

The Data Encryption Standard algorithm

DES was introduced by the National Bureau of Standards in 1976 and announced in Jan, 1997 as a Federal Information Processing Standard. DES uses a 56 bit key, which means that there are 2^{56} or $7.20576 * 10^{16}$ different keys. In 1997, a Pentium 200 Mhz running specialized software, could test 1,000,000 keys per second. At this rate, it would take 2,285 years to crack one DES encrypted message with that Pentium 200 Mhz computer. Surely, more parallel solutions and faster computers would help this process. As we will see in this article, that is exactly what has happened in the 33 years since DES was introduced. The chart at the end of this article shows this progress.

Pre-1998 DES Cracking Hardware Solutions

The first proposed brute force DES cracking estimates were by Diffie and Hellman in 1977, the same year DES was introduced. The Diffie-Hellman estimates were that a machine could be built for 20 MILLION US Dollars that would crack a DES key in one day. Declining hardware costs allowed Michael Wiener, in 1993, to propose a machine that could be built for less than a MILLION US Dollars. The Wiener machine would have 57,000 specialized DES chips and would be able to crack a DES key by brute force in 3.5 hours. In 1997, Goldberg and Wagner proposed building a DES cracker for \$45,000, which used Field Programmable Gate Arrays, but would only crack a DES key within one year.

The RSA DES Cracking Challenges

By 1997, RSA Data Security (RSA) was convinced that even though DES was still a government standard, it was unsafe for government work. RSA launched its famous **I.1 Secret Key Challenge** with a \$10,000 prize to the winner. The DESCHALL (DES CHALLENGE) team of Rocke Verser, Matt Curtin, and Justin Dolske wrote software to enable a single 200 MHz Pentium system to test approximately 1 million keys/second if it was doing nothing else. At this rate it would take around 2,285 years for the single 200 MHz Pentium to search the entire key-space. In January, 1998, using a collection of computers running continuously for 96 days, the DESCHALL team announced the solution to the first RSA challenge, whose text was "**We need stronger encryption.**"

RSA quickly issued its **II.1 Secret Key Challenge**. At this point, team DESCHALL joined with Distributed.net's super network to enable anyone interested to participate in the project over the Internet. If you signed up, Distributed.net would download a client for your computer (PC's, MAC's, Unix Computers, even older ones like Apple 2's). Your particular client would be given only a small portion of the key space to test.

Many university lab managers signed up whole fleets of computers. The brute force cracking software either ran in the background or full time at night when the labs were closed. During this project, a maximum of 14,000 unique hosts in a 24 hour period worked on the Secret Key Challenge. The DESCHALL/Distributed.net group solved the problem in 41 days. The DESCHALL/Distributed.net team "**got lucky**" in that it found the proper key after searching less than 25% of the key space. At that time, about 7 billion keys per second were being tested. The owner of the computer who found the solution was awarded \$4,000 of the prize, with the rest going to the originator of the project. The secret message for the II.1 challenge was "**Many hands make light work.**"

RSA then issued its **II.2 Secret Key Challenge**. This challenge was solved by a custom hardware DES attack computer, known as **Deep Crack**, that was built in 1998 by the Electronic Frontier Foundation at the cost of \$250,000. **Deep Crack** contained 1,856 custom ASIC DES chips housed on 29 circuit boards of 64 chips each. The boards were then fitted in six cabinets and mounted in a Sun-4/470 chassis. The search was coordinated by a single PC which assigned ranges of keys to the chips. The entire machine was capable of testing over 90 billion keys per second. It would take about 9 days to test every possible key at that rate. On average, the correct key would be found in half that time. **Deep Crack** solved the II.2 Secret Key Challenge in only 56 hours. The secret message for the II.2 challenge was "**It's time for those 128-, 192-, and 256-bit keys.**"

RSA then issued its **III.1 Secret Key Challenge**. This challenge was solved by the Distributed.net team working with **Deep Crack** in only 23 hours. Wow, less than a day. Surely, by this time, RSA had proven its point; that we needed stronger encryption. The secret message was "**See you in Rome.**" which was where the second RSA conference was to be held in March, 1999.

The US Government's Development of the AES Algorithm

On Jan 2, 1997, the US National Institute for Standards and Technology, NIST, announced the project for a new algorithm, called AES, to replace DES. Like DES, this was to be "an unclassified, publicly disclosed encryption algorithm capable of protecting sensitive government information well into the next century." However, rather than simply publishing a successor, NIST asked for input from interested parties on how the successor should be chosen. Interest from the open cryptographic community was immediately intense, and NIST received a great many submissions during the three month comment period.

The result of this feedback was a call for new algorithms on September 12, 1997. The algorithms were all to be block ciphers, supporting a block size of 128 bits and key sizes of 128, 192, and 256 bits. Such ciphers were rare at the time of the announcement; the best known was probably Square. In the nine months that followed, fifteen different designs were created and submitted from several different countries. They were, in alphabetical order: CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOKI97, MAGENTA, MARS, RC6, Rijndael, SAFER+, Serpent, and Twofish.

Cryptographers debated the pros and cons of these algorithms, and NIST held two conferences, AES1, August 1998, and AES2, March 1999. In August, 1999, NIST announced that MARS, RC6, Rijndael, Serpent, and Twofish were the "**five AES finalists**". At the AES2 conference, Rijndael and Serpent were the top two, with Rijndael getting 86 positive votes and 10 negatives and Serpent getting 59 positive votes and only 7 negatives. Even though MARS was a finalist, it only got 13 positives and a whopping 83 negatives. After intense analysis of the pros and cons, NIST staged the AES3 conference in April 2000. During AES3, a representative of each of the final five teams made a presentation arguing why their design should be chosen for the AES. On October 2, 2000, NIST announced that Rijndael had been selected as the proposed AES and started the process of making it the official standard by publishing an announcement in the Federal Register on February 28, 2001 for the draft FIPS to solicit comments. On November 26, 2001, NIST announced that AES was approved as FIPS PUB 197. The FIPS standards are all available free from various Internet sources.

NIST won praises from the cryptographic community for the openness and care with which they ran the standards process. Bruce Schneier, one of the authors of the losing Twofish algorithm, wrote after the competition was over that "I have nothing but good things to say about NIST and the AES process".

The COCACOBANA Project

Even after the AES standardization, research into cracking DES continued. The next significant effort occurred with the introduction of the COCACOBANA (Cost-Optimized Parallel COde Breaker or COCO) project. COCO's use Field Programmable Gate Arrays (FPGAs) instead of the ASICs that DEEP CRACK uses. FPGAs are much cheaper, are commercially available, and can be programmed for different functions. The first version of COCO was built in 2006, at a build cost of only \$10,000. COCO will recover a DES key in under 6.4 days on average. Adjusting for inflation, COCO shows a cost decrease factor of 30 over DEEP CRACK. The original

DES Brute Force Cracking Efforts 1977 to 2010

COCO machine could achieve a throughput of more than 65 billion keys per second using Xilinx Spartan-3 1000 FPGAs. By 2008, SciEngines COCO machines could break DES in an average time of a single day. By 2009, SciEngines new product, the RIVYERA, achieved a throughput of over 280 billion keys/sec using 128 Xilinx Spartan-3 5000 FPGAs in a single 3 HU hardware accelerated server, and in 2010, the RIVYERA machines could test 292 billion keys/sec second, using only 75% of the peak power consumption of the original COCO machines. Wow!

Future Developments in Brute Force Decryption Methods

The DEEP CRACK, COCO, and now RIVYERA machines prove that hardware capability increases at rapid rates, and that DES is no longer safe. The table below shows the increase in speeds.

Year	Equipment	DES Keys/Sec	Cracking Time 50% key space	Cost of Equipment
1977	Diffie Hellman		< 1 Day	\$20,000,000
1993	Wiener		3.5 Hours	\$1,000,000
1997	Goldberg Wagner		1 Year	\$45,000
1997	200 Mhz Pentium	1,000,000	1143 Years	\$2,000
1998	Deep Crack	80,000,000,000	4.5 Days	\$250,000
2006	Cocacobana	65,000,000,000	6.4 Days	\$10,000
2008	SciEngines COCO	280,000,000,000	< 1 Day	< \$15,000
2010	SciEngines RIVYERA	292,000,000,000	< 1 Day	< \$15,000
2010	Intel Core I5 - 2.66 GHz	26,000,000	43 Years	\$800

Where would your modern Intel I5, 2.66 GHz computer fit in? A popular benchmark is called PassMark. The 200 Mhz Pentium 2 has a PassMark value of 90, while the Core I5 2.66 Ghz system has a PassMark value of 2366. **This ratio is about 26.3; so your Core I5 will take about 87 years, or about 43 years if we find the key in the first 50% of our tries.** This easily shows how significant both the Deep Crack and the COCO efforts were.