International journal of science, engineering, and information technology
Volume 01, Issue 01, July 2017
Journal homepage: https://journal.trunojoyo.ac.id/ijseit

Comparative Analysis of AES-Turbo Code Combination Encryption Method on Three Variations AES Key

Rendra Bayu Adi S

Department of Informatics Engineering, Bangkalan, Indonesia

ABSTRACT

Data communication is a process of sending information from two or more points using a binary code. In data communication sometimes it does not run smoothly, while the obstacle in the process of sending information is data theft until data damage Information is exposed to noise in the process. Therefore we need an application that can provide information security and at the same time avoid damage to data due to noise. One such application is to combine AES cryptographic techniques with forward techniques error correction in the form of Turbo code. This study aims to combine the two techniques and apply to text data and analyze based on the length of the encryption key owned by AES. The analysis shows that the AES-turbo cryptographic combination algorithm can work optimally with the percentage of data returned 100% at the SNR of 15 dB. In testing the avalance effect also shows that a 256-bit key length is safer, this is evidenced by the Avalanche Effect trial of 24.77362%. But in testing the data execution time, the longer the key the longer it takes for encryption and decryption. Thus for the selection of 3 key variations of AES that are more efficient and effective, that is by using a 128-bit key.

Keywords: AES, Turbo code, AES-Turbo.

Article History
Received 12 February 16 Received in revised form 16 February 17 Accepted 03 May 17

1. Introduction

Sending or exchanging data is things that often happen in the world information technology [1]. Development rapid delivery or data exchange has an impact big, namely data security issues sent [2]. Data sent sometimes often containing important information data even very secret and must be maintained its safety. Data sending done through communication services cyberspace, usually a threat occurs so much crime. With the threat of crime such as interception, consequently data can fall on unauthorized people even data will be misused by unauthorized party [1]. other than that sometimes in data communication noise in the form of noise (3) so the data sent is vulnerable to damage. Data damage here i.e in the form of reduced or added bits the bit in the data that causes the data it was not like before sending.

To overcome some of the problems above can be done by applying a combination of cryptographic and techniques FEC (Forward Error Correction). The combination used is AES (Advanced Encryption Standard) As cryptographic techniques and Turbo Code as FEC (Forward Error Correction). AES is encryption that uses symmetric key. This standard consists of 3 block ciphers, namely AES-128, AES-192 and AES-256, which was adopted from that collection the larger one that was originally published as Rijndael. Each cipher has a 128-bit size, with a size keys are 128, 192, and 256, respectively bit [4]. Whereas Turbo Code is one of the FEC (Forward Error Correction) methods.

FEC is a method that is able to correct errors from information which is transmitted. Correction of errors is done by using coding techniques before the data is sent and before the data is received [5]. AES combination method and Turbo Code it has been studied before, namely research from Hakan CAM, Volkan OZDURAN and Osman N. UCAN named AES-Turbo. In this study explained that the two techniques can be combined by placing the turbo encoder in AES encryption in the first iteration after SubBytes and placing the decoder turbo in the AES decryption in the last iteration before SubBytes so that the process is not mutually exclusive or becomes an entity [6]. The AES-Turbo combination becomes safer because there is an encoder added to the encryption process.

This encoder also functions as an error correction as well as scrambling the bits after SubBytes. In this study, the authors used the method on the encryption side to analyze the comparison of these combinations against three key variations of AES with the test parameters namely the time required for encryption & decryption (data execution time), avalanche effects and BER (Bit Error Rate).

* *Corresponding author.*
E-mail address: 120411100038@student.trunojoyo.ac.id.

E-ISSN 2548-4214

2. Literature Review

2.1. Advanced Encryption Standard (AES)

AES is a type of cryptographic technique established by the United States standard institution called NIST (National Institute of Standards and Technology). In 2001 NIST finally published AES as a document processing standard on the FIPS-PUB 197 document. AES used a component always has an inverse with a 128-bit block length. AES key can have a key length of 128, 192,256 bits. AES encoding uses an iterative process called round. The number of rounds used by AES depends on the length of the key used. Round keys are generated based on key ones given [10]. AES supports key lengths of 128 bits to 256 bits. The key length and block size can be chosen independently, and each block is encrypted for a certain number of turns.

AES decryption algorithm is as follows first addRoundKey: X-or between states initial (ciphertext) with a cipher key. Step this is also called the initial round. Round of Nr - 1 time. That process sperformed on each round are. InvShiftRow: shift array rows wrapping state. InvSubByte: substitution of bytes with using the Inverse S- substitution table box. AddRoundKey: performs an X-or operation between the current state and the round key. InvMixColumn: randomize data on each column state array. Final round: the process for the last round:

- InvShiftRow.
- Inv SubByte.
- AddRoundKey

2.2. Turbo Code

In 1993, Berrou, and Glavieux Thitimajshima developed a canal coding techniques corrects signal errors that have been received at the receiver. Coding technique this is called Turbo Code. Turbo Code is a new paradigm for forward error-correction. This turbo code works achieve error correction performance approaching the limits of Shannon's theory. For BER value (bit error rate) 10−5 and rate code ½ required Eb / No equal to 0.7 dB [11].

The encoder consists of two encoders Recursive Systematic Convolutional (RSC) that is identical connected parallel and the second RSC encoder previously passed to a inter layer. Then the results of both The encoder is punctured, then in multiplex with information input. In the decoder, it consists of two decoders log-MAP that is connected in parallel.

Log-MAP 1 decoder input is a bit systematically received from a canal has disturbed noise $yk\ s$, redundant bit parity $yk\ p$ and feedback from the results log-MAP decoder 2 [11]. An outline of the turbo code process can be seen in Figure 1 for the encoder and 2 for decoders.

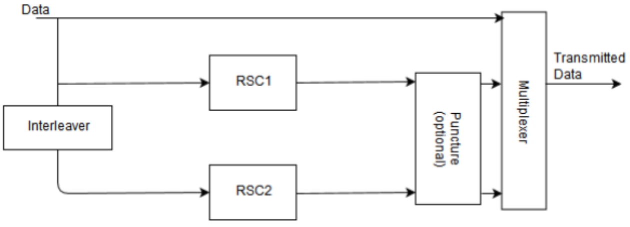

Figure 1. Turbo code encoder

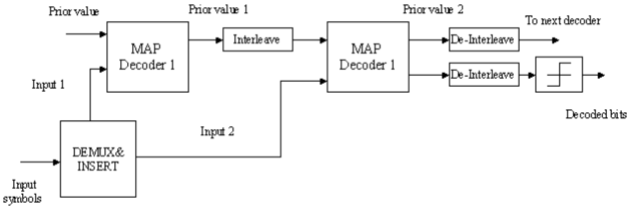

Figure 2. Turbo code decoder

3. Methods

On the encryption side there is a turbo encoder placed after sub bytes in the first iteration. In looping the first iteration of the data is entered into turbo encoder, so output data it is doubled from the data before entering the turbo encoder. Then the encoder output data it will be queued per 128 bits (in accordance with AES provisions) and at process until it becomes ciphertext, after the next 128 bits will be processed too until it becomes ciphertext and combined with the initial ciphertext. After that the bit stream is sent through wireless.

On the decryption side, the data is processed is ciphertext with a length of 256 bits (twice the length of the initial data). Then ciphertext will be processed per 128 bits and carried out the same process to Next 128 bit ciphertext. Before entering the data decoder turbo queued per 128 bits and then joined back to 256 bits and processed turbo decoder so that it becomes data 128 bit.

4. Result

Tests are carried out to see the time required for encryption & decryption (data execution time), avalanche effects and BER (Bit Error Rate).

4.1. BER performance against SNR

This trial shows the performance of BER through the ideal channel and AWGN for SNR values of 5 dB - 15 dB. This trial was conducted with 2721 characters of input data (equivalent to 1 page article), key length (128-bit, 192-bit, 256-bit), and 1 iteration.

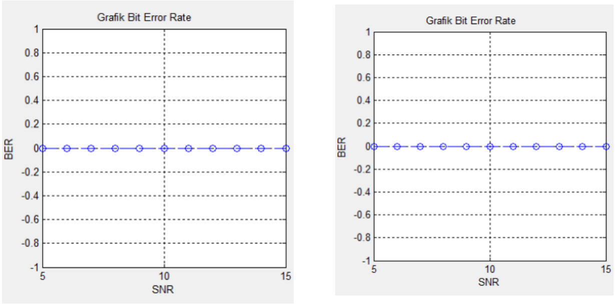

Figure 3. **(a)** with 128-bit key; **(b)** with 128-bit key.

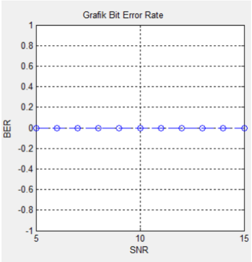

Figure 3. (c) with 256-bit key

In figure Figure 3 we can see Graph BER data text on the Ideal channel.

In Figure 4 it can be seen that the performance of BER on an ideal channel is a straight line with a Bit Error Rate value of 0 which means there is no noise in the information sent. Figure 4 BER graph in text on AWGN channel

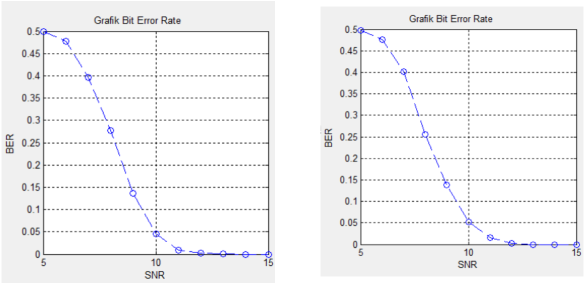

Figure 4. (a) with 128-bit key; **(b)** with 128-bit key.

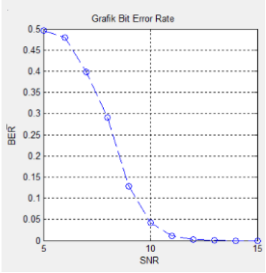

Figure 4. (c) with 256-bit key

Figure 4. shows a decrease in the bit error rate (BER) at SNR of 6 dB and stops at SNR of 13 dB, which means that at SNR more than 13 dB above data which before encryption can match the data after decryption even though it is exposed to AWGN noise.

From the data in Figure 4. the percentage of data that has been calculated is returned and is represented in Table 1.From table 1 we can see the data execution time,

- The longer the key the longer the time needed for encryption and decryption,
- The longer the data the longer the time needed for encryption and decryption,
- The time required for decryption is longer than the time required for encryption, with an average selection of 9,1878 sec.

Table 1. AES execution test table Turbo

Scenario	Key Length	Size (characters)	Time (sec)	
			Encription	Decription
		2721	40.287	42.6001
1	128	5388	71.9148	77.5686
		7826	134.252	147.08
		2721	42.3097	85.082
2	192	5388	78.5176	160.437
		7826	142.238	50.8395
		2721	46.3046	93.319
3	256	5388	83.868	93.319
		7826	156.692	177.139

5. Conclusion

From the results of research that has been done, conclusions can be drawn as follows:

- Data text (plaintext) is encrypted (ciphertext) then added noise AWGN can be decrypted back into data text (plaintext) using SNR ⩾ 15 dB.
- AES-Turbo cryptographic algorithm combination by using 3 key variations it was found that 256-bit key was safer, this is evidenced by the Avalanche trial Effect of 24.77362%. Then for encryption and decryption time in combination AES-Turbo cryptographic algorithm, increasingly key length the longer the time needed for encryption and decryption. Thus for the selection of 3 variations AES key is more efficiency and effectiveness namely by using a 128-bit key.

References

[1] Widarma, A. Kombinasi Algoritma AES, RC4 dan Elgamal dalam Skema Kriptografi Hybrid untuk Keamanan Data.Universitas Sumatera Utara.2016

[2] Kalangi, J, A. Pembuatan Aplikasi Steganography pada File Audio Mp3 dengan Metode Parity Coding.Universitas Kompter Indonesia.2010

[3] Kuswanto, Dwi. Unjuk Kerja Turbo Code pada Kanal Flat Fading. Institut Teknologi Sepuluh Nopember. 2004.

[4] National Institute of Standards and Technology. 2000. Advanced Encryption Standard, FIPS-197.

[5] Setiawan, E, F.Simulasi Kode Hamming, Kode BCH, dan Kode Reed-Solomon untuk Optimalisasi Forward Error Correction.Universitas Muhammadiyah Surakarta. 2014

[6] CAM, Hakan., OZDURAN, Volkan., Osman N. UCAN. A combined encryption and error correction scheme: AES-Turbo. Journal of electrical & electronics engineering, 1: 861-866. 2009.

[7] Darwis, Fajri. Analisis Performansi BER dengan Pengkodeaan Concatenated Viterbi / Reed-Solomon dan Turbo pada Jaringan VSAT untuk Hubungan antar BTS dan BSC. Universitas Indonesia. 2008.

[8] Marisman, Aji Fitrah, dan Hidayati, Anita. Pembangunan aplikasi pembanding kriptografi dengan Caesar chipper dan Advance Encryption Standard (AES) untuk file teks. Jurnal Penelitian Komunikasi dan Opini Publik, 19.3 . 2015.