A SELF-STUDY COURSE IN BLOCK-CIPHER CRYPTANALYSIS

Bruce Schneier

ADDRESS: Counterpane Internet Security, In., 3031 Tisch Way, San Jose CA 95128 USA. schneier@counterpane.com.

ABSTRACT: Studying cryptanalysis is difficult because there is no standard textbook, and no way of knowing which cryptanalytic problems are suitable for different levels of students. This paper attempts to organize the existing literature of block-cipher cryptanalysis in a way that students can use to learn cryptanalytic techniques and ways to break new algorithms.

KEYWORDS: Cryptanalysis, block ciphers.

1 INTRODUCTION

Ever since writing *Applied Cryptography*, I have been asked to recommend a book on cryptanalysis. My unfortunate answer is that while there are several good books on cryptography, there are no books, good or bad, on cryptanalysis. It is a void that I don't see being filled anytime soon; cryptanalysis is such a fast-moving field that any book of techniques would be obsolete before it was printed. And even if the book could somehow remain current, it would do little to teach cryptanalysis.

The only way to learn cryptanalysis is through practice. A student simply has to break algorithm after algorithm, inventing new techniques and modifying existing ones. Reading others' cryptanalysis results helps, but there is no substitute for experience.

This answer prompts another question: where does one get practice? The Internet is an endless source of mediocre algorithm designs, and some even creep into the academic literature, but the beginning cryptanalysis student has no way of knowing which algorithms are worth studying and which are beyond his ability. Trying to break algorithms that have already been broken (without looking at the breaks first) is the only answer.

Now the question becomes: which ciphers should one try to break, and in what order? This paper is my attempt at an answer, and in this answer, I hope to facilitate the study of cryptanalysis.

This is a self-study course in block-cipher cryptanalysis. With it, a student can follow a semi-ordered path through the academic literature and emerge out the other side fully capable of breaking new algorithms and publishing new cryptanalytic results.

What I have done is to list published algorithms and published cryptanalyses in a coherent order: by type of cryptanalysis and difficulty. A student's task is to read papers describing algorithms, and then attempt to reproduce published cryptanalytic results. (It is definitely more difficult to learn cryptanalysis from academic papers than from a distilled textbook, but the sooner a student gets used to reading academic papers, the better off he will be.) The results, in other published papers, serve as an "answer key."

The answer key is never definitive; it is very probable that there are other, and better, attacks than what has been published. Some cryptanalysis papers contain mistakes. Students taking this course could end up with publishable results themselves.

Even the best student will not be able to find every published break without looking at the associated cryptanalysis paper. Many of these results were discovered by some of the best cryptanalytic minds in academia. I feel that a student should spend at least a week trying to break an algorithm without looking at the cryptanalysis paper, and after that just quickly skimming the result—or just reading the abstract, introduction, and conclusion—and then again trying to break the algorithm for at least another three days.

If a student still can't break the cipher, it makes sense at this point to read and study the published cryptanalysis. If a student can't break any of the ciphers—especially the easy ones—it's a good indication that he should find another line of work.

The lessons are in order, but the ordering is loose in places. The first lessons are easier, but then I try to mix things up a bit. Students should feel free to skip lessons that are hard and go back to them, or even skip a few entirely (there are quite a lot of them). It is also not my intention for a student to fully complete one lesson before going on to the next. A smart student will probably work on several lessons at once.

Good luck.

2 WHAT DOES IT MEAN TO "BREAK" A CIPHER?

Breaking a cipher doesn't necessarily mean finding a practical way for an eavesdropper to recover the plaintext from just the ciphertext. In academic cryptography, the rules are relaxed considerably. Breaking a cipher simply means finding a weakness in the cipher that can be exploited with a complexity less

than brute-force. Never mind that brute-force might require 2^{128} encryptions; an attack requiring 2^{110} encryptions would be considered a break. Breaks might also require unrealistic amounts of known or chosen plaintext—2^{56} blocks—or unrealistic amounts of storage: 2^{80}. Simply put, a break can just be a "certificational weakness": evidence that the cipher does not perform as advertised.

Successful cryptanalysis might mean showing a break against a reduced-round variant of the cipher—8-round DES versus the full 16-round DES, for example—or a simplified variant of the cipher. Most breaks start out as cryptanalysis against reduced-round variants, and are eventually (maybe years later) extended to the full cipher. In fact, a break on a reduced-round version of a cipher is often a publishable result.

3 WHY BLOCK CIPHERS?

Academic research in block ciphers has progressed along a different course than research in stream ciphers. Block cipher papers have traditionally been concrete designs (with specific parameters and names) or breaks of those designs. Stream cipher papers are more often general design or analysis techniques, with general applications and examples. While stream-cipher cryptanalysis is at least as important as block cipher cryptanaysis, and in military circles more important, it is much harder to string a course together using existing academic papers. A good survey paper on stream ciphers is available online at `http://www.rsasecurity.com/rsalabs/technotes`.

4 PREREQUISITES

It will be almost impossible to understand some cryptanalytic results without a good understanding of simple concepts from probability and statistics. *The Handbook of Applied Cryptography* has a very fast-paced introduction of a great deal of probability theory; however, students learning this for the first time may find that a dedicated textbook on probability and statistics provides a gentler introduction to the subject.

Other topics from discrete mathematics and computer science are also useful, though they are not strictly necessary to know. A student should know, or be prepared to learn, linear algebra, group theory, complexity theory, combinatorics, and graph theory. These could be profitably studied concurrently with cryptanalysis.

It is impossible to really understand a cryptanalytic attack without implementing it. Implementing an attack described in a paper can be very instructive; implementing a new attack of your own invention often exposes subtleties that

theoretical analysis fails to. For that reason, mathematical programming in a language such as C is also a required skill.

4.1 Historical Background

The cryptanalysis of pre-computer encryption algorithms is not really applicable to the cryptanalysis of modern algorithms, but it makes for interesting reading and is a good example of the mindset required to perform cryptanalysis. I don't consider this a required prerequisite, but the interested student should consider reading Helen Fourche Gaines, *Cryptanalysis: A Study of Ciphers and their Solution* (Dover Publications, 1939). Also interesting are the volumes written by William F. Friedman and reprinted by Aegean Park Press: *Elements of Cryptanalysis*; *Military Cryptanalysis*, Parts I, II, III, and IV; *The Riverbank Publications*, Parts I, II, and III; and *Military Cryptanalytics*, Part I, Vol. 1 and 2, and Part II, Vol. 1 and 2. Aegean Park Press is at *http://www.aegeanparkpress.com/books/*.

A careful reading of David Kahn, *The Codebreakers* (The Macmillan Company, 1967), is indispensible for an understanding of the history of cryptography. I recommend it highly.

5 OBTAINING COURSE MATERIAL

The papers used in the course come from the proceedings of many different conferences. I have tried to avoid obscure publications, but invariably some have crept in. This means that many good block ciphers are not listed above: CAST is a prime example. Please don't take a cipher's exclusion from the list as evidence of strength or weakness; it is simply a matter of availability.

Almost all papers come from Springer-Verlag conference proceedings, all published in the *Lecture Notes in Computer Science* (LNCS) series. Most university libraries subscribe to the entire LNCS series. At a minimum, a student should have the CD-ROM consisting of all the Crypto and Eurocrypt proceedings (available from Springer-Verlag), and the proceedings from the Fast Software Encryption (FSE) series. There are many more papers in those proceedings worth reading than the ones listed here.

I maintain a Web page at `http://www.counterpane.com` with pointers to the papers on the WWW. Among the CD-ROM, the FSE proceedings, and my Web resources, it is possible to do almost everything in the course.

6 THE COURSE

6.1 Background

Read at least two of the following: B. Schneier, *Applied Cryptography, Second Edition* (John Wiley & Sons, 1996); D.R. Stinson, *Cryptography: Theory and Practice* (CRC Press, 1995); and A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, 1997). Concentrate on the chapters on block ciphers, but I recommend strongly that you read the entire books.

6.2 Basic Cryptanalysis

Try to cryptanalyze the following simplified algorithms:

- 8-round RC5 without any rotations.
- 8-round RC5 with the rotation amount equal to the round number.
- 12-round DES without any S-boxes.
- 8 rounds of Skipjack's rule B. (A description of Skipjack can be found on the World Wide Web.)
- 4-round DES.
- A generic cipher that is "closed" (i.e., encrypting with key A and then key B is the same as encrypting with key C, for all keys).
- 6-round DES.
- 4 rounds of Skipjack's rule A followed by four rounds of Skipjack's rule B.

All of these algorithms are described in B. Schneier, *Applied Cryptography, Second Edition* (John Wiley & Sons, 1996) and A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, 1997). If you can't break the specific variants listed above, what further simplifications can you break? Can you break even more reduced-round variants?

6.3 Cryptanalysis of FEAL

It seems that almost every modern cryptanalytic attack works against FEAL. First read the algorithm: A. Shimizu and S. Miyaguchi, "Fast Data Encipherment Algorithm FEAL" (*Advances in Cryptology — EUROCRYPT '87 Proceedings*, Springer-Verlag, 1988, pp. 267–278). Now, try to break it. Some attacks can be found in: B. Den Boer, "Cryptanalysis of F.E.A.L." (*Advances in Cryptology — EUROCRYPT '88 Proceedings*, Springer-Verlag, 1988, pp. 275–280); H. Gilbert

and P. Chasse, "A Statistical Attack on the FEAL-8 Cryptosystem" (*Advances in Cryptology — CRYPTO '90 Proceedings*, Springer-Verlag, 1991, pp. 22–33); and A. Tardy-Corfdir and H. Gilbert, "A Known Plaintext Attack of FEAL-4 and FEAL-6" (*Advances in Cryptology — CRYPTO '91 Proceedings*, Springer-Verlag, 1992, pp. 172–182). You can also reinvent both differential and linear cryptanalysis if you try hard enough.

6.4 Differential Cryptanalysis

Read Chapters 1 through 5 of E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard* (Springer-Verlag, 1993). If you can't find the book, read E. Biham and A. Shamir, "Differential Cryptanalysis of the Full 16-Round DES (*Advances in Cryptology — CRYPTO '91 Proceedings*, Springer-Verlag, 1992, pp. 487–496).

6.5 Differential Cryptanalysis of FEAL

Attack FEAL using differential cryptanalysis. One solution, which is the first paper to talk about differential attacks, is S. Murphy, "The Cryptanalysis of FEAL-4 with 20 Chosen Plaintexts" (*Journal of Cryptology*, V. 2, N. 3, 1990, pp. 145–154). Also see Chapter 6 of E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard* (Springer-Verlag, 1993).

6.6 Differential Cryptanalysis of LOKI-89

The first version of LOKI is now called LOKI-89. Read L. Brown, J. Pieprzyk, and J. Seberry, "LOKI: A Cryptographic Primitive for Authentication and Secrecy Applications" (*Advances in Cryptology — AUSCRYPT '90 Proceedings*, Springer-Verlag, 1990, pp. 229–236). Find a differential attack; a solution is in L.R. Knudsen, "Cryptanalysis of LOKI" (*Advances in Cryptology — ASIACRYPT '91*, Springer-Verlag, 1993, pp. 22–35). Biham and Shamir's book also discusses this cryptanalysis.

6.7 Differential Cryptanalysis of MacGuffin

Read M. Blaze and B. Schneier, "The MacGuffin Block Cipher Algorithm" (*Fast Software Encryption, Second International Workshop Proceedings*, Springer-Verlag, 1995, pp. 97–110). Try to break the cipher. A differential attack is in V. Rijmen and B. Preneel, "Cryptanalysis of MacGuffin" (*Fast Software Encryption, Second International Workshop Proceedings*, Springer-Verlag, 1995, pp. 353–358).

There are many more attacks, none of which have been published. It is worth spending time on this algorithm, even going back to it again later in this course. As you learn more techniques, you will discover more attacks.

6.8 Differential Cryptanalysis of Khafre

Read the description of Khafre in R.C. Merkle, "Fast Software Encryption Functions" (*Advances in Cryptology — CRYPTO '90 Proceedings*, Springer-Verlag, 1991, pp. 476–501). Try to break it. A differential attack is in E. Biham and A. Shamir, "Differential Cryptanalysis of Snefru, Khafre, REDOC II, LOKI, and Lucifer" (*Advances in Cryptology — CRYPTO '91 Proceedings*, Springer-Verlag, 1992, pp. 156–171). See also Biham and Shamir's book.

6.9 Differential Cryptanalysis of PES

The precursor to IDEA was PES; see 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). Try to break it using differential cryptanalysis. Results (and a redesign) are in X. Lai, J. Massey, and S. Murphy, "Markov Ciphers and Differential Cryptanalysis" (*Advances in Cryptology — CRYPTO '91 Proceedings*, Springer-Verlag, 1991, pp. 17–38).

6.10 Linear Cryptanalysis

Read M. Matsui, "Linear Cryptanalysis Method for DES Cipher" (*Advances in Cryptology — EUROCRYPT '93 Proceedings*, Springer-Verlag, 1994, pp. 386–397). Try to improve on the results. A solution is in M. Matsui, "The First Experimental Cryptanalysis of the Data Encryption Standard" (*Advances in Cryptology — CRYPTO '94 Proceedings*, Springer-Verlag, 1994, pp. 1–11).

6.11 Linear Cryptanalysis of FEAL

Try to break FEAL using linear cryptanalysis techniques. Solutions are in M. Matsui and A. Yamagishi, "A New Method for Known Plaintext Attack of FEAL Cipher" (*Advances in Cryptology — EUROCRYPT '92 Proceedings*, Springer-Verlag, 1993, pp. 81–91), and K. Ohta and K. Aoki, "Linear Cryptanalysis of the Fast Data Encipherment Algorithm" (*Advances in Cryptology — CRYPTO '94 Proceedings*, Springer-Verlag, 1994, pp. 12–16). See also S. Moriai, K. Aoki, and K. Ohta, "Improving the Search Algorithm for the Best Linear Ex-

pression" (*Advances in Cryptology — CRYPTO '95 Proceedings*, Springer-Verlag, 1995, pp. 157–170).

6.12 Conditional Differential Characteristics

Conditional characteristics are introduced in I. Ben-Aroya and E. Biham, "Differential Cryptanalysis of Lucifer" (*Advances in Cryptology — CRYPTO '93 Proceedings*, Springer-Verlag, 1994, pp. 187–199). Read Sections 1–3, on Lucifer and conditional characteristics. Then try to find the attack before reading Section 4. Read the beginning of Section 5, on RDES. Try to find the attack before reading the rest of the paper.

6.13 Rotational Related-Key Cryptanalysis

Read the results against LOKI-89 and LOKI-91 in E. Biham, "New Types of Cryptanalytic Attacks Using Related Keys" (*Journal of Cryptology*, V. 7, N. 4, 1994, pp. 229–246). If you can't get the journal, read the preliminary copy (*Advances in Cryptology — EUROCRYPT '93*, Springer-Verlag, 1994, pp. 398–409). Attack the DES variant described in Section 5 (section 6 in the Eurocrypt version).

6.14 Differential-Linear Cryptanalysis

Read S. Langford and M. Hellman, "Differential-Linear Cryptanalysis" (*Advances in Cryptology — CRYPTO '94 Proceedings*, Springer-Verlag, 1994, pp. 17–26). Try to apply these techniques to FEAL. The answer is in K. Aoki and K. Ohta, "Differential-Linear Cryptanalysis of FEAL-8" (*IEICE Transactions: Fundamentals of Electronics, Communications, and Computer Sciences (Japan)*, V. E79-A, N. 1, 1996, pp. 20–27). Good luck finding the above; it's a Japanese journal.

6.15 Relations Between Differential and Linear Cryptanalysis

Read E. Biham, "On Matsui's Linear Cryptanalysis" (*Advances in Cryptology — EUROCRYPT '94 Proceedings*, Springer-Verlag, 1995, pp. 398–412), and F. Chabaud and S. Vaudenay, "Links Between Differential and Linear Cryptanalysis" (*Advances in Cryptology — EUROCRYPT '94 Proceedings*, Springer-Verlag, 1995, pp. 356–365).

6.16 Higher-Order Differential Cryptanalysis

If you can find it, read X. Lai, "Higher Order Derivatives and Differential Cryptanalysis" (*Communications and Cryptograpy*, Kluwer Academic Publishers, 1994, pp. 227–233). Read Section 4 of L.R. Knudsen, "Truncated and Higher Order Differentials" (*Fast Software Encryption, 2nd International Workshop Proceedings*, Springer-Verlag, 1995, pp. 196–211).

6.17 Higher-Order Differential Cryptanalysis of KN-Cipher

Read K. Nyberg and L.R. Knudsen, "Provable Security Against Differential Cryptanalysis" (*Journal of Cryptology*, V. 8, N. 1, 1995, pp. 27–37). The cipher in Section 5 is called KN-Cipher; try to break it using higher-order differentials. Kiefer is also described in K. Kiefer, "A New Design Concept for Building Secure Block Ciphers" (*Proceedings of Pragocrypt '96*, CTU Publishing House, 1996, pp. 30–41. A good solution is in T. Shimoyama, S. Moriai, and T. Kaneko, "Improving the Higher Order Differential Attack and Cryptanalysis of the *KN* Cipher" (*Information Security. First International Workshop ISW '97 Proceedings*, Springer-Verlag, 1998, pp. 32–42).

6.18 Multiple Linear Approximations

Read B. Kaliski Jr., and M. Robshaw, "Linear Cryptanalysis Using Multiple Approximations" (*Advances in Cryptology — CRYPTO '94 Proceedings*, Springer-Verlag, 1994, pp. 26–39). Try to break FEAL using these techniques. One solution is in B. Kaliski Jr., and M. Robshaw, "Linear Cryptanalysis Using Multiple Approximations and FEAL" (*Fast Software Encryption, Second International Workshop Proceedings*, Springer-Verlag, 1995, pp. 249–264).

6.19 Cryptanalysis of TWOPRIME

Read C. Ding, V. Niemi, A. Renvall, and A. Salomaa, "TWOPRIME: A Fast Stream Ciphering Algorithm" (*Fast Software Encryption, 4th International Workshop Proceedings*, Springer-Verlag, 1997, pp. 88–102). TWOPRIME is really a block cipher. Try to break it; there are all sorts of attacks. Results are in D. Coppersmith, D. Wagner, B. Schneier, and J. Kelsey, "Cryptanalysis of TWOPRIME" (*Fast Software Encryption, 5th International Workshop Proceedings*, Springer-Verlag, 1998, pp. 32–48).

6.20 Cryptanalysis of Blowfish

Read B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)" (*Fast Software Encryption, Cambridge Security Workshop Proceedings*, Springer-Verlag, 1994, pp. 191–204), and try to break Blowfish. Some results were published in S. Vaudenay, "On the Weak Keys in Blowfish" (*Fast Software Encryption, 3rd International Workshop Proceedings*, Springer-Verlag, 1996, pp. 27–32). There is also a differential attack against five-round Blowfish in V. Rijmen's PhD thesis.

6.21 Cryptanalysis of ICE

Read M. Kwan, "The Design of ICE Encryption Algorithm" (*Fast Software Encryption, 4th International Workshop Proceedings*, Springer-Verlag, 1997, pp. 69–82). A differential attack is in B. Van Rompay, L.R. Knudsen, and V. Rijmen, "Differential Cryptanalysis of ICE Encryption Algorithm" (*Fast Software Encryption, 5th International Workshop Proceedings*, Springer-Verlag, 1998, pp. 270–283.

6.22 Cryptanalysis of LOKI-91

LOKI was redesigned; the new version was called LOKI-91. Read L. Brown, M. Kwan, J. Pieprzyk, and J. Seberry, "Improving Resistance to Differential Cryptanalysis and the Redesign of LOKI" (*Advances in Cryptology — ASIACRYPT '91 Proceedings*, Springer-Verlag, 1993, pp. 36–50). Look for any kind of cryptanalysis; some results can be found in L.R. Knudsen, "Cryptanalysis of LOKI91" (*Advances in Cryptology — AUSCRYPT '92*, Springer-Verlag, 1993, pp. 196–208). A linear attack (on LOKI-91 and LOKI-89) can be found in T. Tokita, T. Sorimachi, and M. Matsui, "Linear Cryptanalysis of LOKI and s^2DES" (*Advances in Cryptology — ASIACRYPT '94*, Springer-Verlag, 1995, pp. 293–303).

6.23 Cryptanalysis of CMEA

Read Sections 1 and 2 of D. Wagner, B. Schneier, and J. Kelsey, "Cryptanalysis of the Cellular Message Encryption Algorithm" (*Advances in Cryptology — CRYPTO '97 Proceedings*, Springer-Verlag, 1997, pp. 526–537). Try to break the algorithm before reading the rest of the paper.

6.24 Cryptanalysis of IDEA

IDEA is described (it's called IPES) in X. Lai, J. Massey, and S. Murphy, "Markov Ciphers and Differential Cryptanalysis" (*Advances in Cryptology — EUROCRYPT '91 Proceedings*, Springer-Verlag, 1991, pp. 17–38). The easiest analysis is to try to find weak keys; one answer is in J. Daemen, R. Govaerts, and J. Vandewalle, "Weak Keys for IDEA" (*Advances in Cryptology — CRYPTO '93 Proceedings*, Springer-Verlag, 1994, pp. 224–231). Look for other attacks; some solutions are in W. Meier, "On the Security of the IDEA Block Cipher" (*Advances in Cryptology — EUROCRYPT '93 Proceedings*, Springer-Verlag, 1994, pp. 371–385), and P. Hawkes and L. O'Connor, "On Applying Linear Cryptanalysis to IDEA" (*Advances in Cryptology — ASIACRYPT '96*, Springer-Verlag, 1996, pp. 105–115).

6.25 Truncated Differentials

Read L.R. Knudsen, "Truncated and Higher Order Differentials" (*Fast Software Encryption, 2nd International Workshop Proceedings*, Springer-Verlag, 1995, pp. 196–211), Sections 1 though 4. Try to apply the techniques of truncated differentials before reading the results in Section 5. Try to break SAFER using truncated differentials. Results are in L.R. Knudsen and T.A Berson, "Truncated Differentials of SAFER *Fast Software Encryption, 3rd International Workshop Proceedings*, Springer-Verlag, 1996, pp. 15–26).

6.26 Differential Related-Key Cryptanalysis

Read 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, 1996, pp. 237–251). Try to apply the techniques to 3-Way, DES-X, and TEA before reading J. Kelsey, B. Schneier, and D. Wagner, "Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA" (*Information and Communications Security, First International Conference Proceedings*, Springer-Verlag, 1997, pp. 203–207).

6.27 Generalizations of Linear Cryptanalysis

Read C. Harpes, G. Kramer, and J. Massey, "A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-up Lemma" (*Advances in Cryptology — EUROCRYPT '95 Proceedings*, Springer-Verlag, 1995, pp. 24–38), C. Harpes and J. Massey, "Partitioning Cryptanalysis" (*Fast Software Encryption, 4th International Workshop Proceedings*, Springer-Verlag, 1997, pp. 13–27).

Try to apply the techniques to DES before reading Appendix C of the second paper. Read Sections 1 though 4 of B. Kaliski Jr. and M. Robshaw, "Linear Cryptanalysis Using Multiple Approximations" (*Advances in Cryptology — CRYPTO '94 Proceedings*, Springer-Verlag, 1994, pp. 26–39). Try applying the techniques to LOKI91 before reading Section 5.

6.28 Cryptanalysis of Akelarre

Read G. Álvarez, D. De la Guia, F. Montoya, and A. Peinado, "Akelarre: A New Block Cipher Algorithm" (*Workshop on Selected Areas in Cryptography (SAC '96) Workshop Record*, Queens University, 1996, pp. 1–14). Try to break the algorithm. Results are in L.R. Knudsen and V. Rijmen, "Two Rights Sometimes Make a Wrong" (*Workshop on Selected Areas in Cryptography (SAC '97) Workshop Record*, School of Computer Science, Carleton University, 1997, pp. 213–223) and N. Ferguson and B. Schneier, "Cryptanalysis of Akelarre" (*Workshop on Selected Areas in Cryptography (SAC '97) Workshop Record*, School of Computer Science, Carleton University, 1997, pp. 201–212). A description of Akelarre is in the last paper, if you can't find any of the others.

6.29 Whitening

Read J. Kilian and p. Rogaway, "How to Protect DES Against Exhaustive Key Search" (*Advances in Cryptology — CRYPTO '96 Proceedings*, Springer-Verlag, 1996, pp. 252–267).

6.30 Theory of Differential and Linear Cryptanalysis

Read the following papers: K. Nyberg, "Linear Approximation of Block Ciphers" (*Advances in Cryptology — EUROCRYPT '94 Proceedings*, Springer-Verlag, 1995, pp. 439–444), K. Nyberg and L. Knudsen, "Provable Security Against a Differential Attack," (Journal of Cryptology, V. 8, N. 1, 1995, pp. 27–37), and K. Nyberg and L. Knudsen, "Provable Security Against a Differential Cryptanalysis" (*Advances in Cryptology — CRYPTO '92 Proceedings*, Springer-Verlag, 1993, pp. 566–574).

6.31 Cryptanalysis of VINO

Read A. Di Porto and W. Wolfowicz, "VINO: A Block Cipher Including Variable Permutations" (*Fast Software Encryption, Cambridge Security Workshop*

Proceedings, Springer-Verlag, 1994, pp. 205–210). No cryptanalysis has been published; try to be the first.

6.32 Interpolation Attack

Read Sections 1 through 3.3 of T. Jakobsen and L. Knudsen, "The Interpolation Attack on Block Ciphers" (*Fast Software Encryption, 4th International Workshop Proceedings*, Springer-Verlag, 1997, pp. 28–40). Read the modifications to SHARK in Section 3.4, and attempt to break it before reading the rest of the paper.

6.33 Attacks on Non-Surjective Round Functions

Read E. Biham and A. Biryukov, "An Improvement of Davies' Attack on DES" (*Advances in Cryptology — EUROCRYPT '94 Proceedings*, Springer-Verlag, 1995, pp. 461–467). Also worth reading is B. Rijmen, B. Preneel, and E. De Win, "On Weaknesses of Non-surjective Round Functions" (*Designs, Codes, and Cryptography*, V. 12, N. 3, 1997, pp. 253–266).

6.34 Cryptanalysis of Khufu

Read the description of Khufu in R.C. Merkle, "Fast Software Encryption Functions" (*Advances in Cryptology — CRYPTO '90 Proceedings*, Springer-Verlag, 1991, pp. 476–501). Try to break it. An analysis is in H. Gilbert and P. Chauvaud, "A Chosen-Plaintext Attack on the 16-Round Khufu Cryptosystem" (*Advances in Cryptology — CRYPTO '94 Proceedings*, Springer-Verlag, 1994, pp. 359–368.)

6.35 Cryptanalysis of SAFER

Read J. L. Massey, "SAFER K-64: A Byte-Oriented Block-Ciphering Algorithm" (*Fast Software Encryption, Cambridge Security Workshop Proceedings*, Springer-Verlag, 1994, pp. 1–17). Try to attack the cipher. Results can be found in J. L. Massey, "SAFER K-64: One Year Later" (*Fast Software Encryption, 2nd International Workshop Proceedings*, Springer-Verlag, 1995, pp. 212–241); S. Vaudenay, "On the Need for Multipermutations: Cryptanalysis of MD4 and SAFER" (*Fast Software Encryption, Second International Workshop Proceedings*, Springer-Verlag, 1995, pp. 286–297); and L.R. Knudsen, "A Key-Schedule Weakness in SAFER K-64" (*Advances in Cryptology—CRYPTO '95 Proceedings*, Springer-Verlag, 1995, pp. 274–286).

6.36 Modes of Operation

Read E. Biham, "On Modes of Operation" (*Fast Software Encryption, Cambridge Security Workshop Proceedings*, Springer-Verlag, 1994, pp. 116–120) and E. Biham, "Cryptanalysis of Multiple Modes of Operation" (*Advances in Cryptology — ASIACRYPT '94 Proceedings*, Springer-Verlag, 1995, pp. 278–292). Read Sections 1 and 2 of E. Biham, "Cryptanalysis of Ladder-DES" (*Fast Software Encryption, 4th International Workshop Proceedings*, Springer-Verlag, 1997, pp. 134–138). Try to break the construction before reading the rest of the paper. Also read D. Wagner, "Analysis of Some Recently Proposed Modes of Operation" (*Fast Software Encryption, 5th International Workshop Proceedings*, Springer-Verlag, 1998, pp. 254–269), and try to break the constructions before reading the analysis.

6.37 Advanced Cryptanalysis of IDEA

Try to break IDEA using truncated differentials and differential-linear characteristics. Results are in J. Borst, L.R. Knudsen, and V. Rijmen, "Two Attacks on Reduced IDEA" (*Advances in Cryptology — EUROCRYPT '97*, Springer-Verlag, 1997, pp. 1–13) and P. Hawkes, "Differential-Linear Weak Key Classes of IDEA" (*Advances in Cryptology — EUROCRYPT '98 Proceedings*, Springer-Verlag, 1998, pp. 112–126).

6.38 Cryptanalysis of TEA

Read D. Wheeler and R. Needham, "TEA, a Tiny Encryption Algorithm" (*Fast Software Encryption, 2nd International Workshop Proceedings*, Springer-Verlag, 1995, pp. 97–110). No cryptanalysis, except of the key schedule, has been published; try to be the first.

6.39 Cryptanalysis of RC5

Read R.L. Rivest, "The RC5 Encryption Algorithm" (*Fast Software Encryption, 2nd International Workshop Proceedings*, Springer-Verlag, 1995, pp. 86–96). Try to break RC5. You can find some results in B.S. Kaliski and Y.L. Yin, "On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm" (*Advances in Cryptology—CRYPTO '95 Proceedings*, Springer-Verlag, 1995, pp. 445–454); L.R. Knudsen and W. Meier, "Improved Differential Attacks on RC5" (*Advances in Cryptology — CRYPTO '96 Proceedings*, Springer-Verlag, 1996, pp. 216–228); and A.A. Selcuk, "New Results in Linear Cryptanalysis of RC5" (*Fast*

Software Encryption, 5th International Workshop Proceedings, Springer-Verlag, 1998, pp. 1–16).

6.40 Cryptanalysis of MISTY

Read M. Matsui, "New Structure of Block Ciphers with Provable Security Against Differential and Linear Cryptanalysis" (*Fast Software Encryption, 3rd International Workshop Proceedings*, Springer-Verlag, 1996, pp. 205–218) and M. Matsui, "New Block Encryption Algorithm MISTY" (*Fast Software Encryption, 4th International Workshop Proceedings*, Springer-Verlag, 1997, pp. 54–68). The only published cryptanalytic result I know of is in Japanese: H. Tanaka, K. Hisamatsu, and T. Kaneko, "Higher Order Differential Attack of MISTY without FL Functions" (The Institute of Electronics, Information, and Communication Engineers, ISEC98-5, 1998).

6.41 Cryptanalysis of Square

Read J. Daemen, L. Knudsen, and V. Rijmen, "The Block Cipher Square" (*Fast Software Encryption, 4th International Workshop Proceedings*, Springer-Verlag, 1997, pp. 149–165), except for Section 6. Try to attack the cipher before reading that section.

6.42 AES Submissions

In 1998, the National Instutute of Standards and Technology solicited candidate block ciphers to replace DES. Fifteen submissions were received, of which five have been selected for the second round. Read about the process and the submissions at the NIST Web site, which includes links to details on the various submissions and links to various papers on cryptanalysis: `http://www.nist.gov/aes/`. Break what you can; send NIST the results. Here's your chance to affect the future encryption standard.

7 CONCLUSION

The only way to become a good algorithm designer is to be a good cryptanalyst: to break algorithms. Lots of them. Again and again. Only after a student has demonstrated his ability to cryptanalyze the algorithms of others will his own designs be taken seriously.

Given that many many ciphers are invented every year—some published, some patented, some proprietary—how do cryptanalysts know which ones are worth

further study? They look at the pedigree of the algorithm. An algorithm that has been invented by someone who has shown that he can break algorithms—he's studied the literature, perhaps using this course, and published a few breaks on his own that had not been discovered before—is much more likely to invent a secure cipher than someone who has done a cursory read of the literature and then invented something. In both cases the inventor believes his cipher is secure; in the former case the inventor's opinion is worth something.

Cryptanalysts also look at the supporting documentation associated with the design. Again, design is easy and analysis is hard. Designs that come with extensive analyses—breaks of simplified variants, reduced-round versions, alternate implementations—show that the inventor knew what he was doing when he created the cipher. When we designed Twofish, we spent over 1000 man-hours on cryptanalysis. We wrote a book consisting primarily of cryptanalysis. To us, this level of work is what it takes to design a new cipher. Only after this level of analysis by the designers should third-party cryptanalysis start. It's the "price of admission," as it were.

Anyone can create an algorithm that he himself cannot break. It's not even very difficult. What is difficult is cryptanalysis. And only an experienced cryptanalyst can design a good cipher. And the only way to get that experience is to analyze other people's ciphers.

BIOGRAPHICAL SKETCH

Bruce Schneier is Chief Technical Officer of Counterpane Internet Security, Inc., a managed security firm, and a cryptography consultant. He designed the Blowfish algorithm, still unbroken after years of cryptanalysis, and the Twofish encryption algorithm that is currently a finalist for AES. Schneier is the author of *Applied Cryptography* (John Wiley & Sons, 1994 and 1996), the seminal work in its field. Now in its second edition, Applied Cryptography has sold over 100,000 copies worldwide and has been translated into three languages. His papers have appeared at dozens of international conferences. He is a frequent writer and lecturer on the topics of cryptography, computer security, and privacy.