Team Epic

Paul Eccleston

Joseph Noyes

Jeffrey Webb

CS 465 Program 1

This document will measure the times for encryption, decryption, and brute force. These times will be drawn from our shell script and provided in this document at the appropriate portion. Each portion will have average time and standard deviation for three types of encryption/decryption: DES, 3DES, AES-128. There were a total of 10 runs per type. There will be a table with all the data provided at the beginning of each section except brute force. In addition, all data was taken in nanoseconds for encryption and decryption. At the end will be a description the procedures used and how the results compare to each other.

1. Encryption

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| DES | .214937 | .017388 | .017104 | .017851 | .017081 | .017622 | .016751 | .013462 | .013851 | .0138718 |
| 3DES | .088253 | .023602 | .037155 | .037666 | .037782 | .033856 | .035584 | .032821 | .031163 | .023481 |
| AES | .013037 | .018192 | .013893 | .017192 | .027946 | .020935 | .011792 | .011187 | .011983 | .0109838 |

* 1. The DES average time is 0.035992 nanoseconds and has a standard deviation of 0.059671 nanoseconds.
  2. The 3DES average time is 0.038136 nanoseconds and has a standard deviation of 0.017437 nanoseconds.
  3. The AES-128 average time is 0.015715 nanoseconds and has a standard deviation of 0.000027 nanoseconds.

1. Decryption

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| DES | .011529 | .011192 | .009404 | .009129 | .009449 | .008806 | .009396 | .009268 | .009182 | .009221 |
| 3DES | .096005 | .032201 | .031792 | .032620 | .067780 | .033361 | .034033 | .023642 | .021871 | .022272 |
| AES | .011830 | .013705 | .008623 | .007637 | .007906 | .007961 | .007804 | .007996 | .007769 | .007889 |

* 1. The DES average time is 0.009658 nanoseconds and has a standard deviation of 0.000872 nanoseconds.
  2. The 3DES average time is 0.033614 nanoseconds and has a standard deviation of 0.022537 nanoseconds.
  3. The AES-128 average time is 0.013925 nanoseconds and has a standard deviation of 0.000029 nanoseconds.

1. Brute Force

|  |  |  |
| --- | --- | --- |
| DES | 5929 attempts/min | 1.387374 x 10^8 decades |
| 3DES | 9136 attempts/min | 4.674658 x 10^41 decades |
| AES | 6077 attempts/min | 6.380316 x 10^28 decades |

1. Procedures

The encryption and decryption were done using bash shell script and openssl. A program was created to run ten iterations of encryption using the three methods, followed by ten decryptions of each. The brute force was done allowing the bash script to try to decrypt the file over a period of time, then calculating out based on the number of decades it would take for completion.

1. Conclusion

Based on average time and standard deviation, AES-128 is the best for encryption and decryption. The method performs very quickly with very little deviation. Plus no system can brute force the encryption in any reasonable amount of time. The worst is DES since it takes the longest with quite a bit of deviation with decryption and encryption. In addition, it takes significantly less time to brute force the password as opposed to the others. While 3DES takes more time to brute force, the speeds are greatly slower than AES. Encryption and decryption times in 3DES are nearly two times slower and 3DES deviates by nearly ten times more. AES proves to be the better encryption and decryption to use.

1. Possible Errors

Two points of error could be possible in the procedures. First, many of these are computer performance driven. One person’s computer (or even a super computer) could perform the operations faster than another’s. Second, the first one or two decryption and encryption take quite a bit longer than later ones. The margin of error in such an occurrence leads to less reliable data for an accurate conclusion. Despite these problems, the conclusion drawn is supported by several iterations. A company would be better off using AES or 3DES than DES. DES is highly likely to be hacked based on the difference from the other two methods.