Distinguished Lecture in Computer Security, Sixth Annual Computer Security Applications Conference, Tucson, December 3-7, 1990.

The Data Encryption Standard Fifteen Years of Public Scrutiny

Dorothy E. Denning
Digital Equipment Corporation
Systems Research Center
130 Lytton Avenue
Palo Alto, California 94301

> Within fifteen years, [the DES] will be rendered totally insecure.
> – *Whitfield Diffie and Martin Hellman, 1976*

Introduction

In 1973, the National Bureau of Standards (NBS), now known as the National Institute of Standards and Technology (NIST), solicited proposals for a standard data encryption algorithm for use by Federal agencies for cryptographic protection of sensitive unclassified information. From those submitted, NBS, with the advice of the National Security Agency (NSA), chose an algorithm developed by IBM. The algorithm, which was named the Data Encryption Standard (DES), was published in the *Federal Register* in 1975 [27, 28] together with a call for comments. In 1977, NBS issued Federal Information Processing Standard (FIPS) Publication 46, announcing the DES as the federal encryption standard and giving its specifications [29]. In 1983 and again in 1988, NBS reviewed and reaffirmed the DES. The current standard, which was issued as FIPS 46-1 in 1988, reaffirms the standard until 1993 [30]. The algorithm has been adopted by the American National Standards Institute (ANSI) for information processing systems and financial services [34].

The DES encrypts 64-bit blocks with a 56-bit key K. After an initial permutation of the bits, a plaintext block goes through 16 iterations ("rounds") of a complex function and then passes through a final permutation that yields the ciphertext block. During each round i, the right half of the block is expanded to 48-bits and XORed with a 48-bit internal key K_i derived from K. The result then passes through eight S-boxes, which are nonlinear substitutions mapping 6 input bits into 4 output bits. The 32-bit result is then permuted and XORed with the left half of the block. Finally, the two halves of the block are swapped before going through the next round. The security of the algorithm depends on the nonlinear S-boxes, since the remaining parts of the algorithm are all linear and thus easily attacked. It does not, however, depend on the secrecy of the algorithm, since the complete algorithm, including the contents of the S-boxes, is public knowledge.

The DES can be used in four modes of operation: Electronic Codeboook (ECB), which encrypts a single block; Cipher Block Chaining (CBC), which XORes each plaintext block in a stream of data to its preceding ciphertext block before encrypting it; Cipher Feedback (CFB), which XORes each character in a stream to a key character derived by encrypting the preceding eight ciphertext characters; and Output Feedback (OFB), which uses the DES to generate a random key stream that is XORed with a plaintext stream. For a description of the DES and the different modes, see Denning [12], Davies [10], or Meyer and Matyas [24].

IBM originally designed the algorithm to use a 128-bit key. Prior to the call for comments, the key size was reduced to 56 bits and the design of the S-boxes was classified by NSA. These two factors raised doubts about the security of DES, and led to considerable public scrutiny during the fifteen years that have passed since. The next three sections report on the results of this continuing examination. I have divided the period into three intervals: the interval between the call for comments in 1975 and adoption as the standard in 1977, the interval following adoption until the first CRYPTO conference in 1981, and the interval since 1981.

1975-1977: The Pre-Adoption Years

On October 22, 1975, Martin Hellman of Stanford University sent a letter to the NBS expressing concerns about the DES: "Whit Diffie and I have become concerned that the proposed data encryption standard, while probably secure against commercial assault, may be extremely vulnerable to attack by an intelligence organization." [34]. Diffie and Hellman also made their concerns publicly known through the ACM Forum [14], where they said they believed that the DES "is currently vulnerable to attack by the intelligence community and

that within fifteen years it will be rendered totally insecure due to the rapidly falling cost of computation."

They specifically argued that the 56-bit key was too small, and that a special purpose machine could determine a key within half a day by exhaustive search under a known-plaintext attack [14, 15]. The machine would consist of a million LSI chips, and each chip would check one key per microsecond. Thus, a million chips would check 10^{12} keys per second. Since there are about 10^{17} keys total, the entire key space could be searched in about one day. On the average only half the key space would have to be searched, so the average search time would be about half a day. Diffie and Hellman also noted that the search time for a key would be dramatically lower if keys were formed from eight alphabetic characters rather than random bit strings, since the search space would be less than 10^{12}.

The cost of the machine would be about $20 million. If the cost were amortized over five years, the cost per solution would then be $5,000. They estimated that the cost of the machine would drop to $200,000 in ten years, making the cost per solution $50. Because the time required for an exhaustive search grows exponentially in the key length, Diffie and Hellman recommended that the key length be 128 or longer. They speculated that if the key were not lengthened, the DES might have to be replaced in as few as five years.

Hellman and others at Stanford examined additional characteristics of the DES for strengths and weaknesses, publishing their results as a Stanford report [16]. They found that the DES is invariant under complementation of the plaintext, key, and ciphertext, making it possible to reduce the search effort by 50% in a partially chosen plaintext attack. They also found that the S-boxes were closer to linear than they had expected, and that their structure was similar to one that could be used to build a trap door into the system. The found other structure in the S-boxes, for example, three of the rows in S4 could be derived from the fourth. They concluded that the S-boxes were carefully chosen to satisfy certain properties, and that this may have weakened them and made them suspect. They argued that a randomly chosen S-box would be at least as good as one selected from a probabilistically small, specially structured set, and that persons involved with the design, who knew the structure, would have a significant advantage in cryptanalysis. Their recommendations included increasing the rounds from 16 to at least 32, using less-structured S-boxes, lengthening the key to 128 bits or more, introducing the key in a more complex way, making the key-scheduling algorithm more nonlinear, and adding complexity to one of the permutations used to derive each internal key. They also encouraged the public release of DES's design principles and certification effort.

After two years of evaluation of the DES, NBS organized two workshops to help them reach their final decision [26, 34]. The first, held in August, 1976, was convened to examine the feasibility of building the special purpose machine described by Diffie and Hellman. The participants at the workshop challenged the feasibility of implementing their machine with technology available at the time, concluding "A machine which finds, on the average, one key per day could probably not be built until 1990, and the probability factor of it being available even then is estimated to be between 0.1 and 0.2. In addition the cost of such a machine would be several tens of millions of dollars." [36]. However, Diffie and Hellman stuck with their original estimate of $20 million [15].

Now that 1990 has arrived, it is worth noting that no million-processor machine is available. Gordon Bell speculates that a connection machine with a million processors could be built by 1995 at a cost that is likely to be over $50 million [3]. However, such a machine would be more complicated than needed to search for DES keys. Hellman believes that a DES search machine could be built today for under $1 million.

The second workshop was held in September, 1976 [5]. Three of the participants, Robert Morris, Neil Sloane, and Aaron Wyner, published an assessment of the DES following the workshop [26]. They listed three features of the DES that they believed were positive. First, the DES is a product cipher that iterates two different operations several times. Second, the algorithm is public knowledge; only the keys need be secret. Third, it is possible to increase security with multiple encryption, that is, by encrypting two or more times with different keys.

They also listed two features that they assessed as weaknesses. First is the key size. They supported Diffie's and Hellman's claim that 56 bits is inadequate. Second is the classification of the design of the S-boxes. They raised the possibility that the S-boxes could contain "trapdoors" or "Trojan horses" that would compromise security. Some of their findings seem to have been influenced by a report published by the Lexar Corporation [8]. Although this report does not acknowledge Hellman or his group at Stanford, it is identical in contents to the Stanford report [16] cited earlier, suggesting an unreported relationship.

Morris, Sloane, and Wyner recommended that the DES not be adopted in its present form. They urged that the key size be increased to at least 64 bits and preferably 128 bits, that the S-boxes be redesigned according to a publicly announced system, and that the number of iterations of the basic loop be increased from 16 to at least 32. They further recommended that if NBS is unwilling to alter the design, that users be at least notified that a key of eight typed characters is weak, and that added security can be obtained through multiple encryption.

NBS decided to adopt the proposed standard, without modification, after the second workshop. Miles Smid and

Dennis Branstad [34] of NBS reported that the potential users and vendors agreed that while the key could have been longer, 56 bits would be adequate for the next 10-15 years. They were also concerned that any increase in key length could make implementations unexportable to potential markets. However, in adopting the algorithm, they recommended that the algorithm be reviewed every few years, which it has.

1977-1981: The Early Post-Adoption Years

In 1979, *IEEE Spectrum* published a debate on the security of the DES featuring articles by Hellman, George Davida of the University of Wisconsin and the National Science Foundation, Walter Tuchman of IBM, Dennis Branstad of NBS, and the NSA [35]. Hellman claimed the "DES will be totally insecure within 10 years," repeating many of his earlier arguments. He also outlined a new time-memory-processor technique that trades search time for memory and multiprocessing in a chosen plaintext attack [17, 2]. The cost of the machine would be $5 million. By working on 100 keys in parallel, the cost per solution would be $10. However, as noted in the paper, the attack requires more than a year of pre-computation time in one configuration, and is easily foiled by avoiding electronic codebook mode.

Davida said that the time-memory attack broke DES in its basic form, but that the basic DES design was rather good. He also noted that the DES had bypassed the peer review process used with other standards, where representatives from the government, industry, and academia actively participate in the design and evaluation process.

Tuchman challenged the claims of Hellman, citing the results of the first NBS workshop in 1976. He said that NSA had not tampered with the DES and had certified that the DES was free of any known statistical or mathematical weaknesses. He also pointed out that the key size of the DES could be effectively increased to 112 bits with triple encryption without making the hardware obsolete. The method successively encrypts, decrypts, and then encrypts again using one key for the two encryptions and a second key for the decryption. Branstad said that Hellman's data did not support his conclusions, and that the DES will satisfy the security requirements of a wide range of applications for many years.

Allegations that the NSA might have tampered with the DES led the U.S. Senate Select Committee on Intelligence to investigate the matter [10]. Their report, which was issued in 1979, exonerated the NSA. The report also stated that the NSA had convinced IBM that a shorter key size was adequate, and that the majority of scientists consulted believed the DES was adequate for its intended use and time-span.

In 1980, Hellman reported on a study he made of the DES in output feedback mode (OFB) [18]. Recall that in this mode, the DES is used to produce a key stream that is XORed with the plaintext stream. To generate the key stream, a shift register is used as input to the DES, and the leftmost n bits of each output block are appended to the key stream and fed back into the shift register. Now, a stream cipher can be broken if the cryptanalyst can obtain two ciphertext streams encrypted under the same key stream, so it is important that the key stream not repeat. Hellman showed that if fewer than 64 bits were fed back through the loop, then the generated key stream could have a short cycle, repeating in a day. He argued that a stronger cipher could be obtained by replacing the feedback shift register with a counter.

In 1981, Ralph Merkle and Hellman published an article challenging Tuchman's claim that triple encryption using two keys was as secure as using a single 112-bit key [23]. They showed that it could be theoretically broken under a chosen-plaintext attack using about 2^{56} operations and 2^{56} keys stored on 4 billion tapes. Although their attack is not practical, they claim it shows that using 112 bits in triple encryption mode may be weaker than using a single 112 bit key.

1981-1990: The CRYPTO Years

In August of 1981, the first CRYPTO conference was held at the University of California in Santa Barbara. The purpose of the conference was to bring together people who were doing public-domain research in cryptography. The CRYPTO conferences at UCSB became a yearly event, and led to the formation of the International Association for Cryptologic Research (IACR) in 1983. The IACR subsequently sponsored CRYPTO and its European counterpart, EUROCRYPT. Since 1981, almost all of the research results on the DES have been presented at a CRYPTO conference.

At CRYPTO 81, Donald Davies presented a paper describing four functional regularities of the DES algorithm and one regularity of the structure of permutations [9]. Some of these regularities show up as "weak" or "semi-weak" keys. Weak keys have the property that encryption and decryption are the same operation; thus, two successive encryptions with a weak key restores the plaintext. Semi-weak keys come in pairs and have the property that successive encryption with each key in a pair restores the plaintext. Davies found 4 weak and 12 semi-weak keys. These keys should be avoided since they have the effect of yielding repetitions of the internal keys generated for each round.

The following year, Hellman and Reyneri reported on a study to analyze the DES for a statistical property named

"drainage," which allowed them to compare the DES with a truly random function [19]. To compute drainage, one first picks a plaintext block and generates a list of say 100 starting keys. For each key, the plaintext block is encrypted, and then the result is fed back through the key and the plaintext re-encrypted. This feedback process through the key is continued until it cycles. Hellman and Reyneri show that for a fixed plaintext, one would expect 80% of the initial keys to drain into a common cycle. Although the results of their initial experiments using an all-zero plaintext block led to all of the keys draining into the same cycle, further experiments confirmed their 80% estimate, thereby demonstrating no statistical irregularity with respect to drainage.

At CRYPTO 83, Marc Davio and others reported on a study to analyze the inner structure of the DES [11]. While they did not find any weaknesses in the DES, they did discover properties in the algorithm that enabled them to express it in a way that would simplify and speed up hardware and software implementations. Frank Hoornaert, Jo Goubert, and Yvo Desmedt presented an efficient hardware implementation the following year at CRYPTO 84 [20].

Also at CRYPTO 84, Desmedt, Jean-Jacques Quisquater, and Davio described new properties of the S-boxes, showing that if the DES had only a few rounds, it would be a weak system [13]. They drew no conclusions about the 16-round DES. Jim Reeds and J. Manferdelli reported that they looked for linear factors in individual rounds of the DES, but did not find any [31].

At EUROCRYPT 85, Burton Kaliski, Ronald Rivest, and Alan Sherman [21] reported on a study to determine if the DES were closed under functional composition. If it were, then for any key K, there would exist many pairs of keys such that successive encryption with the two keys would be equivalent to encryption with K. This would imply that the DES would be vulnerable to a meet-in-the-middle known-plaintext attack that would run in 2^{28} steps approximately by exploiting the "birthday paradox." They tested DES under a meet-in-the-middle closure test and a cycling closure test, and found that it was highly unlikely that the DES was closed or generated a small group.

At CRYPTO 85, David Chaum and Jan-Hendrik Evertse presented further results showing that if the DES had fewer rounds, it could be weak [7]. They showed that a variant of the DES consisting of the first 4, 5, or 6 rounds could be attacked with speed-ups of 2^{19}, 2^{9}, and 2^{2} respectively over exhaustive search. They also showed that their method, which uses a meet-in-the-middle strategy, does not work with 8 or more rounds. Kaliski, Rivest, and Sherman [22] reported on further cycling experiments on the DES to determine if was a "pure cipher," meaning that successive encryption, decryption, and encryption with any three keys is equivalent to encryption with a single key. Their results showed it was highly unlikely the DES was pure, and that it behaved like a random set of permutations. They also found short cycles with two weak keys. Shamir [32] reported on some interesting anomalies he found in the S-boxes, which produced a correlation between one of the input bits to each S-box and the XOR of the four output bits. Although he had not yet found a way of using these anomalies in an attack, he argued that they demonstrated deficiencies of current certification techniques and the need for provably secure cryptosystems.

Although the design documents on the S-boxes were never declassified, the report from the second NBS workshop in 1976 contained a list of design criteria obtained from the NSA [5]. At CRYPTO 86, Ernest Brickell, Judy Moore, and M. Purtill [6] showed that the anomalies reported by Shamir at CRYPTO 85 were likely to exist in any S-boxes generated according to these criteria. Moore and Gustavus Simmons [25] reported on an in-depth study of the cycle structure of the DES using weak and semi-weak keys. Neither paper uncovered any new weaknesses in DES.

At CRYPTO 89, Carlisle Adams and Stafford Tavares [1] claimed that good S-boxes satisfying the design criteria are easy to generate. They suggested that DES be extended to make the key select which S-boxes to use from a standard set.

At CRYPTO 90, Eli Biham and Shamir presented a new type of cryptanalytic attack that can break an 8-round version of the DES in less than two minutes and a 15-round version faster than exhaustive search [4]. However, at 16 rounds it requires 2^{58} steps, which makes it slower than exhaustive search. Thus, it does not threaten the standard DES. The attack, called *differential cryptanalysis*, is a chosen plaintext attack based on the principle that when the XOR of two plaintexts satisfies a certain property, it is possible to perform a statistical attack on the key given the two plaintexts and their corresponding ciphertexts. The statistical attack is possible because the S-boxes, while nonlinear, generate a highly skewed distribution of XOR outputs for given XOR inputs. For example, S1 maps the XOR input of '30' hexidecimal to an XOR output of '4' with probability 1/4. Since the output of an S-box is 4-bits, an even distribution would map each input XOR into each output XOR with probablity 1/16.

In principle, the DES could use a key up to $16 * 48 = 768$ bits since a different 48-bit internal key is generated for each of the 16 rounds. One of Biham's and Shamir's surprising results was that increasing the key length, while keeping the rest of the algorithm intact, does not strengthen the DES. In particular, they were able to break an 8-round version of the DES with $8 * 48 = 384$ independent internal key bits in less than two minutes. A 16-round DES with a key size of 768 bits would be

breakable within 2^{61} steps. At the same time, however, their results show that increasing the number of rounds can add considerable strength to the algorithm.

Biham and Shamir further found that changing the contents or order of the S-boxes could weaken the DES. In particular, DES with random S-boxes is easy to break.

The attack is applicable to other DES-like cryptosystems. For example, it can break the proposed Japanese Fast Data Encryption Algorithm (FEAL) [33] in less time than exhaustive search for up to 31 rounds.

When the DES last came up for renewal, the NBS published a call for comments in the *Federal Register* suggesting three alternatives: reaffirm the standard for another five years, withdraw the standard, and revise the applicability of the standard. Of the thirty-three comments received, thirty-one supported reaffirmation for another five years [34]. One organization said it had no comments, but did not oppose reaffirmation, and one recommended that the DES apply only to financial transactions.

Conclusions

The two major criticisms of the DES were its key length, which was judged to be too short, and the S-boxes, which were suspect of having trapdoors because their design was classified. The results of Biham and Shamir demonstrated that a longer key would have had little effect on the strength of the algorithm with 16 rounds. These results, however, do not invalidate the use of multiple encryption as a way of substantially increasing the security.

As far as the S-boxes go, the published results, especially those of Biham and Shamir, have suggested that they were carefully designed to resist attack. No trapdoors have been found, and changes to the S-boxes, including making them more random, have been shown to weaken the algorithm. Thus, the evidence suggests that the S-boxes were classified not to conceal trapdoors, but rather for the reason given by Davies [10], namely that their designers had come across principles of cryptographic design that were considered to be important to national security.

DES has been in active field use for over a decade. No instances of successful attack, brute force or otherwise, have yet been published. This is a remarkable pragmatic validation. Although the DES is potentially vulnerable to attack by exhaustive search, the public literature suggests that such attacks can be successfully avoided with triple encryption, especially if three independent keys are used. Thus, the DES with triple encryption may provide adequate protection for its intended application for many years to come.

Acknowledgments

I am grateful to Peter Denning and Marty Hellman for many helpful suggestions. The views expressed here are my own and do not represent those of Digital Equipment Corporation.

References

[1] C. Adams and S. Tavares. Good S-boxes are easy to find. In G. Brassard, editor, *Advances in Cryptology: CRYPTO 89 Proc.* Springer-Verlag, 1989.

[2] H. R. Amirazizi and M. E. Hellman. Time-memory-processor trade-offs. *IEEE Trans. on Information Theory*, 34(3):505–512, May 1988.

[3] G. Bell. The future of high performance computers in science and engineering. *Comm. of the ACM*, 32(9):1091–1101, Sept. 1989.

[4] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. In *Advances in Cryptology: CRYPTO 90 Proc.* Springer-Verlag, 1990. to appear.

[5] D. K. Branstad, J. Gait, and S. Katzke. Report of the workshop on cryptography in support of computer security. National Bureau of Standards, NBSIR 77-1291, 1977.

[6] E. F. Brickell, J. H. Moore, and M. R. Purtill. Structure in the S-boxes of the DES. In A. M. Odlyzko, editor, *Advances in Cryptology: CRYPTO 86 Proc.* Springer-Verlag, 1987.

[7] D. Chaum and J.-H. Evertse. Cryptanalysis of DES with a reduced number of rounds. In H. C. Williams, editor, *Advances in Cryptology: CRYPTO 85 Proc.* Springer-Verlag, 1986.

[8] Lexar Corp. An evaluation of the NBS data encryption standard. Los Angeles, CA, 1976.

[9] D. W. Davies. Some regular properties of the 'data encryption standard' algorithm. In A. Sherman D. Chaum, R. Rivest, editor, *Advances in Cryptology: Proc. of CRYPTO 82.* Plenum Pub. Co., 1983.

[10] D. W. Davies and W. L. Price. *Security for Computer Networks.* John Wiley and Sons, 1984.

[11] M. Davio, Y. Desmedt, M. Fosséprez, R. Govaarts, J. Hulsbosch, P. Neutjens, P. Piret, J. Quisquater, J. Vandewalle, and P. Wouters. Analytical characteristics of the DES. In D. Chaum, editor, *Advances in Cryptology: Proc. of CRYPTO 83.* Plenum Pub. Co., 1984.

[12] D. E. Denning. *Cryptography and Data Security.* Addison-Wesley, Reading, Mass., 1982.

[13] Y. Desmedt, J. Quisquater, and M. Davio. Dependence of output on input in DES: Small avalance characteristics. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology: Proc. of CRYPTO 84*. Springer-Verlag, 1985.

[14] W. Diffie and M. Hellman. A critique of the proposed data encryption standard. *Comm. of the ACM*, 19(3):164–165, Mar. 1976.

[15] W. Diffie and M. Hellman. Exhaustive cryptanalysis of the NBS data encryption standard. *Computer*, 10(6):74–84, June 1977.

[16] M. Hellman, R. Merkle, R. Schroeppel, L. Washington, W. Diffie, S. Pohlig, and P. Schweitzer. Results of an initial attempt to cryptanalyze the NBS data encryption standard. Technical report, Information Systems Lab., Dept. of Electrical Eng., Stanford Univ., 1976.

[17] M. E. Hellman. A cryptanalytic time-memory tradeoff. *IEEE Trans. on Info. Theory*, IT-26(4):401–406, July 1980.

[18] M. E. Hellman. On DES-based, synchronous encryption. Technical report, Dept. of Electrical Eng., Stanford Univ., Stanford, Calif., 1980.

[19] M. E. Hellman and J. V. Reyneri. The distribution of drainage and the data encryption standard. In A. Sherman D. Chaum, R. Rivest, editor, *Advances in Cryptology: Proc. of CRYPTO 82*. Plenum Pub. Co., 1983.

[20] F. Hoornaert, J. Goubert, and Y. Desmedt. Efficient hardware implementation of the DES. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology: Proc. of CRYPTO 84*. Springer-Verlag, 1985.

[21] B. S. Kaliski, R. L. Rivest, and A. T. Sherman. Is the data encryption standard a group? In F. Pichler, editor, *Advances in Cryptology: EUROCRYPT 85 Proc.* Springer-Verlag, 1985.

[22] B. S. Kaliski, R. L. Rivest, and A. T. Sherman. Is DES a pure cipher? In H. C. Williams, editor, *Advances in Cryptology: CRYPTO 85 Proc.* Springer-Verlag, 1986.

[23] R. C. Merkle and M. E. Hellman. On the security of multiple encryption. *Comm. ACM*, 27(7):465–467, July 1981.

[24] C. H. Meyer and S. M. Matyas. *Cryptography: A New Dimension in Computer Data Security*. John Wiley and Sons, 1982.

[25] J. H. Moore and G. J. Simmons. Cycle structure of the DES with weak and semi-weak keys. In A. M. Odlyzko, editor, *Advances in Cryptology: CRYPTO 86 Proc.* Springer-Verlag, 1987.

[26] R. Morris, N. J. A. Sloane, and A. D. Wyner. Assessment of the National Bureau of Standards proposed Federal data encryption standard. *Cryptologia*, 1(3):281–291, July 1977.

[27] National Bureau of Standards. Encryption algorithm for computer data protection: Requests for comments. *Federal Register*, 40(52):12134, March 17 1975.

[28] National Bureau of Standards. Notice of a proposed federal information processing data encryption standard. *Federal Register*, 40(149):12607, August 1 1975.

[29] National Bureau of Standards. Data encryption standard, Jan. 1977. FIPS PUB 46.

[30] National Institute of Standards and Technology. NCSL bulletin, June 1980.

[31] J. A. Reeds and J. L. Manferdelli. DES has no per round linear factors. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology: Proc. of CRYPTO 84*. Springer-Verlag, 1985.

[32] A. Shamir. On the security of DES. In H. C. Williams, editor, *Advances in Cryptology: CRYPTO 85 Proc.* Springer-Verlag, 1986.

[33] A. Shimizu and S. Miyaguchi. Fast data encipherment algorithm feal. In *Advances in Cryptology: EUROCRYPT 87 Proc.* Springer-Verlag, 1987.

[34] M. E. Smid and D. K. Branstad. The data encryption standard: Past and future. *Proc. of the IEEE*, 76(5):550–559, May 1988.

[35] R. Sugarman. On foiling computer crime. *IEEE Spectrum*, 16(7):31–32, July 1979.

[36] W. Tuchman. Hellman presents no shortcut solutions to the DES. *IEEE Spectrum*, 16(7):40–41, July 1979.