p-ISSN 2715-6923, e-ISSN 2721-9186
https://jurnal.unimus.ac.id/index.php/ichi

Check for updates

The Complaint System Based on Whistleblowing Concept and Message Digest 5 Cryptographic Method for Regency Inspectorate Office in Polewali Mandar

Research Article

Mawar[1*], Muhammad Assiddiq[2], Akhmad Qashlim[3]

1. *Departement of Information Systems, University Al Asyariah Mandar, Polewali Mandar 91311, ndonesia*
2. *Departement of Information Systems, UniversityAl Asyariah Mandar, Polewali Mandar 91311, Indonesia*
3. *Departement of education, University Al Asyariah Mandar, Polewali Mandar 91311, Indonesia*

**mawarindryani98@gmail.com (coresponden author)*
dikprof@gmail.com
qashlim@unasman.mail.ac.id

Article history :
Received : 23 Aug 2021
Accepted : 15 Feb 2022
Available online : 17 Feb 2022

ABSTRACT

Inspectorate as an institution that supervises violations in government agencies or organizations. However, when individuals report a deviation, they often get into trouble because the identity of the reporter is not kept secret. So that in this research a complaint system is designed that uses the concept of whistleblowing with the cryptographic method. Where this method uses the Message Digest 5 (MD5) algorithm to lock or encrypt data so that the confidentiality of the reporting data can be maintained. In collecting data, it is done qualitatively, where data is collected through observation, interviews, and literature studies. This study resulted in a complaint system using the whistleblowing concept with the message digest 5 cryptographic method which was used at the Polewali Mandar Regency Inspectorate Office as a medium for reporting violations. With this complaint system, the reporter need not be afraid, because his identity will be encrypted using the Message Digest 5 algorithm.

Keywords: Description, encryption, cryptography, md5 method, whistleblowing.

https://doi.org/10.26714/jichi.v2i2.8033

1. INTRODUCTION

Indonesia has now implemented the smart city concept by utilizing information technology and improving public services (Tolle, 2017). And now public complaints are included as a service that reports information on violations of the code of ethics and behavior of State Apparatus employees (Melani, 2019). To support the needs and interests of the public, bureaucrats within the inspectorate implement good governance in the fields of public administration, supervision, and protection (Angelia Carissa, 2018).

But it often happens when an individual fights irregularities or complains about something, usually the reporter gets into trouble within the organization (Carollo et al., 2020). In preventing cases of accounting violations, Whistleblowing can help disclose violations with good and safe management (Mulfag, 2017). Therefore, with a whistleblowing system, all have the right to express complaints without fear of the identity of the reporter being known to the person being reported, therefore the confidentiality of the identity is maintained safely (Dorset, 2017).

As we know that the security that is owned in a data is very necessary in order to maintain the authenticity and confidentiality of information that has content that only authorized parties can know about the contents of the confidential information (Sinaga et al., 2018). For data security, encryption is needed on a system so that confidentiality and privacy are maintained safely (Hu & Wu, 2015).

To achieve the goal of achieving data security, namely using cryptography. Cryptography has three security aspects, namely, message confidentiality, sender validity, message authenticity and non-repudiation. The ability of cryptographic methods to scramble the contents of data, such as text, images, audio, video and so on to make the data unreadable, hidden or meaningless all the way through transmission or storage (Encryption) (Yu & Yin, 2021).

Based on the previous description, a research was conducted to create a complaint system using the whistleblowing concept with the Message Digest 5 (MD5) cryptography method, so that the identity of the reporter is not known by others.

2. LITERATURE REVIEW

2.1 Complaint system

Reporting a crime is the main action for the victim's journey to reach justice. This interaction is very important, especially with the police for two reasons, the first is that it determines all the tones of future interactions between the victim and the police. Good interactions are likely to instill trust, while bad interactions can damage trust. The second reason is that the police are the only criminal justice institution that many victims contact (Rossetti & Mayes, 2017).

Types of violations detected/reported by supervisors and reviews includes are:

- Gratification
- Deviation from Tasks and Functions
- Conflict of Interest
- Violating applicable laws and regulations
- Corruption Crime

2.2 Whistleblowing system

Whistleblowing is the governance of a company, and provides protection for whistleblowers with a good site, to form the basis for the management of companies reporting actions based on ethical and moral principles. Pelapor disebut dengan *Whistleblower* (Rathi et al., 2015).

Whistleblower is someone who reports information about people who make mistakes or something illegal and dishonest people to the public in an organization. By using this system, the identity of the complainant is protected by law (Uddholm, 2016).

2.3 Cryptography

Cryoptigraphy is a method that is able to keep the secret of a message by converting it into randomized ciphers that are difficult to understand (Karima et al., 2016). In addition, cryptography is also included in the concept of mathematical techniques that are connected to statistical data security such as data integration, archive confidentiality, statistical validation, archive authentication, etc (Kamepalli & Reddy, 2020).

Cryptography has several purposes, including confidentiality, data integration, authentication, and non-repudiation. In cryptography it often appears in terms of terminology, as follows are receiver and sender, plaintext, ciphertext, and messages, encrypt and decrypt.

Cryptography consists of two stages of the process, namely the process of encryption and decryption. This process converts plaintext into ciphertext with certain keys, until the message content is not understood by anyone.

Cryptography can also be interpreted as the science used to maintain messages. At the point when someone sends a message starting with one place and then to the next, the content of the message may be intercepted by an irresponsible party. Cryptography is expected to prevent unapproved meetings to find out the substance of the message sent. Without cryptographic guarantees, the message will be mixed in such a way as to use a cryptographic algorithm so it will convey an arbitrary message that cannot be used before the original message content reappears using cryptographic computations (Mujito & Bagus Susilo, 2016).

1) Encryption. Encryption is a method that can convert ordinary messages into text messages or messages that other people cannot know. This encryption is also called textual content that turns into cipher text;

2) Description. Decryption is a system method that can convert messages in the form of unreadable passwords into messages that can be understood. This way for encryption and decryption is set using a cryptographic key.

In general, the encryption and decryption process is mathematically as follows: EK (M) = C (Encryption Process) DK (C) = M (Decryption Process). The encryption procedure is that message M is declared as message C and uses key K, while the decryption procedure uses key K and makes message C encrypted to produce the initial message as M (Kamepalli & Reddy, 2020).

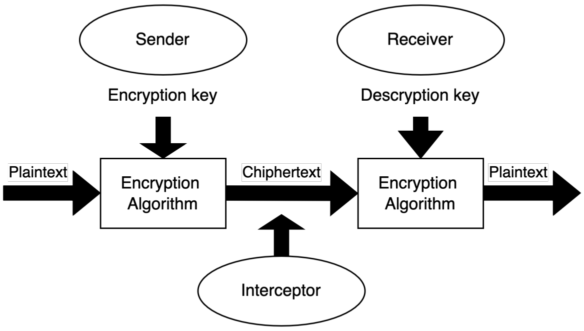


Fig 1. General encryption process.

In the application between the sender and the recipient there must be an understanding or key comparability to connect with each other. System security lies in the key algorithm. Whoever gets the key, then he can open the message delivered. Thus, as long as the correspondence interaction is private, this key remains permanent and remains part of the secret (Prasetyo & Suryana, 2016).

2.4 MD5 Algorithm

The MD5 algorithm is an algorithm that has a 128-bit hash value function, in 1991 Professor Ronald Rivest from MIT designed MD5 to replace the MD4 algorithm which had weaknesses. The advantage of the MD5 algorithm is that the process is faster than the SHA algorithm (Karima et al., 2016).

MD5i is a one-way hashi function designed by Ronald Rivesti in 1991. MD5 is a significant improvement over MD4 after MD4 was attacked by cryptanalysts. The MD5 calculation contributes to the firm size message type and creates a message digest that is 128 bits long (Zein & Adil, 2017).

How to create a message digest on a diagram is as follows:

1) Adding padding bits;
2) Adding the length of the first message;
3) Processing messages in 512-bit block size;
4) Initial value of MD5 buffer

MD5 calculations are hashes commonly used to handle PC and web organizations that are intentionally planned for the following purposes:

1) Security. The security is unavoidable given the absence of a strong algorithm system. An attack that is often used to break Hash calculations is to use beast power.

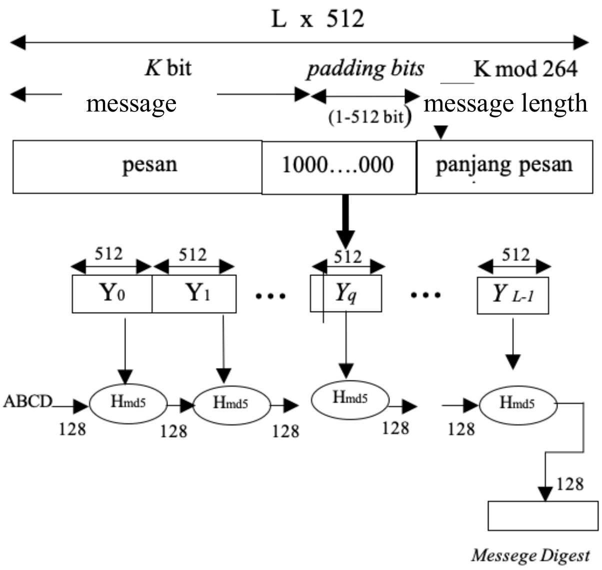


Fig 2. Restriction of message digest with MD5 algorithm.

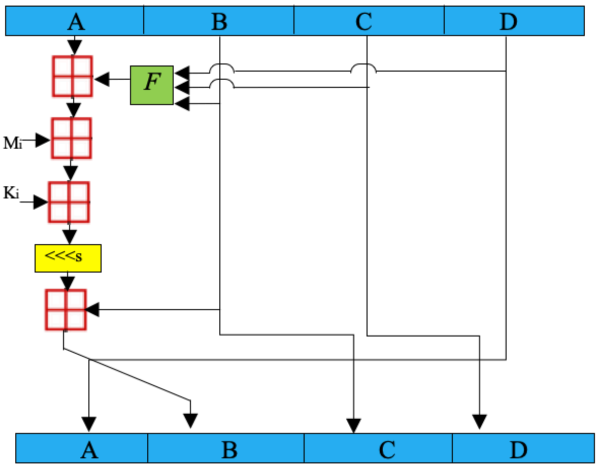


Fig 3. MD5 operation.

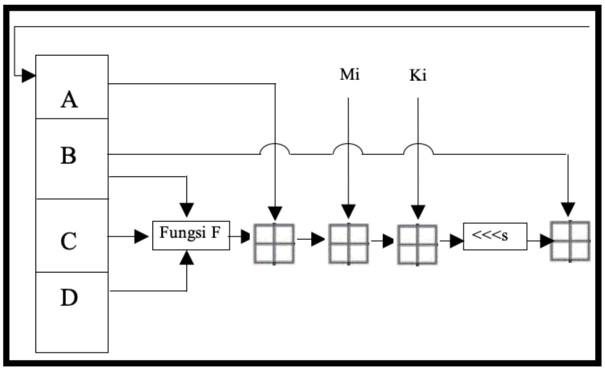


Fig 4. One MD5 operation.

2) Speed. The product used is fast because it relies on 32 bit operands.
3) Simple. Without making use of complex information

structures.

The MD5 (Message Digest 5) algorithm was designed by Ron Rivest and its use is very popular among the open source community as a checksum for downloadable files. MD5 is also often used to store passwords and is also used in digital signatures and certificates. The block size for MD5 is 512 bits while the digest size is 128 bits. Because the word size is set at 32 bits, one block consists of 16 words while the digest consists of 4 words. MD5 is one of the most widely used hash functions (Su & Lastri, 2019).

2.5 How MD5 works

MD5 processes 512-bit blocks, divided into 16 32-bit sub-blocks. The output of the algorithm is set to 4 blocks, each of which is 32 bits in size, which after being combined will form a 128-bit hash value as shown in Fig. 3 (Su & Lastri, 2019). The MD5 consists of 64 operations, aggregated into 4 rounds based on 16 activity operations (see in Fig. 4).

Information :

F : is a nonlinear function, one function is used for each Round,

Mi : represents a 32-bit block of message input,

Ki : represents a 32-bit constant, different for each operation,

<<<I : shows the left bit rotation by s;s varies for each operation,

: shows additional modulo 232

The expected way to confirm message condensation is as follows:

1) Add bit. The message will be given additional bits, so the length will be compared with 4i4i8, 512 mod. This means that the message will have a length that is only 64 bits based on the 512 bit fold. Consistently 16 bit expansion even though message length aligns with 448, 512 bit mod. Expand the bit by adding "i1i" to the beginning and followed by "0" as many times as needed depending on the situation so that the length is the same as i448i, mod i5i1i2.
2) Adding Long Message. After bit expansion, the message actually needs 6i4 bits to align with the 512 bit fold. 64 bits is an illustration of bi(message length before bit expansion is complete). These bits add up to two words (32 bits) and include the lower request first. This message extension is referred to as MiD support.
3) MD5 initiation. In MD5 there are 4 words with 32 bits registered in order to introduce massage digest first. This register is assigned a hexadecimal number.
   - Word A : 01 23 45 67
   - Word B : 89 AB CD EF
   - Word C : FE DC BA 98
   - Word D : 76 54 32 10

   These registers are commonly referred to as chain variables or chain variables.
4) Message Cycle on 16 block. The message process in one of the MD5 blocks has a function for each operation, namely:

   F (X,Y,Z) = (X Y) ((X) Z)
   G (X,Y,Z) = (X Z) (Y (Z))
   H (X,Y,Z) = X Y Z
   I (X,Y,Z) = Y (X (Z))
5) MD5 Results. Indicates the logical operations of XOR, AND, OR and NOT.

2.6 MD5 implementation

Sofwan, A et al: 2006, Here can be seen one operation of MD5 with the operation used as an example is. FF (a,b,c,d,M^j,s,t^i) show a =b+((a + F(b,c,d) + M^j + t^i) <<<s). If Mj represents the jth message of the sub block (from 0 to 15) and <<< s represents the bits to be shifted left by s bits, then the four operations of each round are:

- FF(a,b,c,d,Mj,s,ti) showing a = b + ((a + F(b,c,d) + Mj + ti)<<< s).
- GG(a,b,c,d,Mj,s,ti) showing a = b + ((a + G(b,c,d) + Mj + ti) <<<s).
- HH(a,b,c,d,Mj,s,ti) showing a = b+((a + H(b,c,d) + Mj + ti) <<< s).
- II(a,b,c,d,Mj,s,ti) showing a = b + ((a + I(b,c,d) + Mj + ti) <<< s).
- The constant ti is obtained from the integer 232 x abs(sin(i)), where i is in radians.
- The output of MD5 is 128-bit from the lowest word A and the highest word D, each 32-bit.

3. RESEARCH METHODS

3.1 Research stages

In this research, there are several stages, the first is looking for research problems to be raised, namely the Complaint System Using the Whistleblowing Concept at the Polewali Mandar Regency Inspectorate Office using the Cryptographic Message Digest 5 (MD5) method. then look for some references from journals, books, articles from the internet and other references. then collect data about the need for making Whistleblowing System applications, and looking for information about the needs needed in making applications and other supporting needs. after the data already exists, a system design will be carried out that will be made from existing references, then the process of making the Whistleblowing System Application application with the encryption method is carried out. and finally make a report in the form of a thesis. The steps can be seen in Fig. 5.

3.2 System framework

The framework of the encryption system designed in this study can be seen in Fig. 6.

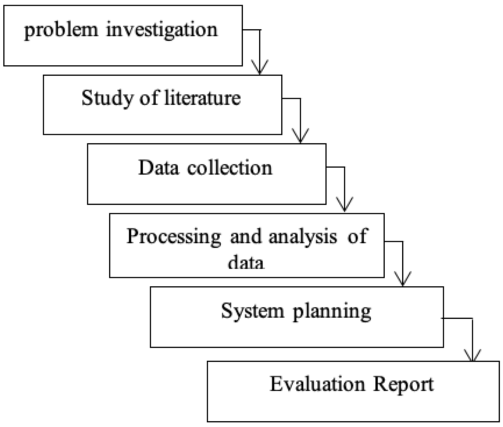


Fig 5. Research stages.

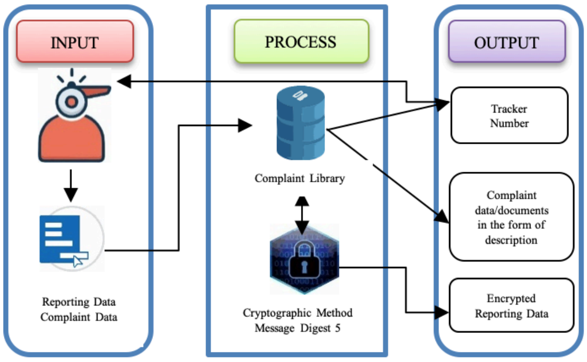

INPUT
PROCESS
OUTPUT
Complaint Library
Cryptographic Method Message Digest 5
Reporting Data Complaint Data
Tracker Number
Complaint data/documents in the form of description
Encrypted Reporting Data

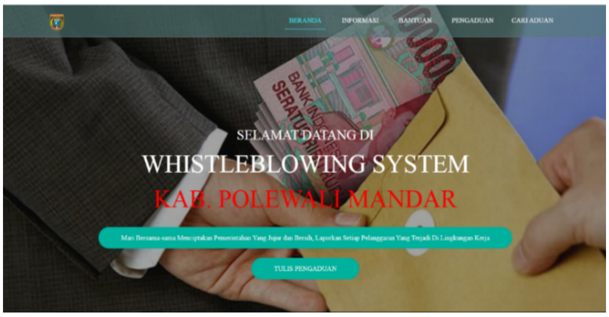
Fig 6. Framework system.

4. RESEARCH RESULT

The results of the research on the complaint system of the inspectorate office using the Whistleblowing concept at the Polewali Mandar Regency Inspectorate Office using MD5 cryptography using the PHP and XAMPP programming languages, the program created must be in accordance with the design that has been designed in such a way that it can meet system users.

At this point, the system design is translated into code in the default programming language. The results can be seen in the form below:

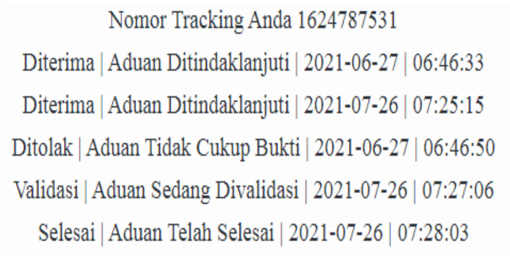
1) Main Menu Form. The dashboard display is the main display on the whistleblowing website, which contains information about the Whistleblowing system, complaint criteria, and steps to make a complaint. And there are several menu views including Home, Information, Complaints, and Find Complaints. The appearance can be seen in Fig. 7. When the complainant wants to start a complaint, the menu write complaint on the selected dashboard. And the data that must be completed in the personal data section is a pseudonym, password, and NIP. And the complaint data section is completed with the reported data, a description of the complaint, along with strong evidence attachments. After the complainant sends the complaint data, the system will automatically display the Tracking number. No Tracking No one knows other than the complainant himself and the purpose is to track the complaint so that the complainant knows that the complaint has reached which stage has been processed by the inspectorate. The status display of the tracking results is in Fig. 8.



SELAMAT DATANG DI
WHISTLEBLOWING SYSTEM
KAB. POLEWALI MANDAR

Mari Bersama-sama Menciptakan Pemerintahan Yang Jujur dan Bersih, Laporkan Setiap Pelanggaran Yang Terjadi Di Lingkungan Kerja

Fig 7. Dashboard form.



Nomor Tracking Anda 1624787531

Diterima | Aduan Ditindaklanjuti | 2021-06-27 | 06:46:33

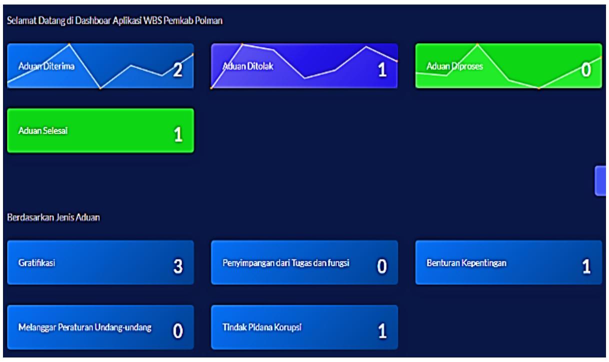
Diterima | Aduan Ditindaklanjuti | 2021-07-26 | 07:25:15

Ditolak | Aduan Tidak Cukup Bukti | 2021-06-27 | 06:46:50

Validasi | Aduan Sedang Divalidasi | 2021-07-26 | 07:27:06

Selesai | Aduan Telah Selesai | 2021-07-26 | 07:28:03

Fig 8. Complaint tracking results.



Selamat Datang di Dashboar Aplikasi WBS Pemkab Polman

Aduan Diterima 2

Aduan Ditolak 1

Aduan Diproses 0

Aduan Selesai 1

Berdasarkan Jenis Aduan

Gratifikasi 3

Penyimpangan dari Tugas dan fungsi 0

Benturan Kepentingan 1

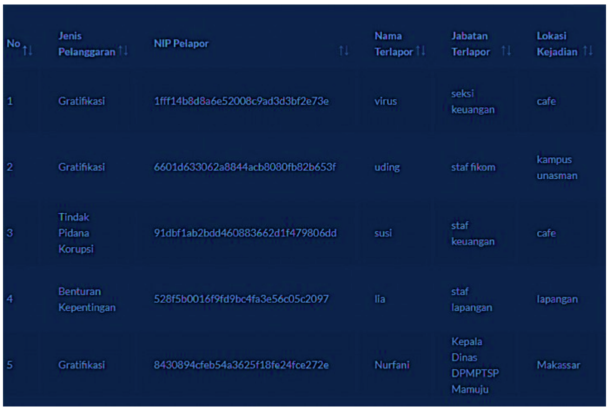
Melanggar Peraturan Undang-undang 0

Tindak Pidana Korupsi 1

Fig 9. Admin dashboard.

2) Admin Dashboard View. In the admin dashboard view, you can immediately see the number of complaints that have been received, rejected, processed, and completed. On this admin page, you can also see the number of types of complaints that come in, such as gratuities, deviations from duties and functions, conflicts of interest, violating laws and regulations, and criminal acts of corruption. The form display in Fig. 9.

3) Complaint Result Form Enter. In this form the admin can see the complaints that have been entered. This form contains data in the form of the type of violation, the NIP of the reporting person that has been encrypted, the name of the reported party, the position of the reported party, location of the incident, district, province, estimated date of incident, download attachments, the reporter (this reporter is to be filled with a pseudonym, not full name). the complainant), the date of the complaint, the time of the complaint, the



No ↑↓	Jenis Pelanggaran ↑↓	NIP Pelapor ↑↓	Nama Terlapor ↑↓	Jabatan Terlapor ↑↓	Lokasi Kejadian ↑↓
1	Gratifikasi	1fff14b8d8a6e52008c9ad3d3bf2e73e	virus	seksi keuangan	cafe
2	Gratifikasi	6601d633062a8844acb8080fb82b653f	uding	staf fikom	kampus unasman
3	Tindak Pidana Korupsi	91dbf1ab2bdd460883662d1f479806dd	susi	staf keuangan	cafe
4	Benturan Kepentingan	528f5b0016f9fd9bc4fa3e56c05c2097	lia	staf lapangan	lapangan
5	Gratifikasi	8430894cfeb54a3625f18fe24fce272e	Nurfani	Kepala Dinas DPMPTSP Mamuju	Makassar

Fig 10. Complaint results.

tracking status, and the process and delete action buttons.

This Whistleblowing complaint system uses the MD5 cryptographic method to encrypt the reporter's NIP, so that the reporter's identity is hidden because it is confidential. The appearance is as follows in Fig. 10.

For information on the status of the complaint, the admin can directly open the process button. After clicking, what appears is the complaint verification process form. This form is a page for processing every incoming complaint, this form contains information about No Tracking, type of violation, name of the reported person, description of the complaint, and change status. In changing this status there are several list options we can see detail in Table 1.

Table 1.The caption must be shown before the table.

Status	Description
Gratification	Complaint reviewed
Received	Complaints are followed up
Rejected	Complaints are not enough evidence
Validation	Complaints are being validated
Finished	Complaint Finished

5. CONCLUSION

Several conclusions can be drawn from the thesis entitled "a complaint system using the whistleblowing concept with the Message Digest 5 (MD5) cryptographic method." With this system, the reporter no longer needs to go to the office to submit his complaint, the identity of the reporter is locked using the Messagei cryptographic has function. Digesti 5 (MD5), Messagei digest 5 is a one-way hash function that can convert Input with variable length into output with but which is 128-bit (randomly generated data).

The complaint system at the inspectorate office uses the concept of whistleblowing with message digest 5 (MD5) data security. The system has successfully received the complaint and then processed it by the admin as planned, however, when the complainant wants to track the complaint using no tracking, this system has not been able to send it automatically to the reporting account which allows the complainant to lose the tracking number. Suggestions for future development no tracking can be sent automatically to email and also this application can be made in mobile form. Thus the suggestions that the author can give, hopefully these suggestions can be used as input for further research.

REFERENCES

Zein & Adil, A. (2017). Aplikasi Media Bantu Pembelajaran Kriptografi dengan Menggunakan Algoritma Message Digest 5 (MD5). *Jurnal Matrik*, *15*(2), 44. https://doi.org/10.30812/matrik.v15i2.33

Akhmad Qashlim. (2018). *Integration of Information System Based on Supply Chain Management (SCM) for Pharmaceutical Warehouse in Mamasa Regency*. *9*(June), 1–8. https://doi.org/10.21512/comtech.v9i1.4027

Angelia Carissa, D. (2018). The Role of the Functional Position of Auditors on Improving the Performance of Bureaucrats in the Inspectorate of Central Java Province. *Soumatera Law Review*, *1*(2), 251–266. https://doi.org/10.22216/soumlaw.v1i2.3718

Carollo, P. L., Pulcher, S., Guerci, M., & Ilmu, D. (2020). *Whistleblowing as an essential practice for responsible management Writer*. 1–21.

Dorset. (2017). *Freedom of Speech: convey to the NHS incorporating Dorset HealthCare's local system*. 1–25.

Hu, D., & Wu, Z. (2015). Hidden Encryption: The Power, Trust, and Costs of Constitutional Collective Oversight. *Hukum Indiana*, *90*, 281–287.

Karima, A., Diyatan, M. N., Informatika, T., Ilmu, F., Universitas, K., & Nuswantoro, D. (2016). *Gost Cryptographic Algorithm With Implementation*. *15*(4), 292–302.

Melani, Y. I. (2019). Academic Service Complaint System Using Responsive Web Design. *Sisfokom*, *08*(1), 39–45.

Mujito, M., & Bagus Susilo, A. (2016). File Cryptography Application Using Blowfish Method and Base64 Method at the Department of Population and Civil Registration of South Tangerang City. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *5*(2), 54. https://doi.org/10.32736/sisfokom.v5i2.39

Mulfag, M. R. P. (2017). Intention to Whistleblowing on Government Internal Auditor. *Jurnal Sains Dan Seni ITS*, *6*(1), 51–66.

Polly Rossetti, Alex Mayes, A. M. (2017). *System victim Experience, interests and rights of victims of crime in the criminal justice process*. *April*.

Prasetyo, R., & Suryana, A. (2016). Data Security Application with AES Cryptographic Algorithm Technique and Desktop-Based SHA-1 Hash Function. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *5*(2), 61. https://doi.org/10.32736/sisfokom.v5i2.40

Qashlim, A Akhmad, Tandama, R., Khairat, U., Informasi, S., Al, U., Mandar, A., Informasi, S., Al, U., & Mandar, A. (2021). *Hospital Information System Integration for Health Facilities and Referral Services*. 406–412.

Rathi, N. T., Ronald, P. B., & Trotman, L. (2015). *Poor Whistleblower Protection Conditions in India. 2014.*

Yu, F., & Yin, H. (2021, April). Password Cracking of PDF 2.0 documents on GPU. In 2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS) (pp. 721-725). IEEE.

Sinaga, D., Jatmoko, C., Studi, P., Infromatika, T., Komputer, F. I., & Nuswantoro, U. D. (2018). *Implementation of sha512 on 1.2 . file cryptography application*. 978–979.

Su, S., & Lastri. (2019). *Implementation of Messege Digest Algorithm 5 (MD5) and Secure Hash Algorithm (SHA-156) Data Encryption in Setya Aji Flower Farm Bandungan Agrotourism Employee Scheduling System*. *5*, 2019.

Sujitha Kamepalli & Sudharsan Reddy. (2020). *Secure Hash Algorithm (SHA-512) Analysis for Encryption Process in College Web-Based Applications*. *3*, 120–127.

Tolle, H. (2017). *Geotagging and Geofencing Based E-Complaint System Module Design*. *11*(3), 113–129.

Uddholm, J. H. (2016). *Anonymous Javascript Cryptography and Cover Traff ic in Cryptographic Applications and Anonymous Javascript Covers.*

Mawar is born in pinrang 29 September 1998, currently pursuing undergraduate education Computer Science, information systems study program at Al Asyariah Mandar University. The author is conducting a research entitled “The Complaint System of the Polewali Mandar Regency Inspectorate Office Using the Whistleblowing Concept with the Message Digest 5 (Md5) Cryptographic Method"

Muhammad Assiddiq completed megister education in 2006 on the study program Social science education Negeri Makassar University, He has been active as a research lecturer since 2006, and focus on the field of Financial Management, Cost Accounting and Computer Accounting.

Akhmad Qashlim completed master's education in 2014 on the study program Information System Diponegoro University, has been active as a research lecturer since 2014, and focus on the field of Information Systems, Artificial Intelligence, apart from being a lecturer, he also moves a lot on social and environmental activities.