Performances Combination Schemes AES - Turbo Code Based-on Keys Length

Dwi Kuswanto
Department of Informatics Engineering, Engineering Faculty, University of Trunojoyo Madura, Bangkalan, Madura, dwi.kuswanto@trunojoyo.ac.id

Abstract. In data communication the process of sending data in the form of information is susceptible to theft, destruction, modification or repetition of the data sent which causes information to be changed / corrupted according to the original data. One way to guarantee authenticity can be done by utilizing security techniques in the process of sending data, one of which is by using a combination of cryptographic and error correction techniques, namely AES and Turbo Code. This study aims to combine the two techniques and apply them to text data by evaluating based on the length of AES encryption keys. Performance results indicate that AES-Turbo cryptographic combination algorithms can work optimally at SNR greater than or equal to 15 dB, for the best test value for avalanche effects is 24.77 % at 256-bit key lengths and the testing data execution time with an average time of 9.19 seconds, the time required for decryption is longer than the time needed for encryption, and the longer the key the longer it takes for encryption and decryption. For selection of keys length of AES more efficiency and effectiveness that is by using 128-bit key

Keywords: AES, Turbo Code, AES-Turbo Code

1. Introduction

Rapid development in the process of sending or exchanging data brings a great impact, namely the problem of data security [2]. The transmitted data contains highly confidential information and must be kept secure. Delivery of data made through cyberspace communication services, vulnerable the occurrence of threats of crime. With the threat of crimes such as interception (wiretapping), consequently the data can be misused by unauthorized parties [1]. Also in data communication there are other disturbances in the form of noise (noise) [3], so the data sent vulnerable the occurrence of damage. Damage data here can be a reduction or addition of bits in the data that causes the data to change from the original data.

To solve the above problem can be done by applying a combination of cryptography techniques (AES) and Forward Error Correction (FEC) with Turbo Code. AES is an encryption technique that uses symmetric keys. This standard consists of 3 blocks of ciphers, namely AES-128, AES-192 and AES-256 which are adopted from Rijndael. Each cipher has a 128-bit size, with key sizes of 128, 192, and 256 bit [4], respectively. In this study, the authors analyzed the combination of these three AES key variations with test parameters ie time required for encryption and decryption (time of data execution), avalanche effects and BER (Bit Error Rate).
2. Theory

2.1 Advanced Encryption Standard (AES)

AES is a type of cryptographic technique established by a US 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 uses components that always have an inverse with a block length of 128 bits. AES keys can have a key length of 128, 192, 256 bits. AES encryption uses a repeating process called round. The number of rounds used by AES depends on the length of the key used. The round key is generated based on a given key [7]. AES supports 128 bit key lengths up to 256 bits. The key length and block size can be independently selected, and each block is encrypted for a certain number of rounds.

| Type    | Key Length | Block Size | Number of Round (Nr) |
|---------|------------|------------|----------------------|
| AES – 128 | 128 bit    | 128 bit    | 10                   |
| AES – 192 | 192 bit    | 128 bit    | 12                   |
| AES – 256 | 256 bit    | 128 bit    | 14                   |

An Outline of AES algorithm AES can be seen on figure 1.

![Figure 1 Algorithm Encryption and Decryption AES][7]

2.2 Turbo Code

Turbo Code is a new paradigm for forward error-correction. This turbo code succeeded in achieving error correction performance near the boundaries of Shannon's theory. For the BER $10^{-5}$ and ½ code rate required Eb / No of 0.7 dB [8]. An outline of the process turbo code seen on figure 2.
2.3 Avalanche Effect

Avalanche Effect, is one way to determine whether or not its a cryptographic algorithm, which will be known how much bit changes that occur in the ciphertexts due to the encryption process. The greater the avalanche effect the better the cryptographic algorithm [1]. How to calculate the avalanche effect as follows:

\[
Avalanche\;Effect = \frac{\sum \text{perubahan bit ciphertext}}{\sum \text{Keseluruhan Bit ciphertext}} \times 100\% \quad (1)
\]

2.4 Bit Error Rate (BER)

Bit Error Rate is the number of bits received from the data stream through a communication channel that has changed due to noise. High BER indicates that the information received on the receiver side undergoes many changes during transmission. The BER percentage is calculated based on the ratio between the number of bit errors and the total number of bits [3].

\[
\text{Bit Error Rate} = \frac{\sum \text{Bit salah}}{\sum \text{Bit diterima}} \quad (2)
\]

2.5 Signal to Noise Ratio (SNR)

SNR is the ratio of the received signal to the surrounding noise (noise) with decibels (dB) [3]. SNR is measured in decibels (dB) and defined by the formula [3]:

\[
\text{SNR (dB)} = 10 \log_{10} \left( \frac{P_{\text{signal}}}{P_{\text{noise}}} \right) \quad (3)
\]

3. Design System

In AES-Turbo Encryption, there are 5 stages, including Plaintext input, key input, Key expansion, Encryption, CipherText output. In AES-Turbo Decryption, there are 5 stages, including CipherText input, key input, Key expansion, Decryption, PlainText output.

Scenario testing is done by running the program with text input using 3 key variations (128-bit, 192-bit, 256-bit). There are three tests that are Bit Error Rate, Avalanche Effect, Data Execution Time.

4. Implementation System and Analisys

4.1 Performance BER vs SNR

This experiment shows the performance of BER through ideal channel and AWGN for SNR values 5 dB - 15 dB. The test was performed with 2721 characters of input data (key length (128-bit, 192-bit, 256-bit), and 1 iteration (fig 5).
Figure 3 Combination Process of AES-Turbo Cryptography algorithm

Figure 4 Flowchart simulation application combination of AES-Turbo cryptography algorithm
In Figure 5 shows that the performance of BER to the ideal channel in the form of a straight line with the value of Bit Error Rate of 0 which means no noise on the information transmitted.

Figure 6 shows a decrease of error bit rate (BER) at SNR of 6 dB and stops at SNR 13 dB, which means at SNR more than 13 dB and above data which before encryption can match data after being decrypted in spite of AWGN noise, while at SNR 15 dB visible overall return data of 100%.

### 4.2 Experiment Time Execution

This experiment is done by comparing execution time to key length. This trial was conducted with data input as much as 2721, 5913 and 8271 (character), SNR 15 dB, and 1 iteration. Then the execution time can be seen in table 2.

| Scenario | Keys Length | Size (Character) | Time (sec) | Encryption | Decryption |
|----------|-------------|------------------|------------|------------|------------|
| 1        | 128-bit     | 2721             | 40.2879    | 42.6001    |
|          |             | 5388             | 71.9148    | 77.5686    |
|          |             | 7826             | 134.252    | 147.08     |
| 2        | 192-bit     | 2721             | 42.3097    | 46.4917    |
|          |             | 5388             | 78.5176    | 85.082     |
|          |             | 7826             | 142.238    | 160.437    |
| Scenario | Keys Length | Size (Character) | Time (sec) Encryption | Time (sec) Decryption |
|----------|-------------|------------------|-----------------------|-----------------------|
| 3        | 256-bit     | 2721             | 46.3046               | 50.8395               |
|          |             | 5388             | 83.8681               | 93.319                |
|          |             | 7826             | 156.692               | 177.139               |

The time required for decryption is longer than the time required for encryption that is with an average of 9.19 sec.

4.3 Experiment Avalanche Effect

The following is the results of Avalanche Effect testing and the average based on the key length, can be seen in table 3.

Table 3 Average Avalanche Effect Experiment

The slight differences in avalanche effect and the long time difference in the 256-bit key to 128-bit, it can be concluded that for the selection of 3 AES key variations more efficiency and effectiveness is by using 128-bit keys.

5. Conclusion

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

(1) Text data (plaintext) is done encryption (chipertext) then added AWGN noise can be decrypted back into text data (plaintext) by using SNR ≥15 dB.

(2) The combination of AES-Turbo cryptographic algorithms using three key variants found that 256-bit keys were safer, with Avalanche Effect testing of 24.77%. Then for the time of encryption and decryption on a combination of AES-Turbo cryptographic algorithms with an average of 9.19 sec, the longer the key the longer it takes for encryption and decryption.

(3) For selection of 3 key variations of AES more efficiency and effectiveness that is by using 128-bit keys.

6. 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 Komputer 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] 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.
[6] Tampubolon, N. B., Isnanto, R. R., Sinuraya, E. W. Implementasi dan Analisis Algoritma Advanced Encryption Standard (AES) pada Tiga Variasi Panjang Kunci untuk Berkas Multimedia. *TRANSIENT* 4.4 .2015.

[7] Sadikin, R. 2012. *Kriptografi Untuk Keamanan Jaringan*. Yogyakarta: Andi Publisher

[8] Bayu, Rendra, Comparatives Analysis of AES-Turbo Code Combination Encryption Methods on three variation AES Key. Vol 1 Issue 1, *IJSEIT*, 2017.