19] A. Tantoni and M. T. A. Zaen, "Implementasi Double Caesar Cipher Menggunakan Ascii," *J. Inform. Rekayasa Elektron.*, vol. 1, no. 2, p. 24, 2018, DOI: 10.36595/jire.v1i2.56.

[20] Mira, H. D. Purnomo, and I. Sembiring, "Caesar Cipher Algorithm Modification on ASCII Code to Improve Text Message Security," *J. Inf. Technol.*, vol. 2, no. 1, pp. 16–22, 2022, DOI: 10.46229/jifotech.v2i1.293.