IMPLEMENTATION OF AES-128 CRYPTOGRAPHY ON UNMANNED AERIAL VECHILE AND GROUND CONTROL SYSTEM

Farhan Syafaat[1], Alif Finandhita[2]

[1,2] Teknik Informatika – Universitas Komputer Indonesia
Jalan Dipatiukur 112-116 Bandung
E-mail : farhan.syafaat@email.unikom.ac.id[1], alif.finandhita@email.unikom.ac.id[2]

ABSTRACT

Unmanned Aerial Vehicle (UAV) is an unmanned system (Unmanned System), which is an electro-mechanical based system that can carry out programmed missions. UAV requires a Ground Control System (GCS). In the operation of the UAV the task of the GCS is as a monitoring and command station where operators on land can send mission orders and oversee the course of the mission and the condition of the UAV while in the air. Based on the results of research shows that even professional UAVs can still be carried out in the form of Man-in-the-Middle attacks. So that the data sent can be read by the attacker, therefore it requires Advanced Encryption Standard (AES-128) encryption on the data sent by the UAV and received by GCS. AES-128 was chosen because it has a faster processing speed than other AES cryptography and no cryptanalysis has succeeded in hacking AES-128. Application layer encryption was chosen because it is easier to use and more cost effective than hardware encryption in various cases. The results and conclusions that AES-128bit cryptography can be applied to the communication between UAV and GCS so that the attack cannot read the data sent.

Kata kunci : Unmanned Aerial Vehicle (UAV), Ground Control System (GCS), Cryptography, Advanced Encryption Standard (AES), Man-in-the-Middle.

1. INTRODUCTION

In the past four years, various types of non-built devices have been used by civil and scientific circles. This tool complements various equipment to provide data in various applications [1]. Unmanned Aerial Vehicle (UAV) which develops remote sensing applications, UAV is an unmanned system, which is an electro-mechanical based system that can carry out programmed missions [2]. Basically according to autonomous needs, UAVs still need a Ground Control System (GCS). In UAV operations, the task of GCS is as a monitoring and command station where the above operators can receive mission requests and road transport missions and UAV conditions while in the air [3].

UAVs with GCS can communicate in two directions and send data to each other via telemetry. Based on the results of research proving that even professional UAVs can still be carried out in the form of attacks Man-in-the-Middle (MitM), the authors provide two solutions can be used: (1) XBee 868LP on-board encryption, is the only solution that also reduces the risk of Remote AT Commands, and (2) application layer encryption. So that encryption is needed on the data sent and received by GCS [4].

The difficulty of getting hardware that implements encryption that is sold freely in the market and with various considerations, encryption is selected at the application layer level. Application layer encryption is easier to use and more cost effective than hardware encryption in many cases. In particular, when new encryption services are needed for a computing environment that is already used, application layer encryption is more suitable than hardware [5].

Previous research related to UAV and GCS security is that data security between UAV and GCS has been carried out on a One Time Pad basis [6]. Authentication of UAV communication using Caesar Cipher Cryptography has been designed and simulated. The system has undergone initial tests, simulations and the results are satisfactory [7]. The combination of UAV security is done by using the ChaCha key generator as a stream chipper and using the Poly1305 authentication algorithm [8]. Security between Micro Air Vehicle (MAV) and GCS applies the Advanced Encryption Standard (AES) scheme in CTR mode for encryption, SHA-256 for key hashing and Diffie Hellman for key exchange of data transmission using MAVLink protocol [9]. In the research conducted by the author on the application of AES cryptography on UAVs and GCS contributed to making key algorithms that are only known by parties concerned with sending data using radio frequency.

Encryption is the process of securing information by making the information unreadable without special knowledge. At present, AES is a cryptographic algorithm that is safe enough to protect confidential data or information. In 2001, AES was used as the latest cryptographic algorithm standard published by the National Institute of Standards and Technology (NIST). AES algorithm is

a cryptographic algorithm that can encrypt and decrypt data with varying key lengths, namely 128 bits, 192 bits, and 256 bits, knowing that CBC mode is much better than ECB mode in terms of protection [10]. The results of research to encrypt and decrypt all types of files with the AES-256 algorithm, the results of the study show that the AES algorithm with a 256-bit key length can encode the contents of a file so as to secure the file [11], AES encryption can secure multimedia files, bitmap images , and other files [12] [13] [14]. Subsequent research explained that the use of MD5 in SSO encryption can still be hacked, whereas if implemented using AES with dynamic keywords, SSO cannot be hacked [15], subsequent studies can secure E-diplomas using digital signature authentication [16]. Thus it can be concluded that the AES algorithm can secure all types of files.

AES dengan panjang kunci 128 bit (AES-128) memiliki beberapa kelebihan dibandingkan dengan variasi kunci 192 bit dan 256 bit. Salah satunya adalah memiliki waktu proses yang paling cepat yaitu 110.78 ns[17]. Untuk melakukan *cracking* dengan menggunakan *brute force attack* pada AES-128 dibutuhkan waktu 〖1,02 x 10〗^18 Tahun[18]. Enkripsi AES dengan panjang kunci 128 bit cukup baik untuk dilakukan sebagai mana belum adanya *cryptanalysis* yang berhasil meretas AES[19].

Based on the above background, the professional UAV even if without the application of cryptography, then an attack can be carried out and from previous studies regarding the application of cryptographic algorithms applied to UAV and GCS, the AES-128 cryptography has never been applied. The author takes the theme of system security in Unmanned Aerial Vehicle (UAV) and Ground Control System (GCS) with the title "Implementation of AES Cryptography on Unmanned Aerial Vehicle and Ground Control System" as an application that will encrypt and decrypt data transmission between UAV and GCS.

1.1 Research Purpose and Objective

The purpose of writing this research is to build the application of encryption and decryption of data between UAV and GCS using the AES-128 algorithm. While the objective to be achieved from this research is to make the data sent by the Unmanned Aerial Vehicle to the Ground Control System unreadable by the attacker.

1.2 Research Methodology

The research methodology used in this study is divided into several stages. As shown in Figure 1, which is as follows.

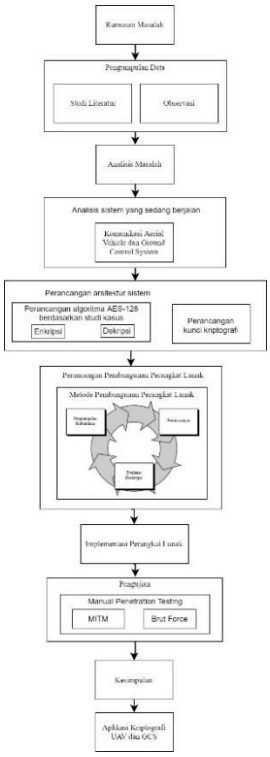

Figure 1. Research Methodology

A description of the steps of the research methodology contained in Figure 1 is as follows:

1. Problem Formulation: Problem formulation is a short sentence in the form of a question about the existence of an independent variable either only one or more variables, the problem formulation is used to explain the problem or issue under investigation.
2. Data Collection: The data collection method used in this study was carried out by literature study and observation.
3. Problem Analysis: The results of problem formulation and data collection produce problem analysis, problems can be validated for research.
4. Analysis of the Current System: At this stage, the current system needs to be analyzed for evaluation of the new system to be created.
5. System Architecture Design: At this stage a new system architecture is seen, which will be applied to UAVs and GCS. The system architecture will discuss new business processes.
6. Software Design: Software design is a gradual process whereby all the requirements or requirements contained in a document are translated into a blueprint that will be used to build software and meet the needs accordingly.
7. Software Development Method: Software development method uses prototype software paradigm. The flow of the prototype method can be seen in Figure 2 for an explanation of each plot prototype method is as follows [20]:

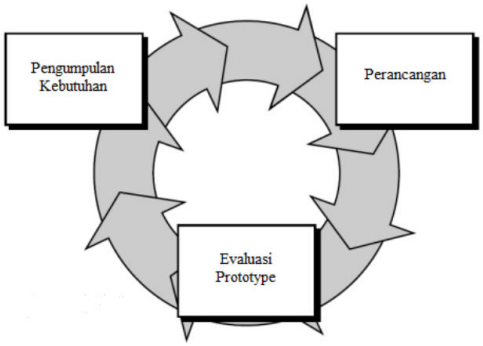

Figure 2. Model Prototype

Needs Collection - Data collection by collecting literature, journals, papers and readings that are related to the title of the study.

Design - The design is done quickly and the design represents all known aspects of the software. This design will be the basis for making a prototype.

Prototype Evaluation - Testing of software created and used to clarify software requirements.

8. Software Implementation: A process of changing system specifications into a system that can be run to be tested.
9. Testing: The test used is Manual penetration testing, namely penetration testing conducted by humans. In this type of testing, the vulnerability and risk of a machine is tested by an expert in its field [21]. In general, test technicians carry out the following methods:

   Data Collection −

   Data collection has an important role for testing. Someone can collect data manually or can use service tools / software (such as web page source code analysis techniques, man-in-the-middle attacks, etc.).

   Vulnerability Assessment − After the data is collected, the testers then identify security weaknesses and take the appropriate preventative measures.

   Actual Exploit − is a typical method used by expert testers to carry out attacks on the target system and also, reduce the risk of attack. In this study using a brute force attack.

   Report Preparation − After the penetration is done, experts prepare a final report that explains everything about the system. Finally the report is analyzed to take corrective steps to protect the target system.
10. Conclusion: Conclusion is a brief statement about the results of the analysis of the description and discussion of the contents of the research, the conclusion contains the facts answers to the questions in the research problem formulation..

2. Research Conten

2.1 Unmanned Aerial Vehicle (UAV)

UAV is short for Unmanned Aerial Vehicle, which is a pilotless aircraft. UAVs can be remotely controlled aircraft for example flown by pilots at ground control stations (GCS) or can fly independently based on pre-programmed flight plans or more complex dynamic automation systems [22].

2.2 Ground Control System (GCS)

The Gorund Control System was created to control and monitor flights, and to receive visualization and recording of images during the flight in realtime. Gorund control system is compatible with various types of UAVs [23].

2.3 Communication System (CS)

Communication System (CS) consists of a radio module system with an antenna at the desired gain (2 dBi, 10 dBi, 30 dBi) and frequency (900-922MHz, 2.4 GHz, 1.3 GHz) through serial communication. Radio Receiver is the basic part found on the ground. The system can be one-way or two-way communication that receives signals from the plane (UAV) to the ground (GCS) [24].

2.4 Cryptography

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, authentication, and data authentication [25].

Cryptography only fulfills four aspects in information security which is the purpose of cryptography, namely confidentiality, data integrity (integrity), data authentication (authentication), and non-repudiation [26].

1. Confidentiality is a service that is used to protect the contents of information from anyone except those who have the authority or secret key to open information that has been encrypted. Cryptography meets the confidentiality aspect because information cannot be directly known.
2. Data integrity is a service that deals with the maintenance of unauthorized data changes. To maintain data integrity, the system must have the ability to detect data manipulation by unauthorized parties, including the insertion, deletion and substitution of other data into actual data.
3. Authentication is a service related to identification / recognition, both as a whole system and the information itself. Two parties communicating with each other must introduce themselves. Information sent over the network must be authenticated, the contents of the data, the time of delivery, and so on. For this reason the cryptographic aspect is usually divided into two main classes namely entity authentication and original data authentication.
4. Non-repudiation is a service that prevents a denial of the delivery or creation of information by the person who sent or made it. For example, one entity may permit the purchase of property by another entity and then try to deny the

authorization granted. A procedure involving a trusted third party is needed to resolve the dispute..

2.5 Cryptographic Algorithm

A reliable cryptographic algorithm is a cryptographic algorithm whose strength lies in the key, not in the confidentiality of the algorithm itself. Based on the key types, cryptographic algorithms are divided into two types namely symmetric algorithms and asymmetric algorithms [26].

2.5.1 Symmetric Key Algorithm

The symmetric key algorithm (symmetric key algorithm) is an algorithm in which the encryption key used is the same as the decryption key so this algorithm is also called a single-key algorithm [26].

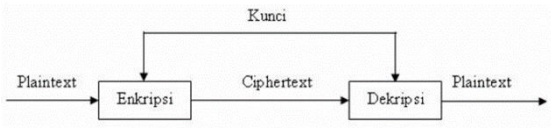

Figure 3. Cryptographic Illustrations with Symmetrical Keys.

2.5.2 Asymmetric Key Algorithm

Asymmetric key algorithm (asymmetric key algorithm) is an algorithm in which the encryption key used is not the same as the decryption key [26].

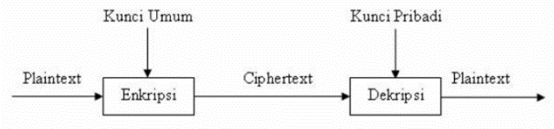

Figure 4. Cryptographic Illustrations with Asymmetric Keys.

2.6 Advanced Encryption Standard (AES)

Advanced Encryption Standard adalah cipher blok simetris yang bisa memproses blok data 128 bit, menggunakan kunci sandi dengan panjang 128, 192, dan 256 bit. Algoritma AES dapat digunakan dengan tiga panjang kunci yang berbeda yang ditunjukkan di atas, dan oleh karena itu "kunci" yang berbeda ini dapat disebut sebagai "AES-128", "AES-192", dan "AES-256".

Each state will undergo a process that consists of four stages, namely, Add Round Key, Sub Bytes, Shift Rows, and Mix Columns. Except in the Mix Columns stage, the other three stages will be repeated in each process while the Mix Columns stage will not be performed in the last stage [27].

2.6.1 ES algorithm encryption process

The AES algorithm encryption process consists of four types of bytes transformation, namely SubBytes, ShiftRows, Mixcolumns, and AddRoundKey. At the beginning of the encryption process, input that has been copied into the state will undergo an AddRoundKey byte transformation. Furthermore, the state will undergo Subbytes, ShiftRows, Mixcolumns, and AddRoundKey transforms as many times as Nr. The process in the AES algorithm is called the round function. The last round is different from the previous round where in the last round, the state did not undergo a MixColumns transformation [28]. Figure 2.3 is the steps for the AES encryption process.

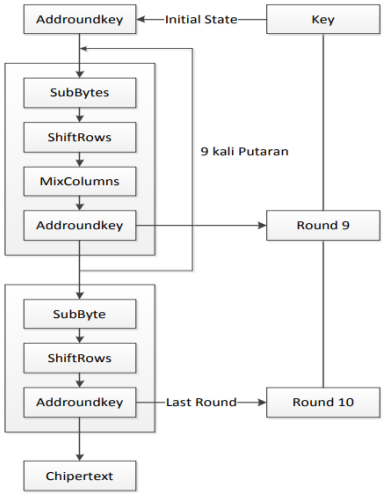

Figure 5. AES algorithm encryption process.

2.6.2 AES Algorithm Decryption Process

The cipher transformation can be reversed and implemented in the opposite direction to produce an easily understood inverse cipher for the AES algorithm. The byte transformations used in inverse ciphers are InvShiftRows, InvSubBytes, InvMixColumns, and AddRoundKey [28]. Figure 6 is the steps of the AES decryption process.

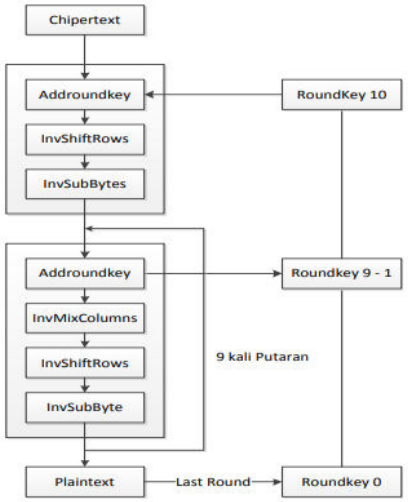

Figure 6. AES algorithm decryption process.

2.7 Sensor on UAV

1. Gyroscope is a device to measure or maintain orientation, with the principle of establishing angular momentum, this tool works in conjunction with an accelerometer. The

mechanism is a spinning wheel with a disc inside which remains stable. This tool is often used on robots or drones and other sophisticated tools.

2. A magnetometer is a sensor that works on the basis of detecting the earth's magnetic force. One of the uses of a magnetometer is to determine the direction of the wind. Magnetic sensors measure magnetic fields. By calculating the angle of the detected magnetic field of the earth, and comparing the angle of measurement with gravity measured with an accelerometer, it is possible to measure the direction of the device with regard to the North with a high degree of accuracy.
3. An accelerometer measures acceleration, which includes acceleration components with device motion and acceleration due to gravity. Accelerometers are also available with single, double or triple axes, which are defined in the coordinate system X, Y, Z. The complex movement period of the device can make orientation calculations difficult, especially during fast and complex motion, where the signal includes the sum of linear acceleration, centripetal acceleration, and gravity.

2.8 Problem analysis

Problem Analysis is the first step of system analysis. This step is needed to find out the problems that are happening in the current system. The following is the point of the problem in this study, namely the data sent by the UAV when cryptographic data has not been implemented yet can be read by the attacker because it is still in the form of plaintext, it is necessary to apply cryptography to secure the data from attack readings.

2.9 Analysis of Current Systems

Ongoing system analysis between UAV and GCS, aims to find out more clearly how the system works. From the sequence of events, an illustration can be made.

2.9.1 Analysis of Unmanned Aerial Vehicle Data Delivery and Ground Control System

In sending data does not have a protocol because the communication media uses radio frequency to transmit data in realtime.

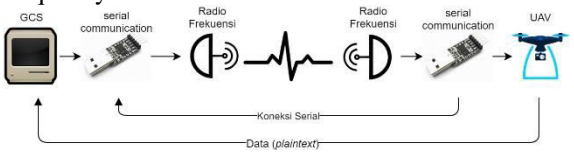

Figure 7. AES algorithm decryption process.

Figure 7 above explains how the data communication process can take place between the UAV and GCS. Where UAV and GCS use radio frequencies that have the same frequency. First GCS opens a serial connection after that the UAV boots automatically will open a serial connection, after connecting the UAV can automatically send data to GCS.

2.9.2 Analysis of Sensor Data Sent

Data obtained by sensors residing in the UAV will be transmitted and received by GCS. Following is table 1 results from observing data sent by UAVs to GCS.

Table 1. Table data sensor

No.	*Gyroscope*			*Magnetometer*			*Accelerometer*		
	xgyro	ygyro	zgyro	roll	pitch	yaw	xacc	yacc	zacc
1.	-1	0	0	-0.006028093	-0.003806141	0.1218428	-2	20	-1001
2.	0	1	0	-0.00604068	-0.003788484	0.1216723	-4	20	-997
3.	0	0	-1	-0.00609304	-0.003684698	0.1214509	-3	22	-998
4.	0	1	0	-0.00606191	-0.003721761	0.121368	0	21	-1001
5.	-2	0	0	-0.005961491	-0.003736289	0.1212841	-2	23	-997

2.10 Plain Text Analysis

From the sensor data table, it can analyze the plaintext that will be used as input for the system. Here is the plaintext data:

Table 2. Table data plaintext

Iterasi	*Plaintext*
1.	-1|0|0|-0.006028093|-0.003806141|0.1218428|-2|20|-1001
2.	0|1|0|-0.00604068|-0.003788484|0.1216723|-4|20|-997
3.	0|0|-1|-0.00609304|-0.003684698|0.1214509|-3|22|-998
4.	0|1|0|-0.00606191|-0.003721761|0.121368|0|21|-1001
5.	-2|0|0|-0.005961491|-0.003736289|0.1212841|-2|23|-997

2.11 Drone Analysis

The type of UAV used at the time of observation is in the form of a quadcopter drone, the drone has functions for system testing, flight training, or doing simulations, this drone is called a training drone.

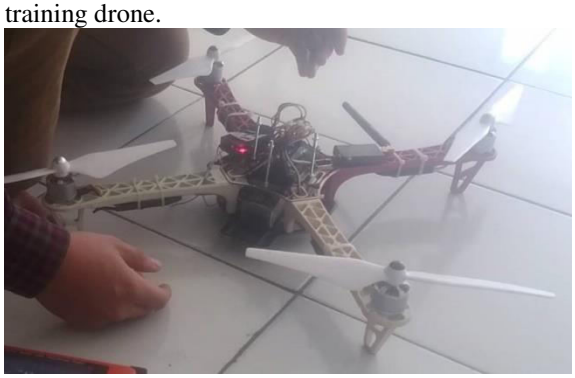

Figure 8. *Drone Quadcopter*

2.12 Analysis of Attack Methods

One method of attacking data transmission between UAVs and GCS is Man-in-the-Middle (MitM). MitM is a technique in network security where intruders place themselves in the middle of two or more devices that communicate with each other. In picture 9 is an illustration of the Man-in-the-Middle attack.

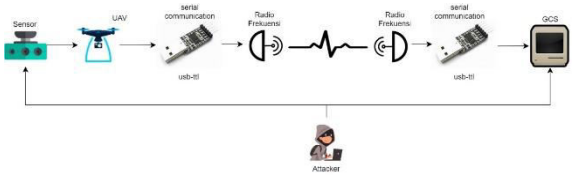

Figure 9. Man-in-the-Middle Process

Attacker can enter the system and retrieve data that is being sent [29].

2.13 AES Algorithm Analysis

2.13.1 Encryption Process

As an example the following case plaintext in the form of data from the magnetometer (roll) sensor and key using the date plus the reverse date :

Plaintext : -0.006028093
HEX : 2d 30 2e 30 30 36 30 32 38 30 39 33 30 30 30 30
Key : 3004201991024003
HEX : 33 30 30 34 32 30 31 39 39 31 30 32 34 30 30 33

Then the results obtained rounkey-1 to round key-10

36	04	3D	09
34	04	35	05
F3	C2	F2	C2
2C	15	27	14

RoundKey 2

5F	5B	66	6F
11	15	20	25
09	CB	39	FB
2D	38	1F	0B

RoundKey 3

64	3F	59	36
1E	0B	2B	0E
22	E9	D0	2B
85	BD	A2	A9

RoundKey 4

C7	F8	A1	97
EF	E4	CF	C1
F1	18	C8	E3
80	3D	9F	36

RoundKey 5

AF	57	F6	61
FE	1A	D5	14
F4	EC	24	C7
08	35	AA	9C

RoundKey 6

75	22	D4	B5
38	22	F7	E3
2A	C6	E2	25
E7	D2	78	E4

RoundKey 7

24	06	D2	67
07	25	D2	31
43	85	67	42
32	E0	98	7C

RoundKey 8

63	65	B7	D0
2B	0E	DC	ED
53	D6	B1	F3
B7	57	CF	B3

RoundKey 9

2D	48	FF	2F
26	28	F4	19
3E	E8	59	AA
C7	90	5F	EC

RoundKey 10

CF	87	78	57
8A	A2	56	4F
F0	18	41	ED
D2	42	1D	F1

Figure 10. Roundkey results

After going through several stages in the encryption process, the plaintext changes to chippertext, the results of the encryption process can be seen in Figure 11.

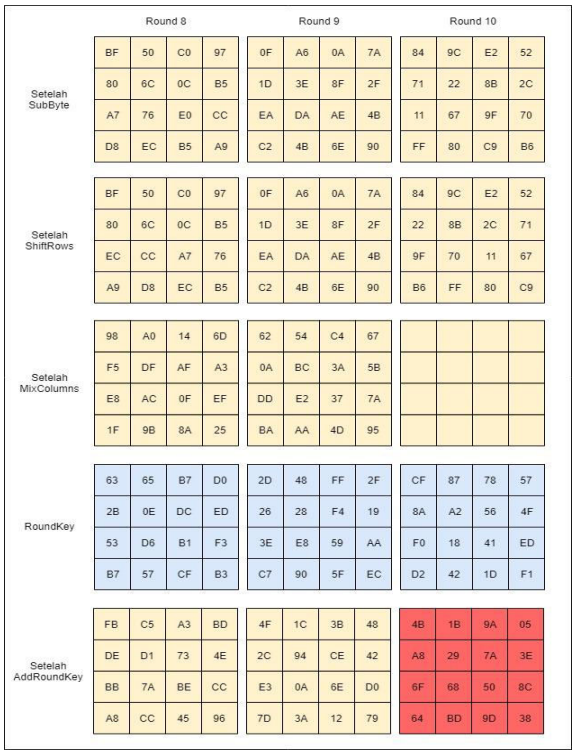

Figure 11. The end result is encryption

2.13.2 Decryption Process

The decryption process is changing the chippertext back into plaintext form, the final result of the decryption process is shown in Figure 12.

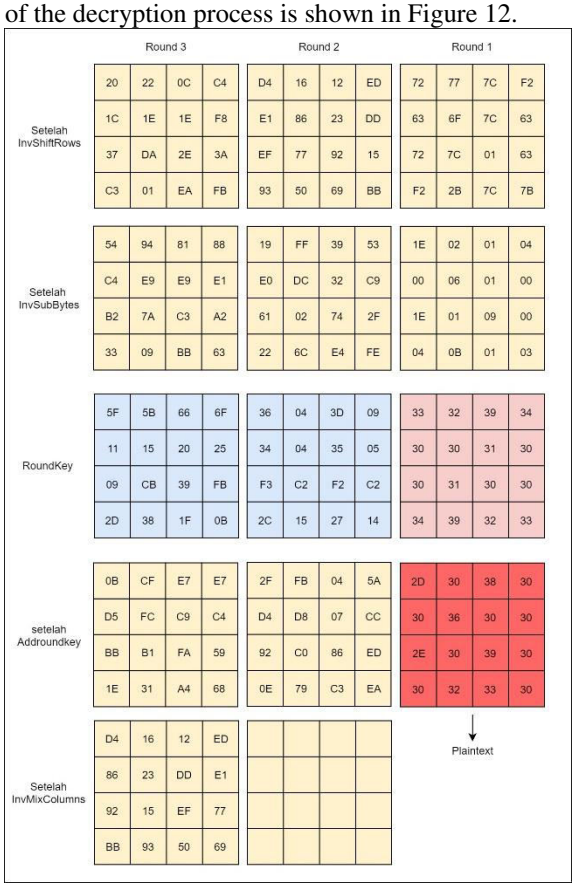

Figure 11. The final decryption result

2.14 Key Generation Analysis

For initial key initialization, with the date plus the date reversed Key = "date" + "reverse (date)", for example :

Key = “30042019” + “91024003” (1)

Key = “3004201991024003”. (2)

Table 3. example Key table

Iterasi	Key
1.	3004201991024003
2.	3004201991024004
3.	3004201991024005
4.	3004201991024006
5.	3004201991024007

2.15 Analysis of System Architecture to be Built

In the communication system between UAV and GCS that will be implemented there are two main functions namely encryption and decryption. System architecture in UAV and GCS cryptography is seen in Figure 12.

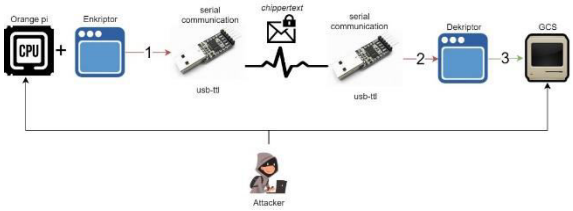

Figure 12. UAV and GCS cryptographic architecture

2.16 Functional Requirements Analysis

2.16.1 Use Case Diagram

The following use cases from UAV and GCS cryptographic applications can be seen in Figure 13.

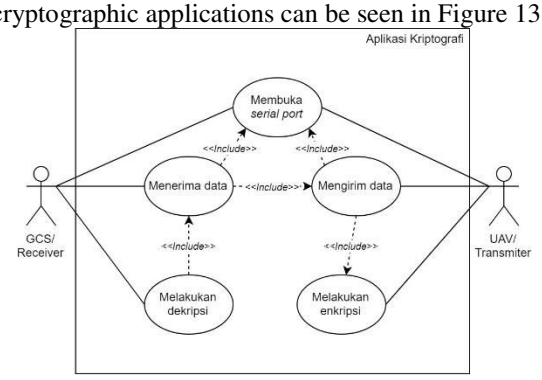

Figure 13. Use Case Diagram

2.16.3 Class Diagram

Following this class diagram of UAV and GCS cryptographic applications can be seen in Figure 15.

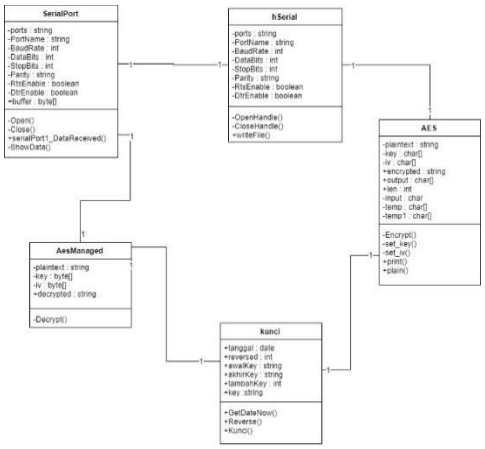

Figure 15. Class diagram

2.17 Interface Implementation

Following is the interface implementation of the UAV and GCS cryptographic applications can be seen in Figure 17.

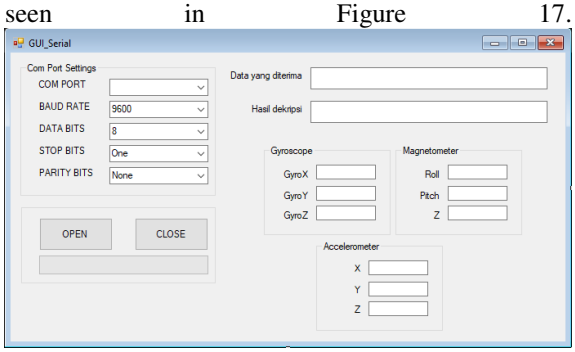

Figure 17. Interface Implementation

2.18 Testing

2.18.1 Manual Penetration Testing

In the testing phase, manual penetration testing is carried out [21] where the data collection is done by man-in-the-middle attack, vulnerability assessment analyzes the data obtained to find weaknesses while in the actual exploit stage is the brute force attack method, continued with report preparation that describes the results of the penetration carried out.

2.18.1.1 Man-in-the-Middle Attack

The purpose of this test is to determine the security level of each communication system between UAV and GCS. The test architecture used can be seen in Figure 18.

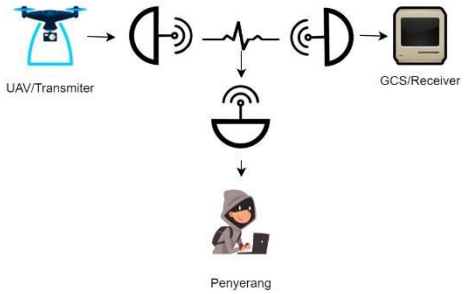

Figure 18. Scema testing MitM[29]

2.18.1.2 Results and Conclusions Man-in-the-Middle attack

Man-in-the-Middle attack test results are obtained based on testing that has been done.

Table 4. Man-in-the-Middle attack test results

No.	Testing scenario	Tapping Experiments	Data Results
1.	Do not use cryptography	Successful deposition	Can be known
2.	Use cryptography	Tapping successfully	Can not be known

2.18.2.1 Brute Force Attack

After the data is obtained, the actual exploit stage is the tester using the brute force method to launch an attack on the system. The author takes an article about "How secure is AES against brute force attacks?" With the following results [18] :

Tabel 5. *Key Size* dan *Combinations Key*

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^9
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

There is also the argument that 128-bit symmetric keys are computationally safe from brute-force attacks. Consider the following:

1. Faster supercomputer: 10.51 Pentaflops = 10.51 Pentaflops = 10.51 x 1015 Flops [Flops = Floating point operations per second]. (1)
2. Jumlah flops yang dibutuhkan kombinasi per cek: 1000. (2)
3. Number of check combinations per second = (10.51 x 1015) / 1000 = 10.51 x 1012.(3)
4. Number of seconds in one year = 365 x 24 x 60 x 60 = 31536000 seconds. (4)
5. Number of Years to break AES with a 128-bit Key

= (3,4 x 1038) / [(10,51 x 1012) x 31536000](5)
= (0,323 x 1026) / 31536000 (6)
= 1,02 x 1018 Year (7)
= 1 bilion bilion Year (8)

2.18.2.1 Brute Force Attack Results and Conclusions

With the combined calculations outlined, it will be very difficult to crack an AES-128bit key, and it can be concluded that AES-128bit is still safe to use even if it is attacked with brute forces even though.

3. Ending

3.1 Conclution

The conclusion of a study can be drawn after carrying out the process of implementation and testing. The following are some points that can be concluded in the study based on the results of the tests that have been obtained, the data obtained by the attacker using the man-in-the-middle attack method was successfully obtained, but the data cannot be read by the attacker because it has become a chippertext, whereas in testing brute-force attack to crack an AES-128bit key is not possible, so security using AES-128 cryptography is still appropriate to use today, until a super computer is found that is faster than 10.51×10^{15} Flops.

3.1 Suggestion

Suggestions in this study are useful for developing applications that are made. The suggestion for application development is to choose the first key combination that will be used because it will have an impact on the key combination on the 1st, 2nd loop, etc. Therefore the need for a difficult key combination.

REFERENCES

[1] R. Shofiyanti, "Teknologi Pesawat Tanpa Awak Untuk Pemetaan Dan Pemantauan Tanaman Dan Lahan Pertanian," Inform. Pertan., vol. 20, no. 2, pp. 58–64, 2011.

[2] Wikantika. K. 2009. Unmanned Mapping Technology: Development and Applications. Workshop Sehari "Unmanned Mapping Technology: Development and Applications" (UnMapTech2008). Bandung, Indonesia. 9 Juni 2008.

[3] A. A. Farghani, R. Sumiharto, and S. B. Wibowo, "Purwarupa Ground Control System untuk Pengamatan dan Pengendalian Unmanned Aerial Vehicle Bersayap Tetap," Indones. J. Electron. Instrum. Syst., vol. 3, no. 1, pp. 1–10, 2013.

[4] N. Rodday, "Exploring Security Vulnerabilities of Unmanned Aerial Vehicles," no. Noms, p. 95, 2015.

[5] D. H. B, J. Lee, D. Kim, D. Kwon, K. H. Ryu, and D. Lee, "LEA : A 128-Bit Block Cipher for Fast Encryption on Common Processors," vol. 1, pp. 3–27, 2014.

[6] I. Avdonin, M. Budko, M. Budko, V. Grozov, and A. Guirik, "A method of creating perfectly secure data transmission channel between unmanned aerial vehicle and ground control station based on One-Time pads," Int. Congr. Ultra Mod. Telecommun. Control Syst. Work., vol. 2017–November, pp. 410–413, 2018.

[7] B. S. Rajatha, C. M. Ananda, and S. Nagaraj, "Authentication of MAV communication using Caesar Cipher cryptography," 2015 Int. Conf. Smart Technol. Manag. Comput. Commun.

Control. Energy Mater. ICSTM 2015 - Proc., no. May, pp. 58–63, 2015.
[8] M. Podhradsky, C. Coopmans, and N. Hoffer, “Improving communication security of open source UAVs: Encrypting radio control link,” 2017 Int. Conf. Unmanned Aircr. Syst. ICUAS 2017, pp. 1153–1159, 2017.
[9] N. Prapulla, S. Veena, and G. Srinivasalu, “Development of algorithms for MAV security,” 2016 IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. RTEICT 2016 - Proc., pp. 799–802, 2017.
[10] J. Thakur and K. Nagesh, “DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis,” Int. J. Emerg. Technol. Adv. Eng., vol. 1, no. 2, pp. 6–12, 2011.
[11] V. Yuniati, G. Indriyata, and A. C Rachmat, “Enkripsi Dan Dekripsi Dengan Algoritma Aes 256,” J. Inform., vol. 5, no. 1, pp. 23–31, 2009.
[12] A. Rosyadi, “Implementasi Algortma Kriptografi AES Untuk Enkripsi dan Dekripsi Email,” Transient, pp. 1–6, 2012.
[13] G. W. Bhaudhayana, I M. Widiartha, “Implementasi Algoritma Kriptografi AES 256 dan Metode Steganografi Lsb pada Gambar Bitmap” 16 Jurnal Ilmu Komputer Vol.VIII, No. 2, September 2015, hlm.15-25
[14] N. B. Tampubolon, R. R. Isnanto, and E. W. Sinuraya, “Implementasi Dan Analisis Algoritma Advanced Encryption Standard (Aes) Pada Tiga Variasi Panjang Kunci Untuk Berkas Multimedia,” Transient, vol. 4, no. 4, 2015.
[15] Z. Musliyana, T. Y. Arif, and R. Munadi, “Peningkatan Sistem Keamanan Autentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia,” J. Rekayasa Elektr., vol. 12, no. 1, p. 21, 2016.
[16] Finandhita, A., dan I. Afrianto “Development of E-Diploma System Model with Digital Signature Authentication Development of E-Diploma System Model with Digital Signature Authentication,” pp. 0–6, 2018.
[17] M. Gupta, S. Mahto, and A. Patel, “Advanced Encryption Standard on Reconfigurable Logic,” vol. 50, no. 6, pp. 305–309, 2017.
[18] How secure is AES against brute force attacks?, 10 Juni 2019 [Online]. Available: https://www.eetimes.com/document.asp?doc_id=1279619
[19] Does Size Matter? AES 128-Bit Encryption is (Probably) Good Enough, 10 Juni 2019 [Online]. Available: https://security-architect.com/does-size-matter-aes-128-bit-encryption-is-probably-good-enough/
[20] R. S dan M. Shalahuddin. Rekayasa Perangkat Lunak. Informatika. 2013.
[21] tutorialspoint (2017, Jul.8) Penetration Testing - Manual & Automated [online]. Available : https://www.tutorialspoint.com/penetration_testing/penetr ation_testing_manual_automated.htm
[22] The UAV - Unmanned Aerial Vechile, 4 Maret 2019 [Online]. Available: https://www.theuav.com/
[23] Ground Control Station (GCS), 4 Maret 2019 [Online]. Available: http://a-techsyn.com/gcs/
[24] Communication System (CS), 4 Maret 2019 [Online]. Available: http://a-techsyn.com/gcs/cs/
[25] Kim, David, dan Michael G Solomon. 2012. Fundamentals of Information Systems Security. Jones & Bartlett Learning, United State of America.
[26] Munir, Rinaldi. Kriptografi. Informatika, Bandung. 2006.
[27] F. Information, “Announcing the ADVANCED ENCRYPTION STANDARD (AES),” 2001.
[28] Setyaningsih, Emy. Kriptografi & Implementasinya menggunakan MATLAB. Andi, Yogyakarta,2015.
[29] A. Setiyadi, “Implementasi Modul Network MITM Pada Websploit sebagai Monitoring Aktifitas Pengguna dalam Mengakses Internet,” vol. 2017, pp. 113–120, 2017.