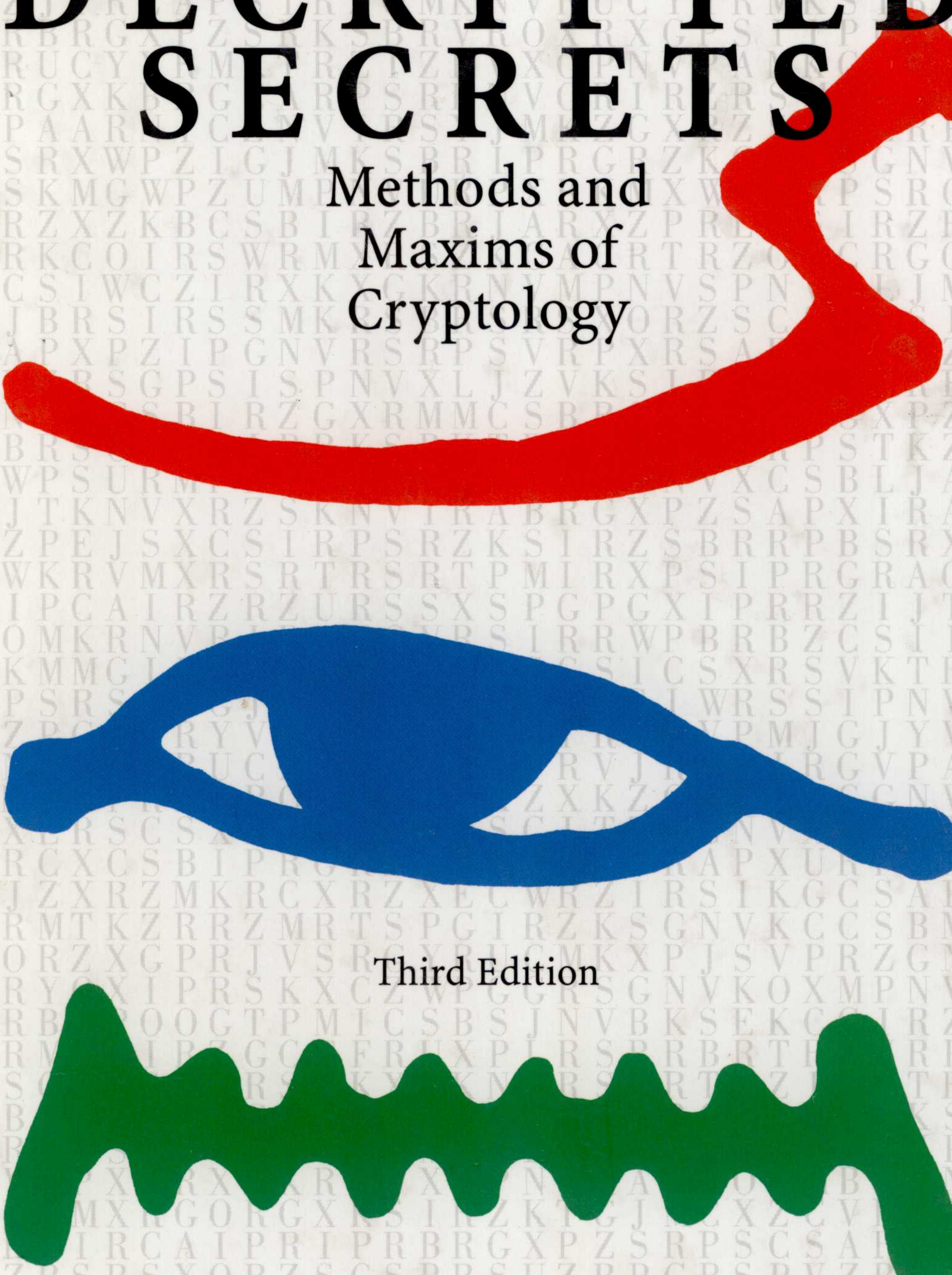
F. L. BAUER

DECRYPTED SECRETS

Methods and Maxims of Cryptology



Third Edition

Springer

Friedrich L. Bauer

Decrypted Secrets

Methods and Maxims of Cryptology

Third, Revised and Updated Edition

With 167 Figures, 26 Tables,
and 16 Color Plates

Springer

Dr. rer. nat. Dr. ès sc. h.c. Dr. rer. nat. h.c. mult. Friedrich L. Bauer
Professor Emeritus of Mathematics and Computer Science
Munich Institute of Technology
Department of Computer Science
Arcisstrasse 21
80333 Munich, Germany

ACM Computing Classification (1998): E.3, D.4.6, K.6.5, E.4
Mathematics Subject Classification (1991): 94A60, 68P25

ISBN 3-540-42674-4 Springer-Verlag Berlin Heidelberg New York

ISBN 3-540-66871-3 2nd ed. Springer-Verlag Berlin Heidelberg New York

Library of Congress Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Bauer, Friedrich L.: Decrypted Secrets : Methods and Maxims of Cryptology /
Friedrich L. Bauer. – Third, Revised and Updated Edition – Berlin; Heidelberg; New York;
Barcelona; Hong Kong; London; Milan; Paris; Tokyo: Springer, 2002
ISBN 3-540-42674-4

Springer-Verlag Berlin Heidelberg NewYork,
a member of BertelsmannSpringer Science+Business Media GmbH
http://www.springer.de

Cover Design: Design & Concept E. Smejkal, Heidelberg
Color Photos: Reinhard Krause, Deutsches Museum München
Typesetting: By the author in TEX

Printed on acid-free paper SPIN 10853358 45/3142ud – 5 4 3 2 1 0

Preface

Towards the end of the 1960s, under the influence of the rapid development of microelectronics, electromechanical cryptological machines began to be replaced by electronic data encryption devices using large scale integrated circuits. This promised more secure encryption at lower prices. Then, in 1976, Diffie and Hellman opened up the new cryptological field of public key systems. Cryptography, hitherto cloaked in obscurity, was emerging into the public domain. Additionally, ENIGMA revelations awoke the public interest.

Computer science was a flourishing new field, too, and computer scientists became interested in several aspects of cryptology. But many of them were not well enough informed about the centuries-long history of cryptology and the high level it had attained. I saw some people starting to reinvent the wheel, and others who had an incredibly naive belief in safe encryption, and I became worried about the commercial and scientific development of professional cryptology among computer scientists and about the unstable situation with respect to official security services.

This prompted me to offer lectures on this subject at the Munich Institute of Technology. The first series of lectures in the winter term 1977/78, backed by the comprehensive and reliable book *The Codebreakers* (1967) by David Kahn, was held under the code name 'Special Problems of Information Theory' and therefore attracted neither too many students nor too many suspicious people from outside the university.

Next time, in the summer term 1981, my lectures on the subject were announced under the open title 'Cryptology'. This was seemingly the first publicly announced lecture series under this title at a German, if not indeed a Continental European, university.

The series of lectures was repeated a few times, and in 1986/87 lecture notes were printed which developed into Part I of this book. Active interest on the side of the students led to a seminar on cryptanalytic methods in the summer term 1988, from which Part II of the present book originated.

The 1993 first edition of my book *Kryptologie*, although written mainly for computer science students, found lively interest also outside the field. It was reviewed favorably by some leading science journalists, and the publisher followed the study book edition with a 1995 hardcover edition under the title *Entzifferte Geheimnisse* [Decrypted Secrets], which gave me the opportunity to round out some subjects. Reviews in American journals recommended also an English version, which led to the present book.

It has become customary among cryptologists to explain how they became acquainted with the field. In my case, this was independent of the Second World War. In fact, I was never a member of any official service—and I consider this my greatest advantage, since I am not bound by any pledge of secrecy. On the other hand, keeping eyes and ears open and reading between the lines, I learned a lot from conversations (where my scientific metier was a good starting point), although I never know exactly whether I am allowed to know what I happen to know.

It all started in 1951, when I told my former professor of formal logic at Munich University, Wilhelm Britzelmayr, of my invention of an error-correcting code for teletype lines[1]. This caused him to make a wrong association, and he gave me a copy of Sacco's book, which had just appeared[2]. I was lucky, for it was the best book I could have received at that time—although I didn't know that then. However, I devoured the book. Noticing this, my dear friend and colleague Paul August Mann, who was aware of my acquaintance with Shannon's redundancy-decreasing encoding, gave me a copy of the now-famous paper by Claude Shannon called *Communication Theory of Secrecy Systems*[3] (which in those days was almost unavailable in Germany as a Bell System Technical Report). I was fascinated by this background to Shannon's information theory, which I was already familiar with. This imprinted my interest in cryptology as a subfield of coding theory and formal languages theory, fields that held my academic interest for many years to come.

Strange accidents—or maybe sharper observation—then brought me into contact with more and more people once close to cryptology, starting with Willi Jensen (Flensburg) in 1955, Karl Stein (Munich) in 1955, Hans Rohrbach, my colleague at Mainz University in 1959, as well as Helmut Grunsky, Gisbert Hasenjäger, and Ernst Witt. In 1957, I became acquainted with Erich Hüttenhain (Bad Godesberg), but our discussions on the suitability of certain computers for cryptological work were in the circumstances limited by certain restrictions. Among the American and British colleagues in numerical analysis and computer science I had closer contact with, some had been involved with cryptology in the Second World War; but no one spoke about that, particularly not before 1974, the year when Winterbotham's book *The Ultra Secret* appeared. In 1976, I heard B. Randall and I. J. Good revealing some details about the Colossi in a symposium in Los Alamos. As a science-oriented civilian member of cryptological academia, my interest in cryptology was then and still is centered on computerized cryptanalysis. Other aspects

[1] DBP No. 892767, application date January 21, 1951.

[2] Général Luigi Sacco, *Manuel de Cryptographie.* Payot, Paris 1951.

[3] Bell Systems Technical Journal **28**, Oct. 1949, pp. 656–715.

of signals intelligence ('SIGINT'), for example traffic analysis and direction finding, are beyond the scope of the book; the same holds for physical devices screening electromechanical radiation emitted by cipher machines.

The first part of this book presents cryptographic methods. The second part brings on cryptanalysis, above all, the facts that are important for judging cryptographic methods and are intended to save the user from unexpected pitfalls. This follows from Kerckhoffs' maxim: Only a cryptanalyst can judge the security of a crypto system. A theoretical course on cryptographic methods alone seems to me to be bloodless. But a course on cryptanalysis is problematic: Either it is not conclusive enough, in which case it is useless, or it is conclusive, but touches a sensitive area. There is little clearance in between. I have tried to cover at least all the essential facts that are in the open literature or can be deduced from it. No censorship took place.

Cryptology is a discipline with an international touch and a particular terminology. It may therefore be helpful sometimes to give in the book references to terms in foreign language.

My intellectual delight in cryptology found an application in the collection 'Informatik und Automatik' of the Deutsches Museum in Munich which I built up in 1984–1988, where there is a section on cryptological devices and machines. My thanks go to the Deutsches Museum for providing color plates of some of the pieces on exhibit there.

And thanks go to my former students and co-workers in Munich, Manfred Broy, Herbert Ehler, and Anton Gerold for continuing support over the years, moreover to Hugh Casement for linguistic titbits, and to my late brother-in-law Alston S. Householder for enlightenment on my English. Karl Stein and Otto Leiberich gave me details on the ENIGMA story, and I had fruitful discussions and exchange of letters with Ralph Erskine, Heinz Ulbricht, Tony Sale, Frode Weierud, Kjell-Ove Widman, Otto J. Horak, Gilbert Bloch, Arne Fransén, and Fritz-Rudolf Güntsch. Great help was given to me by Kirk H. Kirchhofer from the Crypto AG, Zug (Switzerland). Hildegard Bauer-Vogg supplied translations of difficult Latin texts, Martin Bauer, Ulrich Bauer and Bernhard Bauer made calculations and drawings. Thanks go to all of them.

The English version was greatly improved by J. Andrew Ross, with whom working was a pleasure. In particular, my sincere thanks go to David Kahn who encouraged me ("The book is an excellent one and deserves the widest circulation") and made quite a number of proposals for improvements of the text. Finally, I have to thank once more Hans Wössner from Springer-Verlag for a well functioning cooperation of long standing. The publisher is to be thanked for the fine presentation of the book. And I shall be grateful to readers who are kind enough to let me know of errors and omissions.

Grafrath, Autumn 2001 F. L. Bauer

List of Color Plates

Contents

Part I: Cryptography

ars ipsi secreta magistro
[An art secret even for the master]
Jean Robert du Carlet, 1644

Protection of sensitive information is a desire
reaching back to the beginnings of human culture.
Otto Horak, 1994

The People

W. F. Friedman

M. Rejewski

A. M. Turing

Only a few years ago one could say that cryptology, the study of secret writing and its unauthorized decryption, was a field that flourished in concealment—flourished, for it always nurtured its professional representatives well. Cryptology is a true science: it has to do with knowledge (Latin *scientia*), learning and lore. By its very nature it not only concerns secretiveness, but remains shrouded in secrecy itself—occasionally even in obscurity. It is almost a secret science. The available classic literature is scant and hard to track down: under all-powerful state authorities, the professional cryptologists in diplomatic and military services were obliged to adopt a mantle of anonymity or at least accept censorship of their publications. As a result, the freely available literature never fully reflected the state of the art—we can assume that things have not changed in that respect. Nations vary in their reticence: whereas the United States of America released quite generous information on the situation in the Second World War, the Soviet Union cloaked itself in silence. That was not surprising; but Great Britain has also pursued a policy of secretiveness which sometimes appears excessive—as in the COLOSSUS story. At least one can say that the state of cryptology in Germany was openly reported after the collapse of the Reich in 1945.[1]

Cryptology as a science is several thousand years old. Its development has gone hand in hand with that of mathematics, at least as far as the persons are concerned—names such as François Viète (1540–1603) and John Wallis (1616–1703) occur. From the viewpoint of modern mathematics, it shows traits of statistics (William F. Friedman, 1920), combinatory algebra (Lester S. Hill, 1929), and stochastics (Claude E. Shannon, 1941). The Second World War finally brought mathematicians to the fore: for example, Hans Rohrbach (1903–1993) in Germany and Alan Mathison Turing (1912–1954) in England; A. Adrian Albert (1905–1972) and Marshall Hall (1910–1990) were engaged in the field in the United States, also J. Barkley Rosser, Willard Van Orman Quine, Andrew M. Gleason, and the applied mathematicians Vannevar Bush (1890–1974) and Warren Weaver (1894–1978). And there was Arne Beurling (1905–1986) in Sweden, Marian Rejewski (1905–1980) in Poland, Maurits deVries in the Netherlands, Ernst S. Selmer (b. 1920) in Norway.

The mathematical disciplines that play an important part in the current state of cryptology include number theory, group theory, combinatory logic, com-

[1] Hans Rohrbach (1948), *Mathematische und maschinelle Methoden beim Chiffrieren und Dechiffrieren.* In: FIAT Review of German Science 1939–1941: Applied Mathematics, Part I, Wiesbaden 1948.

plexity theory, ergodic theory, and information theory. The field of cryptology can already be practically seen as a subdivision of applied mathematics and computer science. Conversely, for the computer scientist cryptology is gaining increasing practical importance in connection with access to operating systems, data bases and computer networks, including data transmission.

One could also mention a few present-day mathematicians who have been engaged in official cryptology for a time. Some would prefer to remain incognito.

Quite generally, it is understandable if intelligence services do not reveal even the names of their leading cryptologists. Admiral Sir Hugh P. F. Sinclair, who became in 1923 chief of the British Secret Intelligence Service (M.I.6), had the nickname 'Quex'. Semi-officially, he and his successor General Sir Stewart Graham Menzies (1890–1968), were traditionally known only as "C". Under them were a number of 'Passport Control Officers' at the embassies as well as the cryptanalytic unit at Bletchley Park. And the name of Ernst C. Fetterlein (dec. 1944), who was till the October Revolution head of a Russian cryptanalytic bureau (covername Popov) and served the Government Code and Cypher School of the British Foreign Office since June 1918, was mentioned in the open cryptological literature only incidentally in 1985 by Christopher Andrew and in 1986 by Nigel West.

Professional cryptology is far too much at risk from the efforts of foreign secret services. It is important to leave a potential opponent just as much in the dark about one's own choice of methods ('encryption philosophy') as about one's ability ('cryptanalytic philosophy') to solve a message that one is not meant to understand. If one does succeed in such unauthorized decryption—as the British did with ENIGMA-enciphered messages from 1940 till 1945—then it is important to keep the fact a secret from one's opponents and not reveal it by one's reactions. As a result of British shrewdness, the relevant German authorities, although from time to time suspicious, remained convinced until the approaching end of the war (and some very stubborn persons until 1974) that the ciphers produced by their ENIGMA machines were unbreakable.

The caution the Allies applied went so far that they even risked disinformation of their own people: Capt. Laurance F. Safford, U.S. Navy, Office of Naval Communications, Cryptography Section, wrote in an internal report of March 18, 1942, a year after the return of Capt. Abraham Sinkov and Lt. Leo Rosen from an informative visit in February 1941 to Bletchley Park: "Our prospects of ever [!] breaking the German 'Enigma' cipher machine are rather poor." This did not reflect his knowledge. But he was addressing U.S. Navy leadership.

In times of war, matériel and even human life must often be sacrificed in order to avoid greater losses elsewhere. In 1974, Group Captain Winterbotham said Churchill let Coventry be bombed because he feared defending it would reveal that the British were reading German ENIGMA-enciphered messages. This story was totally false: As the targets were indicated by changing code-words, this would not in fact have been possible. However, the British were initially very upset when, in mid-1943, the Americans began systematically to destroy all the tanker U-boats, whose positions they had learnt as a result of cracking the 4-rotor ENIGMA used by the German submarine command. The British were justifiably concerned that the Germans would suspect what had happened and would greatly modify their ENIGMA system again. In fact they did not, instead ascribing the losses (incorrectly) to treachery. How legitimate the worries had been became clear when the Allies found out that for May 1, 1945, a change in the ENIGMA keying procedures was planned that would have made all existing cryptanalytic approaches useless. This change "could probably have been implemented much earlier if it had deemed worthwhile" (Ralph Erskine).

This masterpiece of security work officially comprised "intelligence resulting from the solution of high-grade codes and ciphers". It was named by the British for short "special intelligence" and codenamed ULTRA, which also meant its security classification. The Americans similarly named MAGIC the information obtained from breaking the Japanese cipher machines they dubbed PURPLE. Both ULTRA and MAGIC remained hidden from Axis spies.

Cryptology also has points of contact with criminology. References to cryptographic methods can be found in several textbooks on criminology, usually accompanied by reports of successfully cryptanalyzed secret messages from criminals still at large—smugglers, drug dealers, gun-runners, blackmailers, or swindlers—and some already behind bars, usually concerning attempts to free them or to suborn crucial witnesses. In the law courts, an expert assessment by a cryptologist can be decisive in securing their conviction. During the days of Prohibition in the U.S.A., Elizebeth S. Friedman née Smith (1892–1980), wife of the famous William Frederick Friedman (1891–1969)[2] and herself a professional cryptologist, performed considerable service in this line. She did not always have an easy time in court: counsel for the defence expounded the theory that anything could be read into a secret message, and that her cryptanalysis was nothing more than "an opinion". The Swedish cryptologist Yves Gyldén (1895–1963), a grandson of the astronomer Hugo Gyldén, assisted the police in catching smugglers in 1934. Only a few criminal cryptologists are known, for example the New Yorker Abraham P. Chess in the early 1950s.

Side by side with state cryptology in diplomatic and military services have stood the amateurs, especially since the 19th century. Starting with the revelation of historic events by retired professionals such as Étienne Bazeries[3], to the after-dinner amusements practised by Wheatstone[4] and Babbage[5],

[2] Friedman, probably the most important U.S. American cryptologist of modern times, introduced in 1920 the *Index of Coincidence*, the sharpest tool of modern cryptanalysis.

[3] Étienne Bazeries (1846–1931), probably the most versatile French cryptologist of modern times, author of the book *Les chiffres secrets dévoilés* (1901).

[4] Sir Charles Wheatstone (1802–1875), English physicist, professor at King's College, London, best known for Wheatstone's bridge (not invented by him).

[5] Charles Babbage (1791–1871), Lucasian Professor of Mathematics at the University of Cambridge, best known for his Difference Engine and Analytical Engine.

with a journalistic cryptanalytic background ranging from Edgar Allan Poe to the present-day *Cryptoquip* in the *Los Angeles Times*, accompanied by excursions into the occult, visiting Martians, and terrorism, cryptology shows a rich tapestry interwoven with tales from one of the oldest of all branches of cryptology, the exchange of messages between lovers.

The letter-writer's guides that appear around 1750 soon offered cryptographic help, like *De geheime brieven-schryver, angetoond met verscheydene voorbeelden* by a certain G. v. K., Amsterdam 1780, and *Dem Magiske skrivekunstner*, Copenhagen 1796. A century later, we find *Sicherster Schutz des Briefgeheimnisses*, by Emil Katz, 1901, and *Amor als geheimer Bote. Geheimsprache für Liebende zu Ansichts-Postkarten*, presumably by Karl Peters, 1904.

Sicherster Schutz des Briefgeheimnisses
Eine unbedingt sichere Geheimschrift für
Liebende und Freunde, Geschäftsleute
und Politiker etc.
Von unbefugten nicht zu entziffern.
von Emil Katz.

Mixed with sensational details from the First and Second World Wars, an exciting picture of cryptology in a compact, consolidated form first reached a broad public in 1967 in David Kahn's masterpiece of journalism and historical science *The Codebreakers*. In the late 1970s there followed several substantial additions from the point of view of the British, whose wartime files were at last (more or less) off the secret list, among the earliest *The Secret War* by Brian Johnson, later *The Hut Six Story* by Gordon Welchman. Cryptology's many personalities make its history a particularly pleasurable field.

Commercial interest in cryptology after the invention of the telegraph concentrated on the production of code books, and around the turn of the century on the design and construction of mechanical and electromechanical ciphering machines. Electronic computers were later used to break cryptograms, following initial (successful) attempts during the Second World War. A programmable calculator is perfectly adequate as a ciphering machine. But it was not until the mid-1970s that widespread commercial interest in encrypting private communications became evident ("Cryptology goes public," Kahn 1979); the options opened up by integrated circuits coincided with the requirements of computer transmission and storage. Further contributing to the growth of cryptology were privacy laws and fears of wiretapping, hacking and industrial espionage. The increased need for information security has given cryptology a hitherto unneeded importance. Private commercial applications of cryptology suddenly came to the fore, and led to some unorthodox keying arrangements, in particular asymmetric public keys first proposed publicly in 1976 by Whitfield Diffie and Martin Hellman. More generally, lack of adequate copyright protection for computer programs has encouraged the use of encryption methods for software intended for commercial use.

However, the demand for "cryptology for everyman" raises contradictions and leads to a conflict of interests between the state and scientists. When cryptology use becomes widespread and numerous scientists are occupied in public with the subject, problems of national security arise. Typically, authorities in the United States began to consider whether private research into cryptology should be prohibited—as private research into nuclear weapons was. On May 11, 1978, two years after the revolutionary article by Diffie and Hellman, a high ranking judicial officer, John M. Harmon, assistant attorney general, Office of Legal Counsel, Department of Justice, wrote to Dr. Frank Press, science advisor to the President: "The cryptographic research and development of scientists and mathematicians in the private sector is known as 'public cryptography'. As you know, the serious concern expressed by the academic community over government controls of public cryptography led the Senate Select Committee on Intelligence to conduct a recently concluded study of certain aspects of the field." These aspects centered around the question of whether restraints based on the International Traffic in Arms Regulation (ITAR) "on dissemination of cryptographic information developed independent of government supervision or support by scientists and mathematicians in the private sector" are unconstitutional under the First Amendment, which guarantees freedom of speech and of the press. It was noted: "Cryptography is a highly specialized field with an audience limited to a fairly select group of scientists and mathematicians ... a temporary delay in communicating the results of or ideas about cryptographic research therefore would probably not deprive the subsequent publication of its full impact."

Cryptological information is both vital and vulnerable to an almost unique degree. Once cryptological information is disclosed, the government's interest in protecting national security is damaged and may not be repaired. Thus, as Harmon wrote in 1978, "a licensing scheme requiring prepublication submission of cryptographic information" might overcome a presumption of unconstitutionality. Such a scheme would impose "a prepublication review requirement for cryptographic information, if it provided necessary procedural safeguards and precisely drawn guidelines," whereas "a prior restraint on disclosure of cryptographic ideas and information developed by scientists and mathematicians in the private sector is unconstitutional."

Furthermore, in the 1980s, the Department of Justice warned that export controls on cryptography presented "sensitive constitutional issues".

Let us face the facts: cryptosystems are not only considered weapons by the U.S. Government—and not only by the U.S. Government—they *are* weapons, weapons for defense and weapons for attack. The Second World War has taught us this lesson.

Harmon wrote moreover: "Atomic energy research is similar in a number of ways to cryptographic research. Development in both fields has been dominated by government. The results of government created or sponsored research in both fields have been automatically classified because of the immi-