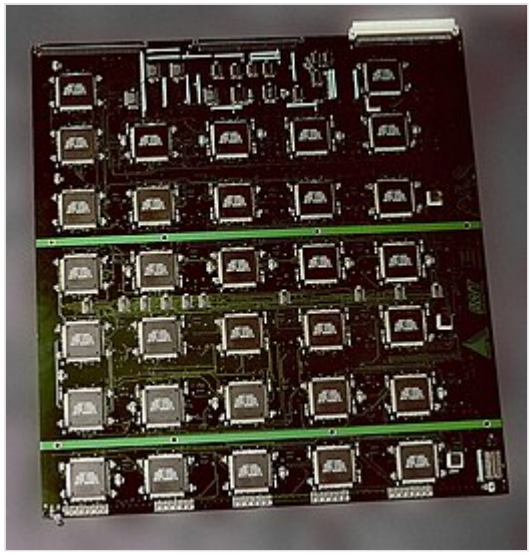
EFF DES cracker

In cryptography, the **EFF DES cracker** (nicknamed "**Deep Crack**") is a machine built by the Electronic Frontier Foundation (EFF) in 1998, to perform a brute force search of the Data Encryption Standard (DES) cipher's key space – that is, to decrypt an encrypted message by trying every possible key. The aim in doing this was to prove that the key size of DES was not sufficient to be secure.

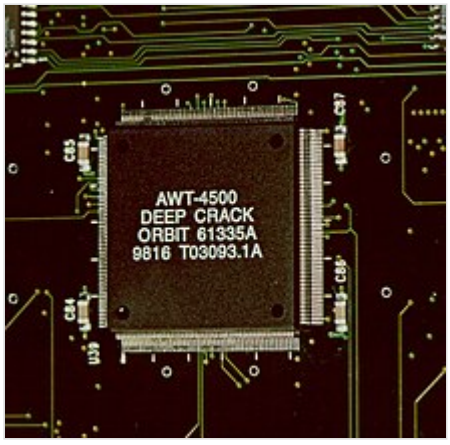
Detailed technical data of this machine, including block diagrams, circuit schematics, VHDL source code of the custom chips and its emulator, have all been published in the book *Cracking DES*. Its public domain license allows everyone to freely copy, use, or modify its design. To avoid the export regulation on cryptography by the US Government, the source code was distributed not in electronic form but as a hardcopy book, of which the open publication is protected by the First Amendment. Machine-readable metadata is provided to facilitate the transcription of the code into a computer via OCR by readers.[1]



The EFF's US$250,000 DES cracking machine contained 1,856 custom chips and could brute force a DES key in a matter of days — the photo shows a two-sided DES Cracker circuit board fitted with 64 Deep Crack chips

Background

DES uses a 56-bit key, meaning that there are 2^{56} possible keys under which a message can be encrypted. This is exactly 72,057,594,037,927,936, or approximately 72 quadrillion possible keys. One of the major criticisms of DES, when proposed in 1975, was that the key size was too short. Martin Hellman and Whitfield Diffie of Stanford University estimated that a machine fast enough to test that many keys in a day would have cost about $20 million in 1976, an affordable sum to national intelligence agencies such as the US National Security Agency.[2] Subsequent advances in the price/performance of chips kept reducing that cost until, twenty years later, it became affordable for even a small nonprofit organization such as the EFF to mount a realistic attack.[3]



The EFF's DES cracker "Deep Crack" custom microchip

The DES challenges

DES was a federal standard, and the US government encouraged the use of DES for all non-classified data. RSA Security wished to demonstrate that DES's key length was not enough to ensure security, so they set up the DES Challenges in 1997, offering a monetary prize. The first DES Challenge was solved in 96 days by the DESCHALL Project led by Rocke Verser in Loveland, Colorado. RSA Security set up DES Challenge II-1, which was solved by distributed.net in 39 days in January and February 1998.[4]

In 1998, the EFF built Deep Crack (named in reference to IBM's Deep Blue chess computer) for less than $250,000.[5] In response to DES Challenge II-2, on July 15, 1998, Deep Crack decrypted a DES-encrypted message after only 56 hours of work, winning $10,000. The brute force attack showed that cracking DES was

actually a very practical proposition. Most governments and large corporations could reasonably build a machine like Deep Crack.

Six months later, in response to RSA Security's DES Challenge III, and in collaboration with distributed.net, the EFF used Deep Crack to decrypt another DES-encrypted message, winning another $10,000. This time, the operation took less than a day – 22 hours and 15 minutes. The decryption was completed on January 19, 1999. In October of that year, DES was reaffirmed as a federal standard, but this time the standard recommended Triple DES.

The small key space of DES and relatively high computational costs of Triple DES resulted in its replacement by AES as a Federal standard, effective May 26, 2002.

Technology

Deep Crack was designed by Cryptography Research, Inc., Advanced Wireless Technologies, and the EFF. The principal designer was Paul Kocher, president of Cryptography Research. Advanced Wireless Technologies built 1,856 custom ASIC DES chips (called *Deep Crack* or *AWT-4500*), 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.[6]

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.

Paul Kocher of Cryptography Research posing in front of Deep Crack

In 2006, another custom hardware attack machine was designed based on FPGAs. COPACOBANA (COst-optimized PArallel COdeBreaker) is able to crack DES at considerably lower cost.[7] This advantage is mainly due to progress in integrated circuit technology.

In July 2012, security researchers David Hulton and Moxie Marlinspike unveiled a cloud computing tool for breaking the MS-CHAPv2 protocol by recovering the protocol's DES encryption keys by brute force. This tool effectively allows members of the general public to recover a DES key from a known plaintext–ciphertext pair in about 24 hours.[8]

References

1. Electronic Frontier Foundation (1998). *Cracking DES - Secrets of Encryption Research, Wiretap Politics & Chip Design* (https://web.archive.org/web/20131017055750/http://cryptome.org/jya/cracking-des/cracking-des.htm). Oreilly & Associates Inc. ISBN 1-56592-520-3. Archived from the original (http://cryptome.org/jya/cracking-des/cracking-des.htm) on October 17, 2013. Retrieved October 30, 2016.
2. "DES (Data Encryption Standard) Review at Stanford University – Recording and Transcript" (http://www.toad.com/des-stanford-meeting.html). 1976. Archived (https://web.archive.org/web/20220228142103/http://www.toad.com/des-stanford-meeting.html) from the original on February 28, 2022. Retrieved June 26, 2022.
3. "DES Cracker Project" (https://web.archive.org/web/20130622022127/https://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/). *EFF.org*. Archived from the original (https://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker) on June 22, 2013. Retrieved October 9, 2013.
4. David C. McNett (February 24, 1998). "The secret message is..." (http://lists.distributed.net/pipermail/announce/1998/000037.html) distributed.net. Archived (https://web.archive.org/web/20160304000105/http://lists.distributed.net/pipermail/announce/1998/000037.html) from the original on March 4, 2016. Retrieved February 27, 2014.

5. "DES Cracker Project" (https://web.archive.org/web/20170507231657/https://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_des_faq.html). EFF. Archived from the original (https://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_des_faq.html) on May 7, 2017. Retrieved July 8, 2007. "On Wednesday, July 17, 1998 the EFF DES Cracker, which was built for less than $250,000, easily won RSA Laboratory's "DES Challenge II" contest and a $10,000 cash prize."
6. Electronic Frontier Foundation (1998). *Cracking DES – Secrets of Encryption Research, Wiretap Politics & Chip Design* (https://archive.org/details/crackingdes00elec). Oreilly & Associates Inc. ISBN 1-56592-520-3.
7. "COPACOBANA – Special-Purpose Hardware for Code-Breaking" (http://www.sciengines.com/copacobana/faq.html). *www.sciengines.com*. Archived (https://web.archive.org/web/20160724092435/http://www.sciengines.com/copacobana/faq.html) from the original on July 24, 2016. Retrieved April 26, 2018.
8. "Divide and Conquer: Cracking MS-CHAPv2 with a 100% success rate" (https://web.archive.org/web/20160316174007/https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/). *CloudCracker.com*. July 29, 2012. Archived from the original (https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/) on March 16, 2016. Retrieved March 16, 2016.

External links

- The DES Cracker (https://web.archive.org/web/20170507231657/https://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_des_faq.html) at the Electronic Frontier Foundation
- Photos of the machine (http://www.cryptography.com/resources/whitepapers/DES-photos.html) at Cryptography Research
- A FPGA implementation using 48 Virtex-6 LX240Ts (http://crack.sh/)
- ASIC design from 1994 that could crack DES in 24 hours with 256 custom chips (https://davesource.com/Projects/DEStiny/)