

Testing A Variety of Encryption Technologies

T. J. Henson

April 9, 2001

U.S. Department of Energy

Lawrence
Livermore
National
Laboratory

DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

This work was performed under the auspices of the U. S. Department of Energy by the University of California, Lawrence Livermore National Laboratory under Contract No. W-7405-Eng-48.

This report has been reproduced directly from the best available copy.

Available electronically at <http://www.doc.gov/bridge>

Available for a processing fee to U.S. Department of Energy
And its contractors in paper from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831-0062
Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-mail: reports@adonis.osti.gov

Available for the sale to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-mail: orders@ntis.fedworld.gov
Online ordering: <http://www.ntis.gov/ordering.htm>

OR

Lawrence Livermore National Laboratory
Technical Information Department's Digital Library
<http://www.llnl.gov/tid/Library.html>

Testing A Variety of Encryption Technologies
by
Teena J. Henson

Abstract:

Review and test speeds of various encryption technologies using Entrust Software. Multiple encryption algorithms are included in the product. Algorithms tested were IDEA, CAST, DES, and RC2. Test consisted of taking a 7.7 MB Word document file which included complex graphics and timing encryption, decryption and signing. Encryption is discussed in the GIAC Kickstart section: Information Security: The Big Picture – Part VI.

Selection Criteria:

The reason for this choice of subject matter is that encryption technologies have become an important aspect of computer security with the explosion of E-Commerce on the World Wide Web. Prior to the necessity to pass credit card information via the Internet, most encryption technologies were used by banking and U.S. Government agencies. Since anyone with a connection to the Internet and a credit card can purchase goods from anywhere in the world, the protection of account information is critical to the success of E-Commerce.

Term to be added to the KickStart Glossary:

Rijndael – An encryption algorithm developed by two Belgium researchers: Dr. Joan Daemen and Dr. Vincent Rijmen. Rijndael (pronounced Rhine Doll) has been selected by the National Institute of Standards and Technology (NIST) as the Advanced Encryption Standard (AES). The AES is a cryptographic algorithm that will be used by U.S. Government organizations to protect sensitive, unclassified information.

Similar Topics for Review:

Public Key Infrastructure (PKI), Steganography, and Code-Breaking challenges are topics that are related to or include encryption technologies.

Main Text:

As an Information Systems Security professional who is tasked with informing customers about computer security issues, encryption technologies and their use are becoming the “hot” topics for today. My organization has been working very hard to secure our systems and our networks. In accomplishing this work, I came to realize that our customers didn’t mind the added security as long as it doesn’t interfere with getting the work done. Also, any additional requirements placed on our customers has to be easy to use. The next step in security for our site is to really look at the data that we pass around the world. Does it contain any sensitive information? If so, how do we protect it when we send it via the

Internet? We must encrypt any data that we deem "not for public dissemination".

Encryption does not come without issues. Recently, there were restrictions on export of encryption technologies with certain key sizes. Also, the ability to decrypt transmissions to protect our national security is a charter of the National Security Agency (NSA). In order to prevent foreign governments from acquiring cryptography that the NSA could not break and as an advisor to the Bureau of Export Administration (BXA), the NSA has been able to restrict the export of encryption technologies with large key sizes. Prior to 1999, encryption technologies were considered "munitions" and therefore, fell under export control regulations. The big fear was that the FBI and the NSA would not be able to "wiretap and read" suspect transmissions from foreign governments or terrorists. The NSA has many resources for decryption, but the stronger the key, the more money and time it takes to break the code. In January 2000, export restrictions on encryption technologies were dramatically relaxed. Exports of technologies without a license are allowed as long as the recipients are not foreign governments or embargoed destinations.

Most encryption algorithms are based on problems that are difficult to solve. Difficult means that more computational requirements are needed to find the solution to the problem. Polynomial time, one-way functions, elliptic curve discrete logarithms, factoring, and prime numbers – are used to create encryption algorithms. Peers generally do strength testing. Creators of algorithms publish them and challenge anyone to "break the code". DES was broken by brute-force through a combined effort of Distributed.Net and Electronic Frontier Foundation (EFF). A combination of a specially designed supercomputer and 100,000 PCs on the Internet were used to break this code.

Entrust is the software that has been chosen by our headquarters for encrypting information. Entrust contains many encryption algorithms for use within the product. I have tested each available algorithm and timed the encryption of a complex document. The reason for this is two-fold. Speed of the algorithm is a major factor in determining the usability of a product. It is also a major consideration when determining a government standard. For example, Rijndael was chosen as the Advanced Encryption Standard (AES), the replacement for DES, because it had the best combination of security, performance, efficiency and ease of implementation. Rijndael is based on the algorithm Square. The algorithm is well suited for both software and hardware implementations. CAST-256 was eliminated from the final round of competition for the AES because it was considered a "slow" algorithm. I was curious what the differences were in speed of encryption between the various algorithms and when using different key sizes. During my research on encryption technologies, I reviewed a Frequently Asked Questions (FAQ) document from RSA Laboratories, on

cryptography. RSA is one of the leading providers of encryption software. RSA claimed that its product – RC2 – was 2-3 times faster than DES when implemented in software.

The algorithms I tested include CAST, IDEA, RC2, DES, and Triple DES.

CAST – A 64 bit Feistel cipher created by Carlisle Adams and Stafford Tavares. CAST has key sizes up to 128 bits. Entrust includes CAST-40, CAST-64, CAST-80 and CAST-128. All key sizes were tested.

IDEA – A 128 bit Block cipher created by X. Lai and J. L. Massey. IDEA – International Data Encryption Algorithm was described in an RSA FAQ as having speed similar to DES.

DES/Triple DES – A 56-bit block cipher. DES is the Data Encryption Standard that will be replaced by AES, the Advanced Encryption Standard. DES was originally named Lucifer and was developed and patented by IBM. The National Security Agency (NSA) and NIST played a key role in the development of Lucifer into DES. Triple DES uses DES to perform triple encryption. DES has been broken by brute force and is considered insecure.

RC2 – RSA-owned algorithm. RC2-40 and RC2-128 were tested. Ronald Rivest (the R in RSA) developed this variable key size, block cipher algorithm. It is stated in the RSA FAQ that RC2 is 2-3 times faster than DES as implemented in software. RC2 has been broken and is considered insecure.

As described above, the document used for the test was created in Word. The file included both text and graphics. The file size was 7.7 MB. The test was conducted by setting the encryption algorithm within the Entrust software. The document was encrypted, decrypted, signed, and encrypted and signed, and the amount of time it took to accomplish those tasks was noted. The table shows the results of the test process.

Algorithm Used	Time to Encrypt	Time to Decrypt	Time to Sign	Time to Decrypt Signing	Time to Encrypt and Sign	Time to Decrypt Both an Encrypted and Signed File
CAST-40	~8 sec	~3 sec	~7 sec	~2 sec	~8 sec	~2 sec
CAST-64	~7 sec	~2 sec	~7 sec	~2 sec	~7 sec	~2 sec
CAST-80	~7 sec	~2 sec	~10 sec	~4 sec	~7 sec	~3 sec
CAST-128	~7 sec	~3 sec	~8 sec	~2 sec	~7 sec	~3 sec
IDEA	~10 sec	~4 sec	~7 sec	~2 sec	~10 sec	~5 sec
DES	~9 sec	~3 sec	~8 sec	~3 sec	~9 sec	~4 sec
Triple DES	~14 sec	~6 sec	~7 sec	~2 sec	~14 sec	~5 sec
RC2-40	~14 sec	~6 sec	~7 sec	~2 sec	~14 sec	~6 sec
RC2-128	~14 sec	~6 sec	~7 sec	~2 sec	~14 sec	~5 sec

Review of the results from the test reveals some interesting information. It appears that the CAST algorithm, independent of key size, is the fastest overall in this test. CAST-128 is considered quite secure and the 256-bit version – CAST-256 was in the final 15 for the AES. Is CAST really the fastest algorithm? Or since it is owned by Entrust, has it been optimized for use in their software?

Triple DES and the RC2 products are fairly equal in performance. According to RSA, the RC2 algorithm is supposed to be 2-3 times faster than DES when implemented in software. The results of this test don't show that to be true.

The bottom line regarding encryption technologies is this. Use the encryption technology that gives you the level of security you feel is necessary to protect your data. If the technology takes more time to encrypt your data, but is impossible to break in the time period that you need to protect your data (e.g. one year), then spend the extra time protecting it. On the other hand, don't spend one hundred dollars worth of time protecting a two dollar part; but spend that one hundred dollars protecting the million dollar design of the two dollar part.

For Further Information:

Author: RSA Laboratories

Title: RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1

Year: 2000

Publisher: RSA Security Inc.

<http://www.nist.gov/aes> Web page for the National Institute of Standards and Technology's Advanced Encryption Standard (AES)

<http://distributed.net> Web page for Distributed.Net. Includes a list of four projects related to code breaking that Distributed.Net is working on.

<http://www.eff.com> Web page for the Electronic Frontier Foundation.

<http://www.nsa.gov> Web page for the National Security Agency (NSA).