Mobile and Forensics
Vol. 5, No. 2, September 2023, pp. 42-48
ISSN: 2714-6685 (online), 2656-6257 (print)
DOI: http://dx.doi.org/10.12928/mf.v5i2.8451

Hybird Autokey Cipher Algorithm Implementation Reverse Key and Standard Data Encryption for App-Based Text Messages

[1,]Risandio Ilham Lazuardi, [2,]Nuril Anwar
[1,2]Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[1,*]risandio1800013899@webmail.uad.ac.id
[2,]nuril.anwar@tif.uad.ac.id
[*]correspondence email

Abstract

The development of the internet facilitates public communication in sharing information. Along with the advancement of technology in the communication segment, there were various threats to it. Many applications had sophisticated security systems, but the actions in exploiting these security systems were also increasingly diverse. This study implemented a combination of classic and modern algorithms, namely autokey cipher reverse key and DES to protect data from these crimes. This research develops encryption and decryption applications using the agile method, the technique used because of the time spent on the built progress of applications with a cycle for the development process. With this cycle utilized, the method was suitable for developing applications in the short term and revising or improving applications in each cycle. The research resulted in security applications having the function of helping people secure data so that they could prevent and complicate digital criminal acts.

Keywords: agile, mobile application, autokey, DES, encryption, reverse, texts

INTRODUCTION

Technology enables instant and efficient communication across vast distances. With tools such as internet and email, people can connect and exchange information in real-time and access all the Information that they needed[1]. Hardware like smartphone also provides a diverse range of communication channels to suit different preferences and needs, from phone calls and text messages to emails, social media, and video chats, individuals can choose the most appropriate medium to convey their messages and connect with other including sending or keeping data that may include their private detail[2]. Use of technology like this has become an integral part of communication, shaping the way we connect, collaborate, and exchange information. Its urgency lies in its ability to enhance efficiency, connectivity, accessibility, and global collaboration, ultimately improving our personal and professional lives[3]. The rise of smartphones and mobile applications has revolutionized communication. With development in form of applications, also known as an app, refers to a software program or computer program designed to perform specific tasks or functions for end-users[4]. Applications are typically developed for use on various devices such as computers, smartphones, tablets, and other electronic devices[5]. Product of application is as following messaging apps like WhatsApp, WeChat, and Telegram enable instant messaging, voice and video calls, and media sharing. Social media apps like Facebook, Twitter, and Instagram facilitate social networking also other group like reddit make the communication on a global scale easier[6]. With all its benefit of the technology people also exploit them to earn personal gain, often do things in such ways that label them as cybercriminal, act like stealing data, spoofing, and other technology abuse for their own benefit, moreover guide to do things like this

Article History: *Received June 23, 2023; Revised August 15, 2023; Accepted August 30, 2023*

is easy to find, Internet provide all information both beneficial and harmful[7]. One way of other things to prevent cybercrime is use cryptography, cryptography is the practice of secure communication and data protection through the use of mathematical algorithms. It involves the transformation of plaintext (readable information) into ciphertext (encoded or scrambled information) to ensure confidentiality, integrity, and authentication[8]. Cryptography plays a crucial role in information security, including secure communication channels, data encryption, digital signatures, authentication protocols, and secure storage mechanisms[9]. The development of the internet facilitates public communication in sharing information is increasingly fast[10]. Along with the advancement of technology in the communication segment, there were various threats to it[11]. Many applications had sophisticated security systems, but the actions in exploiting these security systems were also increasingly diverse[12]. The Autokey cipher is a symmetric encryption technique that belongs to the family of substitution ciphers[13]. It operates by using a key that is as long as the plaintext message being encrypted. Each character of the plaintext is combined with a corresponding character from the key to produce the ciphertext, autokey have unique key generation, first step is to generate a key that is at least as long as the plaintext message. The key can be any sequence of characters, but it should be kept secret to maintain the security of the cipher[14]. Other algorithm that used in this research is DES (Data Encryption Standard) is a symmetric encryption algorithm that was widely used for secure data transmission and storage in the past. It was developed by IBM in the 1970s and later adopted as a standard by the U.S. government[15]. Cybercrime often target personal and sensitive information such as financial data, social security numbers, healthcare records, and intellectual property[16]. Safeguarding this information is crucial to maintain privacy and protect individuals and organizations from identity theft, financial fraud, and reputational damage. This study implemented a combination of classic and modern algorithms, namely autokey cipher reverse key and DES to protect data from these crimes and develops encryption and decryption applications using the agile method, the technique used because of the time spent on the built progress of applications with a cycle for the development process. With this cycle utilized, the method was suitable for developing applications in the short term and revising or improving applications in each cycle. The research resulted in security applications having the function of helping people secure data so that they could prevent and complicate digital criminal acts. With purpose in attempt to create new solution for protecting personal data, by combining the algorithm of cryptography and implement it on an application, to create tools with function for protecting data in form of alphabetical symbol, with tools that can run on mobile smartphone and simple usage without eat big resource on smartphone specification.

METHODS

For developing the application is using Agile method, Agile methodology, or Agile for short, is an iterative and incremental approach to project management and software development[17]. It emphasizes flexibility, collaboration, and adaptive planning to deliver high-quality products efficiently. Agile methodologies originated as a response to traditional waterfall methodologies, which followed a sequential and linear process, seems like this method look like Waterfall but Agile is more adaptive with its recycle process for more improvisation[18].

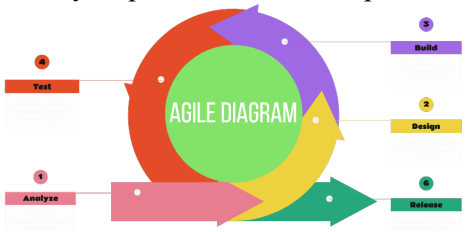

Fig 1. Agile Method

Agile projects are divided into small increments called iterations or sprints. Each iteration typically lasts from one to four weeks and delivers a functional product increment. This iterative

approach allows for continuous feedback, adaptation, and improvement throughout the development process Rather than creating detailed and rigid plans upfront, Agile teams focus on maintaining a prioritized product backlog—a list of features or requirements. The team selects a subset of items from the backlog for each iteration, based on feedback. Agile methodologies emphasize continuous learning and improvement. Teams regularly reflect on their processes and seek ways to enhance efficiency, quality, and collaboration. Retrospectives at the end of each iteration help identify strengths, weaknesses, and areas for improvement. Popular Agile methodologies include Scrum, Kanban, Lean, and Extreme Programming (XP). Each methodology has its specific practices and ceremonies, but they all share the core Agile values and principles. Agile methodologies have gained popularity due to their ability to address rapidly changing business requirements, increase customer satisfaction, and deliver value incrementally. They are widely used in software development but can also be applied to various projects and domains where flexibility and collaboration are essential[19].

RESULT AND DISCUSSIONS

The Application is need to focus on its important requirement first, the first important aspect is to analyze the functional and non-functional requirement, a functional requirement is a requirement that contains several steps which will then be executed by the system. In addition, system requirements also contain any information that must be issued by the system, such as commands that match the functionality of the application can be executed properly without any bugs that make the program error or not run as it should, on the other hand non-functional requirements are requirements that describe how the system will function in the future. Defining non-functional requirements requires an understanding of system characteristics and limitations, such as how application will perform on every situational condition for example like without internet, or how many RAM that used for running. When the application is opened a splash screen will appear which will be followed by the main menu, the main menu contains the form used for the encryption and decryption process, when the user has filled in and selected the menu will display the results of the process then the user can copy text to use in chat and so on, with the step according to the execution time, the user starts by opening the application and filling out the form with input for plaintext and the key to be used, the system will respond to the key to carry out the process that the user will choose, either in the form of encryption or decryption, return the value from the menu in the form encryption results and the option to copy text.

Fig 2. The Splash Screen

This application is started with a splash screen that will give the user little information in form of display some basic introductory information such as the logo just before the app loads completely and entering the main menu, design itself is very simple, when things are simple, they are easier

to learn and remember. When the screen are filled with unnecessary information, it make the Information unclear and takes attention away from the key points.

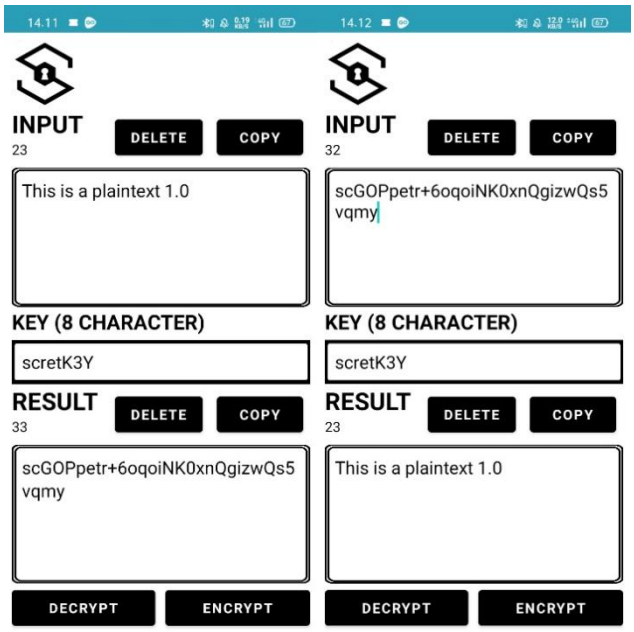

Fig 3. The Menu

The main menu is pretty simple consists of several form fields that will be filled in by the user, for the first column is a place to fill in the initial text in the form of plaintext or ciphertext, then the second column will contain the key to be used in this application, the key form will follow the criteria of the DES algorithm where the key is entered must be eight letters in total, and for the last column is the place that will be used as a viewer of the results of encryption or decryption, and in each column there are delete and copy buttons to make it easier for users to operate.
For autokey itself is using reverse method, a method for string builder that use for reverse the input word.

```
StringBuilder revkey = new
StringBuilder(keytext.getText().toString().toUpperCase());
                    String Algo1 = autoencrypt(normal,
revkey.reverse().toString());
```

Fig 4. Reverse key method

The reverse process on the String key is done using the String Builder, so that the String key gets the reverse code extension which can be used to reverse the order of the Strings in it, and the use of this extension is done in calling the autokey encryption algorithm.

```
if(i<keytext.getText().toString().length()) {
    int x = (normal.charAt(i) + key.charAt(i - j) + 26) % 26;
    x += 'A';
    cipher += (char) (x);
}
else {
    int x = (normal.charAt(i) + Character.toUpperCase(normal.charAt(k-j))+ 26) % 26;
    x += 'A';
    cipher += (char) (x);
    k+=1;
}
```

Fig 5. Autokey algorithm

The process of encryption and decryption is using conditional code, to separate between the sequence of letters that have exceeded the number of key letters or not, Autokey ciphers offer a higher level of security compared to polyalphabetic ciphers with fixed keys due to the absence of key repetition within a single message. Consequently, traditional techniques such as Kasiski examination or index of coincidence analysis cannot be applied to decipher the ciphertext, unlike similar ciphers that employ a single repeated key. However, the method have a significant vulnerability.

```
byte[] cleartext = value.getBytes( charsetName: "UTF-8");
SecretKeySpec key = new SecretKeySpec(keytext.getText().toString().getBytes(), algorithm: "DES");
Cipher cipher = Cipher.getInstance( transformation: "DES/ECB/ZeroBytePadding");
cipher.init(Cipher.ENCRYPT_MODE,key);
crypted = Base64.encodeToString(cipher.doFinal(cleartext),Base64.DEFAULT);
```

Fig 6. DES encryption

For DES algorithm using Android Studio with java language, the process is just using the function within base64 library, by utilizing the Base64 library which has an encoding extension to carry out the encryption process, using try and catch as an anticipation of errors, by using try and catch errors can be detected when the process in the try is executed. The key is created using the Secret Key Spec command which is used to create a key from a byte array where the command requires the key parameter to be inputted in the initial display, then the key will be processed and stored in the key variable.

To process plaintext, we use the Cipher command which has various basic extension functions in the encryption and decryption process. To create a cipher object, we need to call the Get Instance method which aims to perform a transformation (a String that has a description of the operations performed) and has parameters in the form of algorithms, methods, and paddings. And the last step in encryption calls the function on base64, namely the encode to String method using the cipher and key encryption parameters that have been processed earlier, using to String because the value of the parameter that is called is in the form of bytes so that the code returns the form to String.

```
byte[] bytesDecoded = Base64.decode(coded.getBytes( charsetName: "UTF-8"),Base64.DEFAULT);
SecretKeySpec key = new SecretKeySpec(keytext.getText().toString().getBytes(), algorithm: "DES");
Cipher cipher = Cipher.getInstance( transformation: "DES/ECB/ZeroBytePadding");
cipher.init(Cipher.DECRYPT_MODE, key);
byte[] txtDecrypted = cipher.doFinal(bytesDecoded);
result = new String(txtDecrypted);
```

Fig 7. DES decryption

the decryption process has the same flow as the encryption process, with the condition that if the input begins with *"code=="* the String value will be truncated by six characters and enter the truncated value into the result storage variable, then there is a difference in the initial method by using "DECRYPT_MODE".

To assess satisfaction or comfort in using the application, System Usability Scale (SUS) is used for this application, SUS itself is a questionnaire that is used to evaluate the usability of products and services. These survey questions are used as a quantitative method to evaluate and get actionable insights on the usability of a wide variety of new systems which may be either software or hardware.

Table 1. System Usability Scale Test

No	Respondent	Q1 (x-1)	Q2 (5-x)	Q3 (x-1)	Q4 (5-x)	Q5 (x-1)	Q6 (5-x)	Q7 (x-1)	Q8 (5-x)	Q9 (x-1)	Q10 (5-x)	∑	Score
1	Respondent 1	3	3	4	4	4	4	4	4	2	4	36	90
2	Respondent 2	4	2	3	4	2	2	3	3	3	3	29	72,5
3	Respondent 3	4	4	4	4	4	4	4	4	4	4	40	100
4	Respondent 4	2	3	2	2	2	2	2	2	2	2	22	55
5	Respondent 5	3	4	2	4	3	3	3	2	3	4	31	77,5
6	Respondent 6	3	3	4	3	2	3	4	3	4	4	33	82,5
7	Respondent 7	3	4	4	3	3	3	3	3	3	3	32	80
8	Respondent 8	2	4	4	4	4	4	4	4	4	4	36	95
9	Respondent 9	2	3	3	4	1	2	3	4	2	2	27	67,5
10	Respondent 10	2	4	2	2	3	3	3	3	2	2	26	65
												312	780
Average = 780/10 = 78													

The final result obtained is an SUS value of 78 which can be interpreted as a good value. The System Usability Scale assessment uses a maximum value of 4 so that the x-1 and 5-x formulas are used to achieve this maximum value.

Based on assessment research in the System Usability Scale using the SUS score with a description if a value is above 68 it will be considered above average and a value below 68 is considered below average, so with a score of 78 obtained the application is considered to have quality that is below above average

CONCLUSION

Final product is an encryption-decryption application has been generated successfully using a combination of the Hybrid Autokey Cipher Reverse Key Algorithm and Data Encryption Standard, Application is runs smoothly according to its function his application will be used to help secure data in the form of encoded text messages.

Applications that have been tested both in terms of technical and user convenience and have met the standard criteria for similar utility applications.

REFERENCES

[1] and P. J. S. Benckendorff, Pierre J., Zheng Xiang, *Tourism information technology*. Cabi, 2019.

[2] P. Daponte, L. De Vito, F. Picariello, and M. Riccio, "State of the art and future developments of measurement applications on smartphones," *Measurement*, vol. 46, no. 9, pp. 3291–3307, Nov. 2013, doi: 10.1016/j.measurement.2013.05.006.

[3] S. Herring, *Culture, technology, communication: Towards an intercultural global village*. Suny Press, 2001.

[4] A. Holzinger, P. Treitler, and W. Slany, "Making Apps Useable on Multiple Different Mobile Platforms: On Interoperability for Business Application Development on Smartphones," 2012, pp. 176–189. doi: 10.1007/978-3-642-32498-7_14.
[5] C. L. Ventola, "Mobile devices and apps for health care professionals: uses and benefits.," *P T*, vol. 39, no. 5, pp. 356–364, May 2014.
[6] Y. Y. Lee and C. L. Gan, "Applications of SOR and para-social interactions (PSI) towards impulse buying: the Malaysian perspective," *J. Mark. Anal.*, vol. 8, no. 2, pp. 85–98, Jun. 2020, doi: 10.1057/s41270-020-00077-5.
[7] J. R. C. Nurse, "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit," in *The Oxford Handbook of Cyberpsychology*, A. Attrill-Smith, C. Fullwood, M. Keep, and D. J. Kuss, Eds., Oxford University Press, 2019, pp. 662–690. doi: 10.1093/oxfordhb/9780198812746.013.35.
[8] L. Y. Connolly and D. S. Wall, "The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures," *Comput. Secur.*, vol. 87, p. 101568, Nov. 2019, doi: 10.1016/j.cose.2019.101568.
[9] A. K. Mandal, C. Parakash, and A. Tiwari, "Performance evaluation of cryptographic algorithms: DES and AES," in *2012 IEEE Students' Conference on Electrical, Electronics and Computer Science*, IEEE, Mar. 2012, pp. 1–5. doi: 10.1109/SCEECS.2012.6184991.
[10] D. Buhalis and P. O'Connor, "Information Communication Technology Revolutionizing Tourism," *Tour. Recreat. Res.*, vol. 30, no. 3, pp. 7–16, Jan. 2005, doi: 10.1080/02508281.2005.11081482.
[11] S. G. Qureshi and S. K. Shandilya, "Advances in Cyber Security Paradigm: A Review," 2021, pp. 268–276. doi: 10.1007/978-3-030-49336-3_27.
[12] S. C. Moser, "Communicating climate change: history, challenges, process and future directions," *WIREs Clim. Chang.*, vol. 1, no. 1, pp. 31–53, Jan. 2010, doi: 10.1002/wcc.11.
[13] R. E. Klima and N. P. Sigmon, *Cryptology: Classical and Modern with Maplets*. 2012. doi: 10.1201/b12269.
[14] A. M. No Froomkin, *Metaphor is the key: cryptography, the clipper chip, and the constitution*, 143rd ed. U. Pa. L., 1994.
[15] G. Singh and S. Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," *Int. J. Comput. Appl.*, vol. 67, no. 19, pp. 33–38, Apr. 2013, doi: 10.5120/11507-7224.
[16] K. T. Smith, A. Jones, L. Johnson, and L. M. Smith, "Examination of cybercrime and its effects on corporate stock value," *J. Information, Commun. Ethics Soc.*, vol. 17, no. 1, pp. 42–60, Jan. 2019, doi: 10.1108/JICES-02-2018-0010.
[17] and M. A. D. Syed Nisar Bukhari, Ashaq Hussain Dar, "Review and analysis of applying agile methodology in software development," *Int. J. Sci. Tech. Adv.*, vol. 2, no. 4, pp. 187–190, 2016.
[18] M. STOICA, M. MIRCEA, and B. GHILIC-MICU, "Software Development: Agile vs. Traditional," *Inform. Econ.*, vol. 17, no. 4/2013, pp. 64–76, Dec. 2013, doi: 10.12948/issn14531305/17.4.2013.06.
[19] I. G. Stamelos and P. Sfetsos, *Agile software development quality assurance*. 2007. doi: 10.4018/978-1-59904-216-9.