PERFORMANCE ANALYSIS OF AES VS. TDEA

R.N.B. Herath, T.M.S. Buddika
Supervised by: Dr. Roshan Ragel and Mr. C.A. Munasinghe
Department of Computer Engineering - University of Peradeniya - Sri Lanka

Abstract
Advanced Encryption Standard (AES) and Triple Data Encryption Algorithm (TDEA) are two of the most widely used symmetric key cryptographic algorithms of this era. TDEA is more established due to its roots in DES (Data Encryption Standard) while AES has been proved more secure by numerous researches and studies. Our study analyses the speeds of operations of AES vs. TDEA under varying conditions.

1. Introduction
AES [1] specifies the Rijndael algorithm [2], a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. The different variations of the algorithm when used with the three different key lengths indicated above are referred to as “AES-128”, “AES-192”, and “AES-256”.
TDEA [3] is so named because it applies the Data Encryption Standard (DES) [4] algorithm three times to each data block. It consists of three DES keys (K1, K2, and K3) each with an effective length of 56 bits. The National Institute for Standards and Technology (NIST) approves two keying options where, (1) K1, K2 and K3 are independent keys; (2) K1 and K2 are independent keys and K3 = K1.
The NIST states that through the year 2030, TDEA and the AES will coexist as Federal Information Processing Standards (FIPS) approved algorithms – thus, allowing for a gradual transition to AES. Speed benchmarks for AES and TDEA can be found under Crypto++ 5.6.0 Benchmarks [5]. Our study is more concentrated on comparing AES and TDEA over a wider data range and considers all NIST approved confidentiality modes of operation [6] – ECB, CBC, OFB, CFB and CTR.

2. Design and Implementation
Both algorithms, AES and TDEA, were implemented using the Java Cryptography Extension. Standard code segments were used for encryption and decryption. Tests were conducted for the following two scenarios.
- Local Encryption/Decryption
  Data on a host were encrypted and decrypted locally using variants of the two ciphers.
- Transferring Encrypted data over a LAN
  Data in a client machine were encrypted using variants of the two ciphers and streamed out to a server machine where the stream was decrypted.

The Local Encryption/Decryption tests were conducted with sun jre1.6.0_02 on a Microsoft Windows XP Professional platform with an Intel(R) Core(TM)2 Duo CPU T5670 @ 1.80GHz and 1024MB of physical memory at 667MHz. Java time calculations give 15ms accuracy for this system.
The above machine was also used as the client in Transferring Encrypted data over a LAN tests. The server had an Intel(R) Core(TM)2 Duo CPU E7300 @ 2.66GHz with 2048 MB of physical memory at 667 MHz. The server used an Openjdk-6-jre version 6b12-0ubuntu6.4, on an Ubuntu 8.10 platform. Java time calculations give 1ms accuracy for this system.
We conducted the Local Encryption/Decryption tests over three data ranges – 200KB to 1000KB in 100KB
increments, 1MB to 10MB in 1MB increments and 10MB to 100MB in 10MB increments. Only the 1st and 2nd data ranges were tested for Transferring Encrypted data over a LAN. Both test scenarios involved AES-128, AES-192, AES-256 and the two keying options of TDEA subject to the five confidentiality modes of operations.

3. Results
In Local Encryption/Decryption, all modes take the same basic shape for all data ranges: approximately linear with a clear, significant difference between AES and TDEA.

![Figure 1: Local Encryption with OFB Mode for 200KB – 1000KB Data](image1)

![Figure 2: Local Decryption with ECB Mode for 1MB – 10MB Data](image2)

![Figure 3: Local Decryption with CFB Mode for 10MB – 100MB Data](image3)

![Figure 4: Server Decryption with CBC Mode for 200KB – 600KB Data](image4)

![Figure 5: Server Decryption with CFB Mode for 600KB – 1000KB Data (Zoomed in View)](image5)
Figure 6: Server Decryption with OFB Mode for 1MB – 5MB Data (Zoomed in View)

Figure 7: Server Decryption with CTR Mode for 5MB – 10MB Data (Zoomed in View)

Figure 4 depicts the average time taken by the cipher variants operating in CBC mode in the 200KB – 1000KB data range. Figures 5 through 7 provide zoomed in views of decryption times taken for CFB, OFB and CTR modes different data ranges.

4. Discussion

In Local Encryption/Decryption if we consider AES alone, greater speeds can be observed for smaller key lengths. This is due to the fact that AES-128, AES-192 and AES-256 go through 10, 12 and 14 rounds respectively.

The speeds of the two TDEA variants are approximately equal. This can be explained by the following two facts: The number of rounds for both keying options are equal (48 rounds) and the total number of key bits for both keying options is equal-168 bits.

For all variations of the ciphers, AES is always faster than TDEA in all data ranges with no overlapping or intersections between the curves.

In Transferring Encrypted data over a LAN tests the speed difference between AES cipher variants and TDEA cipher variants have reduced significantly.

For CTR mode the speed difference between AES cipher variants and TDEA cipher variants can be considered insignificant.

If we consider AES alone, the previous relationship between speed and key length can be perfectly seen only for smaller file sizes. This could be caused by network propagation delays. However the time differences between the three key variants are practically insignificant.

5. Conclusion

AES and TDEA are commonly used block ciphers approved by the NIST. The speeds of the two ciphers depend on the application. Our study shows AES to be faster than TDEA under all tested conditions. However both ciphers seem competent for general use yielding only an insignificant time difference for small data sizes.

6. References