Cryptographic Technology: Fifteen Year Forecast

Whitfield Diffie

BNR INC.
Mountain View, California

February 1981

Abstract

This paper examines the forces driving public development of cryptography today and projects the course of the field over the next fifteen years with attention to the possible influence of government regulation.

This paper was prepared, under contractual arrangements to CRC Systems, in support of the Commerce Department (National Telecommunications and Information Administration, Special Projects Office) response to a White House Office of Science and Technology Policy request that the secretaries of the Departments of Commerce and Defense propose a national policy on cryptography.

BNR

CONTENTS

CONTENTS i

SUMMARY iii

PREFACE iv

1. INTRODUCTION 1

2. CRYPTOGRAPHY TODAY 2

3. TRENDS AND INFLUENCES 5
   - 3.1 *Increasing Threats to Communications* 5
   - 3.2 *Advances in Computer Technology* 6
     - 3.2.1 *Decreasing Cost of Computation* 6
     - 3.2.2 *Very Large Scale Integration* 6
     - 3.2.3 *Secure Computing* 6
   - 3.3 *Public Key Cryptography* 7
   - 3.4 *Analog and Voice Encryption* 7
   - 3.5 *Changes in Cryptographic Tradition* 7
     - 3.5.1 *Decline of System Secrecy* 7
     - 3.5.2 *Availability of Cryptographic Expertise* 8
   - 3.6 *Academic Interest in Cryptography* 8
   - 3.7 *The Data Encryption Standard* 9
   - 3.8 *Government Regulation* 10

4. THE PERIOD FROM 1980 TO 1985 12

5. THE PERIOD FROM 1985 TO 1990 13
   - 5.1 *Very Large Scale Integration* 13
   - 5.2 *Public Key Cryptography* 13
   - 5.3 *Secure Computing* 13
   - 5.4 *Voice Technology* 14
   - 5.5 *Personal Computing* 14
   - 5.6 *Adequacy of DES* 14

6. THE PERIOD FROM 1990 TO 1995 15

7. CONCLUSIONS 17

REFERENCES 22

SUMMARY

The emergence of cryptography into technical and political prominence during the 1970's has disquieted its traditional practitioners and led to calls for public regulation of the new field. An essential ingredient in deciding how if at all such regulation is to be carried out is a baseline prediction of the future of cryptography which identifies the areas in which government regulation might be significant.

The past five years have witnessed two major developments: the promulgation of a federal Data Encryption Standard (DES) by the National Bureau of Standards and the development of a new variety of cryptographic systems, public key cryptography, by academic researchers. DES products are now available from many of the major electronics manufacturers and public key systems, with their "digital signature" capability, have been implemented for specialized applications. Major corporations have responded by beginning to study both their own security requirements and the business opportunities, but so far sales of the new equipment have been sluggish.

Trends in modern communications and computing which are expected to influence cryptography include:

- Increasing importance of communication coupled with the increasing vulnerability of communication channels to unauthorized interception or manipulation.
- Developments in computer science which will make cryptography cheaper and easier to apply.
- Rapid development of public key cryptography.
- Inroads into the traditional secrecy that surrounds the practice of cryptography.
- Decline of a government monopoly in the practice of cryptography and and increasing academic and commercial interest in the field.
- A likely need to replace DES before the turn of the century.

These influences may be affected to varying degrees by government regulation.

The report concludes with scenarios for each of the next three five year periods.

- 1980-1985

  DES, implemented in the current LSI technology, will remain viable. Public key

products and the first secure computer operating systems will appear.

- 1985-1990

  Use of VLSI and secure computing, will markedly decrease the cost of cryptography, while similarly decreased cost of eavesdropping will increase the demand. Public key cryptography will be entering its second decade and the development of new, higher performance, systems is likely. Diminished security of DES will make multiple encryption a *de facto* standard for higher security applications.

- 1990-1995

  New technology and new threats will lead to major changes in communication security. Replacement of DES, either by a more secure system based on current technology or by a new product of 1980's research, is virtually certain and unification of the techniques used for protecting classified and unclassified information is likely.

PREFACE

Though aware that prophecy is always an uncertain business, I have not allowed this awareness to influence my use of English. In expressing my degrees of certainty, I have used the overconfident "will" as readily as the unassailable "may." The reader must weigh the strength of my conviction together with my arguments and references in forming his own opinion.

1. INTRODUCTION

Cryptography has developed during the past decade from a little known technical aspect of military and intelligence operations to a widely discussed and much studied adjunct of data communication and storage. Where a decade ago cryptography was almost completely secret, and the government agencies responsible for its practice avoided identification whenever possible, today it is discussed regularly in the nation's leading newspapers and news magazines as well as scientific magazines and technical journals.

This sudden prominence has had a disquieting effect on the conventional practitioners of the subject who fear that the actions of the new civilian cryptographic community will upset the flow of intelligence information and have an ill effect on the security of the United States. Although the instinctive desire of this community is to discourage the new cryptographers, the soundness of such a course of action is placed in doubt by evidence that American well being is also jepardized by lack of security in our own civilian communications - a lack of security which can in large part be blamed on the lack of civilian awareness and understanding of communications intelligence and security which was the rule until very recently.

The conflict in views between those who disparage and those who support development of an unclassified cryptographic technology for application to commercial communications has lead to a need for a considered governmental policy on how, if at all, the new wave of cryptographic activity is to be regulated.

An indispensible input to the formulation of any such policy is a projection of probable developments in communication security and an analysis of the effects that proposed government policies might have.

The following report will attempt to provide a baseline projection of the direction and impact of communication security research and practice and where possible identify the areas in which government regulation might be influential.

2. CRYPTOGRAPHY TODAY

Cryptography is the technique of protecting data by transforming it from a usable and comprehensible "plaintext" form to a scrambled and incomprehensible "ciphertext" form, from which the plaintext can only be recovered by use of a secret "key." The mechanism which performs this transformation is known as a cryptographic system or cryptosystem and the transformations are known as "encryption" and "decryption" respectively.

If the plaintext can, despite the efforts of the designers, be recovered from the ciphertext without the use of the key, the process is called "cryptanalysis" and the system so defeated is said to have been "broken" or "read." The two problems to which cryptography can be applied are called "privacy" and "authentication." The former is the problem of guaranteeing that the contents of a message will not be revealed to any unauthorized party while it is being transmitted from a sender to a receiver. The latter is the problem of guaranteeing that the message which reaches the receiver is actually one transmitted by the sender and that it has arrived unaltered and on time.

Until recently, the study and use of cryptography were practiced almost entirely by the military, diplomatic, and intelligence communities. During the past decade, however, the vastly increased use of computer operated telecommunications systems has extended interest in cryptography to communications companies, computer manufacturers, banks, and universities, among others.

The two most conspicuous results of this expanded interest have been the promulgation of a cryptographic standard by the National Bureau of Standards and the development of public key cryptography by university researchers.

In 1975, the National Bureau of Standards, published a proposed standard algorithm for data protection. In 1977, after two years of public controversy over its security, this algorithm was adopted as Federal Information Processing Standard 46, the Data Encryption Standard (DES) [DES]. Both the publication of the standard and the controversy over its adoption have focused new attention on cryptography in the technical community.

The Data Encryption Standard, in its basic form, is a "block" cryptosystem; it transforms 64 bits (eight characters) of plaintext into 64 bits of ciphertext under the control of a 56 bit key. The encryption takes place in sixteen rounds. During each round, the left thirty-two bits are combined in a reversible way with the result of a complex substitution and transposition of the right 32 bits. The new left half is then interchanged with the old (unaltered) right half and the two halves play opposite roles in the next round. The substitution and transposition operation on the right half is controlled by a 48 bit subset

of the key bits, which varies from round to round.

In the three and one half years since its adoption as a standard, DES has enjoyed great success with manufacturers, making a sweeping change in the availability of cryptographic products. Where before these were available only from a few specialized companies, now approximately a dozen major computer and electronics manufacturers are producing equipment ranging from individual DES chips to stand alone link encryption units to cryptographically protected automated teller machines.

The second recent development, public key cryptography [Diffie76b], is almost exactly the same age as DES and has been prospering within its own sphere. This proposal for cryptographic systems in which some of the keying material could be made public in such a way as to permit both freer and more secure communication has developed into such a thriving area of research that it has often been confused for a competing product.

A public key cryptosystem is one in which the conversion of plaintext to ciphertext and the conversion of ciphertext to plaintext are done using different keys. Furthermore, given one of the keys, it is just as difficult to discover the other as it would be to discover the plaintext given only a sample of the ciphertext. This separation of the keys for encrypting and decrypting makes it possible to disclose one (the public key) while retaining the other (the secret key.)

Because the public key can be revealed without compromising the secret key, the process of providing suitable keys to the sender and receiver ("key distribution") can be made both freer and more secure. Public key cryptosystems also make possible a new form of authentication called a "digital signature." A message that has been encrypted with a secret key could only have been created by the holder of that secret key. The identity of the creator can, however, be verified by anyone who has the corresponding public key. This property (creatable by only one person but recognizable by many) allows the digital signature to play much the same role in electronic communication that a written signature plays in paper communication.

Public key cryptography was discovered in the spring of 1975 and the first paper on the subject appeared in June 1976 [Diffie76a]. In the intervening four years two major approaches, drawn from different areas of mathematics, have been found for implementing it.

The first of these [Rivest], called the RSA system after its inventors' initials, is drawn from number theory. It is based on the concept of a prime number (a number that cannot be evenly divided by any numbers except itself and one) and on the relative ease with which a pair of primes can be multiplied together compared with the difficulty of factoring their product to discover the two primes. Like DES, the RSA system is a block system, though in this case the blocks must be five to ten times as long for the system to be secure. A block of plaintext is encrypted by exponentiation in a finite arithmetic structure. The exponent in this operation together with the product of the primes comprise the public key. The inverse operation can be performed only by those who know the pair of primes (the secret key). Because this cryptosystem requires dozens of multiplications of numbers hundreds of digits in length, its operation is quite slow. The fastest versions so far constructed can process

thousands of bits per second as compared with millions for some DES implementations.

The second public key system [Merkle], called the "trapdoor knapsack system," has its roots in a field called combinatorial mathematics. Here the trick is that given a list of numbers it is easy to add up the whole list or any specified subset, but given instead a list of numbers and a sum it is extremely difficult to discover a subset which totals to exactly that sum. The name is imaginatively derived from the notion of attempting to choose just the right set of rods from those in a box so that when packed into a long thin knapsack, the rods would fit tightly and not rattle. In order to do encryption in this system, the input block is treated as a specification of which numbers are to be selected from a list and added up; the output is their sum. The trapdoor knapsack system is based on Merkle's discovery that if the list of numbers is constructed correctly, certain details of that construction constitute a secret key which allows the constructor to take the sum and discover which members of the list were added. Unlike the RSA system, knapsack systems are quite fast. Unfortunately, the public key is a list of approximately one hundred numbers, each of about thirty digits in length, which is quite unwieldy.

Although these first approaches fall short of conventional cryptographic systems in performance (speed or storage requirements), both have already found application [Simmons, Myers].

At present, the most active area of communication security is the development and standardization of protocols for the use of cryptography in modern data communication systems. Experiments in cryptographic network security are being carried out at various laboratories [Myers, Shanning] and an effort to set standards has been underway over the past two years in the American National Standards Institute and such governmental bodies as the National Bureau of Standards, the National Communication System, and the National Security Agency.

At present, despite substantial research activity and study by "Fortune 500" companies of their security requirements [IRD], the market for the new cryptographic products has been sluggish. Many feel, however, that as electronics funds transfer and other developments in communications progress the cryptographic market will improve dramatically[Burstyn,MAPTEK].

3. TRENDS AND INFLUENCES

3.1 *Increasing Threats to Communications*

Two major trends in modern communication technology combine to make communications increasingly vulnerable to eavesdropping.

- The use of microwave radio and satellite relay to replace cables allows an eavesdropper to intercept with a mobile or fixed antenna without taking the risk of any physical intrusion into the communication path. Such links are employed by virtually all domestic telecommunication carriers.

- The use of digital (particularly packetized) formats for more and more forms of data allows the eavesdropper to analyze the intercepted traffic by computer, searching for key words in the body of the message or examining the packet headers for the addresses of the sender and receiver.

These threats, which make all but voice communication vulnerable to low budget eavesdropping operations, are being joined by rapid development of voice processing technology. At present, speaker independent word recognition is just beginning to become available on the commercial market [Spectrum, Electronics, EMMS]. By the latter half of the decade, this technology will have progressed to where word recognition, speaker recognition, and possibly full voice understanding (voice typewriter) robust enough to be applied in the adverse environment of wiretapping will be commercially available. It is also possible that voice synthesis will progress to a point where authentication by speaker recognition will no longer be useful.

These threats appear at a time when security of communications is growing in importance for an ever broadening area of society. It is widely felt that international economic competition will intensify during the remainder of the century in an environment of increasing scarcity of resources and military standoff. This will give economic and commercial communications an intelligence value akin to that currently attached only to military transmissions and place civilian communication systems under substantial pressure to improve their security.

3.2 *Advances in Computer Technology*

3.2.1 *Decreasing Cost of Computation*

It is a surprising fact that decreases in the cost of computation do not benefit the cryptosystem designer and the cryptanalyst equally. If a cryptographic method is of any value at all - if cryptanalysis takes an effort which is more than a linear function of the effort required to produce the cryptogram - a decrease in the cost of computation benefits the cryptographer to the detriment of the cryptanalyst. This is because the increased computing power that the system designer can afford to employ on encryption will require a more than proportional increase on the part of the cryptanalyst.

The improvement in security of modern cryptographic systems over those available at the time of World War II can be credited largely to the factor of one million reduction in the cost of computation which has occurred over the intervening period and this trend will make the construction of secure cryptosystems easier and easier as time goes on. What is and will probably remain difficult is constructing highly efficient cryptosystems - cryptosystems which are minimal in number of components or maximal in speed.

3.2.2 *Very Large Scale Integration*

At present, semiconductor technology permits the Data Encryption Standard to be implemented on a single silicon chip but will not accommodate DES as one of several components of a larger structure. By the mid-eighties, when chips with 100,000 to 1,000,000 devices will be common, cryptography will be integrated into packages performing broader communication functions. This will be aided by the development of custom LSI. The cost of electronic shielding now required in the highest grade cryptographic equipment will decline as the cryptodevices and their associated optically isolated communication paths are combined in single packages.

3.2.3 *Secure Computing*

Development of secure operating systems, which can be trusted to process the confidential data of several mutually suspicious users simultaneously, is currently an active area of computer science. Although the role that cryptography will play in the inner workings of such systems is yet to be established, cryptography and secure computing are destined to be deeply intertwined. Secure operating systems will play as crucial a role as cryptography in the development of secure computer networks, will simplify the design of communication security hardware, and make possible such flexible techniques as wide implementation of cryptographic algorithms in software.

If cryptography emerges as an important technique in the construction of secure computers, this will create a demand for strong cryptograhic algorithms with better performance than DES. The complexity of DES is comparable to that of the most complex

computer instructions (for example a double precision floating point multiply) and this complexity makes it too slow for use in the instruction stream of a fast computer. At present, the fastest implementations of DES would be adequate for internal use in computers of moderate speed (e.g., PDP-11's) but utterly unable to cope with the memory access requirements of super machines such as the Cray One.

3.3 *Public Key Cryptography*

At present, public key cryptosystems neither offer the performance nor command the trust of conventional systems. Public key cryptography is, however, a field only four years old and judged by this standard is doing exceptionally well. The two major approaches to constructing public key systems [Rivest, Merkle] come from widely separated areas of mathematics and are each good enough to have found application [Simmons, Myers]. This, together with the lack of any significant theoretical limitation on the performance of public key systems, is reason for optimism that more and better examples will be forthcoming in the near future.

3.4 *Analog and Voice Encryption*

Analog encryption devices, primarily used for voice protection, account for a significant portion of the commercial encryption products today. Over the next fifteen years, use of these products will probably decline to an insignificant level in the U.S., due to the spreading digitization of the telephone system and the improving quality of both modems and voice compression equipment.

At present, digital encryption of voice telephony requires either a high speed modem or a complex voice compression system. Either of these is expensive, but both should decline in cost at the same general rate as other computing equipment and reach one percent of their present prices in 1990.

In the meantime, the quality of conventional analog scrambling equipment is being improved and its cost is being decreased by implementing it through digital signal processing technology. New research[Wyner] also gives promise of higher security analog systems.

3.5 *Changes in Cryptographic Tradition*

3.5.1 *Decline of System Secrecy*

The adoption of the Data Encryption Standard by the United States represented a fundamental change in cryptographic tradition whose beneficial effects on communication security may be DES's greatest contribution. Both classical [Kahn] and modern [COMSAT79] cryptographic experience has shown that systems developed in secret, except perhaps by the largest and most experienced cryptologic organizations, are prone to hidden flaws which lead to their downfall. If, on the other hand, a system is made public it

will be subject to scrutiny by a wide range of critics and weaknesses are less likely to be overlooked.

An important beneficiary of this change in tradition may be the developing nations. These nations, which have far less stake in communications intelligence than the established powers, and consequently less interest in keeping good cryptographic systems out of the hands of their opponents, may choose to adopt systems, whether homegrown or imported, whose functioning is public for their next generation of communications facilities.

3.5.2 *Availability of Cryptographic Expertise*

Another change in cryptographic tradition and circumstances is likely to provide a more abundant supply of trained cryptographers.

In the past, very few jobs for cryptographers were available outside of government agencies and those who had held government positions felt constrained by security agreements not to take such jobs after leaving government employ. The widening interest in cryptography outside the government has lead to a normalization of relations between government and industry. Government cryptographers now express willingness to take industry jobs subject to the same constraints which would bind experts with classified experience in other fields such as laser physics or missile guidance. They have explicit information which cannot be shared with the new employer, but feel that their general expertise is not in itself restricted.

Although this would at first appear to be one of the areas most subject to government control, an attempt to tighten the rules would not be likely to succeed without widespread industry cooperation. More stringent statutary restrictions on former government employees would make affected government jobs less desirable and might therefore make it more difficult for federal agencies to recruit their own staffs.

3.6 *Academic Interest in Cryptography*

Academic interest in cryptography, which has been responsible for major cryptographic developments in the past five years, is likely to continue, although not necessarily at a constant level. This interest is abetted by the connection of cryptography with a number of other fields of current interest in mathematics and computer science and the appealing difficulty of constructing public key systems or cryptographic systems with other interesting properties.

The theory of computational complexity has had, and will probably continue to have, the closest connection to cryptography, since cryptography provides a potential application for a wide range of lower bound results in complexity theory. To date, the problem of establishing lower bounds for classical computational problems has proved the most difficult (as well as the most interesting) problem in complexity theory. The possibility of cryptographic application lends interest to results about lower bound problems potentially more tractable than those studied so far.

Several other areas have close structural connections with cryptography. The central problem of cryptanalysis is equivalent to the "machine identification" problem in automatic fault diagnosis, since discovering which part of a mechanism has failed is equivalent to finding the key in a cryptographic system. Cryptanalysis is also related to the problem of decoding in communication theory and to the problem of pattern recognition and both theories show promise of future contributions to cryptanalysis.

Cryptography is valuable to researchers both as a source of new problems and as a field of application for existing results. Academic interest in the subject is a natural outcome of the growth in finite and combinatorial mathematics which began during the sixties and will continue for the foreseeable future.

3.7 *The Data Encryption Standard*

The NBS Data Encryption Standard appears likely to prove adequate for its intended uses during the next five years. On the other hand, it appears unlikely that it can outlive the decade of the 1980s.

Although Diffie and Hellman's 1977 estimate [Diffie77] that a twenty million dollar key exhaustion machine that could break DES in, on average, half a day now appears to have been overly optimistic in some of its details, it seems that following the same architecture and using a modified version of Advanced Micro Devices' newly announced DES chip, a fifty million dollar version with a two day average search time might be achieved by the end of 1981 [Diffie80].

The difficulty of breaking DES by exhaustive search of its keyspace will be diminished by any improvement in semiconductor technology: speed, wafer size, density, or yield, and each of these areas is under active attack. The Deputy Directorate for Research and Engineering of the Department of Defense is sponsoring a program of industry research in Very High Speed Integrated Circuits, which projects a factor of 100 improvement in speed over the next five years. The new field of "wafer scale integration," will probably allow each card in a repetitive structure such as the DES search machine to be placed on a single wafer. Density and yield are fundamental problems of semiconductor manufacture and improvements in both areas are under development throughout the industry.

In August 1976, the National Bureau of Standards held a workshop on the feasibility of building a DES key exhaustion machine [NBS76]. The scenarios proposed by this conference made the prospect seem comfortingly remote at the time, but some now take on a more threatening aspect. In particular, the prediction of a Josephson junction machine capable of achieving Diffie and Hellman's objectives by 1990 is strongly reinforced by IBM's announcement in January 1980 of a prototype Josephson junction computer scheduled for completion in 1985.

These developments suggest that the cost of building a special purpose DES search machine will drop substantially toward the end of the decade, although the problem may not become tractable for general purpose computers till several years thereafter.

3.8 *Government Regulation*

It is difficult to predict the effect of a governmental attempt to regulate cryptographic research, or even to predict whether such an attempt will be made. Suggestions for government policy have ranged from increasing the funding available for cryptographic research through NSF to asking congress for a law that would impose the same kind of government domination that the Atomic Energy Act applies to all nuclear information.

At present, government policies, and the legal means for implementing these policies, are uncertain. Some government agencies, particularly the National Science Foundation, have funded and encouraged unclassified research in cryptography, while others have attempted, through the means at their disposal, to put a damper on the same work. And present indications are that both trends continue.

Speaking before the Armed Forces Communications and Electronics Association on 8 January 1981, Admiral Robert Inman, Director of NSA, announced both that his agency was beginning a program of open funding of cryptographic research in the universities and that researchers at Stanford University, formerly a center of harsh criticism of NSA influence on the Data Encryption Standard, would be among the first recipients.

During the past year, the American Council on Education, at the suggestion of NSA, formed a Public Cryptography Study Group. After several meetings, this committee has come forth with a draft proposal for voluntary prepublication review of cryptographic research papers by the federal government [ACE], under which researchers would be encouraged to submit papers to NSA for examination prior to publication. Earlier drafts contained provisions for some non-voluntary measures and one member of the committee, Prof. George Davida of the Georgia Institute of Technology, has expressed deep concern that the committee's report may be used to argue for mandatory controls at a later date.

In an area not directly related to cryptography, the Export Administration Act was invoked to discourage Russian and Chinese participation in a meeting on bubble memory technology, early in 1980 [Wade80]. In a possibly contradictory spirit, the preamble to a Federal Register announcement of proposed changes in ITAR states, "... provision has been added to make it clear that the regulation of the export of technical data does not purport to interfere with the first amendment rights of individuals [ITAR80]." The effect of such government attempts to restrain publication are hard to predict. As long as they are uncontested, they seem to serve the government's immediate interests. Informal prepublication review, in particular, provides an opportunity for NSA to discuss the consequences of publication with authors, possibly on a confidential basis, and perhaps make them more sympathetic to its point of view. Any attempt to use legal pressure against an uncooperative opponent, however, is likely to result in concerted opposition by the press and widely publicized legal proceedings such as followed the Department of Energy's attempt to stop publication of an article on fusion bombs in "The Progressive" in 1979 [Progressive].

Even though the hearings in the Progressive case were closed, they disclosed more information and attracted more attention than the unimpeded publication of the original

article could have. Were a criminal trial to result from a defendant's refusal to comply with a court restraining order, even more information could be expected come to light.

Cryptographic secrets are among the most fragile and NSA would most likely attempt to avoid a first amendment battle over the publication of independant cryptographic research.

In most of this report, it is tacitly assumed that government influence will continue in an irregular pattern much like the present one and that federal regulation will not be an all pervasive force in public cryptography.

4. THE PERIOD FROM 1980 TO 1985

The Data Encryption Standard will remain viable during this period. Products implementing DES will continue to appear and will offer more elaborate key management and other features as time goes on.

The development of standards for using DES in computer communication networks will dominate cryptographic development for the next two or three years. This, together with increasing public acceptance of cryptography, will result in a wide spectrum of DES based security products in the mid 1980s.

Cryptographic devices will continue to employ the current "LSI" technology, using one or more discreet DES chips, during the next two or three years. Later products will begin a transition to a technology in which cryptography will be placed on the same chip with, for example, a packet switch or voice compressor. These transition products may include a chip with more than one DES device (for reliability) or a microprocessor with a DES instruction.

Security systems employing public keys will continue to be built for special applications and some public key products will no doubt reach the market, probably to provide signatures in value added communication networks.

Current development projects in secure computing will begin to produce multi-level secure operating systems by the early mid-eighties. The role of cryptography in implementing such systems is as yet unclear, but whether or not secure operating systems use cryptography internally, they will be a key component in cryptographically secure communication networks and will sharply reduce the cost of implementing communication security.

5. THE PERIOD FROM 1985 TO 1990

5.1 *Very Large Scale Integration*

By the late 1980s, Very Large Scale Integration will have a profound effect on cryptographic hardware, reducing the cost of high grade communication security equipment by an even bigger factor than the reduction in computing costs generally.

VLSI will permit circuitry that now requires cards or entire racks to be placed on single pieces of silicon. This will make the cost of incorporating DES in an integrated packet switch proportional to the increased area required to include its 5,000 devices in the whole switch's million, an overhead of less than one percent.

Integration of cryptography into larger systems will dramatically reduce the cost of radiation shielding and tamper resistance. Reduced size and smaller power dissipation coupled with internal optical isolation will permit a very high degree of shielding at very little increased cost. The same factors of size and power, coupled with developing tamper resistance technologies, will make it more difficult for an opponent to extract keying information by dismantling the equipment.

5.2 *Public Key Cryptography*

Prospects for development of new and more efficient public key cryptographic systems by the latter part of the eighties are quite good. Public key cryptography is more successful today than algebraic coding theory was at the age of four. The major breakthroughs in that field did not begin till the latter part of its first decade, but then progressed rapidly. The similarity of the two fields is reason for optimism that in the absence of interference public key cryptography will follow a similar course.

Increasing use of the available public key systems in the 1980's will spread awareness of both their advantages and the performance shortcomings of the early examples. The research response to this awareness will probably produce better public key systems in time for use during the first half of the nineties.

5.3 *Secure Computing*

Secure computing will be widespread and the now esoteric techniques used to verify the

correctness of programs will be standard tools of programming. This will make available not only operating systems trusted to manage multiple levels of sensitive information but special purpose programs for encryption or cryptographic control.

The spread of secure computing will also have an effect on the design of computer hardware and special security mechanisms (some of them cryptographic) will be incorporated into computer architecture.

5.4 *Voice Technology*

Speaker independent word recognition products will be common and of adequate quality to be applied in the adverse environment of wiretapping. Speech generation good enough to impersonate a speaker is also possible, but full voice understanding (voice typewriter) is unlikely.

5.5 *Personal Computing*

Personal computing will have developed to the point where many individuals and small companies will have as much computing power as is currently available to laboratories of substantial size. This will broaden the base of research in computer science and probably lead to unanticipated results in cryptography, among other areas.

One likely result is a new breed of hobby cryptographer who can write programs to solve far more sophisticated systems than are currently approached by paper and pencil cryptanalysts.

5.6 *Adequacy of DES*

By the late 1980s the security of DES will become marginal for many applications while remaining adequate for others. The most likely response will be for multiple encryption to become the de facto standard in higher security applications.

6. THE PERIOD FROM 1990 TO 1995

In the early nineties, cryptography and its associated technologies will be highly developed and in extensive use throughout a largely electronic information economy. Secure computing devices containing integrated cryptographic facilities will be widespread. High bandwidth (from 9.6 kilobaud to multi megabaud) digital communications will be nearly ubiquitous.

Threats will increase at the same pace as facilities. Personal computing resources will be vast and computing techniques and facilities adequate to intercept and analyze data and voice traffic will be available even to small organizations. This mature communication security environment will provide the setting for a major overhaul of communication security practice.

By this time, the Data Encryption Standard is certain to require replacement, but what form this replacement will take is as yet uncertain. The most obvious possibilities are:

- Without any actual change in the DES itself, standards for employing DES will be revised to accommodate multiple encryption. (This has the marked disadvantage of decreasing the speed of encryption even further.)

- The DES key schedule will be revised to incorporate more key bits. (This would impose no additional speed penalty.)

- If a larger block size is considered necessary, a system with a similar internal structure, but based on a 128 bit block might be designed.

New developments in cryptographic technology provide another direction in which to look for competing candidates.

- A public key system of adequate performance may be developed and achieve general acceptance.

- Advances in complexity theory may give rise to a proveably secure system.

In 1990, public key cryptography will be fifteen years old and is very likely to have made great strides beyond its present position. As current public key systems are already useable for many purposes, a 1990 public key system adequate as a general standard is a strong possibility.

It is also conceivable, though not likely, that by the early nineties a breakthrough in complexity theory will provide a much higher degree of certainty in the security of cryptograhic systems than is now possible. Such a breakthrough need not necessarily provide a solution to the problems which dominate complexity theory at present nor would the cryptographic system developed from it necessarily be similar to current systems.

The precise impact of such a system would depend on the details of the breakthrough and particularly on the performance of the system. If, however, the theoretical results were strong and the performance acceptable, it would probably see widespread use.

A very probable development is of a less theoretical nature. By the early nineties, voice and data communication networks using DES will be common throughout the federal government and these networks will exist side by side with comparable facilities for classified communications. The cost of this redundancy, coupled with a possible decline in cryptanalytic communications intelligence, may lead the government either to declassify one of its own cryptographic systems or to accept an outside system as adequate for classified use and thereby adopt a single system for all government communications.

7. CONCLUSIONS

Unless perturbed by outside influences, cryptography will continue to develop over the next fifteen years and assume an important position in commercial communication technology. The timescale within that frame can only be approximated because of uncertainty about the rate of market growth, particularly the federal market, the course of standards development, and the possible effect of new government attempts at regulation.

The same technological developments that are making processing, storage, and communication of information the largest and most important part of our national economy, will provide opponents at home and abroad with the means to intercept or disrupt communications in our "information economy" at will. This combination will make a well developed technology for protection of information in transit or storage indispensible. For an adequate cryptographic technology to be available to serve this need, standards for compatibility of cryptographic communication systems must be developed, and research toward systems with both assured security and such new features as the digital signature must be continued.

REFERENCES

[ACE] Draft Final Report of the American Council on Education, Public Cryptography Study Group, January 1981.

[Burstyn] H. P. Burstyn, "Slow Growing Encryption Market to Spurt in '80's," Electronic Business, January 1979, pp. 76-77.

[COMSAT79] S. Lu and L. Lee, "A Simple and Effective Public Key Cryptosystem," Comsat Technical Review, Vol. 9, No. 1, Spring 1979.

This paper was published without review outside Comsat and immediately exposed as a rediscovery of a system considered by Rivest, Shamir, and Adleman and rejected as weak. Their analysis appears in:

Ron Rivest and Len Adleman, "How to Break the Lu-Lee Cryptosystem," to appear, Computer Security Journal.

[DES] "Data Encryption Standard," Federal Information Standards Publication 46, National Bureau of Standards, 15 January 1977.

[Diffie76a] Whitfield Diffie and Martin E. Hellman, "Multiuser Cryptographic Techniques" National Computer Conference, New York, 7-10 June 1976, pp. 109-112.

[Diffie76b] Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography" IEEE Transactions on Information Theory, Vol. IT- 22, No.6, November 1976, pp. 644-654.

[Diffie77] Whitfield Diffie and Martin E. Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard," Computer, Vol. 10, No. 6. June 1977, pp. 74-84.

[Diffie80] Unpublished calculations by Diffie based on 1980 conversations with Advanced Micro Devices personnel.

[Electronics] "NEC Systems Recognize and Speaker's Words," Electronics, 19 June 1980, pp. 69-70.

[EMMS] "Typewriters With Ears, Words with Pix," Electronic Mail and Mes-

sage Systems, Vol. 4, No. 18, 15 September 1980.

[IRD] International Resource Development, "Data and Voice Encryption," March 1979, p. 62.

[ITAR80] "Revision of the International Tariff in Arms Regulations," Federal Register, 45-FR-83970-95, 19 December 1980.

[Kahn] David Kahn, "The Codebreakers, The Story of Secret Writing," New York: Macmillan, 1967.

[MAPTEK] "Unscrambling the Encryption Market," Quantum Science Corporation, MAPTEK Brief vol. 78, no. 424, 31 March 1978.

[Merkle] R. C. Merkle and M. E. Hellman, "Hiding Information and Signatures in Trapdoor Knapsacks" IEEE Transactions on Information Theory, Vol. IT-24, No. 5, September 1978, pp. 525-530.

[Myers] Frank H. Myers, "A Data Link Encryption System," National Telecommunications Conference, Washington, D.C., 27-29 November 1979.

[NBS76] "Report of the 1976 Workshop on Estimation of Significant Advances in Computer Technology" National Bureau of Standards, 30-31 August 1976.

[Progressive] The article, "The H-Bomb Secret, How we got it - Why We're Telling It," by Howard Morland was finally published in The Progressive for November 1979. Most of this issue and the May 1979, "Born Secret," issue of The Progressive are devoted to explaining the legal battle.

[Rivest] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM, Vol. 21, No. 2, February 1978, pp. 120-126.

[Shanning] Brian P. Shanning, "Data Encryption with Public Key Distribution," IEEE EASCON '79, Washington, D.C., 9-11 October 1979.

[Simmons] Gustavus J. Simmons, "Message Authentication Without Secrecy: A Secure Communications Problem Uniquely Solvable by Asymetric Encryption Techniques," IEEE EASCON '79, Washington, D.C., 9-11 October 1979.

[Spectrum] Gadi Kaplan, "Words Into Action I," IEEE Spectrum, Vol. 17, No. 6, June 1980, pp. 22-25.

Raj Reddi, "Words Into Action II," IEEE Spectrum, Vol. 17, No. 6, June 1980, pp. 26-28.

Yasuo Kato, "Words Into Action III," IEEE Spectrum, Vol. 17, No. 6, June 1980, p. 29.

[Wade80] Nicolas Wade, "Science Meetings Catch U.S. - Soviet Chill," Science, 7 March 1980, p. 1056.

[Wyner] Aaron D. Wyner, "An Analog Scrambling Scheme Which Does Not Expand Bandwidth Part I: Discrete Time," IEEE Transactions on Information Theory, Vol. IT-25, No. 3, May 1979, pp. 261-274.

Aaron D. Wyner, "An Analog Scrambling Scheme Which Does Not Expand Bandwidth, Part II: Continuous Time," IEEE Transactions on Information Theory, Vol. IT-25, No. 4, July 1979, pp. 415-424.