Cryptanalytic Progress: Lessons for AES

John Kelsey[1], Niels Ferguson[1], Bruce Schneier[1], and Mike Stay[2]

[1] Counterpane Internet Security, Inc., 3031 Tisch Way, 100 Plaza East, San Jose, CA 95128, USA
[2] AccessData Corp., 2500 N University Ave. Ste. 200, Provo, UT 84606, USA

1 Introduction

The cryptanalytic community is currently evaluating five finalist algorithms for the AES. Within the next year, one or more ciphers will be chosen. In this note, we argue caution in selecting a finalist with a small security margin. Known attacks continuously improve over time, and it is impossible to predict future cryptanalytic advances. If an AES algorithm chosen today is to be encrypting data twenty years from now (that may need to stay secure for another twenty years after that), it needs to be a very conservative algorithm.

In this paper, we review cryptanalytic progress against three well-regarded block ciphers and discuss the development of new cryptanalytic tools against these ciphers over time. This review illustrates how cryptanalytic progress erodes a cipher's security margin. While predicting such progress in the future is clearly not possible, we claim that assuming that no such progress can or will occur is dangerous.

Our three examples are DES, IDEA, and RC5. These three ciphers have fundamentally different structures and were designed by entirely different groups. They have been analyzed by many researchers using many different techniques. More to the point, each cipher has led to the development of new cryptanalytic techniques that not only have been applied to that cipher, but also to others.

2 DES

DES was developed by IBM in the early 1970s, and standardized made into a standard by NBS (the predecessor of NIST) [NBS77]. Rumors about NSA involvement in the design circulated, particularly about the short key length and the S-boxes. For many years, DES has been the most important target for cryptanalysis; many new techniques introduced in the last few years have been measured primarily against DES.

DES is a balanced Feistel cipher, encrypting a 64-bit block with a 56-bit key. The cipher consists of sixteen rounds. In each round, one 32-bit half of the block is fed into a round function, along with 48 bits of key; the 32-bit result is XORed into the other half. DES' strength derives from the combination of 6-bit to 4-bit S-boxes and a 32-bit permutation. As was discovered in the past few years, its strength is extremely sensitive to the precise S-box contents and ordering, and the specific bit permutation used. Small changes often have a catastrophic impact on security.

Year	Complexity
1987	$2^{56.6}$
1990	2^{47}
1993	2^{43}

Table 1. DES Attack Complexity

2.1 Analysis

Following are the major cryptanalytic attacks against DES:

- 1976: For a very small class of weak keys, DES can be broken with complexity 1 [HMS+76].
- 1977: Exhaustive search will become possible within 20 years, breaking DES with complexity 2^{56} [DH77].
- 1980: A time/memory tradeoff can break DES faster at the expense of more memory. DES can be broken with time complexity 1 and 2^{56} memory.
- 1982: For a very small class of semi-weak keys, DES can be broken with complexity 1 [Dav82].
- 1985: A meet-in-the middle attack can break 6-round DES with complexity 2^{52} [CE85].
- 1987: The so-called "Davies Attack" can break DES with complexity $2^{56.6}$, slightly worse than brute force [Dav87].
- 1990: Differential cryptanalysis can break DES with 2^{47} chosen plaintexts. Note that this attack was used in the previous year to break reduced-round versions of DES [BS90], and that DES was optimized against this attack.
- 1992: Related-key cryptanalysis can break a modified version of DES with complexity 2^{17} chosen-key/chosen-plaintext queries [Bih92]. Note that DES was specifically engineered to make this attack impossible.
- 1993: Linear cryptanalysis can break DES with 2^{43} known plaintexts [Mat93].
- 1994: Differential-linear cryptanalysis can break 8-round DES with 768 chosen plaintexts plus a 2^{46} brute-force search [LH94].
- 1994: The Davies attack can be improved, and can break DES with 2^{52} known plaintexts [Bih94].
- 1995: Differential cryptanalysis using partial differentials can break 6-round DES with 32 chosen plaintexts and 2^{20} work [Knu95].
- 1996: Linear cryptanalysis using nonlinear approximations can break DES with 117,824 known plaintexts and a 2^{50} brute-force search. This technique was more effective against other algorithms [KR96].

What is interesting to note, aside from the sheer number of different techniques that have been applied to DES, is how the complexity of analytic cryptanalysis has improved over the years. Table 1 summarizes this trend.

Even today there are minor improvements in linear cryptanalysis that make the best attack even better.

2.2 Current Status

At present, DES' short key size makes it unacceptable for most applications. However, variants such as triple-DES and DESX allow continued use of this cipher.

Despite excellent cryptanalytic progress, brute-force keysearch is still the only practical way known to attack DES. While a number of academic attacks break DES with less work than a keysearch, these require enormous amounts of traffic encrypted under a single key or special circumstances (related-key attacks, power analysis, differential fault analysis, etc.). After more than twenty years of progress against DES, it is widely believed that the cryptographic community has a good grasp on how to attack DES-like ciphers. It would be very surprising to see a massive improvement on the best known attack on DES, though of course, there is no *proof* that such improvements aren't available.

3 PES, IPES, and IDEA

PES, the predecessor to IDEA, was proposed by Lai and Massey in [LM91]. After the publication of differential cryptanalytic techniques, IPES (later renamed IDEA) was derived by making a small change to PES, and was described in [LMM91]. IDEA became widely known for a number of reasons: the reputation of its designers, the elegance of its design, and its use in the early freeware e-mail package PGP.

IDEA encrypts a 64-bit block with a 128-bit key. IDEA consists of two different kinds of "half-round" structures. In the first, a combination of modulo 2^{16} additions and modulo $2^{16}+1$ multiplications are used to combine 64 bits of key material into the 64-bit block. In the second, the 16-bit words are mixed together using a structure called an MA-box, and the two middle resulting words are swapped. Two of these "half-rounds" make one IDEA round. There are a total of 8.5 rounds, because of an additional half-round at the end to make the cipher identical except for key material in the forward and backward directions.

3.1 Analysis

These are the major attacks against IDEA, after the redesign to make the algorithm secure against differential cryptanalysis:

- 1993: For a class of weak keys, 8.5-round IDEA can be broken with two chosen plaintexts [DGV93].
- 1993: A partial distributive attack can break 2-round IDES with 2^{42} complexity [Mei93].
- 1996: A related-key differential attack can break 3.5-round IDEA with 2^{17} adaptive chosen plaintexts, three related-key queries, and about 2^{32} work.
- 1997: A truncated-differential attack can break 3.5-round IDEA for about 1% of the keys with 2^{40} chosen-plaintexts and 2^{51} work. A differential-linear attack can break 3-round IDEA with 2^{30} chosen plaintexts, and about 2^{44} work [BKR97].

Year	Rounds
1993	2
1997	3.5
1999	4.5

Table 2. Rounds of IDEA Cryptanalyzable

– 1999: The miss-in-the-middle impossible differential attack can break 4.5-round IDEA with 2^{64} known plaintexts and 2^{112} work [BBS99].

For IDEA, the most striking improvement is in the number of rounds that can be broken faster than brute force as a function of year (see Table 2).

The three attacks are very different, and are not simply improvements of each other.

3.2 Current Status

IDEA is still a highly regarded cipher. Despite continued progress in cryptanalysis of this cipher, even the best known attacks penetrate just over half of the full cipher. However, it is clear that quite a bit of progress has been made in cryptanalyzing the cipher. Initially, few people had any ideas on how to attack it. Over time, researchers analyzed the interaction between the three operations, from which IDEA derives all its strength, and were able to find weaknesses.

4 RC5

RC5 is an elegant cipher, and is very fast on machines that can handle variable rotates well [Riv95]. Ron Rivest's reputation (as the designer of the MD4 [Riv91] and MD5 [Riv92] hash functions, as well as the then recently leaked RC4 stream cipher [Sch96] (and one of the inventors of the RSA public-key algorithm) ensured that the cipher would get a lot of attention.

RC5 is one of the simplest ciphers ever to be fielded, and yet appears to be quite secure with enough rounds. We can describe its round function here in pseudocode:

$$
\begin{aligned}
L &\leftarrow L \text{ XOR } R \\
L &\leftarrow L <<< R \\
L &\leftarrow L + \text{subkey}[2i] \\
R &\leftarrow R \text{ XOR } L \\
R &\leftarrow R <<< L \\
R &\leftarrow R + \text{subkey}[2i+1]
\end{aligned}
$$

Year	Complexity
1995	2^{62}
1996	2^{53}

Table 3. RC5 Attack Complexity

The cipher was specified with a variable number of rounds, but Rivest originally believed 12 rounds might be sufficient. The simplicity of the cipher makes it very clear that data-dependent rotations are the basis of whatever security it can provide. In later research, it was also made clear that the mixing of XOR and add operations is required for security [KSW99].

4.1 Analysis

The initial 12-round proposal was quickly increased to 16 rounds in light of these attacks:

- 1995: Three results were presented: a differential attack against 9-round RC5 that requires 2^{45} chosen plaintexts, a differential attack against 12-round RC5 that requires 2^{62} chosen plaintexts, and a linear attack against 5-round RC5 that requires 2^{47} known plaintexts [KY95].
- 1996: For a small class of keys, 12-round RC5 can be broken with 2^{10} chosen plaintexts [KSW96].
- 1996: A differential attack can break 12-round RC5 with 2^{53} chosen plaintexts [KM96]. Additionally, for a small class of weak keys, the same attack can break 12-round RC5 with complexity 2^{40} (plus complexity 2^{45} to detect the weak key class).
- 1999: If XOR is replaced by addition in RC5, a mod n attack can break this variant (called RC5P) with 2^{61} texts and 2^{67} work: 16 rounds in the average case, and 19 rounds for a small class of weak keys [KSW99].

This may change soon. A new attack that targets the data-dependent rotations in RC6, a more complicated algorithm, can break 15-round RC6 faster than brute force [KM00]. These techniques may apply to RC5.

4.2 Current Status

RC5 appears to be secure with a sufficient number of rounds. The pace of progress in analyzing data-dependent rotations, however, has made it somewhat difficult to determine what a sufficient number of rounds will be five or ten years in the future. Recent attacks against data-dependent rotations in both RC6 [KM00] and RC5 variants [KSW99] show that the cryptanalytic properties of this primitive are not yet fully understood.

5 Conclusions

The NSA has a saying: "Attacks always get better; they never get worse." The cryptanalysis of these three well-designed ciphers, as well as many less well-designed ones, has followed a trend. At first, a cipher based on some fundamentally new ideas is fielded, and the existing attacks for other ciphers are tried, and generally don't work very well. Over time, analysis of these ciphers improves, as the underlying sources of strength (small S-boxes applied in parallel alternating with bit permutations, mixing of operations from different algebraic groups, data-dependent rotations) are better understood. Improved tools for analyzing these ciphers are developed.

Over the past few years we've seen several new cryptanalytic tools: mod n cryptanalysis, boomerang attacks, slide attacks, inside-out attacks, truncated differentials, impossible differentials, differential meet-in-the-middle attacks, etc. These tools are still being understood and improved as they are applied to different algorithms.

We believe that history makes a case for selecting an AES that is very conservative in terms of number of rounds. The AES candidates were only announced in mid-1998; there has been less than two years of public cryptanalysis for any of the ciphers. Although all the AES finalists can trace their lineage through older designs[1], this is not a reliable metric by any means. Design elements used well in one algorithm can completely break a different algorithm; paper after paper has shown this to be true.

Luckily, NIST is not limited by the number of rounds in the AES candidate submission documents; NIST is free to alter its value in any way. We strongly recommend that NIST take advantage of this freedom. In his first-round comments to NIST on AES, Lars Knudsen suggested a measure for determining the number of rounds of a cipher selected as AES: take the largest number of rounds that can be broken faster than brute force and double it [Knu99]. We agree with the sentiment behind this recommendation, but aren't certain whether an even larger multiplier might be justified.

The distressing thing about cryptography is that we cannot predict the future. We have no way of knowing whether someone will publish a 2^{32} attack on DES next year. Neither its long history of analysis, its alleged NSA pedigree, nor its clever and resourceful designers have protected it from *three* known attacks better than brute-force. Whatever algorithm is selected for AES needs to

[1] Actually, they're not even very old; all the finalists had ancestors in the first three years of FSE:

- Rijndael: 3-Way, Shark
- Twofish: Blowfish, SAFER, Shark
- MARS: RC5, SEAL, MacGuffin
- RC6: RC5
- Serpent: Lucifer, SAFER

be reviewed regularly. There is a huge difference between "I don't know how to break this cipher" and "this cipher can't be broken."

If there's any moral from all of this, it's to be conservative. AES is too important to get wrong.

6 Acknowledgements

References

[BBS99] E. Biham, A. Biryukov, and A. Shamir, "Miss in the Middle Attacks on IDEA and Khufu," *Fast Software Encryption: 6th International Workshop, FSE '99*, Springer-Verlag, 1999, pp. 124–138.

[Bih92] E. Biham, "New Types of Cryptanalytic Attacks using Related Keys," Technical Report #753, Computer Science Department, Technion — Israel Institute of Technology, Sep. 1992.

[Bih94] E. Biham and A. Biryukov, "An Improvement of Davies' Attack on DES," *Advances in Cryptology — EUROCRYPT '94 Proceedings*, Springer-Verlag, 1995, pp. 461–467.

[BKR97] J. Borst, L.R. Knudsen, and V. Rijmen, "Two Attacks on Reduced IDEA (Extended Abstract)," *Advances in Cryptology — EUROCRYPT '97 Proceedings*, Springer-Verlag, 1998, pp. 1–13.

[BS90] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," *Advances in Cryptology — CRYPTO '90 Proceedings*, Springer-Verlag, 1991, pp. 2–21.

[CE85] D. Chaum and J.-H. Evertse, "Cryptanalysis of DES with a Reduced Number of Rounds; Sequences of Linear Factors in Block Ciphers," *Advances in Cryptology — CRYPTO '85 Proceedings*, Springer-Verlag, 1986, pp. 192–211.

[Dav82] D.W. Davies, "Some Regular Properties of the DES," *Advances in Cryptology: Proceedings of Crypto 82*, Springer-Verlag, Plenum Press, 1983, pp. 89–96.

[Dav87] D.W. Davies, *Investigation of a Potential Weakness in the DES Algorithm*, private communications with Eli Biham, 1987.

[DGV93] J. Daemen, R. Govaerts, and J. Vandewalle, "Block Ciphers Based on Modular Arithmetic," *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography*, Rome, Italy, 15–16 Feb. 1993, pp. 80–89.

[DH77] W. Diffie and M.E. Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard," *Computer*, v. 10, n. 6, Jun. 1977, pp. 74–84.

[Hel80] M.E. Hellman, "A Cryptographic Time-Memory Trade Off," *IEEE Transactions on Information Theory*, v.26, n.4, Jul. 1980, pp. 401–406.

[HMS+76] M.E. 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 SEL 76-042, Information Systems Lab, Department of Electrical Engineering, Stanford University, 1976.

[KM96] L.R. Knudsen and W. Meier, "Improved Differential Attacks on RC5," *Advances in Cryptology — CRYPTO '96 Proceedings*, Springer-Verlag, 1997, pp. 216–228.

[KM00] L.R. Knudsen and W. Meier, "Correlations in RC6," draft manuscript.

[Knu95] L.R. Knudsen, "Applications of Higher Order Differentials and Partial Differentials," *K.U. Leuven Workshop on Cryptographic Algorithms*, Springer-Verlag, 1995.

[Knu99] L. Knudsen, "Some Thoughts on the AES Process," comment submitted to NIST, 15 April 1999.

[KR96] L.R. Knudsen and M.J.B. Robshaw, "Nonlinear Approximations in Linear Cryptanalysis," *Advances in Cryptology — EUROCRYPT '96 Proceedings*, Springer-Verlag, 1997, pp. 224–236.

[KSW96] J. Kelsey, B. Schneier, and D. Wagner, "Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES," *Advances in Cryptology — CRYPTO '96 Proceedings*, Springer-Verlag, 1997, pp. 237–251.

[KSW99] J. Kelsey, B. Schneier, and D. Wagner, "Mod n Cryptanalysis, With Applications Against RC5P and M6," *Fast Software Encryption: 6th International Workshop, FSE '99*, Springer-Verlag, 1999, pp. 139–155.

[KY95] B.S. Kaliski Jr. and Y.L. Yin, "On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm," *Advances in Cryptology — CRYPTO '95 Proceedings*, Springer-Verlag, 1996, pp. 171–184.

[LH94] S. Langford and M.E. Hellman, "Cryptanalysis of DES," presented at 1994 RSA Data Security Conference, Redwood Shores, CA, 12–14 Jan. 1994.

[LM91] X. Lai and J. Massey, "A Proposal for a New Block Encryption Standard," *Advances in Cryptology — EUROCRYPT '90 Proceedings*, Springer-Verlag, 1991, pp. 389–404.

[LMM91] X. Lai, J. Massey, and S. Murphy, "Markov Ciphers and Differential Cryptanalysis," *Advances in Cryptology — CRYPTO '91 Proceedings*, Springer-Verlag, 1991, pp. 17–38.

[Mat93] M. Matsui, "Linear Cryptanalysis of DES Cipher (I)," *Proceedings of the 1993 Symposium on Cryptography and Information Security (SCIS 93)*, Shuzenji, Japan, 28–30 Jan, 1993, pp. 3C.1–14. (In Japanese.)

[Mei93] W. Meier, "On the Security of the IDEA Block Cipher," *Advances in Cryptology — EUROCRYPT '93 Proceedings*, Springer-Verlag, 1994, pp. 371–385.

[NBS77] National Bureau of Standards, NBS FIPS PUB 46, "Data Encryption Standard," National Bureau of Standards, U.S. Department of Commerce, Jan 1977.

[Riv91] R.L. Rivest, "The MD4 Message Digest Algorithm," *Advances in Cryptology — CRYPTO '90 Proceedings*, Springer-Verlag, 1991, pp. 303–311.

[Riv92] R.L. Rivest, "The MD5 Message Digest Algorithm," RFC 1321, Apr 1992.

[Riv95] R.L. Rivest, "The RC5 Encryption Algorithm," *Fast Software Encryption, 2nd International Workshop Proceedings*, Springer-Verlag, 1995, pp. 86–96.

[Sch96] B. Schneier, *Applied Cryptography, Second Edition*, John Wiley & Sons, 1996.