CAUCHY –Jurnal Matematika Murni dan Aplikasi
Volume 5(4) (2019), Pages 181-185
p-ISSN: 2086-0382; e-ISSN: 2477-3344

Application of Rectangular Matrices: Affine Cipher Using Asymmetric Keys

Maxrizal[1], Baiq Desy Aniska Prayanti[2]

[1]STMIK Atma Luhur Pangkalpinang
[2]Universitas Bangka Belitung

Email: maxrizal@atmaluhur.c.id, baiqdesyaniska@gmail.com

ABSTRACT

In cryptography, we know the symmetric key algorithms and asymmetric key algorithms. We know that the asymmetric key algorithm is more secure than the symmetric key algorithm. Affine Cipher uses a symmetric key algorithm. In this paper, we introduce the Affine Cipher using asymmetric keys. Asymmetrical keys are formed from rectangular matrices.

Keywords: cryptography, symmetric key algorithms, asymmetric key algorithms, Affine Cipher using asymmetric keys, rectangular matrices

INTRODUCTION

Nowadays, cryptography becomes the main option for securing messaging or data over a communications network. In cryptography, the sender encrypts the message (plaintext) into ciphertext. Furthermore, the receiver describes ciphertext into plaintext. Encryption and decryption in cryptography require key algorithm. If the encryption and decryption use a similar key, the algorithm is called symmetric key algorithms. If the encryption and decryption use a different key, it is called asymmetric key algorithm. The asymmetric key algorithm is also known as modern cryptographic systems. One example of an asymmetric key algorithm is RSA [1,2,3,4].

Affine Cipher is one of the cryptographic algorithms that uses a symmetric key algorithm. It including substitution cipher type. In Affine Cipher [5,6], each plaintext encrypted as $C_i = (aP_i + b) \bmod M$ and described as a $P_i = a^{-1}(C_i - b) \bmod M$, with a and b are integers as private keys.

Based on the above facts, in this study, we will modify the Affine Cipher using asymmetric keys. We will generate a private key and a public key on Affine Cipher. Asymmetrical keys are formed from rectangular matrices.

METHODS

This research is a study of literature research. Some properties of asymmetric keys are obtained from [1,2,3,4]. Furthermore, the properties of Affine Cipher is derived from [5,6].

Submitted: September 26, 2017 Reviewed: October 09, 2017 Accepted: May 31, 2019
DOI: http://dx.doi.org/10.18860/ca.v5i4.4408

RESULTS AND DISCUSSION

Affine Cipher and Affine Cipher Using Asymmetric Keys

In the Affine Cipher [5,6], applied encryption $C_i = (aP_i + b) \bmod M$ and descriptions $P_i = a^{-1}(C_i - b) \bmod M$, where a must be invertible on $\bmod M$ and b is an arbitrary integer. The sender and receiver must save the private key a and b for encryption and description. In this study, we formed

$$C^*_{n\times 1} = (Y_{n\times 1}P_{1\times 1} + B_{n\times 1}) \bmod M$$

$$X_{1\times n}C^*_{n\times 1} = X_{1\times n}(Y_{n\times 1}P_{1\times 1} + B_{n\times 1}) \bmod M$$

$$X_{1\times n}C^*_{n\times 1} = (X_{1\times n}Y_{n\times 1}P_{1\times 1} + X_{1\times n}B_{n\times 1}) \bmod M$$

$$(X_{1\times n}C^*_{n\times 1} - X_{1\times n}B_{n\times 1}) \bmod M = (X_{1\times n}Y_{n\times 1}P_{1\times 1})$$

$$P_{1\times 1} = (X_{1\times n}Y_{n\times 1})^{-1}(X_{1\times n}C^*_{n\times 1} - X_{1\times n}B_{n\times 1}) \bmod M \ldots\ldots\ldots (1)$$

If we suppose $X_{1\times n}Y_{n\times 1} = a$, $X_{1\times n}C^*_{n\times 1} = C$ and $X_{1\times n}B_{n\times 1} = b$, we have the similar decryption as Affine Cipher. Next, we get encryption $C^*_{n\times 1} = (Y_{n\times 1}P_{1\times 1} + B_{n\times 1}) \bmod M$, with the public key $(Y_{n\times 1}, B_{n\times 1})$ and description $P_{1\times 1} = (X_{1\times n}Y_{n\times 1})^{-1}(X_{1\times n}C^*_{n\times 1} - X_{1\times n}B_{n\times 1}) \bmod M$, with the private key$(X_{1\times n})$. Furthermore, encryption and description above, we call as Affine Cipher Using Asymmetric Keys.

Key Generating Algorithm on Affine Cipher Using Asymmetric Keys

Steps to generate of keys algorithm:

- Choose $X_{1\times n}$.
- Choose$Y_{n\times 1}$.
- Calculate $X_{1\times n}Y_{n\times 1}$. If the matrix $X_{1\times n}Y_{n\times 1}$ has no inverse over $\bmod M$, we repeat steps 1) and 2). If matrix $(X_{1\times n}Y_{n\times 1})^{-1}$ exists on $\bmod M$, we have one of a public key $Y_{n\times 1}$ and private key $X_{1\times n}$.
- Choose an arbitrary matrix $B_{n\times 1}$.

So, we get the public key $(Y_{n\times 1}, B_{n\times 1})$ and a private key $(X_{1\times n})$.

Security Analysis on Affine Cipher and Affine Cipher Using Asymmetric Keys

On Affine Cipher Using Asymmetric Key, apply encryption $C^*_{n\times 1} = (Y_{n\times 1}P_{1\times 1} + B_{n\times 1}) \bmod M$, with the public key$(Y_{n\times 1}, B_{n\times 1})$. If the sender sent the message, the attacker (unauthorized recipients) will get a public key $(Y_{n\times 1}, B_{n\times 1})$ and ciphertext $C^*_{n\times 1}$. However, the attacker would be difficult to describe the ciphertext, because the matrix $(Y_{n\times 1})^{-1}$ does not exist.

$$C^*_{n\times 1} = (Y_{n\times 1}P_{1\times 1} + B_{n\times 1}) \bmod M$$

$$(C^*_{n\times 1} - B_{n\times 1}) \bmod M = (Y_{n\times 1}P_{1\times 1})$$

$$P_{1\times 1} = (Y_{n\times 1})^{-1}(C^*_{n\times 1} - B_{n\times 1}) \bmod M \ldots\ldots (2)$$

It means that the plaintext remains safe. Furthermore, we show a comparison Affine Cipher and Affine Cipher Using Asymmetric Keys.

Affine Cipher	Affine Cipher Using Asymmetric Keys
• Symmetric key. • The key is an integer. • Elements on the plaintext and ciphertext one-to-one correspondence (bijective function).	• Asymmetric keys. • The key is matrix pair. • Elements on the plaintext and ciphertext do not one-to-one correspondence (it is not bijective function).

Example

Nisca will send a message to Max. Max generate the public key and private key.

Key generating algorithm:

- Max chooses $X = \begin{bmatrix} 1 & 2 & 1 \end{bmatrix}$.
- He chooses $Y = \begin{bmatrix} 3 \\ 1 \\ 4 \end{bmatrix}$.
- He calculates $XY = \begin{bmatrix} 1 & 2 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \\ 4 \end{bmatrix} = 9$. Note that $9^{-1} \bmod 26 = 3$.
- He chooses an arbitrary matrix $B = \begin{bmatrix} 2 \\ 1 \\ 5 \end{bmatrix}$.
- Max gets the public key $\left(\begin{bmatrix} 3 \\ 1 \\ 4 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 5 \end{bmatrix} \right)$ and private key $\left(\begin{bmatrix} 1 & 2 & 1 \end{bmatrix} \right)$.

Encryption:

Niska received a public key $\left(\begin{bmatrix} 3 \\ 1 \\ 4 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 5 \end{bmatrix} \right)$ from Max. She will send **"USE"** to Max. She converts **"USE"** to 21-19-5. She encrypts $C^*_{n\times 1} = \left(Y_{n\times 1} P_{1\times 1} + B_{n\times 1} \right) \bmod M$. She gets

$$C^*_1 = \left(\begin{bmatrix} 3 \\ 1 \\ 4 \end{bmatrix} \begin{bmatrix} 21 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \\ 5 \end{bmatrix} \right) \bmod 26 = \begin{bmatrix} 13 \\ 22 \\ 11 \end{bmatrix}$$

$$C^*_2 = \left(\begin{bmatrix} 3 \\ 1 \\ 4 \end{bmatrix} \begin{bmatrix} 19 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \\ 5 \end{bmatrix} \right) \bmod 26 = \begin{bmatrix} 7 \\ 20 \\ 3 \end{bmatrix}$$

$$C^*_3 = \left(\begin{bmatrix} 3 \\ 1 \\ 4 \end{bmatrix} \begin{bmatrix} 5 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \\ 5 \end{bmatrix} \right) \bmod 26 = \begin{bmatrix} 17 \\ 6 \\ 25 \end{bmatrix}$$

Niska gets 13-22-11-7-20-3-17-6-25. She converts and sends **"MVKGTCQFY"** to Max.

Description:

Max received **"MVKGTCQFY"** from Nisca**.** He converts 13-22-11-7-20-3-17-6-25. Max knows the public key $\left(\begin{bmatrix}3\\1\\4\end{bmatrix},\begin{bmatrix}2\\1\\5\end{bmatrix}\right)$ and saves the private key $\left(\begin{bmatrix}1 & 2 & 1\end{bmatrix}\right)$. He describes $P_{1\times1}=\left(X_{1\times n}Y_{n\times1}\right)^{-1}\left(X_{1\times n}C^{*}_{n\times1}-X_{1\times n}B_{n\times1}\right)\bmod M$. He calculates $X_{1\times n}Y_{n\times1}=\begin{bmatrix}1 & 2 & 1\end{bmatrix}\begin{bmatrix}3\\1\\4\end{bmatrix}=9$. He gets $\left(X_{1\times n}Y_{n\times1}\right)^{-1}=3$. Next, he gets

$$P_{1\times1}=3\left(\begin{bmatrix}1 & 2 & 1\end{bmatrix}\begin{bmatrix}13\\22\\11\end{bmatrix}-\begin{bmatrix}1 & 2 & 1\end{bmatrix}\begin{bmatrix}2\\1\\5\end{bmatrix}\right)\bmod 26=21$$

$$P_{1\times1}=3\left(\begin{bmatrix}1 & 2 & 1\end{bmatrix}\begin{bmatrix}7\\20\\3\end{bmatrix}-\begin{bmatrix}1 & 2 & 1\end{bmatrix}\begin{bmatrix}2\\1\\5\end{bmatrix}\right)\bmod 26=19$$

$$P_{1\times1}=3\left(\begin{bmatrix}1 & 2 & 1\end{bmatrix}\begin{bmatrix}17\\6\\25\end{bmatrix}-\begin{bmatrix}1 & 2 & 1\end{bmatrix}\begin{bmatrix}2\\1\\5\end{bmatrix}\right)\bmod 26=5$$

Max gets 21-19-5. He converts **"USE".**

CONCLUSION

From this study, we obtained several conclusions, including:

- We can form Affine Cipher Using Asymmetric Keys.
- Affine Cipher Using Asymmetric Keys more secure than Affine Cipher.

.

ACKNOWLEDGMENTS

The research was done well because there is good support from STMIK Atma Luhur Pangkalpinang. Therefore, the author's thank you for the support of funds and policies that are in STMIK Atma Luhur Pangkalpinang so this research can be done and completed.

REFERENCES

[1] Khairnar, D.B., and Sandeep, K., " Secure RSA: Pair-Wise Key Distribution Using Modified RSA Algorithm", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol.6, issue. 4, pp. 383-387, 2016.

[2] Puneeth, M., Farha, J. S., Sandhya, N., and Yamini, M., "RSA and Modified RSA Algorithm Using C Programming", *International Journal of Advanced Engineering Research and Science*, vol.2, issue. 2, pp. 15-20, 2015.

[3] Hussain, A, K., "A Modified RSA Algorithm for Security Enhancement and Redundant Messages Elimination Using K-Nearest Neighbor", *International Journal of Innovative Science, Engineering, and Technology*, vol.2, issue. 1, pp.159-163, 2015.

[4] Deshmukh, S., and Patil, R., "Hybrid Cryptography Technique Using Modified Diffie-Hellman and RSA", *International Journal of Computer Science and Information Technology*, vol.5, issue. 6, pp. 7302-7304, 2014.

[5] Mokhtari, M., and Naraghi, H., "Analysis and Design of Affine and Hill Cipher", *Journal of Mathematics Research*, vol.4, no. 1, pp. 67-77, 2012.

[6] Hussein, L, A., "Internal Affine Stream Cipher", *Computer Engineering and Information Technology Journal*, vol.1, issue. 1, pp. 1-5, 2015.