# Symmetric Cryptography Modification Using Diffie Hellman On RDBMS

**Niko Surya Atmaja**
Universitas Pembangunan Panca Budi

## ABSTRACT

One of the most widely used and freely available RDBMS is MySQL. MySQL users generally do not care about the confidentiality of the contents stored in MySQL. The application of data confidentiality in MySQL generally only uses a username and password to protect MySQL but not its contents. Therefore, it is necessary to apply the confidentiality of the data content in MySQL so that thieves cannot obtain information from the data contained in MySQL by converting the contents of the text stored in MySQL into secret text. This research uses one of the symmetric cryptography, namely vigenere cipher to keep the text stored in MySQL secret. The disadvantage of symmetric cryptography compared to asymmetric is the same encryption and decryption keys. Therefore, this research modifies the key in symmetric cryptography using Diffie Hellman so that the key used becomes asymmetric. So that with symmetric cryptography using Diffie Hellman on the contents of the data stored in MySQL, MySQl gets better confidentiality of its data content

**Keyword : Modification; Cryptography; Symmetric; Diffie Hellman, RDBMS**

***Corresponding Author:***
Niko Surya Atmaja,
Universitas Pembangunan Panca Budi
Jl. Gatot Subroto KM. 4.5 Medan, 20122, Indonesia.
Email : halo@ysmk.org

***Article history:***
Received Feb 19, 2024
Revised Feb 25, 2024
Accepted Feb 29, 2024

## 1. INTRODUCTION

RDBMS is a database that describes the relationship of data in its tables. [1]. Related data has a relationship and dependence on the entire contents of its main table which usually uses the main key and one of the RDBMS that is widely used and provided free of charge is MySQL. [2]. MySQL is widely used to manage data and information. MySQL users generally do not care about confidentiality issues on the contents stored in MySQL. Even though confidentiality in MySQL is very important, because data thieves can steal data stored in MySQL that has no confidentiality. The application of data confidentiality in MySQL generally only uses a username and password to protect MySQL. If the contents of MySQL data are stolen and known, it can harm the owner of MySQL. Therefore, it is necessary to apply the confidentiality of the data content in MySQL so that thieves cannot obtain information from the data contained in MySQL by converting the contents of the text stored in MySQL into secret text. One of the sciences that study how to keep a text secret is cryptography. Cryptography consists of two words, crypto means secret and graphi means text, so cryptography is a secret text. [3]. In cryptography there are two processes, namely encryption and decryption, encryption is a technique for converting original text into secret and decryption is a technique for converting secret text into original text. [4]. However, to be able to keep text secret using cryptography requires the right method so as to get good text confidentiality.

In this study, researchers used one of the symmetric cryptography, namely the vigenere cipher method to keep the text stored in MySQL secret. Vigenere Cipher is one of the methods of symmetric type cryptography that only uses numbers as encryption and decryption keys. [5]. One of the shortcomings of symmetric cryptography compared to asymmetric cryptography is the same encryption and decryption keys. Therefore, this research modifies the key in symmetric cryptography using Diffie Hellman so that the key used becomes asymmetric. Diffie Hellman is a different method from other cryptographic methods that only processes the key exchange from the encrypting user with the decrypting user. [6]. The advantage of Diffie Hellman cryptography is that it can protect the key exchange by forming different keys in the encrypt and decrypt process. So that with symmetric cryptography using

Diffie Hellman on the contents of the data stored in MySQL, MySQL gets better confidentiality of its data content.

## 2. THEORY

A. Modified

Modification is the result of changing the original form into a new form. Usually the original form is changed to perfect the deficiencies that have been encountered or indeed correct the errors encountered. [7]. Modification is also the transformation of the original form into a second form. The original form usually has weaknesses, deficiencies or damage that must be repaired and refined. [8].

B. Cryptography

Cryptography is the study of how to convert original text into secret text with predetermined techniques and formulas. There are several stages carried out in cryptography, namely determining the key, using encryption and using decryption. [9]. Cryptography is not a security technique, because if the device is stolen then cryptography has no relationship other than word processing. Cryptography is the secrecy of text or sentences which aims to make messages that can be read incomprehensible except by people who have a confidentiality agreement. [10].

C. Symmetry

Symmetry is the division of a plane in balance between the right side and the left side. Symmetry is the similarity between two related things. In symmetric cryptography, it is used in the term encrypt and decrypt keys. [11]. Symmetric is a term used to express similarity between two objects. Symmetric cryptography is known for the same two keys, namely the encryption key and the decryption key. Meanwhile, asymmetrical is the opposite of symmetrical, namely the difference between the encryption key and the decryption key. [12].

D. Diffie Hellman

Diffie Hellman is a different method from other cryptographic methods that only process key exchanges from encrypt users with decrypt users. So this method cannot change the original text or text into a secret. [6]. Both the sender and receiver will perform a mathematical calculation whose results are public and private. The public value will be returned to the sender or receiver to search for the next value. The last calculation will get the same value between the sender and receiver. This value will be used as the key in the encryption and decryption process. [13].

Table 1. Diffie Hellman Number Delivery Technique

| Penerima | Pengirim |
|---|---|
| n | g |
| x | y |
| $X = g^x mod\ n$ | $Y = g^y mod\ n$ |
| $K = Y.x\ mod\ n$ | $K = y.X\ mod\ n$ |

Number transmission using the Diffie-Hellman technique can be seen in Table 1. The sender determines the value of n, the receiver determines the value of g as a public number which will then be exchanged. The sender determines the value of x and the recipient determines the value of y which is private. The x and y values are only available to the sender and receiver. The sender and receiver will determine the x and y values based on the exponential modulo calculation. The final calculation of the exponential modulo will produce a value of K where this number will be the same value at the sender and receiver. [14].

E. RDBMS

RDBMS is a database that describes the relationship of data in its tables. The interrelated tables have a primary key as a representative of the entire contents of the main table. [1] RDBMS is a database that has a description of the relationships in all the tables it has. A table is a collection of rows and columns. [2]. There are many types of RDBMS including:

MySQL
MySQL is a database that is used by many people and is free. MYSQL is generally used for data processing media from web applications that are often accessed using PHP. [15].
2. SQL Server
SQL Server is a database that is used by many people because of its speed in processing commands and can be used for free. SQL Server is generally used for data processing media from desktop applications. [16].
3. SQLite
SQLite is a database that is used on portable devices. SQLite is generally used for data processing media on android and ios. [17].
4. PostgreeSQL
PostgreSQL is a database that is used by many people and is free but has no license, PostgreSQL is also most often used for data processing on websites. [18].
5. Oracle
Oracle is a database that is not used by many people and is not available for free, Oracle is widely used in large companies that require a lot of data storage. [19][20].

## 3. METHODS

This research uses several stages, namely using the MySQL database, modifying the *Vigenere* method key, encrypting the *Vigenere* method, decrypting the *Vigenere* method and results. Figure 1 is the stages of the research process organized based on the initial stages to the end of the research.

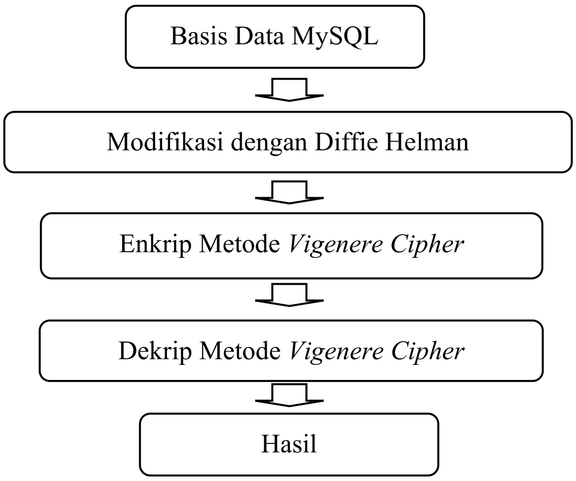

Basis Data MySQL
Modifikasi dengan Diffie Helman
Enkrip Metode *Vigenere Cipher*
Dekrip Metode *Vigenere Cipher*
Hasil

Figure 1. Research Methodology

A. MySQL Database

In the MySQL database, there are tables that contain the text of the stored data. The text of the stored data will be kept secret using the *Vigenere* method. The secret text that has been stored can also be restored to the original text that can be understood.

B. Modification with *Diffie Helman*

The *vigenere* method has the same encrypt and decrypt keys. So that the keys commonly used by the *vigenere* method are formed using *Diffie Hellman*. The *Diffie Hellman* key formation stages are:
The *hellman diffie* stages are as follows:
The encrypting user and the decrypting user agree on the values of n and g
1. The encryption user selects x and calculates:

$X = g^x mod\ n$…………(1)

The encrypt user sends X to the decrypt user.
1. The decrypt user selects y and calculates:

$$Y = g^y mod\ n \ldots\ldots\ldots\ldots(2)$$

The decrypt user sends Y to the encrypt user.
1. The encrypt user calculates the symmetry key K

$$K = Y.x\ mod\ n \ldots\ldots\ldots\ldots(3)$$

1. Pengguna dekrip menghitung kunci simetri K

$$K = y.X\ mod\ n \ldots\ldots\ldots\ldots(4)$$

Then the K value generated by *Diffie Hellman* will be used as the key to encrypt and decrypt the *Vigenere cipher* method.

## C. *Vigenere Cipher* Method Encryption

The *Vigenere* method encryption sums the text with the key which is first converted into a decimal ASCII number. Here is the *Vigenere cipher* encryption formula:

$$Ci = Pi + Ki \ldots\ldots\ldots\ldots(5)$$

Description:
Ci = Secret text resulting from the encryption process
Pi = Original text for the encryption process
Ki = Key for the encryption process
i = Repetition according to the number of texts/keys

The stages of the encryption process are explained as follows:
1. The text to be encrypted is the content of the MySQL database table.
2. Determine the encryption key using *hellman diffie*.
3. Convert the text and key into ASCII Code.
4. Sum the ASCII of the text with the ASCII of the key.
5. The sum result is converted back into characters so that it becomes the secret text.
6. The contents of the MySQL database table are converted into the secret text that has been obtained.

## D. Dekrip Metode *Vigenere Cipher*

The *vigenere* method decrypts the text with the key which is first converted into a decimal ASCII number. Here is the *vigenere cipher* encryption formula :

Description:
Pi = The original text of the decryption process
Ci = Secret text for the decryption process
Ki = Key for the decryption process
i = Repetition according to the number of text/key

1. The stages of the decryption process are explained as follows:
2. The text to be decrypted is the content of the MySQL database table that has become secret text
3. Use the decrypt key from the *hellman diffie* result.
4. Convert the secret text and key into ASCII Code.
5. Subtract the ASCII of the text with the ASCII of the key.
6. The subtraction result is converted back into characters so that it becomes the original text.
7. The contents of the MySQL database table are converted into the original text that has been obtained.

## E. Result

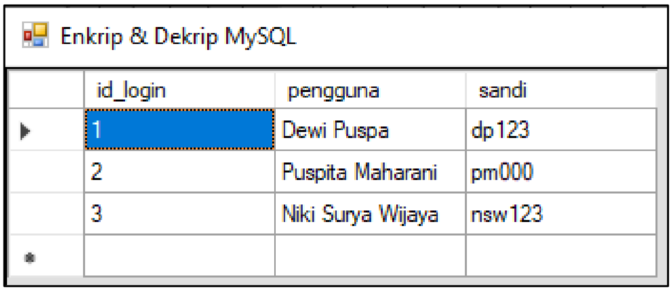
The results obtained after performing the key modification process and the encryption process are the confidentiality of the MySQL database text content in the form of secret text and the results obtained after performing the decryption process are the MySQL database text content that has been secreted into the original MySQL database text content.

## II. Analysis

The discussion is carried out regarding data testing and modification of the vigenere cipher method using Diffie Hellman on RDBMS.

A. MySQL Database

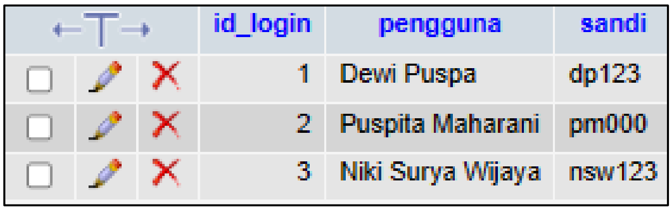
MySQL database is one of the RDBMS that is used as an object to encrypt and decrypt the contents of the MySQL database text*(Record*) from the modified *Vigenere cipher* method using *Diffie Hellman.*



Enkrip & Dekrip MySQL

| | id_login | pengguna | sandi |
|---|---|---|---|
| ▶ | 1 | Dewi Puspa | dp123 |
| | 2 | Puspita Maharani | pm000 |
| | 3 | Niki Surya Wijaya | nsw123 |
| * | | | |

Figure 2. App View



| ←T→ | | | id_login | pengguna | sandi |
|---|---|---|---|---|---|
| □ | ✎ | ✗ | 1 | Dewi Puspa | dp123 |
| □ | ✎ | ✗ | 2 | Puspita Maharani | pm000 |
| □ | ✎ | ✗ | 3 | Niki Surya Wijaya | nsw123 |

Figure 3. *MySQL Database Records*

Figure 2 is a MySQL database *record* that will be kept secret using a modified *vigenere cipher* method using *Diffie Hellman*. All text that can be processed will be converted to secret.

B. Modification with *Diffie Helman*

After obtaining the text to be encrypted, the next stage is the formation of the *Diffie Hellman* key, namely:

1. Encrypt users and decrypt users agree on a value:

n = 97

g = 5

With the condition that g < n.

2. The encrypt user chooses x = 36 and calculates:

$X = g^x mod\ n$

$X = 5^{36}\ mod\ 97$

$X = 14.551.915.228.366.851.806.640.625\ mod\ 97$

$X = 50$

1. The encryption user sends X50 to the decrypt user.
2. 1. The script user selects y = 58 and calculate:

$Y = g^y mod\ n$

$Y = 5^{58}\ mod\ 97$

$Y = 3{,}4694469519536141888238489e + 40\ mod\ 97$

$Y = 44$

The decree user sends Y44 to the encryption user.

**Tabel 2. Proses Pertukaran *Diffie Helman***

| **Penerima** | **Pengirim** |
|---|---|
| n=97 | g=5 |
| x=36 | y=58 |
| $X = g^x mod\ n$<br>$X = 5^{36}\ mod\ 97$<br>$X = 50$ | $Y = g^y mod\ n$<br>$Y = 5^{58}\ mod\ 97$<br>$Y = 44$ |

In Table 2, the *diffie helman diffie helman* exchange process agreed on the value of n = 97, g = 5, x = 36, y = 5. Then the X key that will be sent is 50 and Y is 44 to the encrypting user.

C. *Vigenere* Method Encryption

*Vigenere* method encryption sums the MySQL database *record* text with a key that is first converted into a decimal ASCII number.

The stages of the encryption process are explained as follows:

1. The text to be encrypted is the contents of the MySQL database table in the password *field* . Password: dp123

2. Determine the encryption key using *hellman diffie*.

Obtained:

n = 97<br>
x = 36<br>
Y = 44

Then do the math:

$K = Y.x \: mod \: n = \ 44 * 36 \: mod \: 97 \ = \ 75$

Convert text and key to ASCII Code.

ASCII Teks:
d = 100
p = 112
1 = 49
2 = 50
3 = 51
ASCII Key:
7 = 55
5 = 53

Sum the ASCII of the text with the ASCII of the key.

Table 3. Enkrip Metode *Vigenere*

| **ASCII Pesan** | **100** | **112** | **49** | **50** | **51** |
|---|---|---|---|---|---|
| **ASCII Kunci** | 55 | 53 | 55 | 53 | 55 |
| **ASCII Pesan + ASCII Kunci** | 155 | 165 | 114 | 103 | 106 |

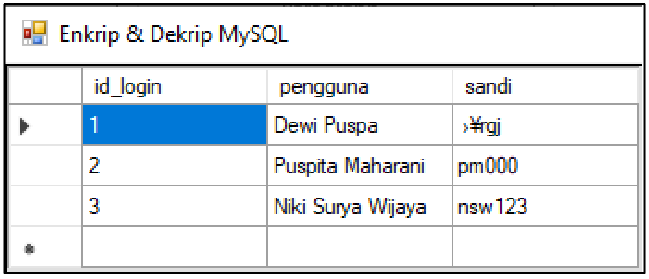
1. The sum result is converted back into characters so that it becomes secret text.

155 = ›
165 = ¥
114 = r
103 = g
106 j

3. This resulted in the secret text '¥rgj.

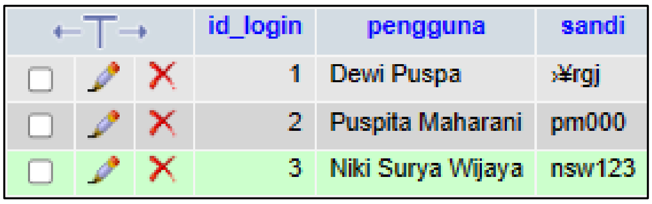
So that the secret text '¥rgj is obtained.

1. The contents of the MySQL database table are converted into the secret text that has been obtained.



| id_login | pengguna | sandi |
|---|---|---|
| 1 | Dewi Puspa | ›¥rgj |
| 2 | Puspita Maharani | pm000 |
| 3 | Niki Surya Wijaya | nsw123 |

Figure 4. Display of MySQL Encryption Results on the Application



| ←T→ | | | id_login | pengguna | sandi |
|---|---|---|---|---|---|
| □ | ✎ | ✕ | 1 | Dewi Puspa | ›¥rgj |
| □ | ✎ | ✕ | 2 | Puspita Maharani | pm000 |
| □ | ✎ | ✕ | 3 | Niki Surya Wijaya | nsw123 |

Figure 5. One of MySQL Database *Records* Becomes Secret Text

D. *Vigenere* Method Decryption

The *Vigenere* method decryption subtracts the secret text of the MySQL database *record* with a key that is first converted into a decimal ASCII number.

The decryption process stages are explained as follows:

The text to be decrypted is the contents of the MySQL database table which has become a secret text, namely in the password *field* .

Sandi : ›¥rgj

1. Use the decrypt key from the *hellman diffie* result.

Obtained:

n = 97<br>
X = 58<br>
y = 50

Then do the math:

$K = y.X \; mod \; n = 50 * 58 \; mod \; 97 = 75$

1. Convert the secret text and key into ASCII Code.

ASCII Teks:

› = 155<br>
¥ = 165<br>
r = 114<br>
g = 103<br>
j = 106

ASCII Key:

7 = 55<br>
5 = 53

1. Subtract the ASCII of the text with the ASCII of the key.

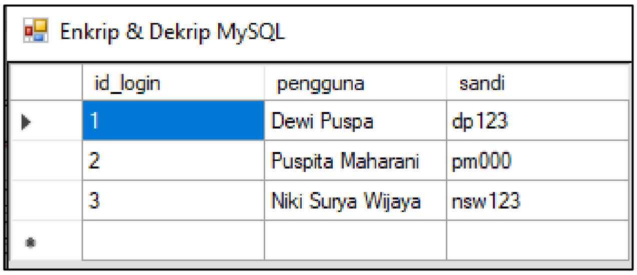
Table 3. Dekrip Metode *Vigenere*

| **ASCII Pesan Rahasia** | **155** | **165** | **114** | **103** | **106** |
|---|---|---|---|---|---|
| **ASCII Kunci** | 55 | 53 | 55 | 53 | 55 |
| **ASCII Pesan Rahasia - ASCII Kunci** | 100 | 112 | 49 | 50 | 51 |

2. The subtraction result is converted back into characters so that it becomes the original text.

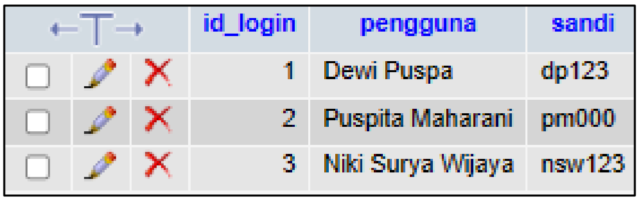
100 = d<br>
112 = p<br>
49 = 1<br>
50 = 2<br>
51 = 3

1. The contents of the MySQL database table are converted into the original text that has been obtained.



| | id_login | pengguna | sandi |
|---|---|---|---|
| ▶ | 1 | Dewi Puspa | dp123 |
| | 2 | Puspita Maharani | pm000 |
| | 3 | Niki Surya Wijaya | nsw123 |
| * | | | |

Figure 6. Display of MySQL Decryption Results in the Application



| | id_login | pengguna | sandi |
|---|---|---|---|
| □ ✎ ✕ | 1 | Dewi Puspa | dp123 |
| □ ✎ ✕ | 2 | Puspita Maharani | pm000 |
| □ ✎ ✕ | 3 | Niki Surya Wijaya | nsw123 |

Figure 7. Original Text of MySQL Database Record.

## 4. CONCLUSION

After carrying out the stages of the research process regarding the modification of symmetric cryptography using Diffie Hellman on RDBMS, it can be concluded that the results of symmetric cryptography modification using Diffie Hellman, namely with the key agreement n = 97, g = 5, x = 36 and y = 38, have produced the same key when encrypting and decrypting the contents of RDBMS, namely 75. With a different key exchange and the same value key processing results, the key in symmetric cryptography becomes asymmetric and gets better key exchange confidentiality.

## ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to the editors who have helped me in the writing process. The help and advice given really helped me to produce quality writing.

## REFERENCES

Mahsun, "Indonesian Journal of Science & Technology," Indones. J. Sci. Learn., vol. 2, no. 2, pp. 8–25, 2020.

A. Wirya and I. A. Mastan, "Aplikasi Penyewaan Ac Berbasis Web Di Pt Cahaya Manunggal," JBASE - J. Bus. Audit Inf. Syst., vol. 5, no. 2, pp. 43–53, 2022, doi: 10.30813/jbase.v5i2.3781.

K. N. Siahaan and Mesran, "Penerapan Algoritma Venigmare Cipher dan Vernam Cipher Dalam Pengamanan Data Teks," J. Sist. Komput. dan Inform., vol. 2, no. 1, pp. 48–52, 2020, doi: 10.30865/json.v2i1.2457.

A. Wijaya, "Modifikasi Algoritma Kriptografi Klasik dengan Implementasi Deterministic Finite Automata melalui Partisi Pesan Asli berdasarkan Kriteria Pesan Bagian," J. Sci. Appl. Technol., vol. 4, no. 2, p. 133, 2020, doi: 10.35472/jsat.v4i2.346.

A. Ridho, C. Mutia, A. Putri, K. Kriptografi, and T. Protocol, "Konsep Three-Pass Protocol Pengam anan Teks Menggunakan Metode Playfair Cipher Dengan Vigenere Cipher baik . Konsep Three-pass protocol hadir untuk menghindari adanya pertukaran kunci antara pengirim dan penerima yang dapat menjadi masalah ketika di trans," vol. 14, no. 1, 2023.

A. P. U. Siahaan, "Pembangkitan Kunci pada Algoritma Hill Cipher menggunakan Teknik Distribusi Angka Diffie-Hellman," Konf. Nas. Teknol. Inf. dan Komput., vol. 6, no. 1, pp. 819–823, 2022, doi: 10.30865/komik.v6i1.5775.

S. Wimaya, A. Ridwan, and S. Winarto, "Modifikasi Beton Fc 9,8 Mpa Menggunakan Abu Ampas Kopi," J. Manaj. Teknol. Tek. Sipil, vol. 3, no. 2, p. 234, 2020, doi: 10.30737/jurmateks.v3i2.1096.

M. F. Imtikhani Nurfadilah, "Modifikasi Perilaku Anak Usia Dini untuk Mengatasi Temper Tantrum pada Anak," J. Pendidik. Anak, vol. 10, no. 1, pp. 69–76, 2021, doi: 10.21831/jpa.v10i1.28831.

M. A. Alomari et al., "Embedded Devices Security: Design and Implementation of a Light RDBMS Encryption Utilizing Multi-Core Processors," IEEE Access, vol. 11, no. March, pp. 19836–19848, 2023, doi: 10.1109/ACCESS.2023.3248300.

S. Almakdi, B. Panda, M. S. Alshehri, and A. Alazeb, "An Efficient Secure System for Fetching Data from the Outsourced Encrypted Databases," IEEE Access, vol. 9, pp. 78474–78494, 2021, doi: 10.1109/ACCESS.2021.3082139.

B. T. Hammad, A. M. Sagheer, I. T. Ahmed, and N. Jamil, “A comparative review on symmetric and asymmetric dna-based cryptography,” Bull. Electr. Eng. Informatics, vol. 9, no. 6, pp. 2484–2491, 2020, doi: 10.11591/eei.v9i6.2470.

S. Kumar, M. S. Gaur, P. Sagar Sharma, and D. Munjal, “A Novel Approach of Symmetric Key Cryptography,” Proc. 2021 2nd Int. Conf. Intell. Eng. Manag. ICIEM 2021, no. April, pp. 593–598, 2021, doi: 10.1109/ICIEM51511.2021.9445343.

Kara, M., Laouid, A., AlShaikh, M., Bounceur, A., & Hammoudeh, M. (2021). Secure key exchange against man-in-the-middle attack: Modified diffie-hellman protocol. Jurnal Ilmiah Teknik Elektro Komputer dan Informatika, 7(3), 380-387.

Ali, S., Humaria, A., Ramzan, M. S., Khan, I., Saqlain, S. M., Ghani, A., ... & Alzahrani, B. A. (2020). An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks. International journal of distributed sensor networks, 16(6), 1550147720925772.

F. Sinata, “ANALISA PERBANDINGAN TINGKAT EFISIENSI ALGORITMA DATA DEFINITION LANGUAGE ( DDL ) COPY , INPLACE , INSTANT DATABASE MYSQL Comparison Analysis Of Efficiency Level Of Mysql Data Definition Language Algorithm Copy , Inplace , Instant Database,” vol. VI, no. 1, pp. 503–508, 2023.

N. Ramsari and A. Ginanjar, “Implementasi Infrastruktur Server Berbasis Cloud Computing Untuk Web Service Berbasis Teknologi Google Cloud Platform,” Conf. Senat. STT Adisutjipto Yogyakarta, vol. 7, 2022, doi: 10.28989/senatik.v7i0.472.

R. B. D. Putra, E. S. Budi, and A. R. Kadafi, “Perbandingan Antara SQLite, Room, dan RBDLiTe Dalam Pembuatan Basis Data pada Aplikasi Android,” JURIKOM (Jurnal Ris. Komputer), vol. 7, no. 3, p. 376, 2020, doi: 10.30865/jurikom.v7i3.2161.

A. D. Praba and M. Safitri, “Studi Perbandingan Performansi Antara Mysql Dan Postgresql,” J. Khatulistiwa Inform., vol. 8, no. 2, pp. 88–93, 2020, doi: 10.31294/jki.v8i2.8851.

S. Astuti et al., “Pemilihan Arsitektur Basis Data Berdasarkan,” pp. 107–121

Subramanian, E. K., & Tamilselvan, L. (2020). Elliptic curve Diffie–Hellman cryptosystem in big data cloud security. Cluster Computing, 23, 3057-3067

## BIOGRAPHIES OF AUTHORS

| | |
|---|---|
| | Niko Surya Atmaja<br>Kelahiran : Medan, 17 Juli 1987<br>Pendidikan : Pascasarjana<br>Keilmuan : Ilmu Komputer |