Inside the Encryption Wars 1985-2000

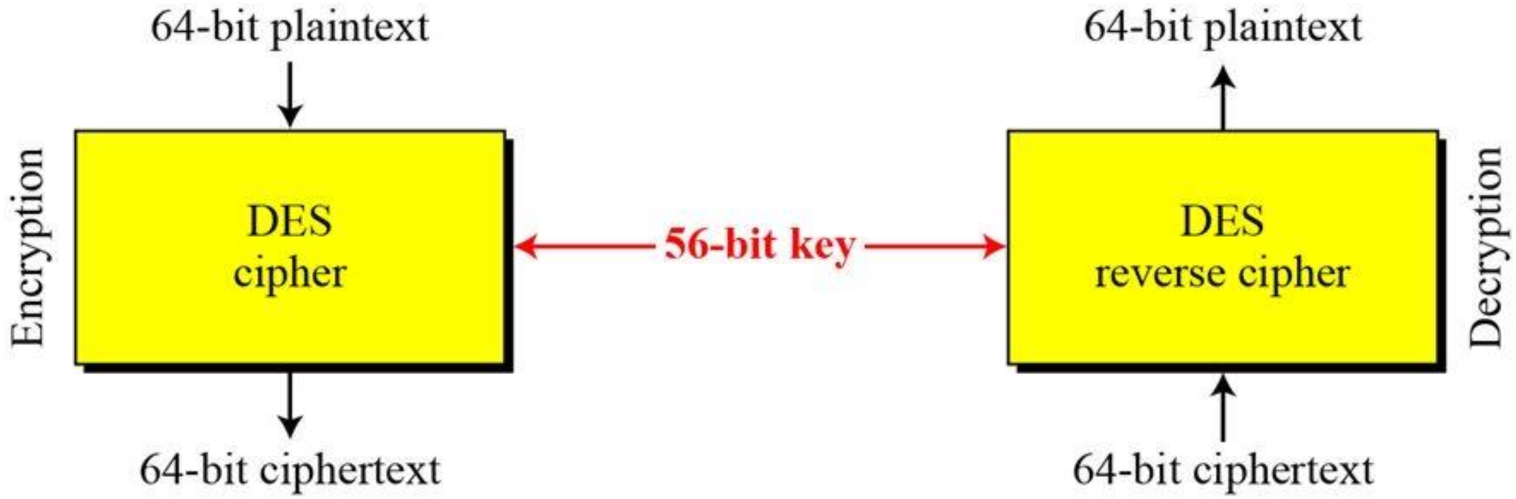
when CRYPTO was short for cryptography

April 20, 2022

Jim Bidzos

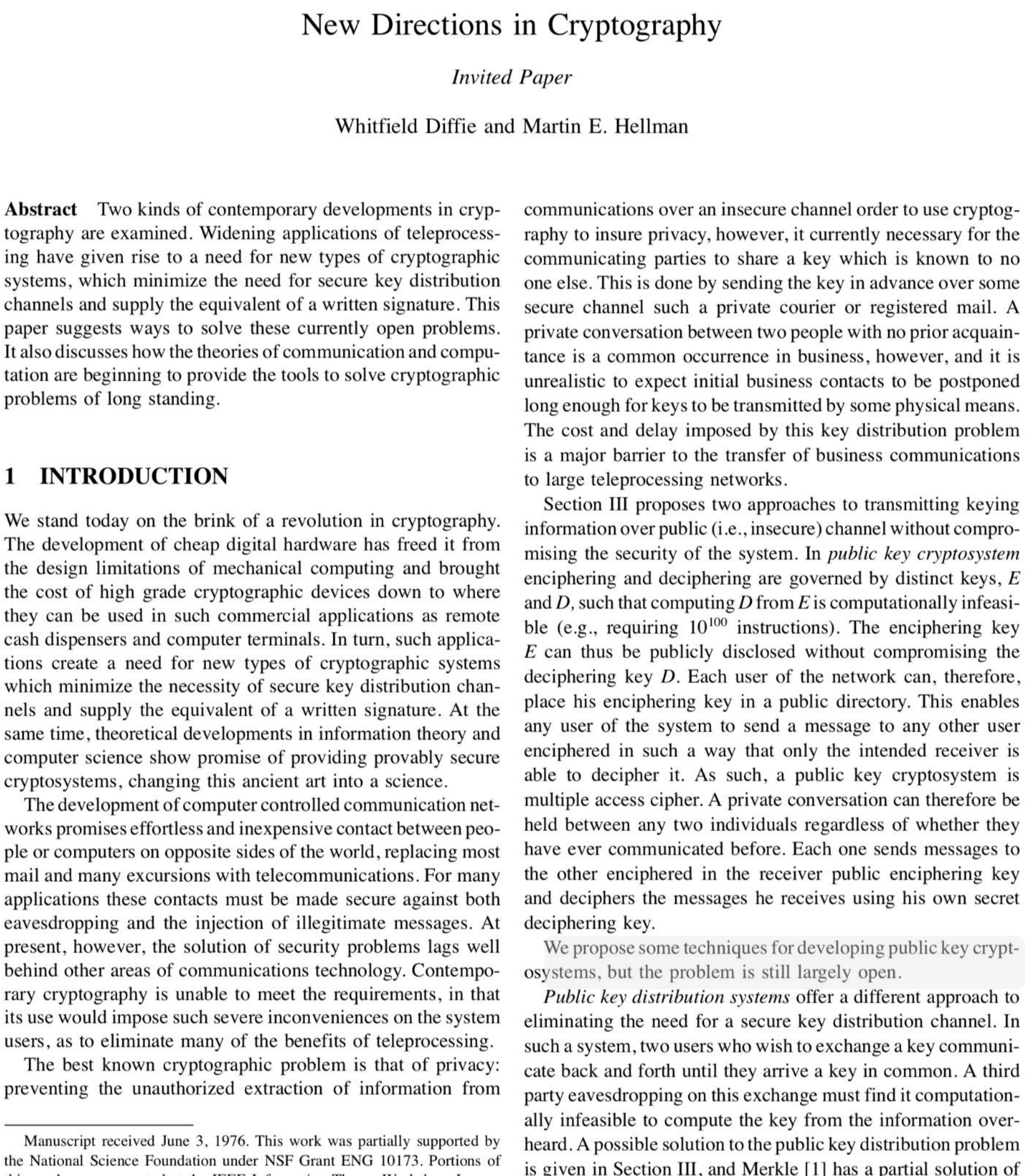
2-7 Data Encryption Standard

In 1973, NIST published a request for proposals for a national symmetric-key cryptosystem. A proposal from IBM, a modification of a project called Lucifer, was accepted as DES. DES was published in the Federal Register in March 1975 as a draft of the Federal Information Processing Standard (FIPS).



1.46

Over at Stanford University… Ralph Merkle, Marty Hellman, Whitfield Diffie



New Directions in Cryptography

Invited Paper

Whitfield Diffie and Martin E. Hellman

Abstract Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

1 INTRODUCTION

We stand today on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

The development of computer controlled communication networks promises effortless and inexpensive contact between people or computers on opposite sides of the world, replacing most mail and many excursions with telecommunications. For many applications these contacts must be made secure against both eavesdropping and the injection of illegitimate messages. At present, however, the solution of security problems lags well behind other areas of communications technology. Contemporary cryptography is unable to meet the requirements, in that its use would impose such severe inconveniences on the system users, as to eliminate many of the benefits of teleprocessing.

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel order to use cryptography to insure privacy, however, it currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such a private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

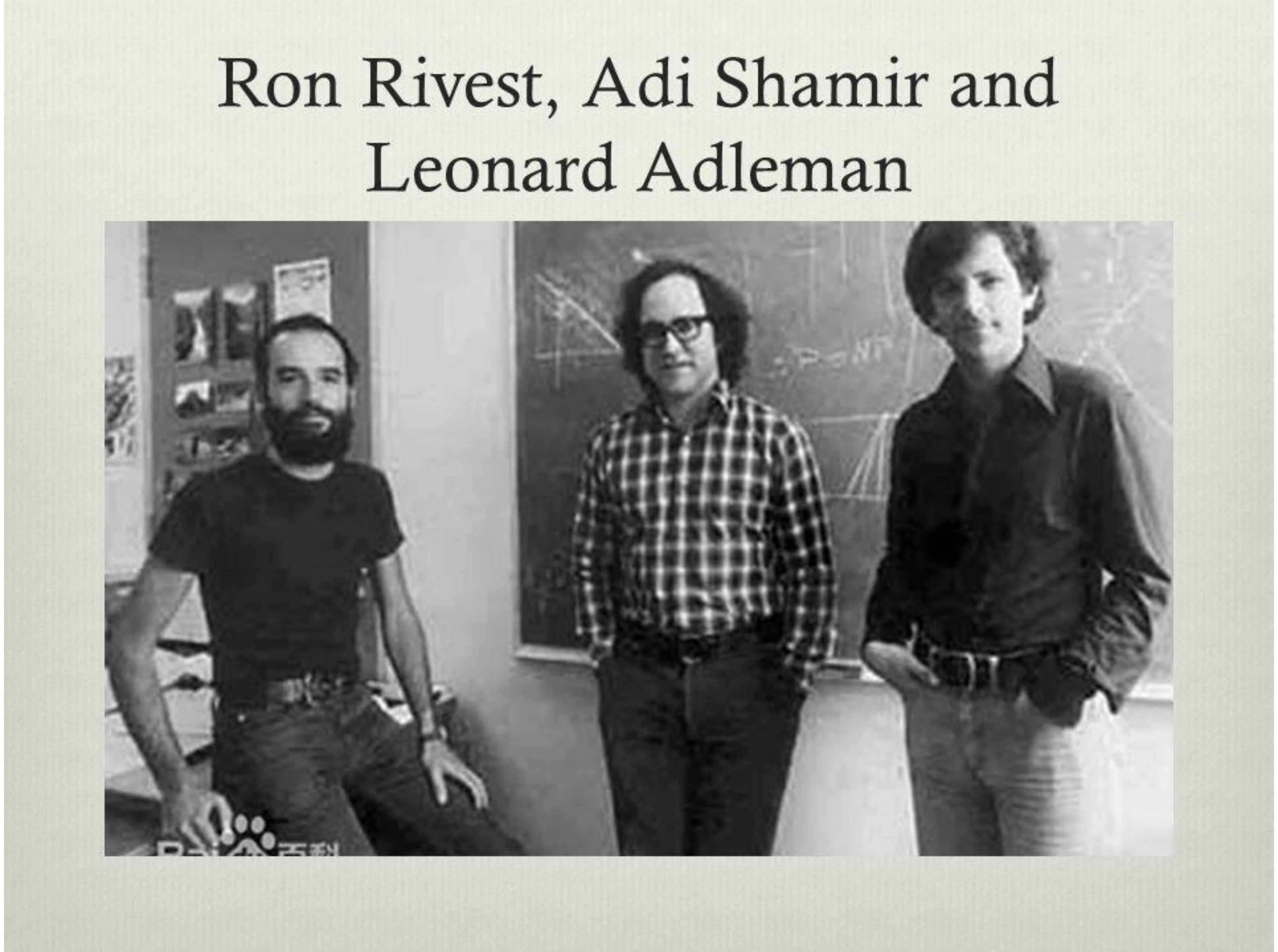
Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channel without compromising the security of the system. In *public key cryptosystem* enciphering and deciphering are governed by distinct keys, E and D, such that computing D from E is computationally infeasible (e.g., requiring 10^{100} instructions). The enciphering key E can thus be publicly disclosed without compromising the deciphering key D. Each user of the network can, therefore, place his enciphering key in a public directory. This enables any user of the system to send a message to any other user enciphered in such a way that only the intended receiver is able to decipher it. As such, a public key cryptosystem is multiple access cipher. A private conversation can therefore be held between any two individuals regardless of whether they have ever communicated before. Each one sends messages to the other enciphered in the receiver public enciphering key and deciphers the messages he receives using his own secret deciphering key.

We propose some techniques for developing public key cryptosystems, but the problem is still largely open.

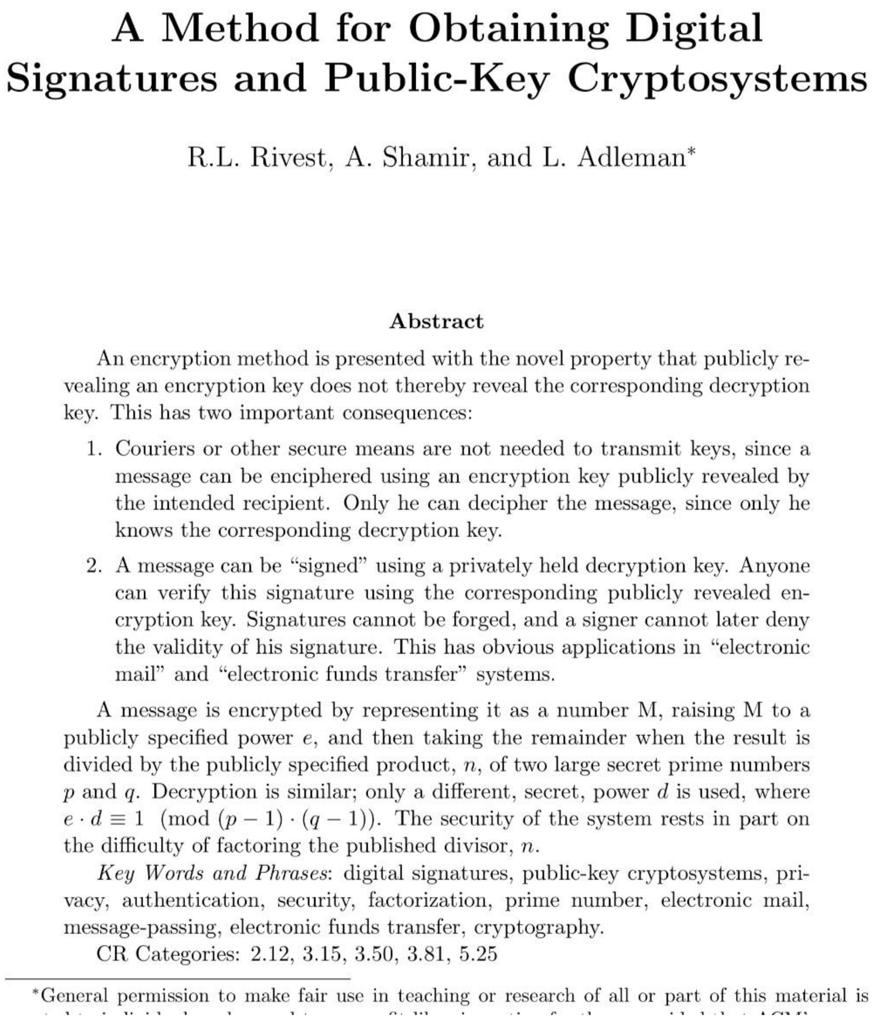
Public key distribution systems offer a different approach to eliminating the need for a secure key distribution channel. In such a system, two users who wish to exchange a key communicate back and forth until they arrive a key in common. A third party eavesdropping on this exchange must find it computationally infeasible to compute the key from the information overheard. A possible solution to the public key distribution problem is given in Section III, and Merkle [1] has a partial solution of

Manuscript received June 3, 1976. This work was partially supported by the National Science Foundation under NSF Grant ENG 10173. Portions of

Over at MIT…



Ron Rivest, Adi Shamir and Leonard Adleman



A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman[*]

Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

1. Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.
2. A message can be "signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in "electronic mail" and "electronic funds transfer" systems.

A message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product, n, of two large secret prime numbers p and q. Decryption is similar; only a different, secret, power d is used, where $e \cdot d \equiv 1 \pmod{(p-1)\cdot(q-1)}$. The security of the system rests in part on the difficulty of factoring the published divisor, n.

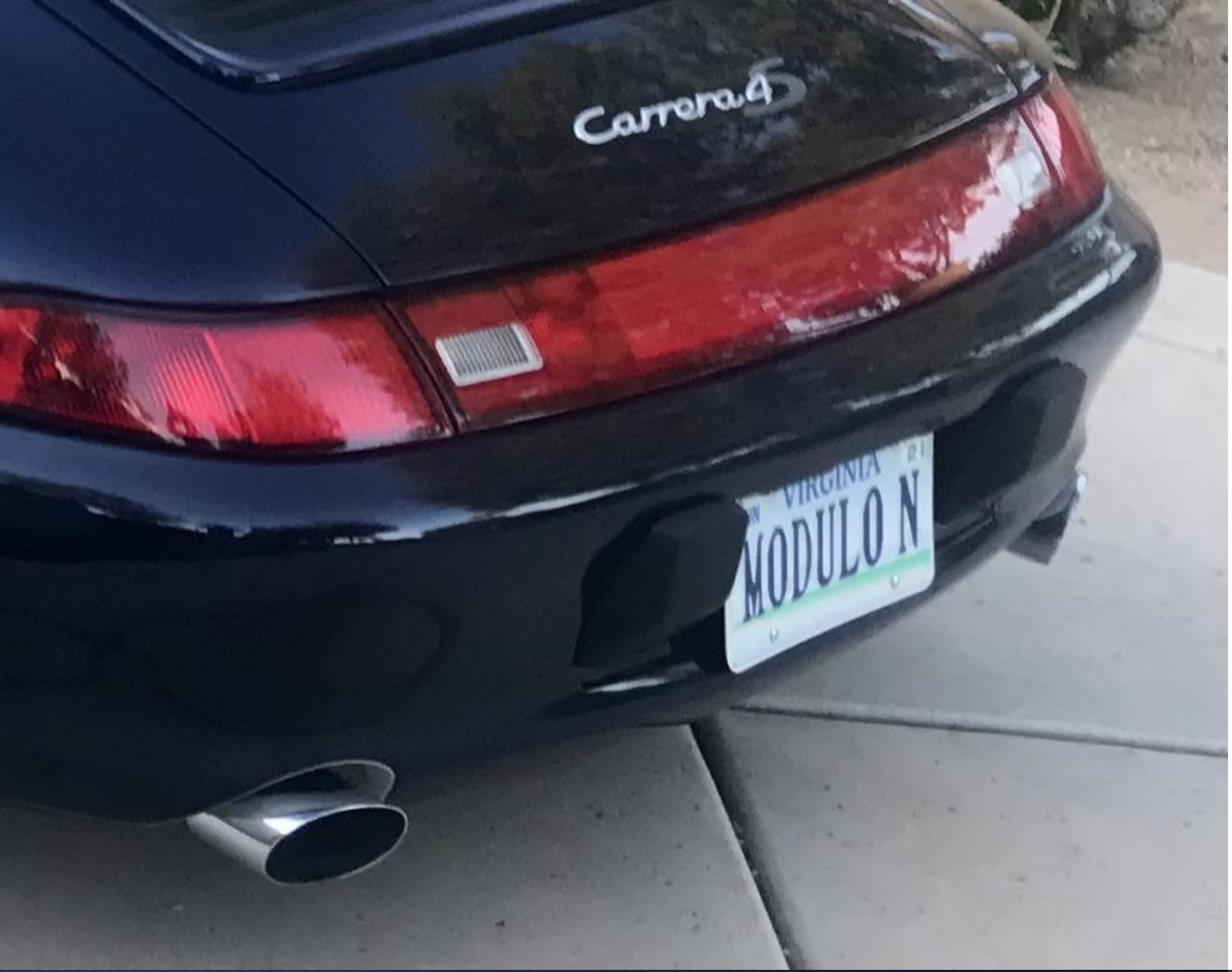
Key Words and Phrases: digital signatures, public-key cryptosystems, privacy, authentication, security, factorization, prime number, electronic mail, message-passing, electronic funds transfer, cryptography.

CR Categories: 2.12, 3.15, 3.50, 3.81, 5.25

[*] General permission to make fair use in teaching or research of all or part of this material is

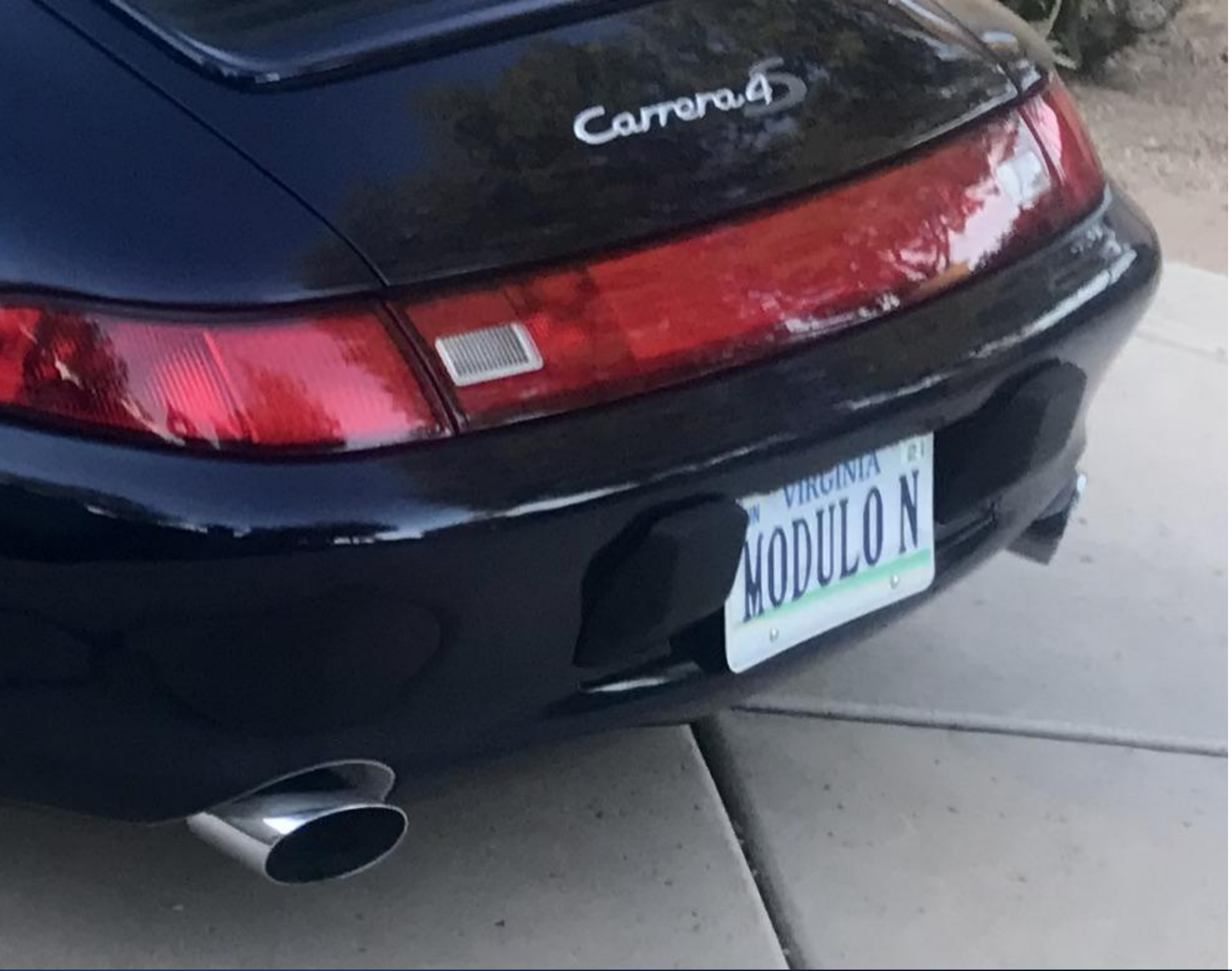
CALIFORNIA
M2EMODN

Carrera 4S
VIRGINIA
21
MODULO N



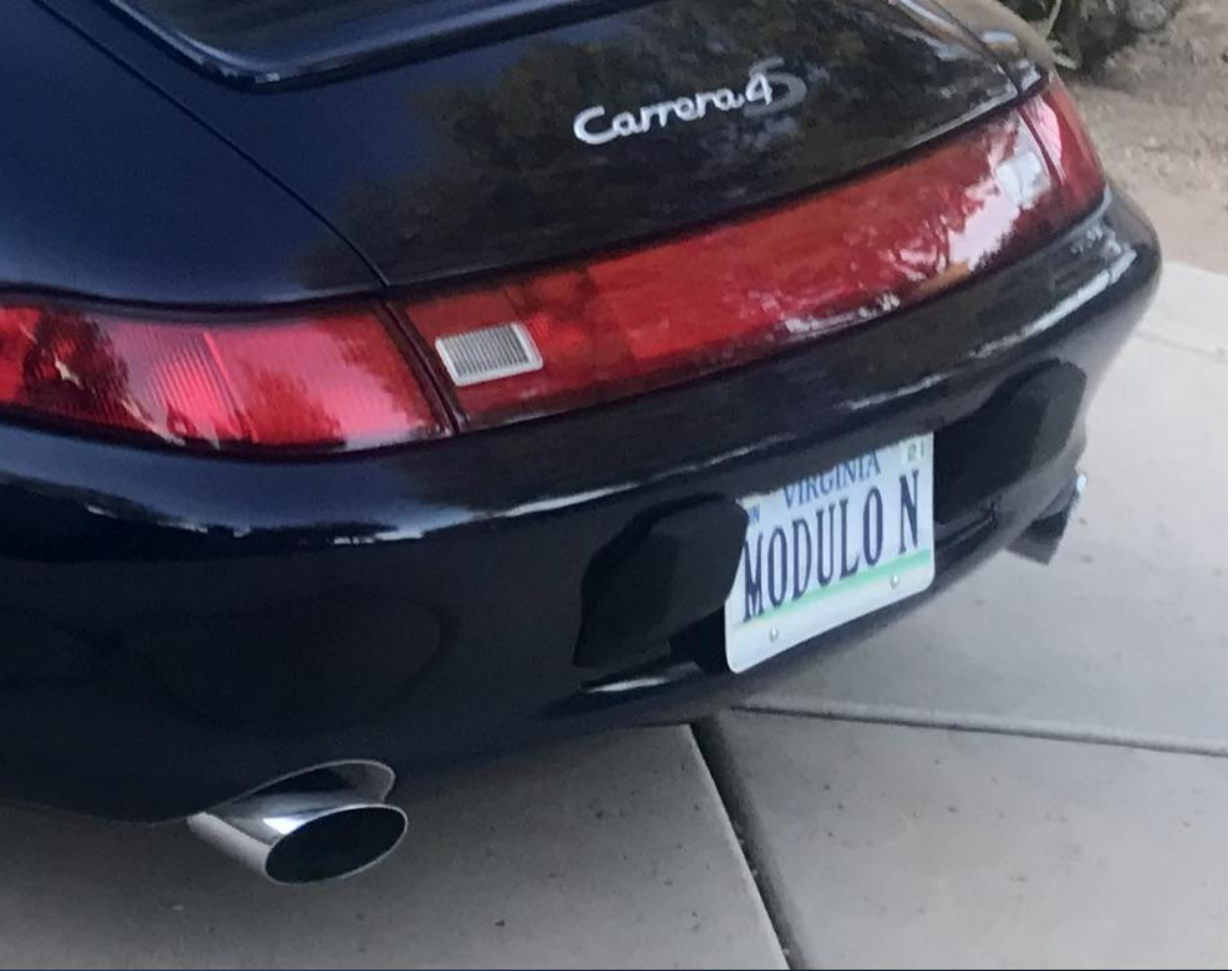
At a Starbucks one day…

- Man: “Hey, is that plate about math?”
- Me (excited): “Well, yes, it is!”



At a Starbucks one day…

- Man: “Hey, is that plate about math?”
- Me (excited): “Well, yes, it is!”
- Man: “Let me guess… you got divorced, had to divide everything, and that car is all you had left?”



At a Starbucks one day…

- Man: “Hey, is that plate about math?”
- Me (excited): “Well, yes, it is!”
- Man: “Let me guess… you got divorced, had to divide everything, and that car is all you had left?”
- Me (disappointed): “Um, no.”

He must have been a divorce lawyer.

Beginnings – 1982-1990

A start and restart. Products and deals. Obstacles. Stability?

Beginnings – 1982-1990

A start and restart. Products and deals. Obstacles. Stability?

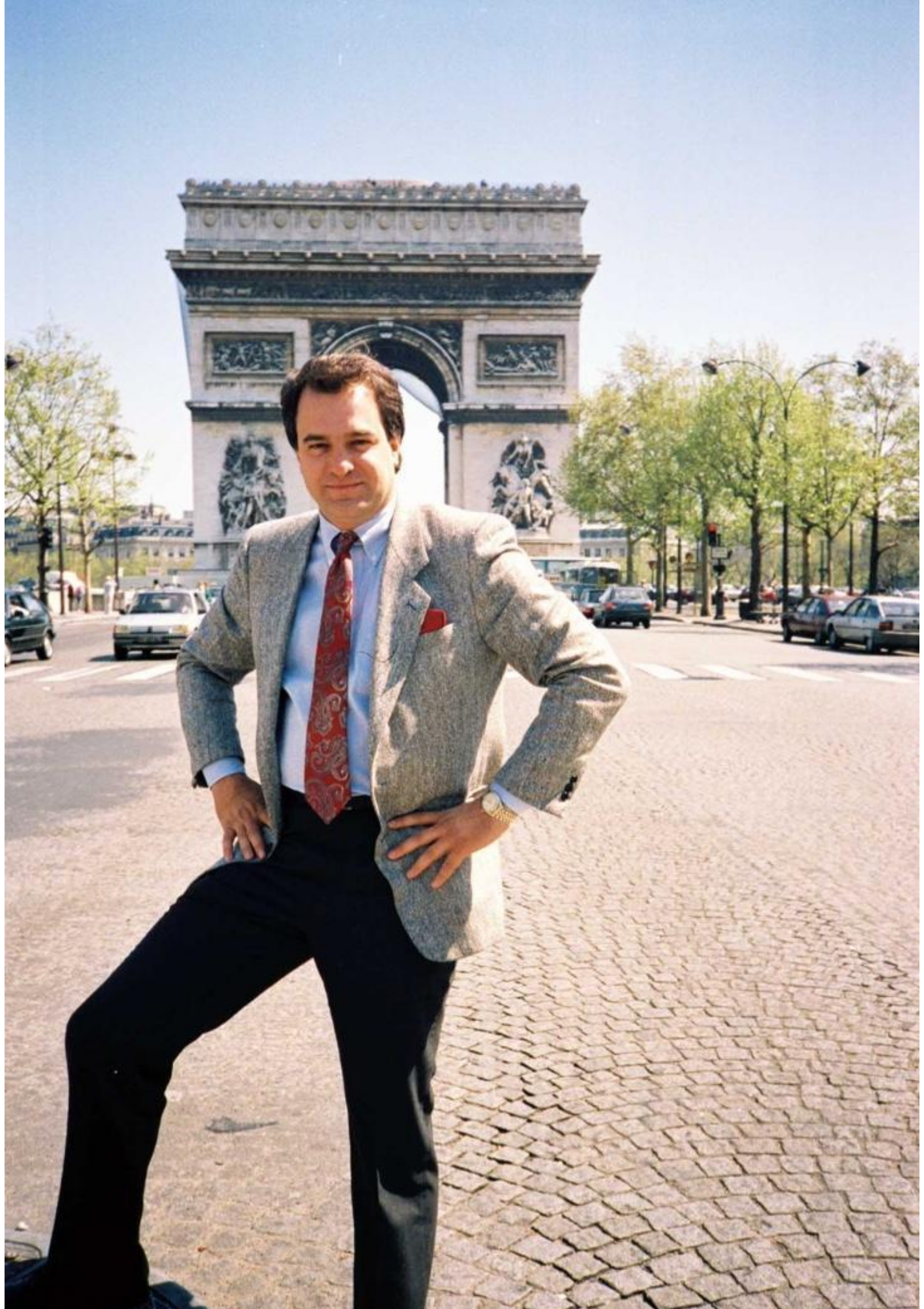
1982: R, S, and A incorporate in Belmont MA; Len Adleman is president.
1983: MIT gets a patent; the new company gets an exclusive license.
1984: A few hires, a chip is designed, a funding round, a move west.

Beginnings – 1982-1990

A start and restart. Products and deals. Obstacles. Stability?

1982: R, S, and A incorporate in Belmont MA; Len Adleman is president.
1983: MIT gets a patent; the new company gets an exclusive license.
1984: A few hires, a chip is designed, a funding round, a move west.
1985: The market is not as ready as thought. Money running out, investors unhappy.

ESCORT
BOSCH
BOB AKIN
DALE WHITTINGTON
JOHN O'STEEN
Scott Smith Olds
ORLANDO FLA
Enjoy
Coca-Cola
GOODYEAR
5
paradyne
KONI
MARCHAL
BBS



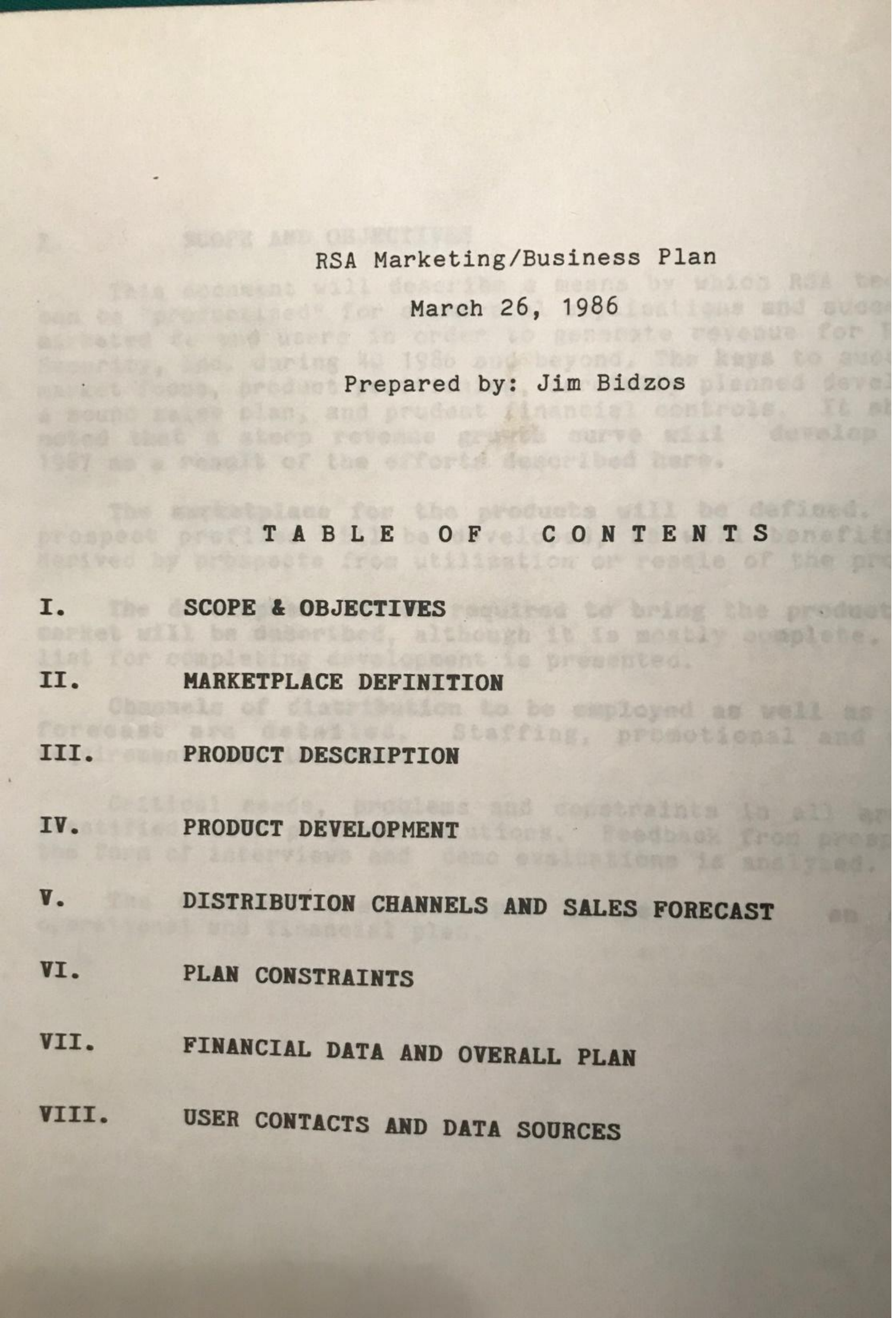
Beginnings – 1982-1990

A start and restart. Products and deals. Obstacles. Stability?

1982: R, S, and A incorporate in Belmont MA; Len Adleman is president.
1983: MIT gets a patent; the new company gets an exclusive license.
1984: A few hires, a chip is designed, a funding round, a move west.
1985: The market is not as ready as thought. Money running out, investors unhappy.
1986: A new person. A new Plan. B formally joins in January. A product launch.
A deal just in time. Venture Capital not available. (Didn't want it anyway.)
Unexpected competition appears. Investor impatience turns to ire.

RSA Survive & Bootstrap Plan

March 1986



RSA Marketing/Business Plan

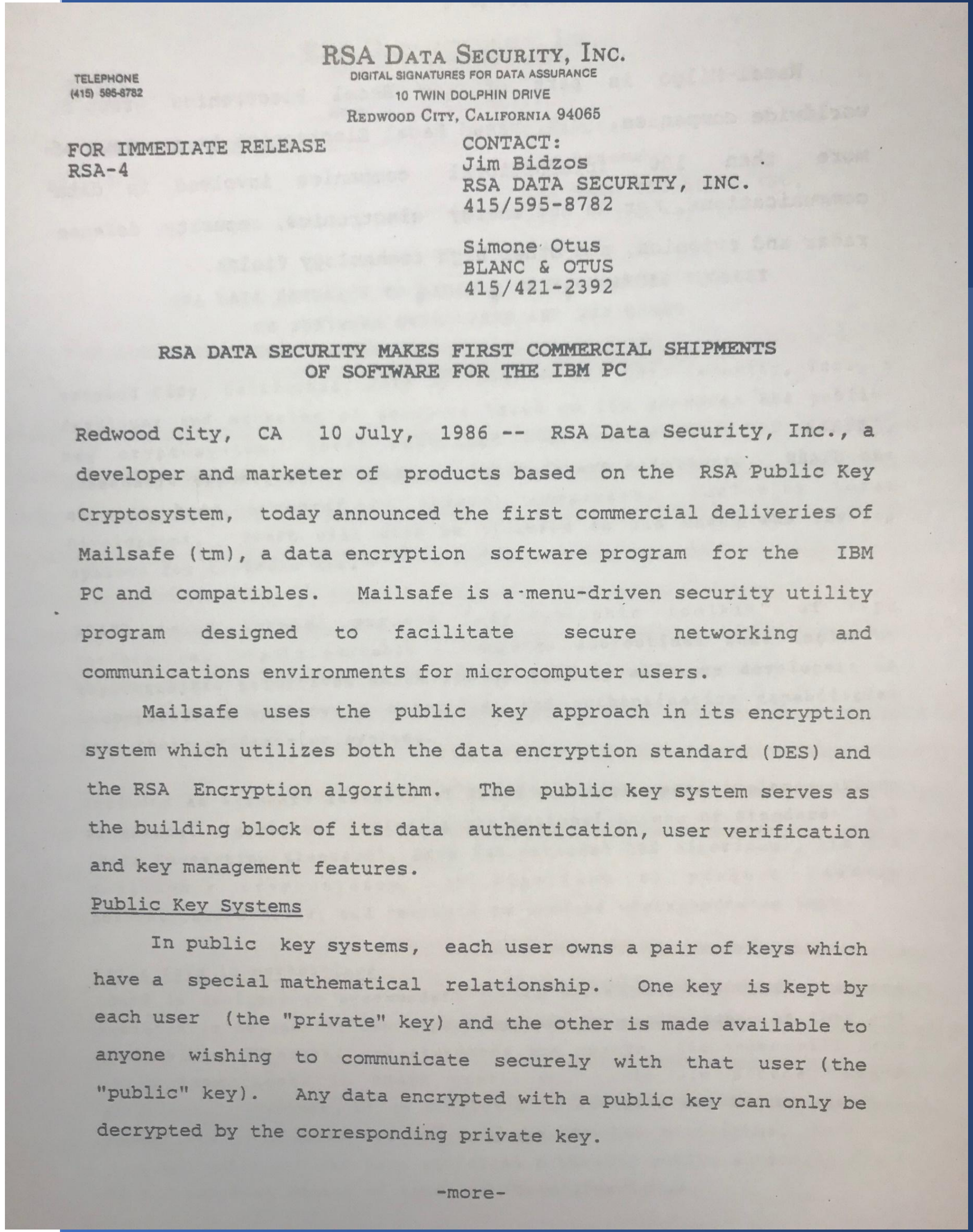
March 26, 1986

Prepared by: Jim Bidzos

TABLE OF CONTENTS

First Shipments of MailSafe

July 1986



RSA DATA SECURITY, INC.
DIGITAL SIGNATURES FOR DATA ASSURANCE
10 TWIN DOLPHIN DRIVE
REDWOOD CITY, CALIFORNIA 94065

TELEPHONE
(415) 595-8782

FOR IMMEDIATE RELEASE
RSA-4

CONTACT:
Jim Bidzos
RSA DATA SECURITY, INC.
415/595-8782

Simone Otus
BLANC & OTUS
415/421-2392

RSA DATA SECURITY MAKES FIRST COMMERCIAL SHIPMENTS
OF SOFTWARE FOR THE IBM PC

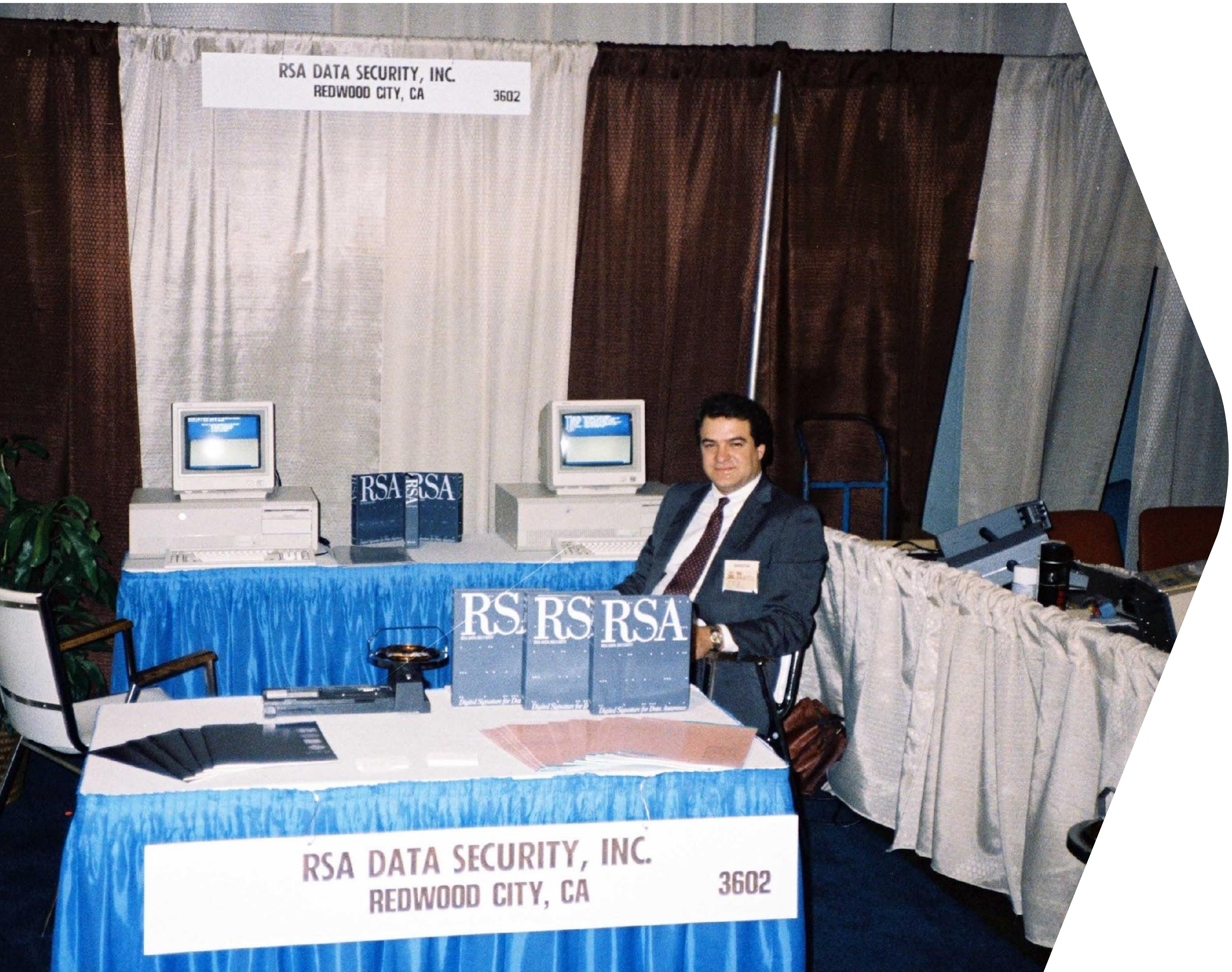
Redwood City, CA 10 July, 1986 -- RSA Data Security, Inc., a developer and marketer of products based on the RSA Public Key Cryptosystem, today announced the first commercial deliveries of Mailsafe (tm), a data encryption software program for the IBM PC and compatibles. Mailsafe is a menu-driven security utility program designed to facilitate secure networking and communications environments for microcomputer users.

Mailsafe uses the public key approach in its encryption system which utilizes both the data encryption standard (DES) and the RSA Encryption algorithm. The public key system serves as the building block of its data authentication, user verification and key management features.

Public Key Systems

In public key systems, each user owns a pair of keys which have a special mathematical relationship. One key is kept by each user (the "private" key) and the other is made available to anyone wishing to communicate securely with that user (the "public" key). Any data encrypted with a public key can only be decrypted by the corresponding private key.

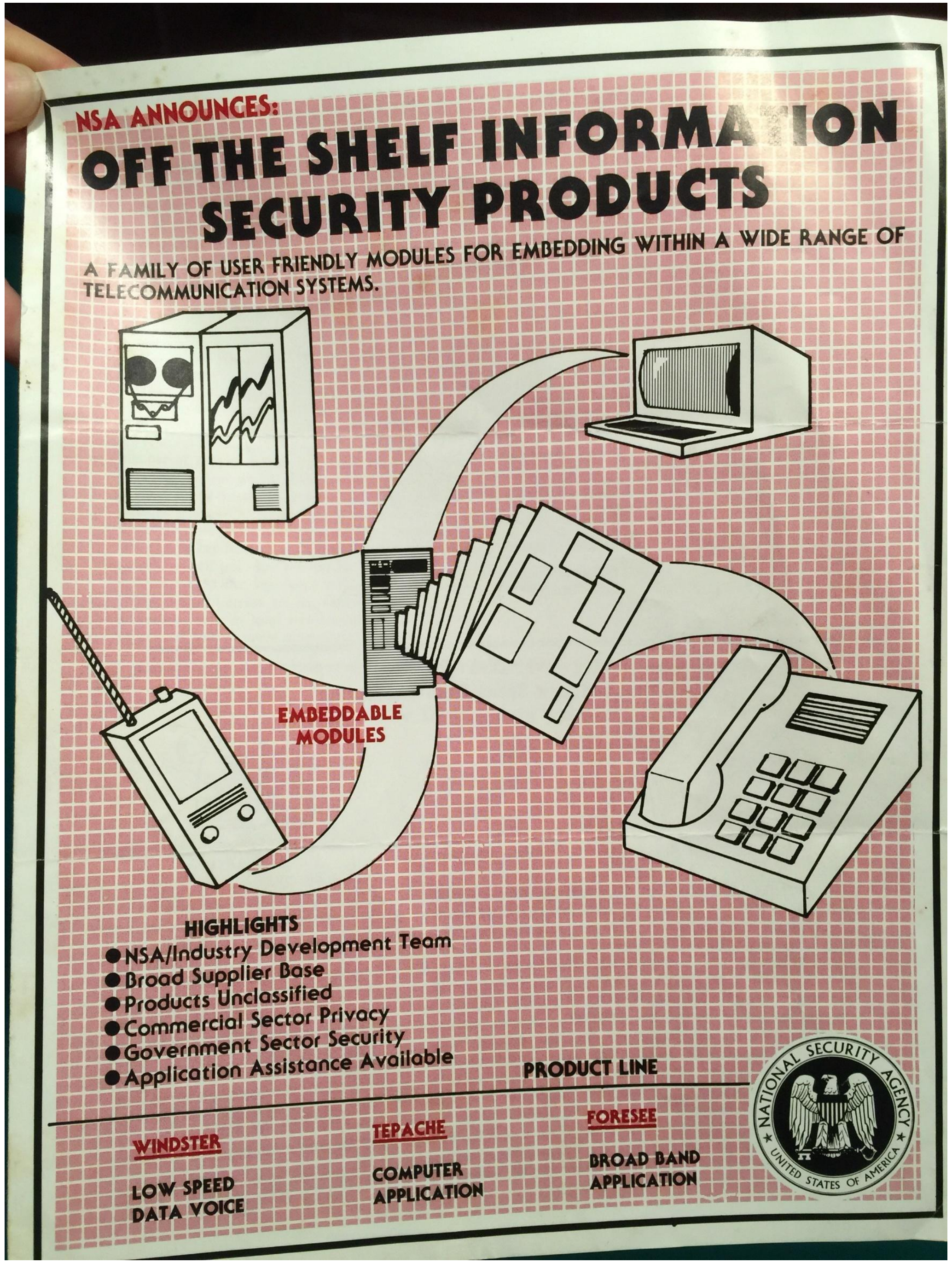
-more-



At FCC 1986 with MailSafe product

September 1986

NSA Headquarters



NSA ANNOUNCES:

OFF THE SHELF INFORMATION SECURITY PRODUCTS

A FAMILY OF USER FRIENDLY MODULES FOR EMBEDDING WITHIN A WIDE RANGE OF TELECOMMUNICATION SYSTEMS.

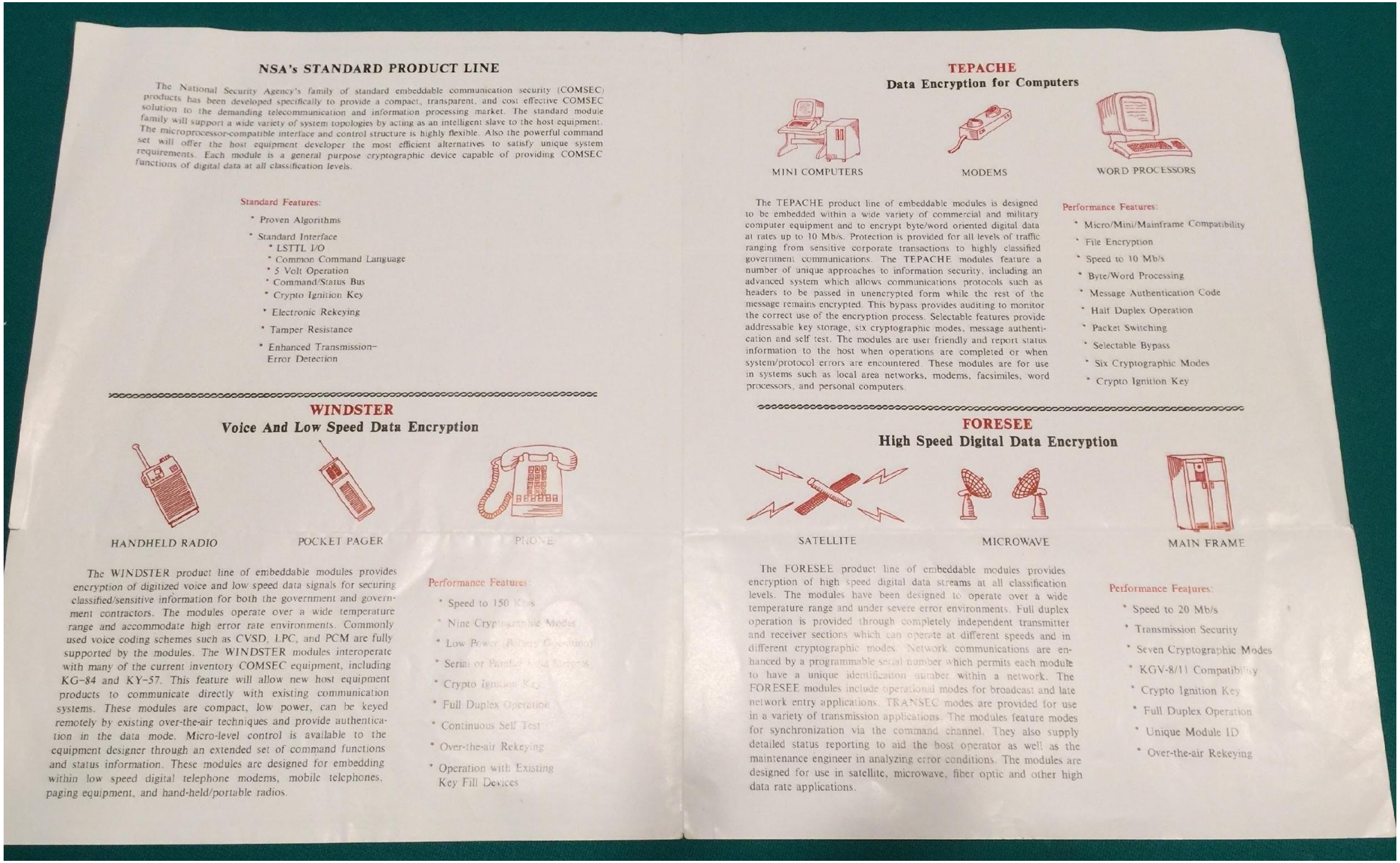
HIGHLIGHTS

- NSA/Industry Development Team
- Broad Supplier Base
- Products Unclassified
- Commercial Sector Privacy
- Government Sector Security
- Application Assistance Available

PRODUCT LINE

WINDSTER	TEPACHE	FORESEE
LOW SPEED DATA VOICE	COMPUTER APPLICATION	BROAD BAND APPLICATION

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA



NSA's STANDARD PRODUCT LINE

The National Security Agency's family of standard embeddable communication security (COMSEC) products has been developed specifically to provide a compact, transparent, and cost effective COMSEC solution to the demanding telecommunication and information processing market. The standard module family will support a wide variety of system topologies by acting as an intelligent slave to the host equipment. The microprocessor-compatible interface and control structure is highly flexible. Also the powerful command set will offer the host equipment developer the most efficient alternatives to satisfy unique system requirements. Each module is a general purpose cryptographic device capable of providing COMSEC functions of digital data at all classification levels.

Standard Features:

- Proven Algorithms
- Standard Interface
  - LSTTL I/O
  - Common Command Language
  - 5 Volt Operation
  - Command/Status Bus
  - Crypto Ignition Key
- Electronic Rekeying
- Tamper Resistance
- Enhanced Transmission–Error Detection

WINDSTER
Voice And Low Speed Data Encryption

HANDHELD RADIO

POCKET PAGER

PHONE

The WINDSTER product line of embeddable modules provides encryption of digitized voice and low speed data signals for securing classified/sensitive information for both the government and government contractors. The modules operate over a wide temperature range and accommodate high error rate environments. Commonly used voice coding schemes such as CVSD, LPC, and PCM are fully supported by the modules. The WINDSTER modules interoperate with many of the current inventory COMSEC equipment, including KG-84 and KY-57. This feature will allow new host equipment products to communicate directly with existing communication systems. These modules are compact, low power, can be keyed remotely by existing over-the-air techniques and provide authentication in the data mode. Micro-level control is available to the equipment designer through an extended set of command functions and status information. These modules are designed for embedding within low speed digital telephone modems, mobile telephones, paging equipment, and hand-held/portable radios.

Performance Features:

- Speed to 150 Kbps
- Nine Cryptographic Modes
- Low Power (Battery Operation)
- Serial or Parallel Data Streams
- Crypto Ignition Key
- Full Duplex Operation
- Continuous Self Test
- Over-the-air Rekeying
- Operation with Existing Key Fill Devices

TEPACHE
Data Encryption for Computers

MINI COMPUTERS

MODEMS

WORD PROCESSORS

The TEPACHE product line of embeddable modules is designed to be embedded within a wide variety of commercial and military computer equipment and to encrypt byte/word oriented digital data at rates up to 10 Mb/s. Protection is provided for all levels of traffic ranging from sensitive corporate transactions to highly classified government communications. The TEPACHE modules feature a number of unique approaches to information security, including an advanced system which allows communications protocols such as headers to be passed in unencrypted form while the rest of the message remains encrypted. This bypass provides auditing to monitor the correct use of the encryption process. Selectable features provide addressable key storage, six cryptographic modes, message authentication and self test. The modules are user friendly and report status information to the host when operations are completed or when system/protocol errors are encountered. These modules are for use in systems such as local area networks, modems, facsimiles, word processors, and personal computers.

Performance Features:

- Micro/Mini/Mainframe Compatibility
- File Encryption
- Speed to 10 Mb/s
- Byte/Word Processing
- Message Authentication Code
- Half Duplex Operation
- Packet Switching
- Selectable Bypass
- Six Cryptographic Modes
- Crypto Ignition Key

FORESEE
High Speed Digital Data Encryption

SATELLITE

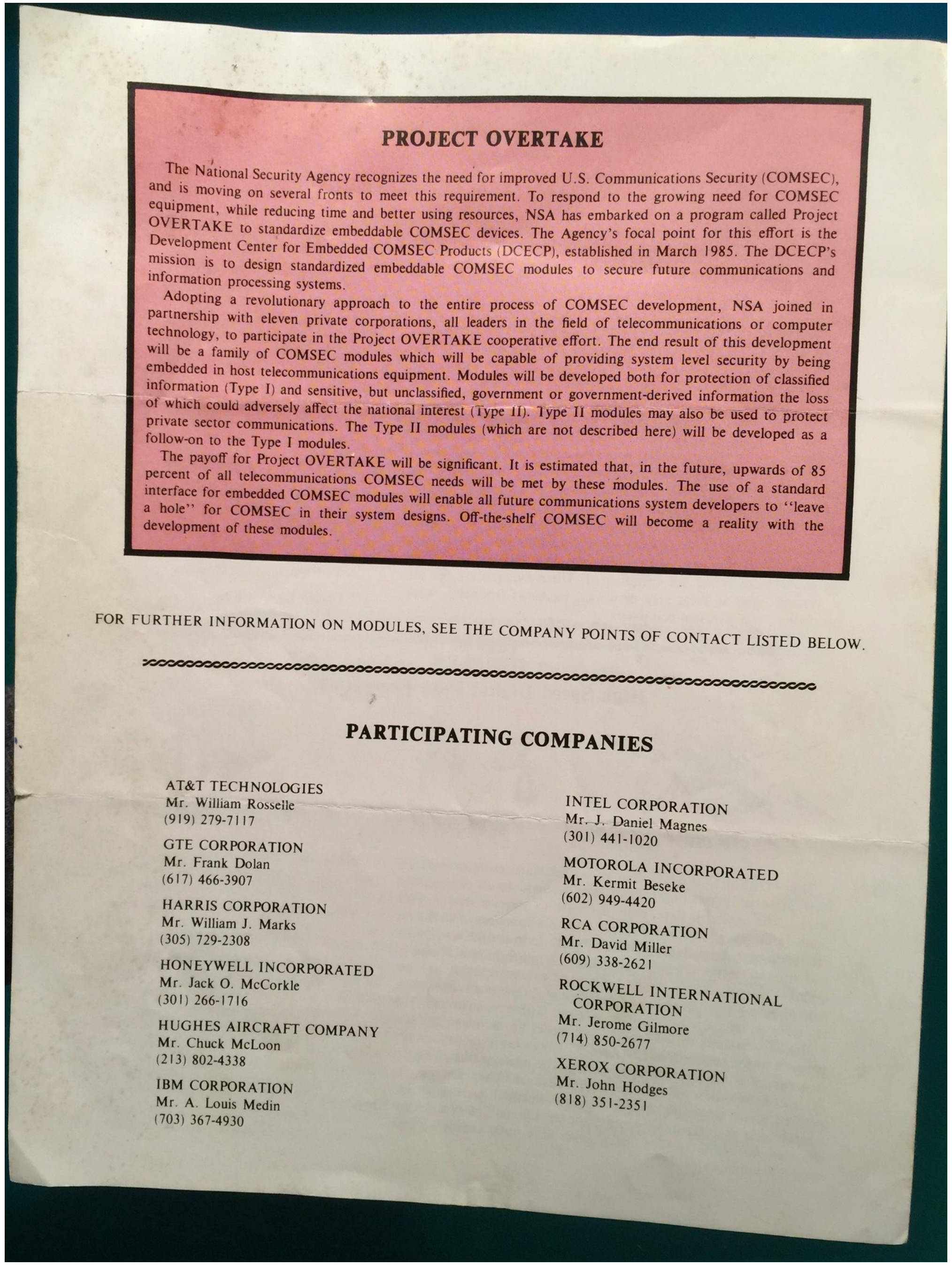
MICROWAVE

MAIN FRAME

The FORESEE product line of embeddable modules provides encryption of high speed digital data streams at all classification levels. The modules have been designed to operate over a wide temperature range and under severe error environments. Full duplex operation is provided through completely independent transmitter and receiver sections which can operate at different speeds and in different cryptographic modes. Network communications are enhanced by a programmable serial number which permits each module to have a unique identification number within a network. The FORESEE modules include operational modes for broadcast and late network entry applications. TRANSEC modes are provided for use in a variety of transmission applications. The modules feature modes for synchronization via the command channel. They also supply detailed status reporting to aid the host operator as well as the maintenance engineer in analyzing error conditions. The modules are designed for use in satellite, microwave, fiber optic and other high data rate applications.

Performance Features:

- Speed to 20 Mb/s
- Transmission Security
- Seven Cryptographic Modes
- KGV-8/11 Compatibility
- Crypto Ignition Key
- Full Duplex Operation
- Unique Module ID
- Over-the-air Rekeying



PROJECT OVERTAKE

The National Security Agency recognizes the need for improved U.S. Communications Security (COMSEC), and is moving on several fronts to meet this requirement. To respond to the growing need for COMSEC equipment, while reducing time and better using resources, NSA has embarked on a program called Project OVERTAKE to standardize embeddable COMSEC devices. The Agency's focal point for this effort is the Development Center for Embedded COMSEC Products (DCECP), established in March 1985. The DCECP's mission is to design standardized embeddable COMSEC modules to secure future communications and information processing systems.

Adopting a revolutionary approach to the entire process of COMSEC development, NSA joined in partnership with eleven private corporations, all leaders in the field of telecommunications or computer technology, to participate in the Project OVERTAKE cooperative effort. The end result of this development will be a family of COMSEC modules which will be capable of providing system level security by being embedded in host telecommunications equipment. Modules will be developed both for protection of classified information (Type I) and sensitive, but unclassified, government or government-derived information the loss of which could adversely affect the national interest (Type II). Type II modules may also be used to protect private sector communications. The Type II modules (which are not described here) will be developed as a follow-on to the Type I modules.

The payoff for Project OVERTAKE will be significant. It is estimated that, in the future, upwards of 85 percent of all telecommunications COMSEC needs will be met by these modules. The use of a standard interface for embedded COMSEC modules will enable all future communications system developers to "leave a hole" for COMSEC in their system designs. Off-the-shelf COMSEC will become a reality with the development of these modules.

FOR FURTHER INFORMATION ON MODULES, SEE THE COMPANY POINTS OF CONTACT LISTED BELOW.

PARTICIPATING COMPANIES

AT&T TECHNOLOGIES
Mr. William Rosselle
(919) 279-7117

GTE CORPORATION
Mr. Frank Dolan
(617) 466-3907

HARRIS CORPORATION
Mr. William J. Marks
(305) 729-2308

HONEYWELL INCORPORATED
Mr. Jack O. McCorkle
(301) 266-1716

HUGHES AIRCRAFT COMPANY
Mr. Chuck McLoon
(213) 802-4338

IBM CORPORATION
Mr. A. Louis Medin
(703) 367-4930

INTEL CORPORATION
Mr. J. Daniel Magnes
(301) 441-1020

MOTOROLA INCORPORATED
Mr. Kermit Beseke
(602) 949-4420

RCA CORPORATION
Mr. David Miller
(609) 338-2621

ROCKWELL INTERNATIONAL
CORPORATION
Mr. Jerome Gilmore
(714) 850-2677

XEROX CORPORATION
Mr. John Hodges
(818) 351-2351

Beginnings – 1982-1990

A start and restart. Products and deals. Obstacles. Stability?

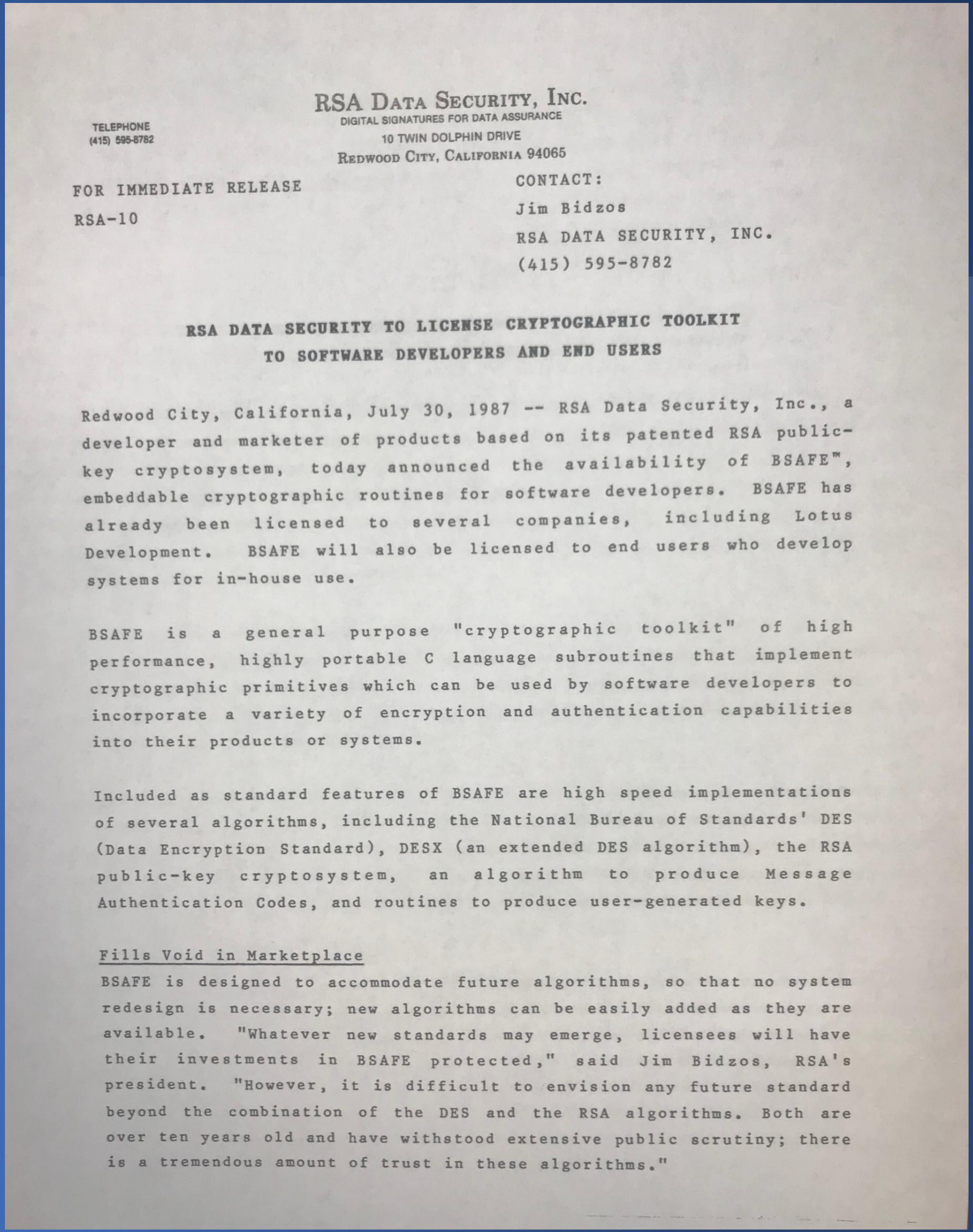
1982: R, S, and A incorporate in Belmont MA; Len Adleman is president.
1983: MIT gets a patent; the new company gets an exclusive license.
1984: A few hires, a chip is designed, a funding round, a move west.
1985: The market is not as ready as thought. Money running out, investors unhappy.
1986: A new person. A new Plan. B formally joins in January. A product launch.
A deal just in time. Venture Capital unavailable. (Didn't want it anyway.)
Unexpected competition appears. Investor impatience turns to ire.
1987: RSA announces BSAFE. Much missionary work. First lawsuit. Steve Dusse hired.

Frequent Flying Missionary

EXHIBITOR
'86
SPEAKER
Jim Bidzos President, RSA
D. James Bidzos RSA Security
James D. James Bidzos President & CEO RSA Data Security
BusinessWeek
Jim Bidzos RSA Data Security
DEXPO East 89 JAMES BIDZOS
CONFERENCE
ONLINE 95
PANELIST
EXHIBITS ONLY
COMDEX Fall '84
EMA
Jim Bidzos President RSA, Inc.
Jim Bidzos RSA Data Security, Inc.
RSA Day in Washington 1996
JIM BIDZOS RSA DATA SECURITY, INC
TeleStrategies
James Bidzos CEO RSA Data Security
JIM BIDZOS UNITED STATES
JAMES BIDZOS FULL INVITE RSA DATA SECURITY INC
Jim RSA Data Security, Inc.
VISITOR JIM BIDZOS
AFCEA D. JAMES BIDZOS RSA DATA SECURITY INC
Jim Bidzos RSA Data Security, Inc.
VIP
CLIPPER
KEY ESCROW
RSA DATA SECURITY
JIM JAMES BIDZOS RSA DATA SECURITY INC.
CONFERENCE/EXHIBITOR
JAMES BIDZOS
INTEROP 89
CONFERENCE FACULTY
DEXPO East 89 JAMES BIDZOS
James Bidzos Redwood City, CA
acm
Jim Bidzos Speaker
1993 SECURITY & VIRUS SYMPOSIUM
Jim Bidzos RSA Data Security, Inc.
CORPCON '86
CONFERENCE
'87
JIM BIDZOS
Banking & Financial Services on the Internet Jim Bidzos RSA Data Security, Inc.
Years of CPSR
D. James Bidzos
Jim Bidzos RSA Data Security, Inc. SPEAKER
sun JAN 20 1995
CRYPTO 86 JIM BIDZOS
Jim Bidzos CRYPTO 87
ISSE 88 JIM BIDZOS RSA DATA
Jim Bidzos CEO RSA Data Security

BSAFE Crypto Toolkit Available for Integration

July 1987



RSA Data Security, Inc.
DIGITAL SIGNATURES FOR DATA ASSURANCE
10 TWIN DOLPHIN DRIVE
Redwood City, California 94065

TELEPHONE
(415) 595-8782

FOR IMMEDIATE RELEASE
RSA-10

CONTACT:
Jim Bidzos
RSA DATA SECURITY, INC.
(415) 595-8782

RSA DATA SECURITY TO LICENSE CRYPTOGRAPHIC TOOLKIT TO SOFTWARE DEVELOPERS AND END USERS

Redwood City, California, July 30, 1987 -- RSA Data Security, Inc., a developer and marketer of products based on its patented RSA public-key cryptosystem, today announced the availability of BSAFE™, embeddable cryptographic routines for software developers. BSAFE has already been licensed to several companies, including Lotus Development. BSAFE will also be licensed to end users who develop systems for in-house use.

BSAFE is a general purpose "cryptographic toolkit" of high performance, highly portable C language subroutines that implement cryptographic primitives which can be used by software developers to incorporate a variety of encryption and authentication capabilities into their products or systems.

Included as standard features of BSAFE are high speed implementations of several algorithms, including the National Bureau of Standards' DES (Data Encryption Standard), DESX (an extended DES algorithm), the RSA public-key cryptosystem, an algorithm to produce Message Authentication Codes, and routines to produce user-generated keys.

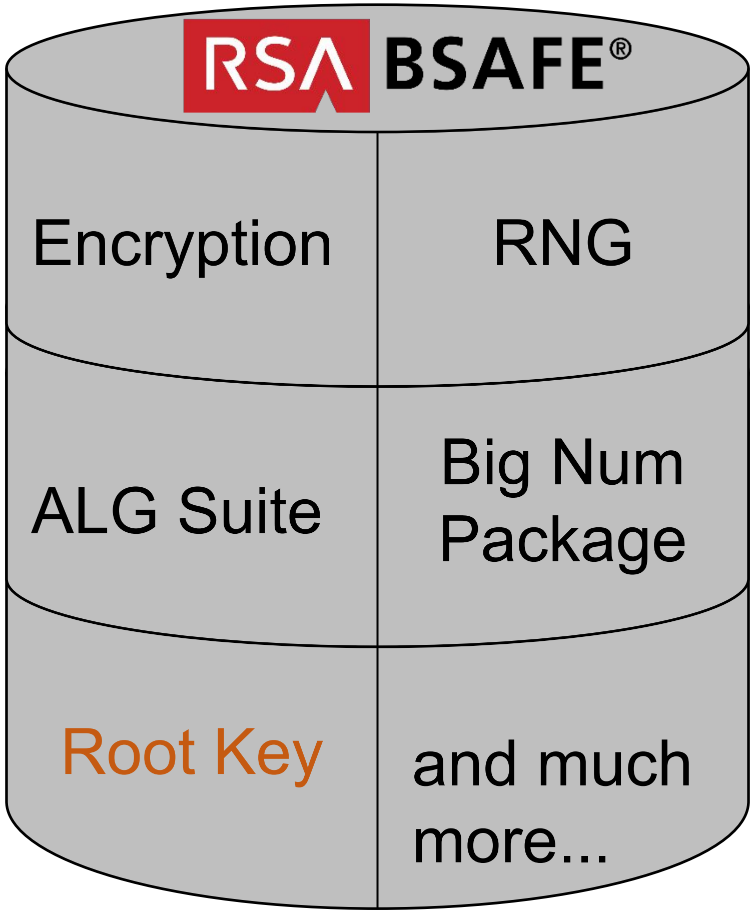
Fills Void in Marketplace

BSAFE is designed to accommodate future algorithms, so that no system redesign is necessary; new algorithms can be easily added as they are available. "Whatever new standards may emerge, licensees will have their investments in BSAFE protected," said Jim Bidzos, RSA's president. "However, it is difficult to envision any future standard beyond the combination of the DES and the RSA algorithms. Both are over ten years old and have withstood extensive public scrutiny; there is a tremendous amount of trust in these algorithms."

Standards compliant (Later)
All IP licensing included

- *Encryption algorithm suite*
  - Public Key
    - D-H
    - RSA
    - DSA (Later)
    - ECC (Later)
  - Symmetric Ciphers (Block + Stream)
    - DES
    - 3DES
    - AES (Later)
    - RCn
    - MDn
  - PRNG
  - Public keys and certs
  - Cert processing

"Cryptographer in a Box"



Beginnings – 1982-1990

A start and restart. Products and deals. Obstacles. Stability?

1982: R, S, and A incorporate in Belmont MA; Len Adleman is president.
1983: MIT gets a patent; the new company gets an exclusive license.
1984: A few hires, a funding round, a move west.
1985: The market is not as ready as thought. Money running out, investors unhappy.
1986: A new person. A new Plan. B formally joins in January. A product launch.
A deal just in time. Venture Capital not available. (Didn't want it anyway.)
Unexpected competition appears. Investor impatience turns to ire.
1987: RSA announces BSAFE. Much missionary work. First lawsuit. Steve Dusse hired.
1988: MIT doubles down on RSA. DEC becomes a customer. B believes a separate company will be needed for certificate services, and it will need to be bigger than RSA.

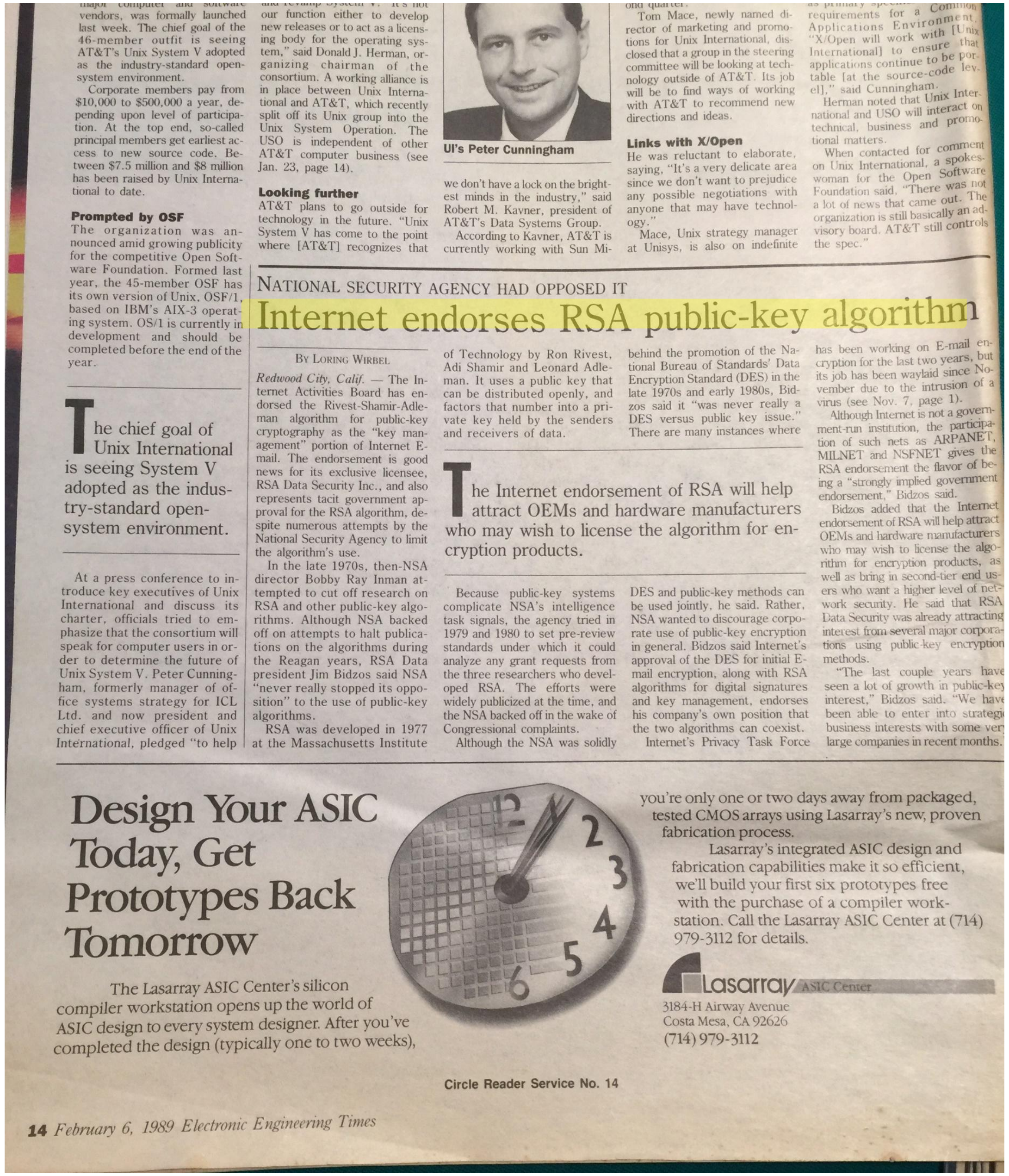
WHY A SEPARATE COMPANY?

- RSA was 100% focused on being an encryption technology & tools provider; Verisign would need to be a services company, entirely different
- It was anticipated that Verisign would go public, raising substantial funds to build secure facilities to protect signing keys
- Verisign needed to be transparent, independent, and not controlled by RSA or any single entity, in order to maintain public trust

Beginnings – 1982-1990

A start and restart. Products and deals. Obstacles. Stability?

1982: R, S, and A incorporate in Belmont MA; Len Adleman is president.
1983: MIT gets a patent; the new company gets an exclusive license.
1984: A few hires, a funding round, a move west.
1985: The market is not as ready as thought. Money running out, investors unhappy.
1986: A new person. A new Plan. B formally joins in January. A product launch.
A deal just in time. Venture Capital not available. (Didn't want it anyway.)
Unexpected competition appears. Investor impatience turns to ire.
1987: RSA announces BSAFE. Much missionary work. First lawsuit. Steve Dusse hired.
1988: MIT doubles down on RSA. DEC becomes a customer. B believes a separate company
will be needed for certificate services, and it will be bigger than RSA. Morris worm.
1989: "Internet" ☺ endorses RSA algorithm. Novell signs up with RSA. Burt Kaliski hired.



major computer and software vendors, was formally launched last week. The chief goal of the 46-member outfit is seeing AT&T's Unix System V adopted as the industry-standard open-system environment.

Corporate members pay from $10,000 to $500,000 a year, depending upon level of participation. At the top end, so-called principal members get earliest access to new source code. Between $7.5 million and $8 million has been raised by Unix International to date.

Prompted by OSF

The organization was announced amid growing publicity for the competitive Open Software Foundation. Formed last year, the 45-member OSF has its own version of Unix, OSF/1, based on IBM's AIX-3 operating system. OS/1 is currently in development and should be completed before the end of the year.

The chief goal of Unix International is seeing System V adopted as the industry-standard open-system environment.

At a press conference to introduce key executives of Unix International and discuss its charter, officials tried to emphasize that the consortium will speak for computer users in order to determine the future of Unix System V. Peter Cunningham, formerly manager of office systems strategy for ICL Ltd. and now president and chief executive officer of Unix International, pledged "to help and revamp System V. It's not our function either to develop new releases or to act as a licensing body for the operating system," said Donald J. Herman, organizing chairman of the consortium. A working alliance is in place between Unix International and AT&T, which recently split off its Unix group into the Unix System Operation. The USO is independent of other AT&T computer business (see Jan. 23, page 14).

Looking further

AT&T plans to go outside for technology in the future. "Unix System V has come to the point where [AT&T] recognizes that we don't have a lock on the brightest minds in the industry," said Robert M. Kavner, president of AT&T's Data Systems Group.

UI's Peter Cunningham

According to Kavner, AT&T is currently working with Sun Mi- [illegible] ond quarter.

Tom Mace, newly named director of marketing and promotions for Unix International, disclosed that a group in the steering committee will be looking at technology outside of AT&T. Its job will be to find ways of working with AT&T to recommend new directions and ideas.

Links with X/Open

He was reluctant to elaborate, saying, "It's a very delicate area since we don't want to prejudice any possible negotiations with anyone that may have technology."

Mace, Unix strategy manager at Unisys, is also on indefinite [illegible] as primary [illegible] requirements for a Common Applications Environment. "X/Open will work with [Unix International] to ensure that applications continue to be portable [at the source-code level]," said Cunningham.

Herman noted that Unix International and USO will interact on technical, business and promotional matters.

When contacted for comment on Unix International, a spokeswoman for the Open Software Foundation said, "There was not a lot of news that came out. The organization is still basically an advisory board. AT&T still controls the spec."

NATIONAL SECURITY AGENCY HAD OPPOSED IT

Internet endorses RSA public-key algorithm

BY LORING WIRBEL

Redwood City, Calif. — The Internet Activities Board has endorsed the Rivest-Shamir-Adleman algorithm for public-key cryptography as the "key management" portion of Internet E-mail. The endorsement is good news for its exclusive licensee, RSA Data Security Inc., and also represents tacit government approval for the RSA algorithm, despite numerous attempts by the National Security Agency to limit the algorithm's use.

In the late 1970s, then-NSA director Bobby Ray Inman attempted to cut off research on RSA and other public-key algorithms. Although NSA backed off on attempts to halt publications on the algorithms during the Reagan years, RSA Data president Jim Bidzos said NSA "never really stopped its opposition" to the use of public-key algorithms.

RSA was developed in 1977 at the Massachusetts Institute of Technology by Ron Rivest, Adi Shamir and Leonard Adleman. It uses a public key that can be distributed openly, and factors that number into a private key held by the senders and receivers of data.

The Internet endorsement of RSA will help attract OEMs and hardware manufacturers who may wish to license the algorithm for encryption products.

Because public-key systems complicate NSA's intelligence task signals, the agency tried in 1979 and 1980 to set pre-review standards under which it could analyze any grant requests from the three researchers who developed RSA. The efforts were widely publicized at the time, and the NSA backed off in the wake of Congressional complaints.

Although the NSA was solidly behind the promotion of the National Bureau of Standards' Data Encryption Standard (DES) in the late 1970s and early 1980s, Bidzos said it "was never really a DES versus public key issue." There are many instances where DES and public-key methods can be used jointly, he said. Rather, NSA wanted to discourage corporate use of public-key encryption in general. Bidzos said Internet's approval of the DES for initial E-mail encryption, along with RSA algorithms for digital signatures and key management, endorses his company's own position that the two algorithms can coexist.

Internet's Privacy Task Force has been working on E-mail encryption for the last two years, but its job has been waylaid since November due to the intrusion of a virus (see Nov. 7, page 1).

Although Internet is not a government-run institution, the participation of such nets as ARPANET, MILNET and NSFNET gives the RSA endorsement the flavor of being a "strongly implied government endorsement," Bidzos said.

Bidzos added that the Internet endorsement of RSA will help attract OEMs and hardware manufacturers who may wish to license the algorithm for encryption products, as well as bring in second-tier end users who want a higher level of network security. He said that RSA Data Security was already attracting interest from several major corporations using public-key encryption methods.

"The last couple years have seen a lot of growth in public-key interest," Bidzos said. "We have been able to enter into strategic business interests with some very large companies in recent months."

14 *February 6, 1989 Electronic Engineering Times*

IAB/IETF endorses RSA algorithm as part of PEM (Privacy Enhanced Mail) spec.

January 1989

Beginnings – 1982-1990

A start and restart. Products and deals. Obstacles. Stability?

1982: R, S, and A incorporate in Belmont MA; Len Adleman is president.

1983: MIT gets a patent; the new company gets an exclusive license.

1984: A few hires, a funding round, a move west.

1985: The market is not as ready as thought. Money running out, investors unhappy.

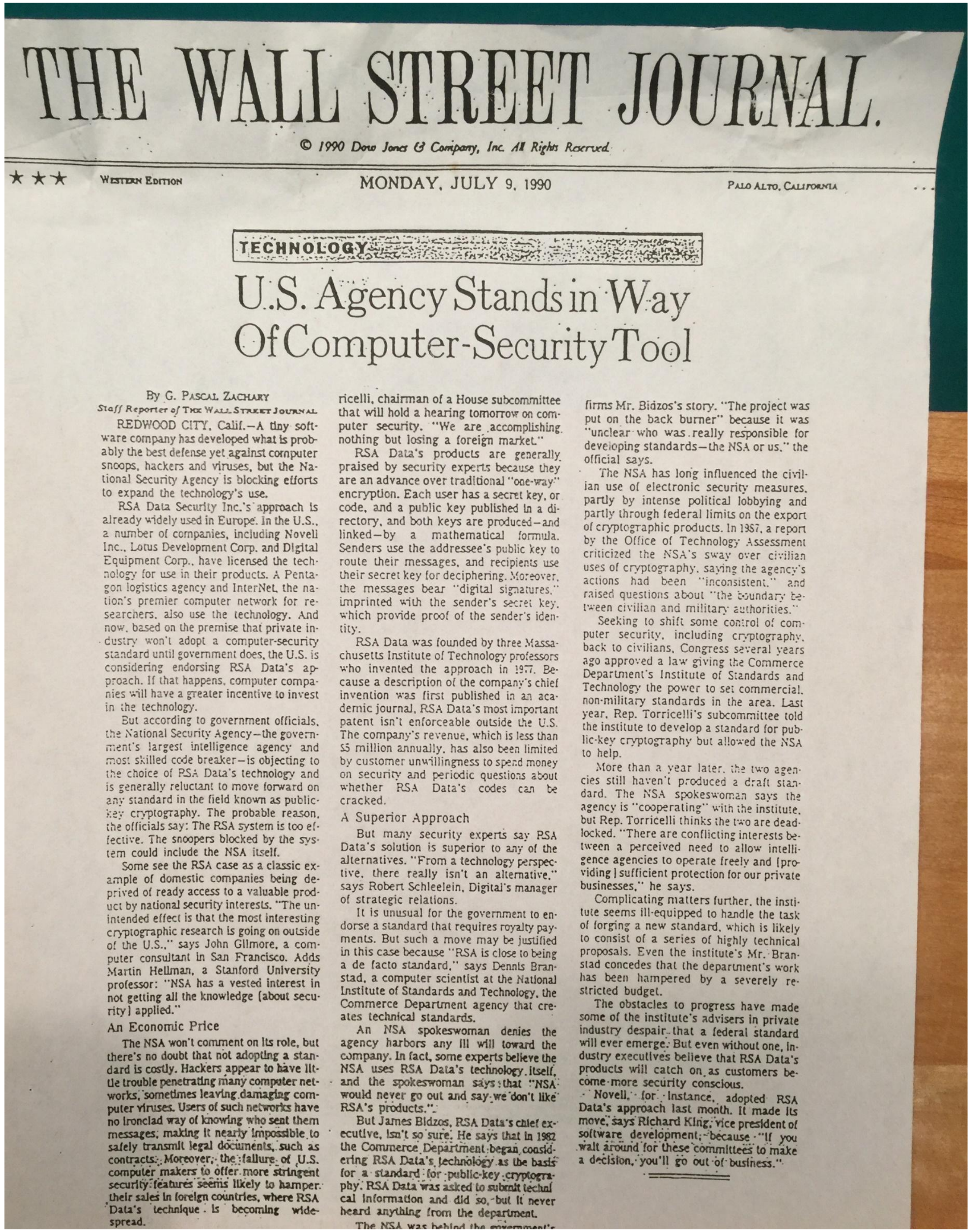
1986: A new person. A new Plan. B formally joins in January. A product launch. A deal just in time. Venture Capital not available. (Didn't want it anyway.) Unexpected competition appears. Investor impatience turns to ire.

1987: RSA announces BSAFE. Much missionary work. First lawsuit. Steve Dusse hired.

1988: MIT doubles down on RSA. DEC becomes a customer. B believes a separate company will be needed for certificate services, and it will be bigger than RSA. Morris worm.

1989: "Internet" ☺️ endorses RSA algorithm. Novell signs up with RSA. Burt Kaliski hired.

1990: Despite much progress, ominous beginnings for the new decade: An uneasy patent peace and a hearing.



THE WALL STREET JOURNAL.

© 1990 Dow Jones & Company, Inc. All Rights Reserved

★★★ WESTERN EDITION MONDAY, JULY 9, 1990 PALO ALTO, CALIFORNIA

TECHNOLOGY

U.S. Agency Stands in Way Of Computer-Security Tool

By G. PASCAL ZACHARY
Staff Reporter of THE WALL STREET JOURNAL

REDWOOD CITY, Calif.—A tiny software company has developed what is probably the best defense yet against computer snoops, hackers and viruses, but the National Security Agency is blocking efforts to expand the technology's use.

RSA Data Security Inc.'s approach is already widely used in Europe. In the U.S., a number of companies, including Novell Inc., Lotus Development Corp. and Digital Equipment Corp., have licensed the technology for use in their products. A Pentagon logistics agency and InterNet, the nation's premier computer network for researchers, also use the technology. And now, based on the premise that private industry won't adopt a computer-security standard until government does, the U.S. is considering endorsing RSA Data's approach. If that happens, computer companies will have a greater incentive to invest in the technology.

But according to government officials, the National Security Agency—the government's largest intelligence agency and most skilled code breaker—is objecting to the choice of RSA Data's technology and is generally reluctant to move forward on any standard in the field known as public-key cryptography. The probable reason, the officials say: The RSA system is too effective. The snoopers blocked by the system could include the NSA itself.

Some see the RSA case as a classic example of domestic companies being deprived of ready access to a valuable product by national security interests. "The unintended effect is that the most interesting cryptographic research is going on outside of the U.S.," says John Gilmore, a computer consultant in San Francisco. Adds Martin Hellman, a Stanford University professor: "NSA has a vested interest in not getting all the knowledge [about security] applied."

An Economic Price

The NSA won't comment on its role, but there's no doubt that not adopting a standard is costly. Hackers appear to have little trouble penetrating many computer networks, sometimes leaving damaging computer viruses. Users of such networks have no ironclad way of knowing who sent them messages, making it nearly impossible to safely transmit legal documents, such as contracts. Moreover, the failure of U.S. computer makers to offer more stringent security features seems likely to hamper their sales in foreign countries, where RSA Data's technique is becoming widespread.

ricelli, chairman of a House subcommittee that will hold a hearing tomorrow on computer security. "We are accomplishing nothing but losing a foreign market."

RSA Data's products are generally praised by security experts because they are an advance over traditional "one-way" encryption. Each user has a secret key, or code, and a public key published in a directory, and both keys are produced—and linked—by a mathematical formula. Senders use the addressee's public key to route their messages, and recipients use their secret key for deciphering. Moreover, the messages bear "digital signatures," imprinted with the sender's secret key, which provide proof of the sender's identity.

RSA Data was founded by three Massachusetts Institute of Technology professors who invented the approach in 1977. Because a description of the company's chief invention was first published in an academic journal, RSA Data's most important patent isn't enforceable outside the U.S. The company's revenue, which is less than $5 million annually, has also been limited by customer unwillingness to spend money on security and periodic questions about whether RSA Data's codes can be cracked.

A Superior Approach

But many security experts say RSA Data's solution is superior to any of the alternatives. "From a technology perspective, there really isn't an alternative," says Robert Schleelein, Digital's manager of strategic relations.

It is unusual for the government to endorse a standard that requires royalty payments. But such a move may be justified in this case because "RSA is close to being a de facto standard," says Dennis Branstad, a computer scientist at the National Institute of Standards and Technology, the Commerce Department agency that creates technical standards.

An NSA spokeswoman denies the agency harbors any ill will toward the company. In fact, some experts believe the NSA uses RSA Data's technology itself, and the spokeswoman says that "NSA would never go out and say we don't like RSA's products."

But James Bidzos, RSA Data's chief executive, isn't so sure. He says that in 1982 the Commerce Department began considering RSA Data's technology as the basis for a standard for public-key cryptography. RSA Data was asked to submit technical information and did so, but it never heard anything from the department.

The NSA was behind the government's

firms Mr. Bidzos's story. "The project was put on the back burner" because it was "unclear who was really responsible for developing standards—the NSA or us," the official says.

The NSA has long influenced the civilian use of electronic security measures, partly by intense political lobbying and partly through federal limits on the export of cryptographic products. In 1987, a report by the Office of Technology Assessment criticized the NSA's sway over civilian uses of cryptography, saying the agency's actions had been "inconsistent," and raised questions about "the boundary between civilian and military authorities."

Seeking to shift some control of computer security, including cryptography, back to civilians, Congress several years ago approved a law giving the Commerce Department's Institute of Standards and Technology the power to set commercial, non-military standards in the area. Last year, Rep. Torricelli's subcommittee told the institute to develop a standard for public-key cryptography but allowed the NSA to help.

More than a year later, the two agencies still haven't produced a draft standard. The NSA spokeswoman says the agency is "cooperating" with the institute, but Rep. Torricelli thinks the two are deadlocked. "There are conflicting interests between a perceived need to allow intelligence agencies to operate freely and [providing] sufficient protection for our private businesses," he says.

Complicating matters further, the institute seems ill-equipped to handle the task of forging a new standard, which is likely to consist of a series of highly technical proposals. Even the institute's Mr. Branstad concedes that the department's work has been hampered by a severely restricted budget.

The obstacles to progress have made some of the institute's advisers in private industry despair that a federal standard will ever emerge. But even without one, industry executives believe that RSA Data's products will catch on as customers become more security conscious.

Novell, for instance, adopted RSA Data's approach last month. It made its move, says Richard King, vice president of software development, because "If you wait around for these committees to make a decision, you'll go out of business."

"But according to government officials, the National Security Agency – the government's largest intelligence agency and most skilled code breaker – is objecting to the choice of RSA Data's technology."

"The probable reason, the officials say: The RSA system is too effective. The snoopers blocked by the system could include the NSA itself."

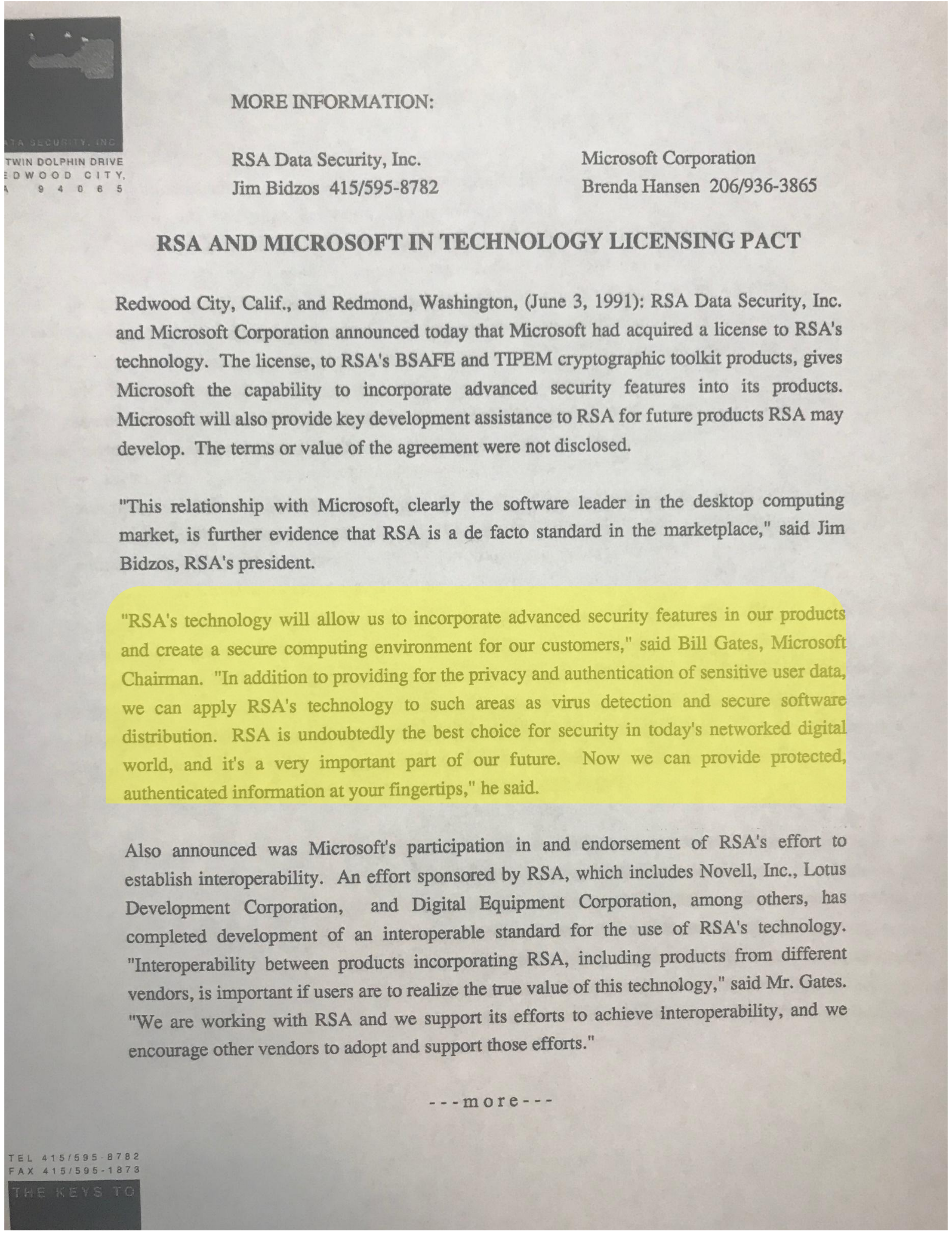
Resistance – 1991-1994

Big wins, bigger challenges. Cause and effect?

Resistance – 1991-1994

Big wins, bigger challenges. Cause and effect?

1991: RSA signs Microsoft (barely), Apple, Sun Microsystems, and more.
PKCS Consortium formed. RSA Factoring Challenge. S266. DSA plans
announced by NIST, designed by NSA. First RSA Conference.



ATA SECURITY, INC

TWIN DOLPHIN DRIVE
EDWOOD CITY,
A 94065

MORE INFORMATION:

RSA Data Security, Inc.	Microsoft Corporation
Jim Bidzos 415/595-8782	Brenda Hansen 206/936-3865

RSA AND MICROSOFT IN TECHNOLOGY LICENSING PACT

Redwood City, Calif., and Redmond, Washington, (June 3, 1991): RSA Data Security, Inc. and Microsoft Corporation announced today that Microsoft had acquired a license to RSA's technology. The license, to RSA's BSAFE and TIPEM cryptographic toolkit products, gives Microsoft the capability to incorporate advanced security features into its products. Microsoft will also provide key development assistance to RSA for future products RSA may develop. The terms or value of the agreement were not disclosed.

"This relationship with Microsoft, clearly the software leader in the desktop computing market, is further evidence that RSA is a de facto standard in the marketplace," said Jim Bidzos, RSA's president.

"RSA's technology will allow us to incorporate advanced security features in our products and create a secure computing environment for our customers," said Bill Gates, Microsoft Chairman. "In addition to providing for the privacy and authentication of sensitive user data, we can apply RSA's technology to such areas as virus detection and secure software distribution. RSA is undoubtedly the best choice for security in today's networked digital world, and it's a very important part of our future. Now we can provide protected, authenticated information at your fingertips," he said.

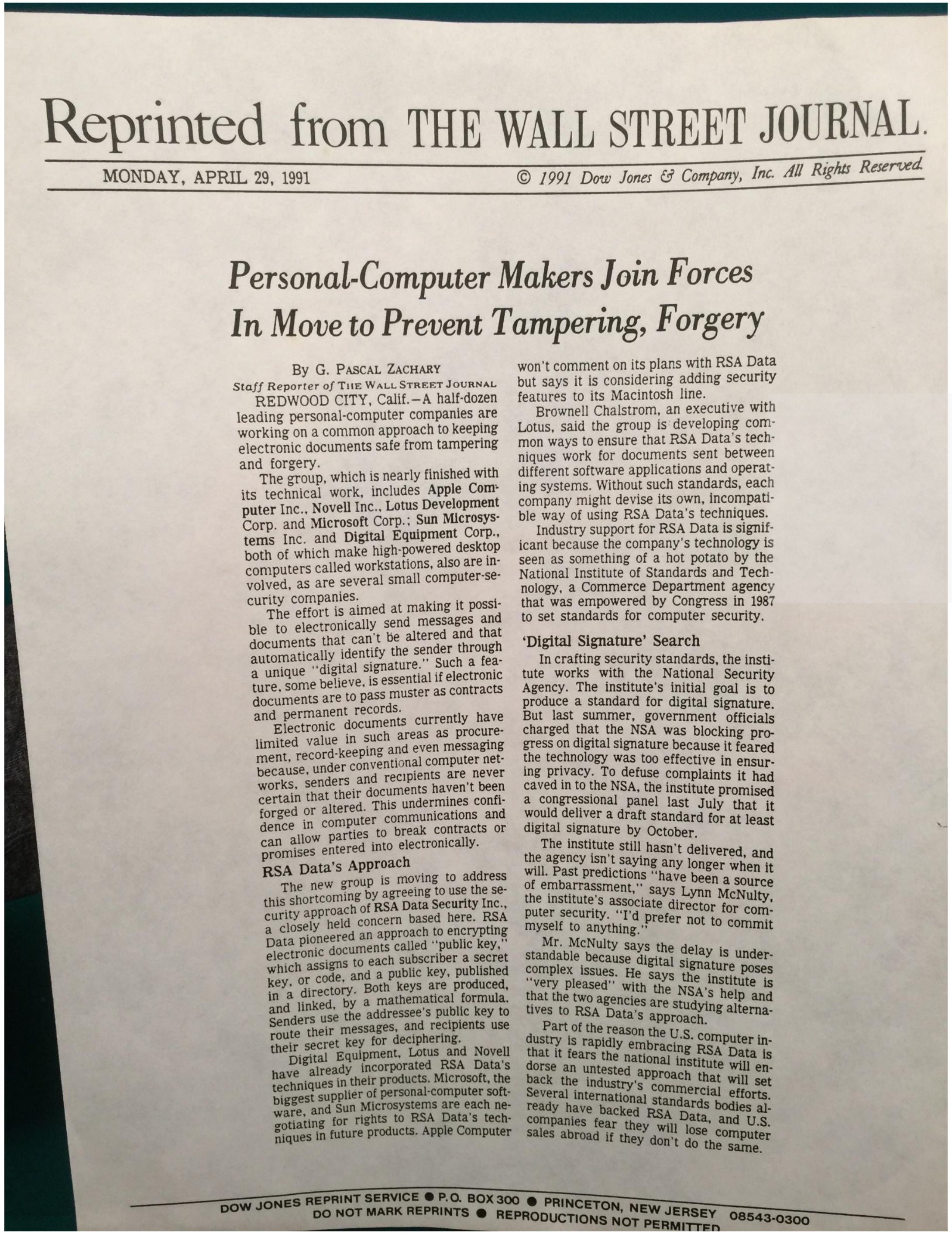
Also announced was Microsoft's participation in and endorsement of RSA's effort to establish interoperability. An effort sponsored by RSA, which includes Novell, Inc., Lotus Development Corporation, and Digital Equipment Corporation, among others, has completed development of an interoperable standard for the use of RSA's technology. "Interoperability between products incorporating RSA, including products from different vendors, is important if users are to realize the true value of this technology," said Mr. Gates. "We are working with RSA and we support its efforts to achieve interoperability, and we encourage other vendors to adopt and support those efforts."

---more---

TEL 415/595-8782
FAX 415/595-1873

THE KEYS TO

"RSA's technology will allow us to incorporate advanced security features in our products and create a secure computing environment for our customers." –Bill Gates, June 1991



Reprinted from THE WALL STREET JOURNAL.

MONDAY, APRIL 29, 1991

Personal-Computer Makers Join Forces In Move to Prevent Tampering, Forgery

By G. PASCAL ZACHARY
Staff Reporter of THE WALL STREET JOURNAL

REDWOOD CITY, Calif.—A half-dozen leading personal-computer companies are working on a common approach to keeping electronic documents safe from tampering and forgery.

The group, which is nearly finished with its technical work, includes **Apple Computer** Inc., **Novell** Inc., **Lotus Development** Corp. and **Microsoft** Corp.; **Sun Microsystems** Inc. and **Digital Equipment** Corp., both of which make high-powered desktop computers called workstations, also are involved, as are several small computer-security companies.

The effort is aimed at making it possible to electronically send messages and documents that can't be altered and that automatically identify the sender through a unique "digital signature." Such a feature, some believe, is essential if electronic documents are to pass muster as contracts and permanent records.

Electronic documents currently have limited value in such areas as procurement, record-keeping and even messaging because, under conventional computer networks, senders and recipients are never certain that their documents haven't been forged or altered. This undermines confidence in computer communications and can allow parties to break contracts or promises entered into electronically.

RSA Data's Approach

The new group is moving to address this shortcoming by agreeing to use the security approach of **RSA Data Security** Inc., a closely held concern based here. RSA Data pioneered an approach to encrypting electronic documents called "public key," which assigns to each subscriber a secret key, or code, and a public key, published in a directory. Both keys are produced, and linked, by a mathematical formula. Senders use the addressee's public key to route their messages, and recipients use their secret key for deciphering.

Digital Equipment, Lotus and Novell have already incorporated RSA Data's techniques in their products. Microsoft, the biggest supplier of personal-computer software, and Sun Microsystems are each negotiating for rights to RSA Data's techniques in future products. Apple Computer won't comment on its plans with RSA Data but says it is considering adding security features to its Macintosh line.

Brownell Chalstrom, an executive with Lotus, said the group is developing common ways to ensure that RSA Data's techniques work for documents sent between different software applications and operating systems. Without such standards, each company might devise its own, incompatible way of using RSA Data's techniques.

Industry support for RSA Data is significant because the company's technology is seen as something of a hot potato by the National Institute of Standards and Technology, a Commerce Department agency that was empowered by Congress in 1987 to set standards for computer security.

'Digital Signature' Search

In crafting security standards, the institute works with the National Security Agency. The institute's initial goal is to produce a standard for digital signature. But last summer, government officials charged that the NSA was blocking progress on digital signature because it feared the technology was too effective in ensuring privacy. To defuse complaints it had caved in to the NSA, the institute promised a congressional panel last July that it would deliver a draft standard for at least digital signature by October.

The institute still hasn't delivered, and the agency isn't saying any longer when it will. Past predictions "have been a source of embarrassment," says Lynn McNulty, the institute's associate director for computer security. "I'd prefer not to commit myself to anything."

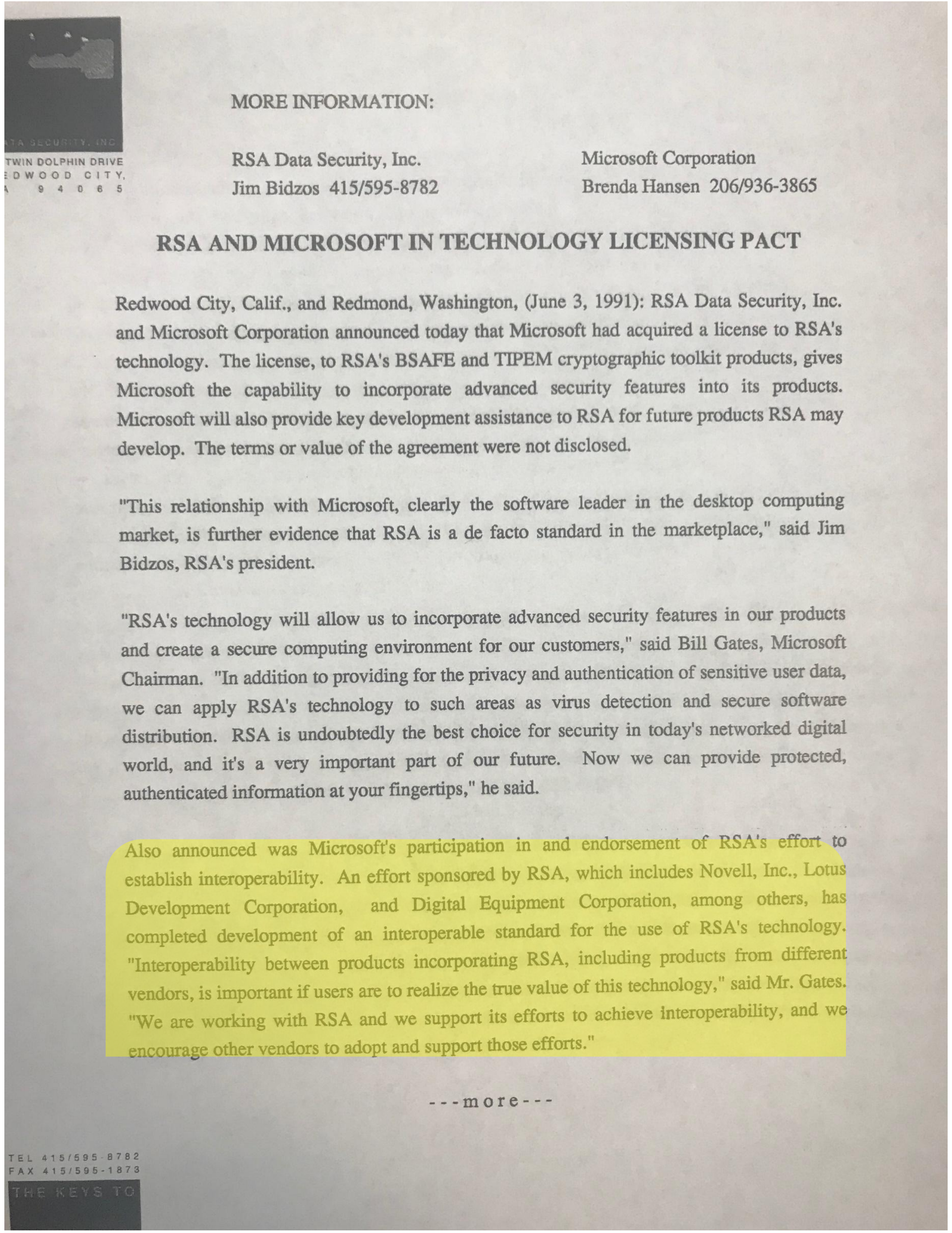
Mr. McNulty says the delay is understandable because digital signature poses complex issues. He says the institute is "very pleased" with the NSA's help and that the two agencies are studying alternatives to RSA Data's approach.

Part of the reason the U.S. computer industry is rapidly embracing RSA Data is that it fears the national institute will endorse an untested approach that will set back the industry's commercial efforts. Several international standards bodies already have backed RSA Data, and U.S. companies fear they will lose computer sales abroad if they don't do the same.

DOW JONES REPRINT SERVICE ● P.O. BOX 300 ● PRINCETON, NEW JERSEY 08543-0300
DO NOT MARK REPRINTS ● REPRODUCTIONS NOT PERMITTED

The PKCS (Public Key Cryptography Standards) consortium is launched, April 1991, with Apple, Novell, Lotus, and Microsoft

"Industry support for RSA Data is significant because the company's technology is seen as something of a hot potato by the National Institute of Standards and Technology."



ATA SECURITY, INC
TWIN DOLPHIN DRIVE
EDWOOD CITY,
A 94065

MORE INFORMATION:

RSA Data Security, Inc.
Jim Bidzos 415/595-8782

Microsoft Corporation
Brenda Hansen 206/936-3865

RSA AND MICROSOFT IN TECHNOLOGY LICENSING PACT

Redwood City, Calif., and Redmond, Washington, (June 3, 1991): RSA Data Security, Inc. and Microsoft Corporation announced today that Microsoft had acquired a license to RSA's technology. The license, to RSA's BSAFE and TIPEM cryptographic toolkit products, gives Microsoft the capability to incorporate advanced security features into its products. Microsoft will also provide key development assistance to RSA for future products RSA may develop. The terms or value of the agreement were not disclosed.

"This relationship with Microsoft, clearly the software leader in the desktop computing market, is further evidence that RSA is a de facto standard in the marketplace," said Jim Bidzos, RSA's president.

"RSA's technology will allow us to incorporate advanced security features in our products and create a secure computing environment for our customers," said Bill Gates, Microsoft Chairman. "In addition to providing for the privacy and authentication of sensitive user data, we can apply RSA's technology to such areas as virus detection and secure software distribution. RSA is undoubtedly the best choice for security in today's networked digital world, and it's a very important part of our future. Now we can provide protected, authenticated information at your fingertips," he said.

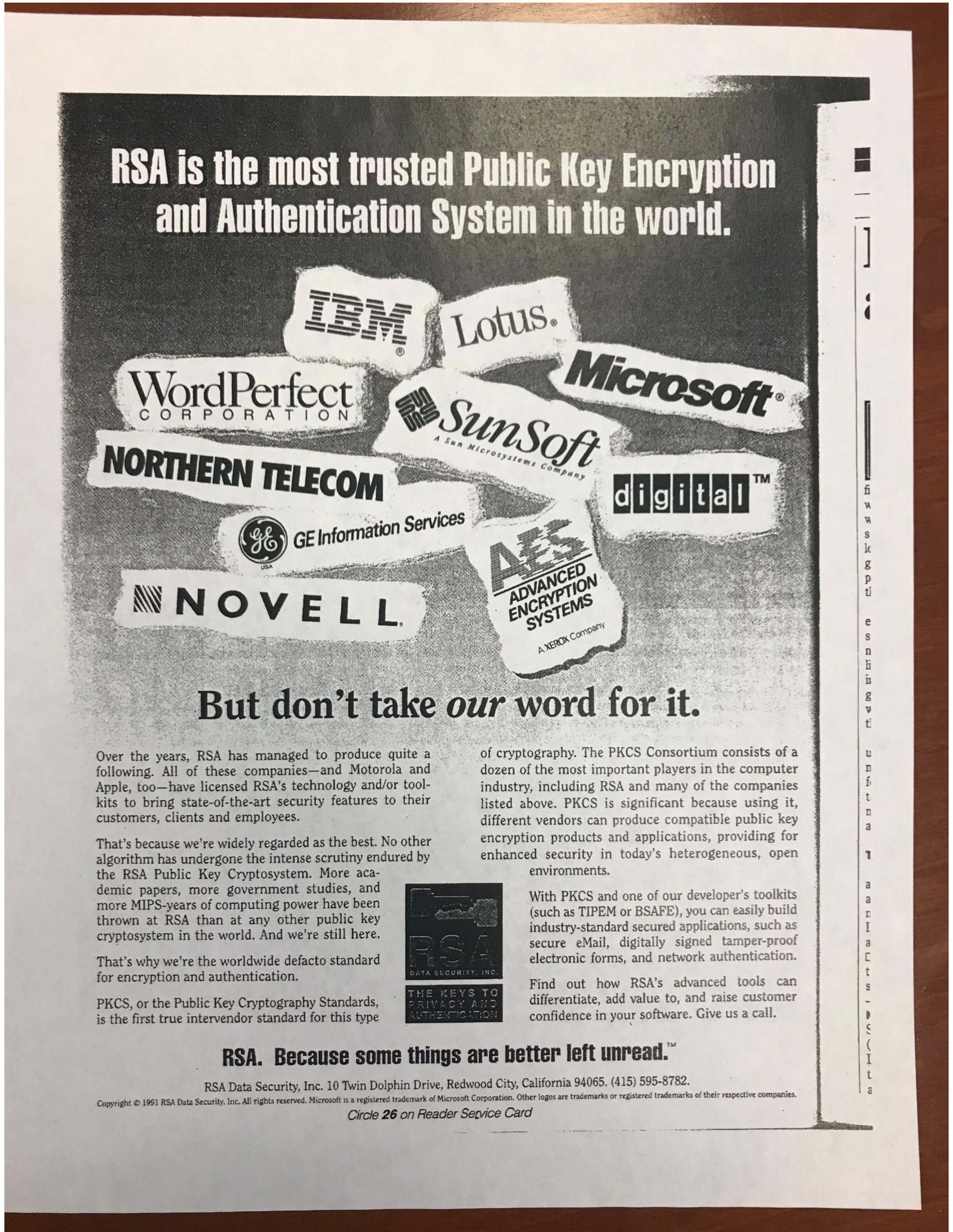
Also announced was Microsoft's participation in and endorsement of RSA's effort to establish interoperability. An effort sponsored by RSA, which includes Novell, Inc., Lotus Development Corporation, and Digital Equipment Corporation, among others, has completed development of an interoperable standard for the use of RSA's technology. "Interoperability between products incorporating RSA, including products from different vendors, is important if users are to realize the true value of this technology," said Mr. Gates. "We are working with RSA and we support its efforts to achieve interoperability, and we encourage other vendors to adopt and support those efforts."

---more---

TEL 415/595-8782
FAX 415/595-1873
THE KEYS TO

"*We are working with RSA, and we support its efforts to achieve interoperability, and we encourage other vendors to adopt and support these efforts*." –Bill Gates, June 1991

The list of RSA customers grows and grows…


IBM
Lotus.
WordPerfect CORPORATION
Microsoft
SunSoft A Sun Microsystems Company
NORTHERN TELECOM
digital™
GE Information Services
NOVELL
AES ADVANCED ENCRYPTION SYSTEMS A XEROX Company
RSA DATA SECURITY, INC.
THE KEYS TO PRIVACY AND AUTHENTICATION

RSA is the most trusted Public Key Encryption and Authentication System in the world.

But don't take *our* word for it.

Over the years, RSA has managed to produce quite a following. All of these companies—and Motorola and Apple, too—have licensed RSA's technology and/or toolkits to bring state-of-the-art security features to their customers, clients and employees.

That's because we're widely regarded as the best. No other algorithm has undergone the intense scrutiny endured by the RSA Public Key Cryptosystem. More academic papers, more government studies, and more MIPS-years of computing power have been thrown at RSA than at any other public key cryptosystem in the world. And we're still here.

That's why we're the worldwide defacto standard for encryption and authentication.

PKCS, or the Public Key Cryptography Standards, is the first true intervendor standard for this type of cryptography. The PKCS Consortium consists of a dozen of the most important players in the computer industry, including RSA and many of the companies listed above. PKCS is significant because using it, different vendors can produce compatible public key encryption products and applications, providing for enhanced security in today's heterogeneous, open environments.

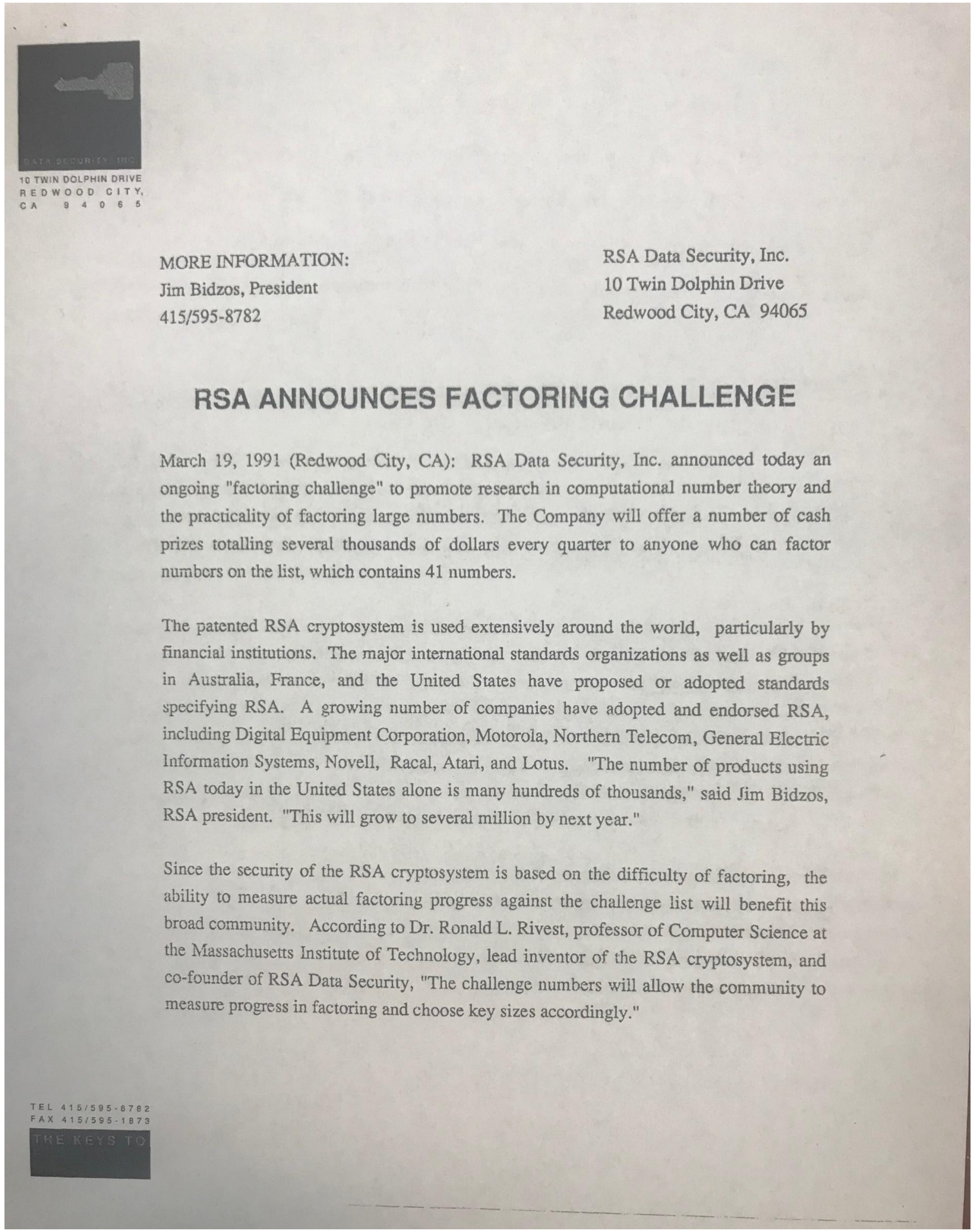
With PKCS and one of our developer's toolkits (such as TIPEM or BSAFE), you can easily build industry-standard secured applications, such as secure eMail, digitally signed tamper-proof electronic forms, and network authentication.

Find out how RSA's advanced tools can differentiate, add value to, and raise customer confidence in your software. Give us a call.

RSA. Because some things are better left unread.™

RSA Data Security, Inc. 10 Twin Dolphin Drive, Redwood City, California 94065. (415) 595-8782.

*Circle **26** on Reader Service Card*



DATA SECURITY, INC.
10 TWIN DOLPHIN DRIVE
REDWOOD CITY,
CA 94065

MORE INFORMATION:
Jim Bidzos, President
415/595-8782

RSA Data Security, Inc.
10 Twin Dolphin Drive
Redwood City, CA 94065

RSA ANNOUNCES FACTORING CHALLENGE

March 19, 1991 (Redwood City, CA): RSA Data Security, Inc. announced today an ongoing "factoring challenge" to promote research in computational number theory and the practicality of factoring large numbers. The Company will offer a number of cash prizes totalling several thousands of dollars every quarter to anyone who can factor numbers on the list, which contains 41 numbers.

The patented RSA cryptosystem is used extensively around the world, particularly by financial institutions. The major international standards organizations as well as groups in Australia, France, and the United States have proposed or adopted standards specifying RSA. A growing number of companies have adopted and endorsed RSA, including Digital Equipment Corporation, Motorola, Northern Telecom, General Electric Information Systems, Novell, Racal, Atari, and Lotus. "The number of products using RSA today in the United States alone is many hundreds of thousands," said Jim Bidzos, RSA president. "This will grow to several million by next year."

Since the security of the RSA cryptosystem is based on the difficulty of factoring, the ability to measure actual factoring progress against the challenge list will benefit this broad community. According to Dr. Ronald L. Rivest, professor of Computer Science at the Massachusetts Institute of Technology, lead inventor of the RSA cryptosystem, and co-founder of RSA Data Security, "The challenge numbers will allow the community to measure progress in factoring and choose key sizes accordingly."

TEL 415/595-8782
FAX 415/595-1873
THE KEYS TO

This was VERY helpful when the 155-decimal digit 9th Fermat number, F9 (2e512+1), was factored in July 1993.

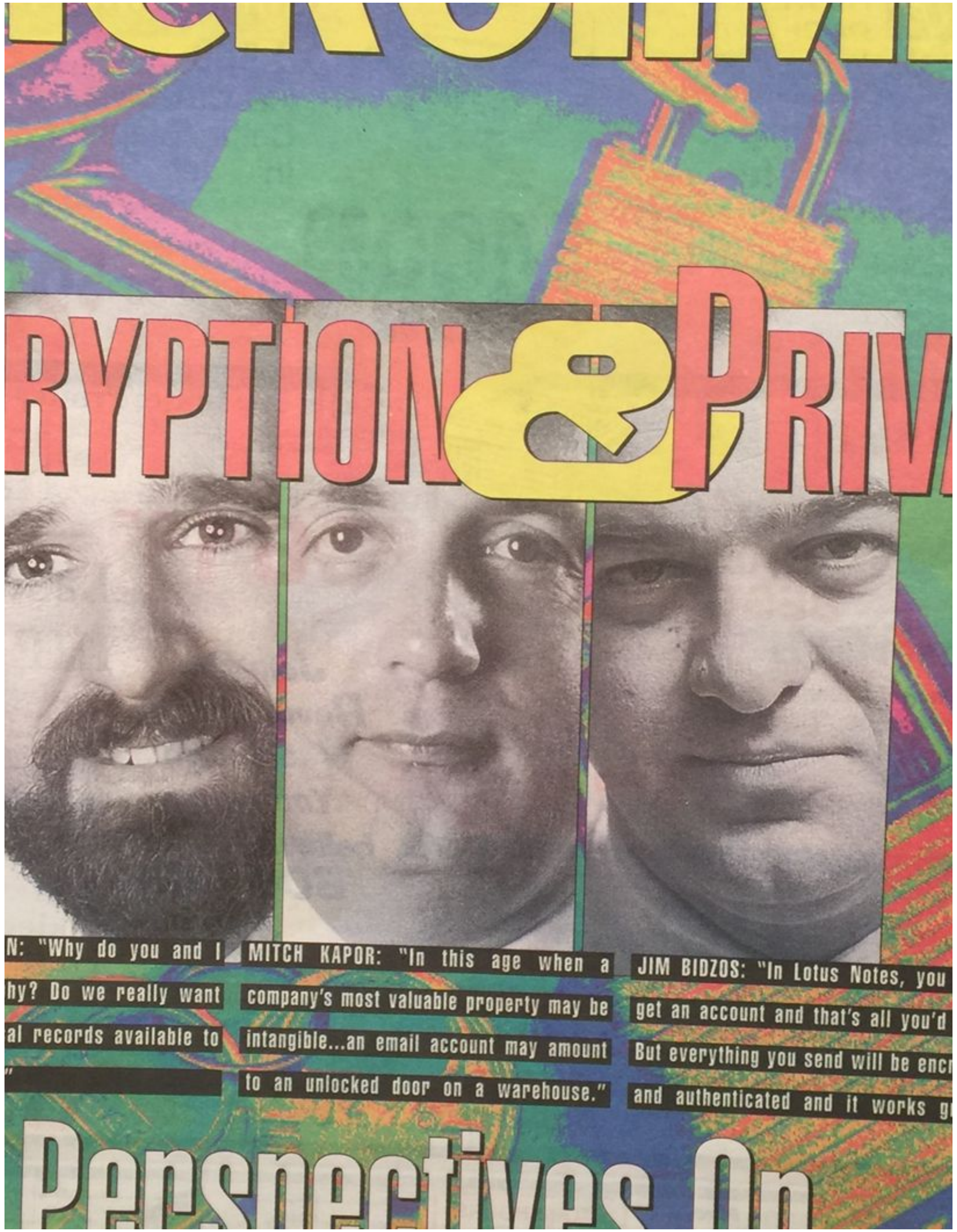
Factor this!

Resistance – 1991-1994

Big wins, bigger challenges. Cause and effect?

1991: RSA signs Microsoft (barely), Apple, Sun Microsystems, and more.
PKCS Consortium formed. RSA Factoring Challenge. S266. DSA plans
announced by NIST, designed by NSA. First RSA Conference.

1992: RSA Laboratories formed. Bernstein and others go to court over export.
Freedom to use crypto becomes a cause célèbre among civil liberties orgs.
MLD arranges meeting between Adm. Bobby Inman, and R and B.



RYPTION & PRIV

N: "Why do you and I hy? Do we really want al records available to "

MITCH KAPOR: "In this age when a company's most valuable property may be intangible...an email account may amount to an unlocked door on a warehouse."

JIM BIDZOS: "In Lotus Notes, you get an account and that's all you'd But everything you send will be encr and authenticated and it works g

Perspectives On

Resistance – 1991-1994

Big wins, bigger challenges. Cause and effect?

1991: RSA signs Microsoft (barely), Apple, Sun Microsystems, and more.
PKCS Consortium formed. RSA Factoring Challenge. S266. DSA plans
announced by NIST, designed by NSA. First RSA Conference.

1992: RSA Laboratories formed. Bernstein and others go to court over export.
Freedom to use crypto becomes a cause célèbre among civil liberties orgs.
MLD arranges meeting between Adm. Bobby Inman, and R and B.

1993: USG fails to acquire Schnorr's DSA patent. During the storm of the century, B
succeeds and immediately flies to NIST. Clipper chip appears.

The following notice was published in the Federal Register, Vol. 58, No. 108, **dated June 8, 1993** under Notices ** National Institute of Standards and Technology Notice of Proposal for Grant of Exclusive Patent License

This is to notify the public that the National Institute of Standards and Technology (NIST) intends to grant an exclusive world-wide license to Public Key Partners of Sunnyvale, California to practice the Invention embodied in U.S. Patent Application No. 07/738.431 and entitled "Digital Signature Algorithm." The rights in the invention have been assigned to the United States of America. The prospective license is a cross-license which would resolve a patent dispute with Public Key Partners and includes the right to sublicense. Notice of availability of this invention for licensing was waived because it was determined that expeditious granting of such license will best serve the interest of the Federal Government and the public.

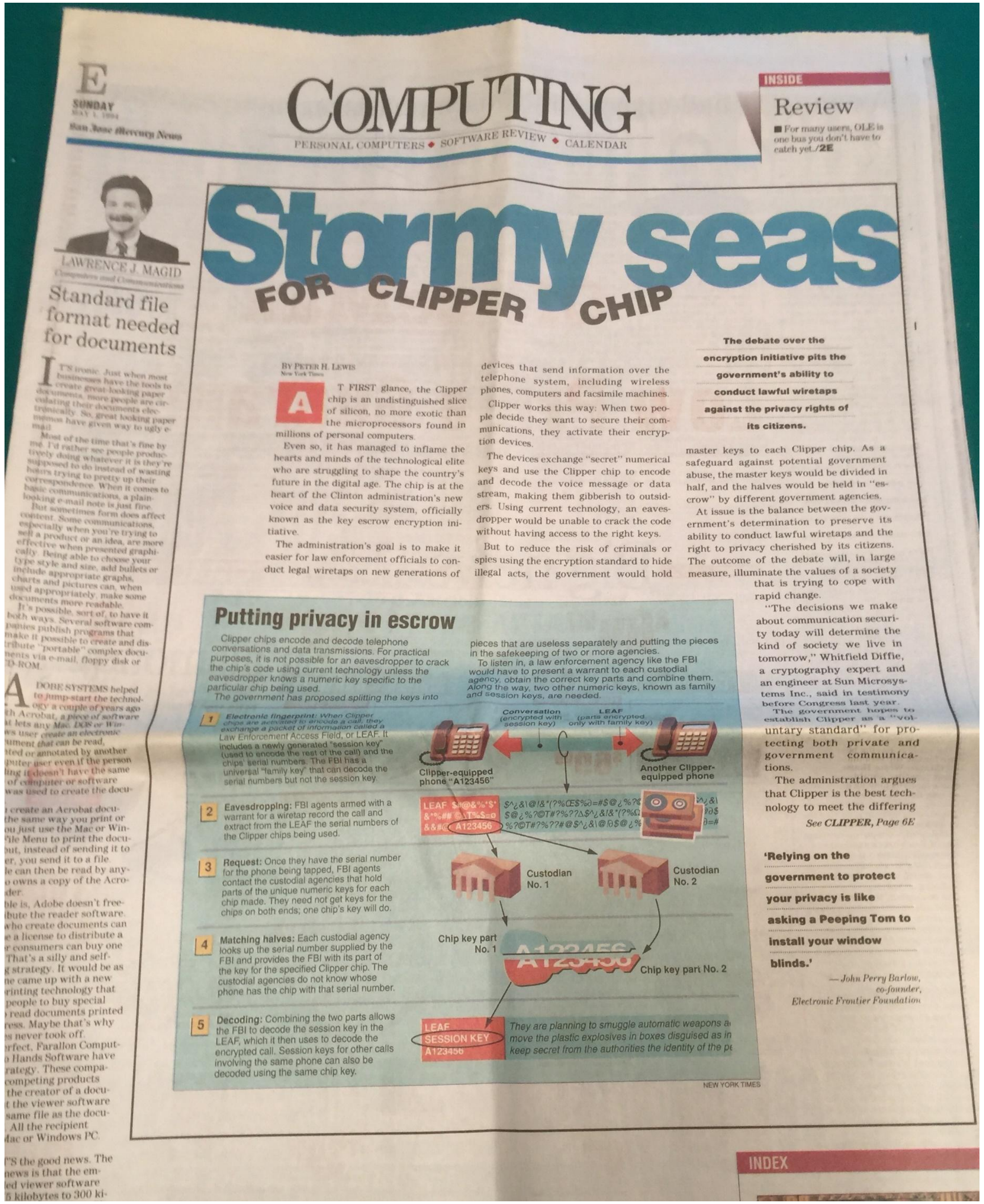
The National Institute for Standards and Technology ("NIST") has announced its intention to grant Public Key Partners ("PKP") sublicensing rights to NIST's pending patent application on the Digital Signature Algorithm ("DSA"). Subject to NIST's grant of this license, PKP is pleased to declare its support for the proposed Federal Information Processing Standard for Digital Signatures (the "DSS") and the pending availability of licenses to practice the DSA. In addition to the DSA, licenses to practice digital signatures will be offered by PKP under the following patents:

Cryptographic Apparatus and Method ("Diffie-Hellman") No. 4,200,770

Public Key Cryptographic Apparatus and Method ("Hellman-Merkle") No. 4,315,552

Exponential Cryptographic Apparatus and Method ("Hellman-Pohlig") No. 4,434,414

Method For Identifying Subscribers And For Generating And Verifying Electronic Signatures In A Data Exchange System ("Schnorr") No. 4,995,082



E
SUNDAY
MAY 1, 1994
San Jose Mercury News

COMPUTING

PERSONAL COMPUTERS ◆ SOFTWARE REVIEW ◆ CALENDAR

INSIDE

Review

■ For many users, OLE is one bus you don't have to catch yet./2E

LAWRENCE J. MAGID
Computers and Communications

Standard file format needed for documents

IT'S ironic. Just when most businesses have the tools to create great-looking paper documents, more people are circulating their documents electronically. So, great looking paper memos have given way to ugly e-mail.

Most of the time that's fine by me. I'd rather see people productively doing whatever it is they're supposed to do instead of wasting hours trying to pretty up their correspondence. When it comes to basic communications, a plain-looking e-mail note is just fine.

But sometimes form does affect content. Some communications, especially when you're trying to sell a product or an idea, are more effective when presented graphically. Being able to choose your type style and size, add bullets or include appropriate graphs, charts and pictures can, when used appropriately, make some documents more readable.

It's possible, sort of, to have it both ways. Several software companies publish programs that make it possible to create and distribute "portable" complex documents via e-mail, floppy disk or CD-ROM.

ADOBE SYSTEMS helped to jump-start the technology a couple of years ago
th Acrobat, a piece of software
at lets any Mac, DOS or Win-
ws user create an electronic
ument that can be read,
ted or annotated by another
puter user even if the person
ling it doesn't have the same
of computer or software
was used to create the docu-

create an Acrobat docu-
the same way you print or
ou just use the Mac or Win-
File Menu to print the docu-
but, instead of sending it to
er, you send it to a file.
le can then be read by any-
o owns a copy of the Acro-
der.
ble is, Adobe doesn't free-
ibute the reader software.
who create documents can
e a license to distribute a
r consumers can buy one
That's a silly and self-
g strategy. It would be as
ne came up with a new
rinting technology that
people to buy special
read documents printed
ress. Maybe that's why
s never took off.
rfect, Farallon Comput-
Hands Software have
rategy. These compa-
competing products
the creator of a docu-
t the viewer software
same file as the docu-
All the recipient
Mac or Windows PC.

'S the good news. The
news is that the em-
ed viewer software
5 kilobytes to 300 ki-

Stormy seas FOR CLIPPER CHIP

BY PETER H. LEWIS
New York Times

AT FIRST glance, the Clipper chip is an undistinguished slice of silicon, no more exotic than the microprocessors found in millions of personal computers.

Even so, it has managed to inflame the hearts and minds of the technological elite who are struggling to shape the country's future in the digital age. The chip is at the heart of the Clinton administration's new voice and data security system, officially known as the key escrow encryption initiative.

The administration's goal is to make it easier for law enforcement officials to conduct legal wiretaps on new generations of devices that send information over the telephone system, including wireless phones, computers and facsimile machines.

Clipper works this way: When two people decide they want to secure their communications, they activate their encryption devices.

The devices exchange "secret" numerical keys and use the Clipper chip to encode and decode the voice message or data stream, making them gibberish to outsiders. Using current technology, an eavesdropper would be unable to crack the code without having access to the right keys.

But to reduce the risk of criminals or spies using the encryption standard to hide illegal acts, the government would hold master keys to each Clipper chip. As a safeguard against potential government abuse, the master keys would be divided in half, and the halves would be held in "escrow" by different government agencies.

The debate over the encryption initiative pits the government's ability to conduct lawful wiretaps against the privacy rights of its citizens.

At issue is the balance between the government's determination to preserve its ability to conduct lawful wiretaps and the right to privacy cherished by its citizens. The outcome of the debate will, in large measure, illuminate the values of a society that is trying to cope with rapid change.

"The decisions we make about communication security today will determine the kind of society we live in tomorrow," Whitfield Diffie, a cryptography expert and an engineer at Sun Microsystems Inc., said in testimony before Congress last year.

The government hopes to establish Clipper as a "voluntary standard" for protecting both private and government communications.

The administration argues that Clipper is the best technology to meet the differing

See CLIPPER, Page 6E

'Relying on the government to protect your privacy is like asking a Peeping Tom to install your window blinds.'

— John Perry Barlow, co-founder, Electronic Frontier Foundation

Putting privacy in escrow

Clipper chips encode and decode telephone conversations and data transmissions. For practical purposes, it is not possible for an eavesdropper to crack the chip's code using current technology unless the eavesdropper knows a numeric key specific to the particular chip being used.

The government has proposed splitting the keys into pieces that are useless separately and putting the pieces in the safekeeping of two or more agencies.

To listen in, a law enforcement agency like the FBI would have to present a warrant to each custodial agency, obtain the correct key parts and combine them. Along the way, two other numeric keys, known as family and session keys, are needed.

1 *Electronic fingerprint:* When Clipper chips are activated to encode a call, they exchange a packet of information called a Law Enforcement Access Field, or LEAF. It includes a newly generated "session key" (used to encode the rest of the call) and the chips' serial numbers. The FBI has a universal "family key" that can decode the serial numbers but not the session key.

2 **Eavesdropping:** FBI agents armed with a warrant for a wiretap record the call and extract from the LEAF the serial numbers of the Clipper chips being used.

3 **Request:** Once they have the serial number for the phone being tapped, FBI agents contact the custodial agencies that hold parts of the unique numeric keys for each chip made. They need not get keys for the chips on both ends; one chip's key will do.

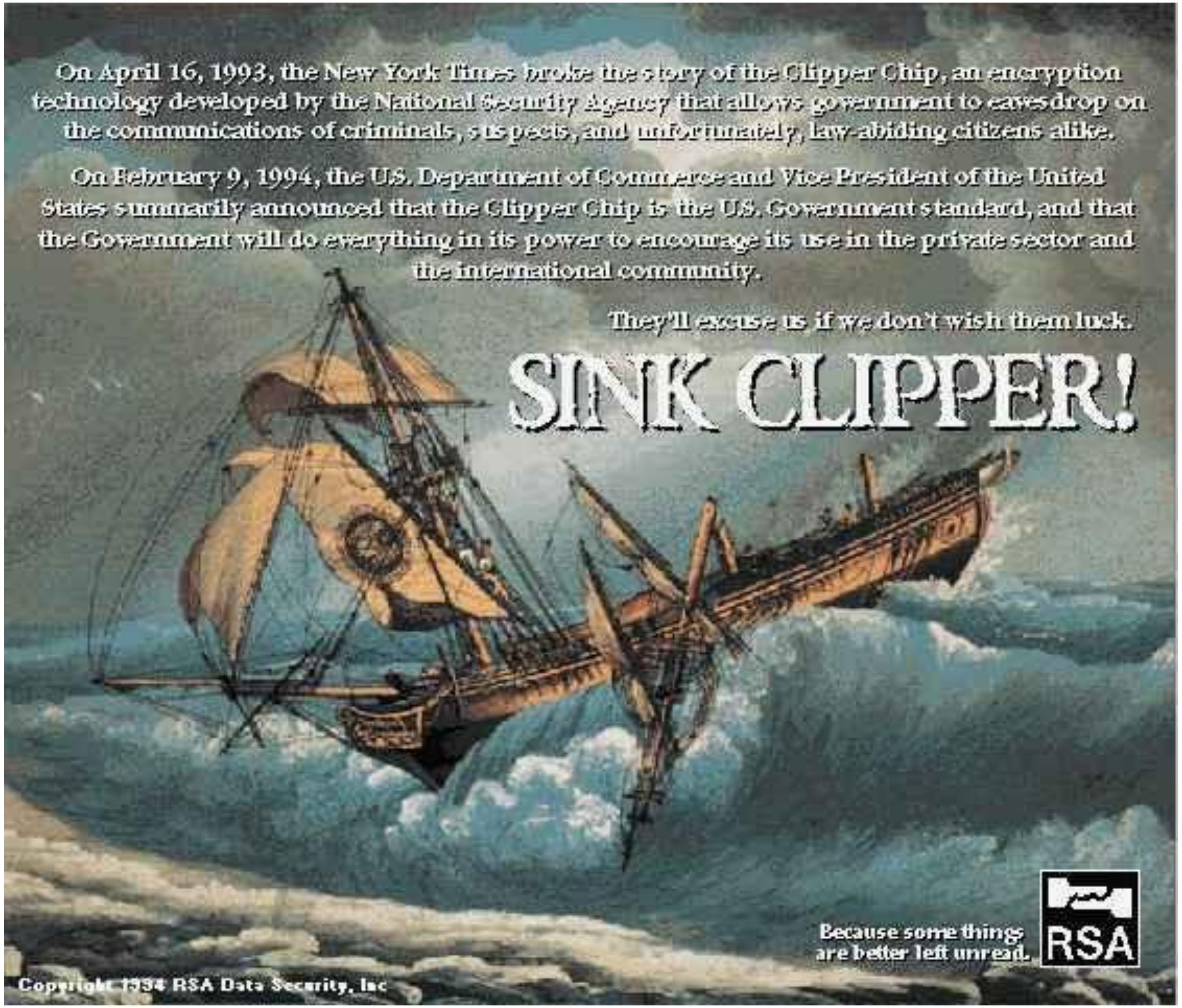
4 **Matching halves:** Each custodial agency looks up the serial number supplied by the FBI and provides the FBI with its part of the key for the specified Clipper chip. The custodial agencies do not know whose phone has the chip with that serial number.

5 **Decoding:** Combining the two parts allows the FBI to decode the session key in the LEAF, which it then uses to decode the encrypted call. Session keys for other calls involving the same phone can also be decoded using the same chip key.

Conversation (encrypted with session key)
LEAF (parts encrypted only with family key)
Clipper-equipped phone "A123456"
Another Clipper-equipped phone
LEAF $#@&%*$* &*%## ©∆T%$=∂ &&#@ A123456
$^¿&\@!&*(?%Œ$%∂=#$@¿%?©
$@¿%?©T#?%??∆$^¿&!&*(?%Ω
%?©T#?%??#@$^¿&\@∂$@¿%
Custodian No. 1
Custodian No. 2
Chip key part No. 1
Chip key part No. 2
A123456
LEAF
SESSION KEY
A123456
They are planning to smuggle automatic weapons a
move the plastic explosives in boxes disguised as in
keep secret from the authorities the identity of the pe

NEW YORK TIMES

INDEX



On April 16, 1993, the New York Times broke the story of the Clipper Chip, an encryption technology developed by the National Security Agency that allows government to eavesdrop on the communications of criminals, suspects, and unfortunately, law-abiding citizens alike.

On February 9, 1994, the U.S. Department of Commerce and Vice President of the United States summarily announced that the Clipper Chip is the U.S. Government standard, and that the Government will do everything in its power to encourage its use in the private sector and the international community.

They'll excuse us if we don't wish them luck.

Resistance – 1991-1994

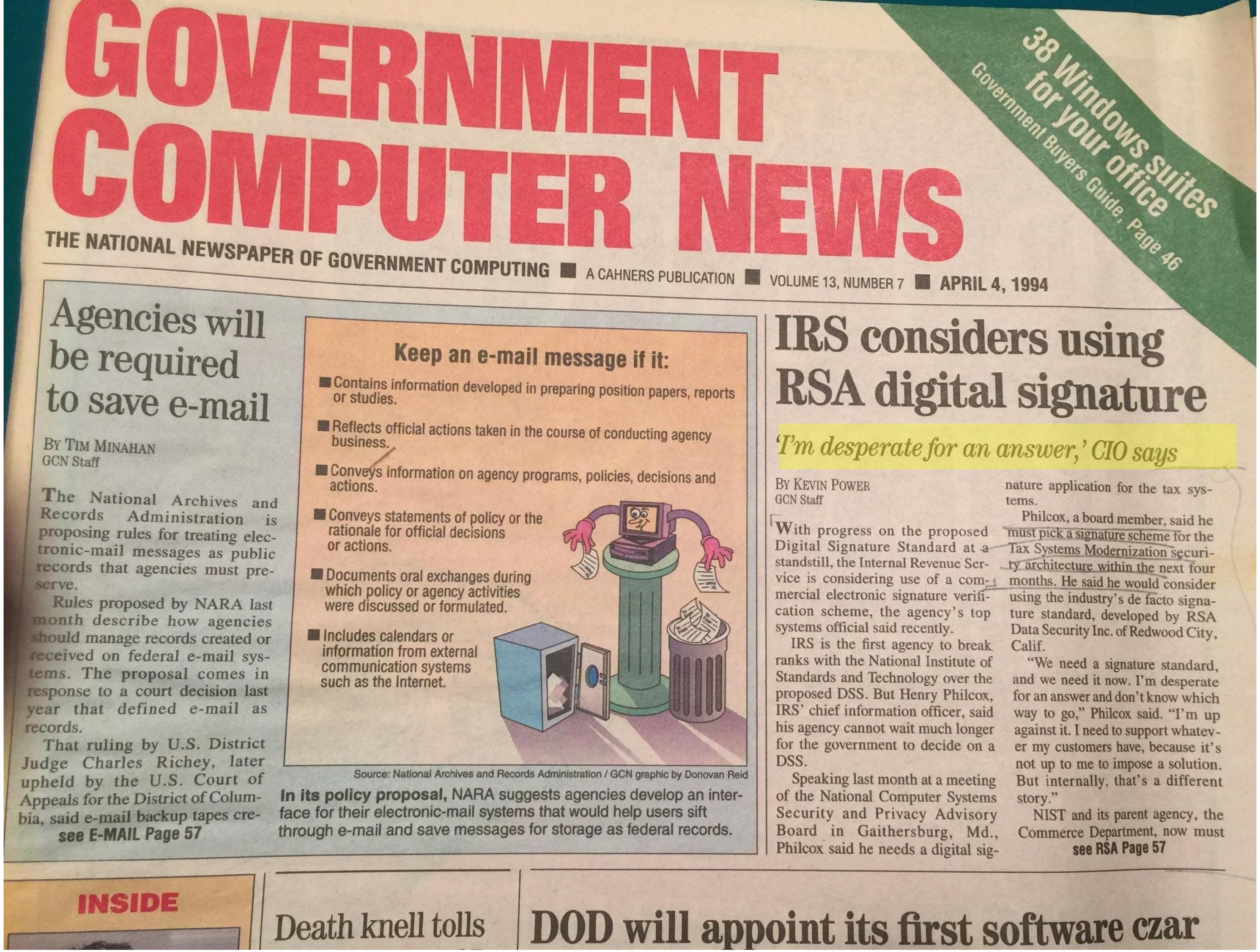
Big wins, bigger challenges. Cause and effect?

1991: RSA signs Microsoft (barely), Apple, Sun Microsystems, and more.
PKCS Consortium formed. RSA Factoring Challenge. S266. DSA plans
announced by NIST, designed by NSA. First RSA Conference.

1992: RSA Laboratories formed. Bernstein and others go to court over export.
Freedom to use crypto becomes a cause célèbre among civil liberties orgs.
MLD arranges meeting between Adm. Bobby Inman, and R and B.

1993: USG fails to acquire Schnorr's DSA patent. During the storm of the century, B
succeeds and immediately flies to NIST. Clipper chip appears.

1994: B butts heads over crypto with Jobs at NeXT.
Pressure mounts for recognition of RSA as a standard. NSA continues to
resist. We sign historic new licensee – No Name? Mosaic? Netscape!



GOVERNMENT COMPUTER NEWS

THE NATIONAL NEWSPAPER OF GOVERNMENT COMPUTING ■ A CAHNERS PUBLICATION ■ VOLUME 13, NUMBER 7 ■ APRIL 4, 1994

38 Windows suites for your office
Government Buyers Guide, Page 46

Agencies will be required to save e-mail

BY TIM MINAHAN
GCN Staff

The National Archives and Records Administration is proposing rules for treating electronic-mail messages as public records that agencies must preserve.

Rules proposed by NARA last month describe how agencies should manage records created or received on federal e-mail systems. The proposal comes in response to a court decision last year that defined e-mail as records.

That ruling by U.S. District Judge Charles Richey, later upheld by the U.S. Court of Appeals for the District of Columbia, said e-mail backup tapes cre-

see E-MAIL Page 57

Keep an e-mail message if it:

- Contains information developed in preparing position papers, reports or studies.
- Reflects official actions taken in the course of conducting agency business.
- Conveys information on agency programs, policies, decisions and actions.
- Conveys statements of policy or the rationale for official decisions or actions.
- Documents oral exchanges during which policy or agency activities were discussed or formulated.
- Includes calendars or information from external communication systems such as the Internet.

Source: National Archives and Records Administration / GCN graphic by Donovan Reid

In its policy proposal, NARA suggests agencies develop an interface for their electronic-mail systems that would help users sift through e-mail and save messages for storage as federal records.

IRS considers using RSA digital signature

'I'm desperate for an answer,' CIO says

BY KEVIN POWER
GCN Staff

With progress on the proposed Digital Signature Standard at a standstill, the Internal Revenue Service is considering use of a commercial electronic signature verification scheme, the agency's top systems official said recently.

IRS is the first agency to break ranks with the National Institute of Standards and Technology over the proposed DSS. But Henry Philcox, IRS' chief information officer, said his agency cannot wait much longer for the government to decide on a DSS.

Speaking last month at a meeting of the National Computer Systems Security and Privacy Advisory Board in Gaithersburg, Md., Philcox said he needs a digital signature application for the tax systems.

Philcox, a board member, said he must pick a signature scheme for the Tax Systems Modernization security architecture within the next four months. He said he would consider using the industry's de facto signature standard, developed by RSA Data Security Inc. of Redwood City, Calif.

"We need a signature standard, and we need it now. I'm desperate for an answer and don't know which way to go," Philcox said. "I'm up against it. I need to support whatever my customers have, because it's not up to me to impose a solution. But internally, that's a different story."

NIST and its parent agency, the Commerce Department, now must

see RSA Page 57

INSIDE

Death knell tolls

DOD will appoint its first software czar

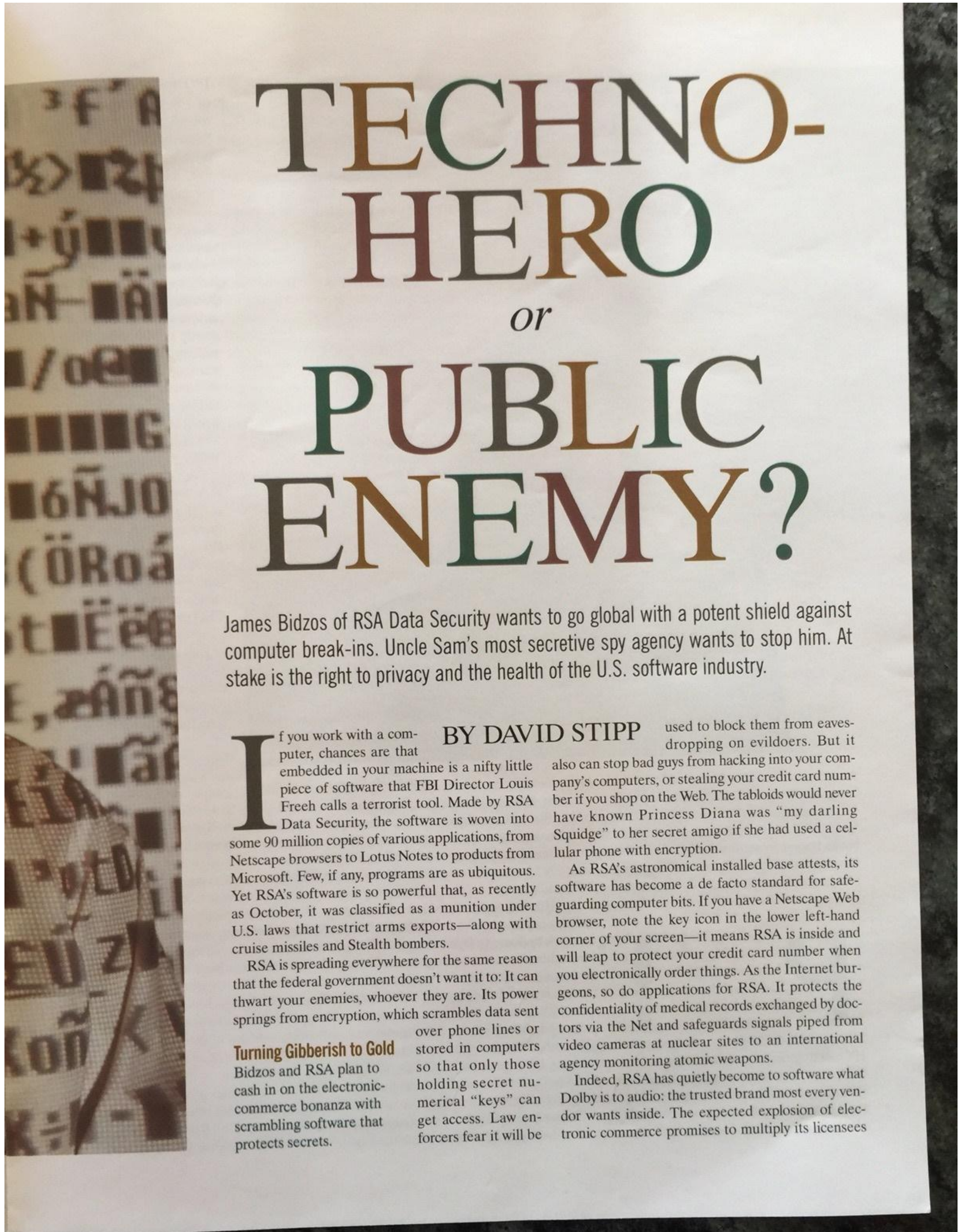
Unstoppable Growth, 1995-2000

The WWW explodes; a new company is created (and one is dissolved); allies help secure a major policy win.

Unstoppable Growth, 1995-2000

The WWW explodes; a new company is created (and one is dissolved); allies help secure a major policy win.

1995: The Internet becomes the WWW with 100MM browsers in use as Microsoft follows with IE.
Verisign formed to be independent CA;
The FBI gets more directly involved in the encryption debate.



TECHNO-HERO *or* PUBLIC ENEMY?

James Bidzos of RSA Data Security wants to go global with a potent shield against computer break-ins. Uncle Sam's most secretive spy agency wants to stop him. At stake is the right to privacy and the health of the U.S. software industry.

BY DAVID STIPP

If you work with a computer, chances are that embedded in your machine is a nifty little piece of software that FBI Director Louis Freeh calls a terrorist tool. Made by RSA Data Security, the software is woven into some 90 million copies of various applications, from Netscape browsers to Lotus Notes to products from Microsoft. Few, if any, programs are as ubiquitous. Yet RSA's software is so powerful that, as recently as October, it was classified as a munition under U.S. laws that restrict arms exports—along with cruise missiles and Stealth bombers.

RSA is spreading everywhere for the same reason that the federal government doesn't want it to: It can thwart your enemies, whoever they are. Its power springs from encryption, which scrambles data sent over phone lines or stored in computers so that only those holding secret numerical "keys" can get access. Law enforcers fear it will be used to block them from eavesdropping on evildoers. But it also can stop bad guys from hacking into your company's computers, or stealing your credit card number if you shop on the Web. The tabloids would never have known Princess Diana was "my darling Squidge" to her secret amigo if she had used a cellular phone with encryption.

As RSA's astronomical installed base attests, its software has become a de facto standard for safeguarding computer bits. If you have a Netscape Web browser, note the key icon in the lower left-hand corner of your screen—it means RSA is inside and will leap to protect your credit card number when you electronically order things. As the Internet burgeons, so do applications for RSA. It protects the confidentiality of medical records exchanged by doctors via the Net and safeguards signals piped from video cameras at nuclear sites to an international agency monitoring atomic weapons.

Indeed, RSA has quietly become to software what Dolby is to audio: the trusted brand most every vendor wants inside. The expected explosion of electronic commerce promises to multiply its licensees

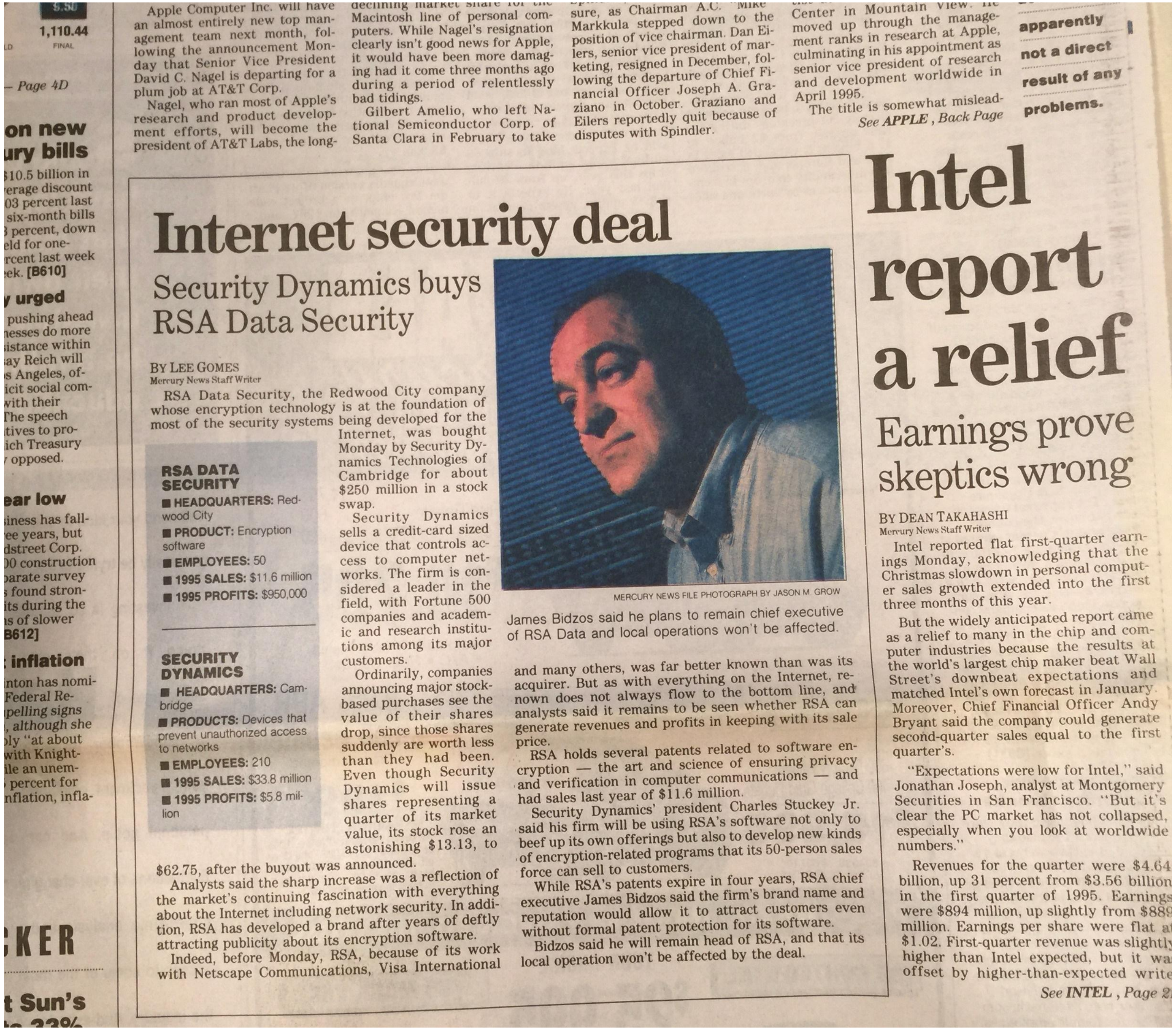
Turning Gibberish to Gold
Bidzos and RSA plan to cash in on the electronic-commerce bonanza with scrambling software that protects secrets.

James Bidzos of RSA Data Security wants to go global with a potent shield against computer break-ins. Uncle Sam's most secretive spy agency wants to stop him. At stake is the right to privacy and the health of the U.S. software industry

Unstoppable Growth, 1995-2000

The WWW explodes; a new company is created (and one is dissolved); allies help secure a major policy win.

1995: The Internet becomes the WWW with 100MM browsers in use as Microsoft follows with IE.
Verisign formed to be independent CA; PKP dissolved after lengthy arbitration.
1996: RSA merges with SDI, becomes a public company. SAFE Act attempted ambush.
RSA Day in Washington. B settles some old family business.
NIST point person for crypto standards (Lynn McNulty) and NSA Deputy
Director for InfoSec (Ed Hart) both join RSA/Verisign. As do many others.



$.50

1,110.44

LD FINAL

– Page 4D

on new
ury bills

$10.5 billion in
erage discount
03 percent last
six-month bills
3 percent, down
eld for one-
rcent last week
ek. **[B610]**

y urged

pushing ahead
nesses do more
sistance within
ay Reich will
s Angeles, of-
icit social com-
with their
The speech
tives to pro-
ich Treasury
y opposed.

ear low

siness has fall-
ee years, but
dstreet Corp.
00 construction
parate survey
s found stron-
its during the
ns of slower
B612]

inflation

nton has nomi-
Federal Re-
pelling signs
, although she
ply "at about
with Knight-
ile an unem-
percent for
nflation, infla-

CKER

t Sun's

Apple Computer Inc. will have an almost entirely new top management team next month, following the announcement Monday that Senior Vice President David C. Nagel is departing for a plum job at AT&T Corp.

Nagel, who ran most of Apple's research and product development efforts, will become the president of AT&T Labs, the long-

declining market share for the Macintosh line of personal computers. While Nagel's resignation clearly isn't good news for Apple, it would have been more damaging had it come three months ago during a period of relentlessly bad tidings.

Gilbert Amelio, who left National Semiconductor Corp. of Santa Clara in February to take

sure, as Chairman A.C. "Mike" Markkula stepped down to the position of vice chairman. Dan Eilers, senior vice president of marketing, resigned in December, following the departure of Chief Financial Officer Joseph A. Graziano in October. Graziano and Eilers reportedly quit because of disputes with Spindler.

Center in Mountain View. He moved up through the management ranks in research at Apple, culminating in his appointment as senior vice president of research and development worldwide in April 1995.

The title is somewhat mislead-

See ***APPLE*** *, Back Page*

apparently
not a direct
result of any
problems.

Internet security deal

Security Dynamics buys RSA Data Security

BY LEE GOMES
Mercury News Staff Writer

RSA Data Security, the Redwood City company whose encryption technology is at the foundation of most of the security systems being developed for the Internet, was bought Monday by Security Dynamics Technologies of Cambridge for about $250 million in a stock swap.

Security Dynamics sells a credit-card sized device that controls access to computer networks. The firm is considered a leader in the field, with Fortune 500 companies and academic and research institutions among its major customers.

Ordinarily, companies announcing major stock-based purchases see the value of their shares drop, since those shares suddenly are worth less than they had been. Even though Security Dynamics will issue shares representing a quarter of its market value, its stock rose an astonishing $13.13, to $62.75, after the buyout was announced.

Analysts said the sharp increase was a reflection of the market's continuing fascination with everything about the Internet including network security. In addition, RSA has developed a brand after years of deftly attracting publicity about its encryption software.

Indeed, before Monday, RSA, because of its work with Netscape Communications, Visa International and many others, was far better known than was its acquirer. But as with everything on the Internet, renown does not always flow to the bottom line, and analysts said it remains to be seen whether RSA can generate revenues and profits in keeping with its sale price.

RSA holds several patents related to software encryption — the art and science of ensuring privacy and verification in computer communications — and had sales last year of $11.6 million.

Security Dynamics' president Charles Stuckey Jr. said his firm will be using RSA's software not only to beef up its own offerings but also to develop new kinds of encryption-related programs that its 50-person sales force can sell to customers.

While RSA's patents expire in four years, RSA chief executive James Bidzos said the firm's brand name and reputation would allow it to attract customers even without formal patent protection for its software.

Bidzos said he will remain head of RSA, and that its local operation won't be affected by the deal.

RSA DATA SECURITY

- **HEADQUARTERS:** Redwood City
- **PRODUCT:** Encryption software
- **EMPLOYEES:** 50
- **1995 SALES:** $11.6 million
- **1995 PROFITS:** $950,000

SECURITY DYNAMICS

- **HEADQUARTERS:** Cambridge
- **PRODUCTS:** Devices that prevent unauthorized access to networks
- **EMPLOYEES:** 210
- **1995 SALES:** $33.8 million
- **1995 PROFITS:** $5.8 million

MERCURY NEWS FILE PHOTOGRAPH BY JASON M. GROW

James Bidzos said he plans to remain chief executive of RSA Data and local operations won't be affected.

Intel report a relief

Earnings prove skeptics wrong

BY DEAN TAKAHASHI
Mercury News Staff Writer

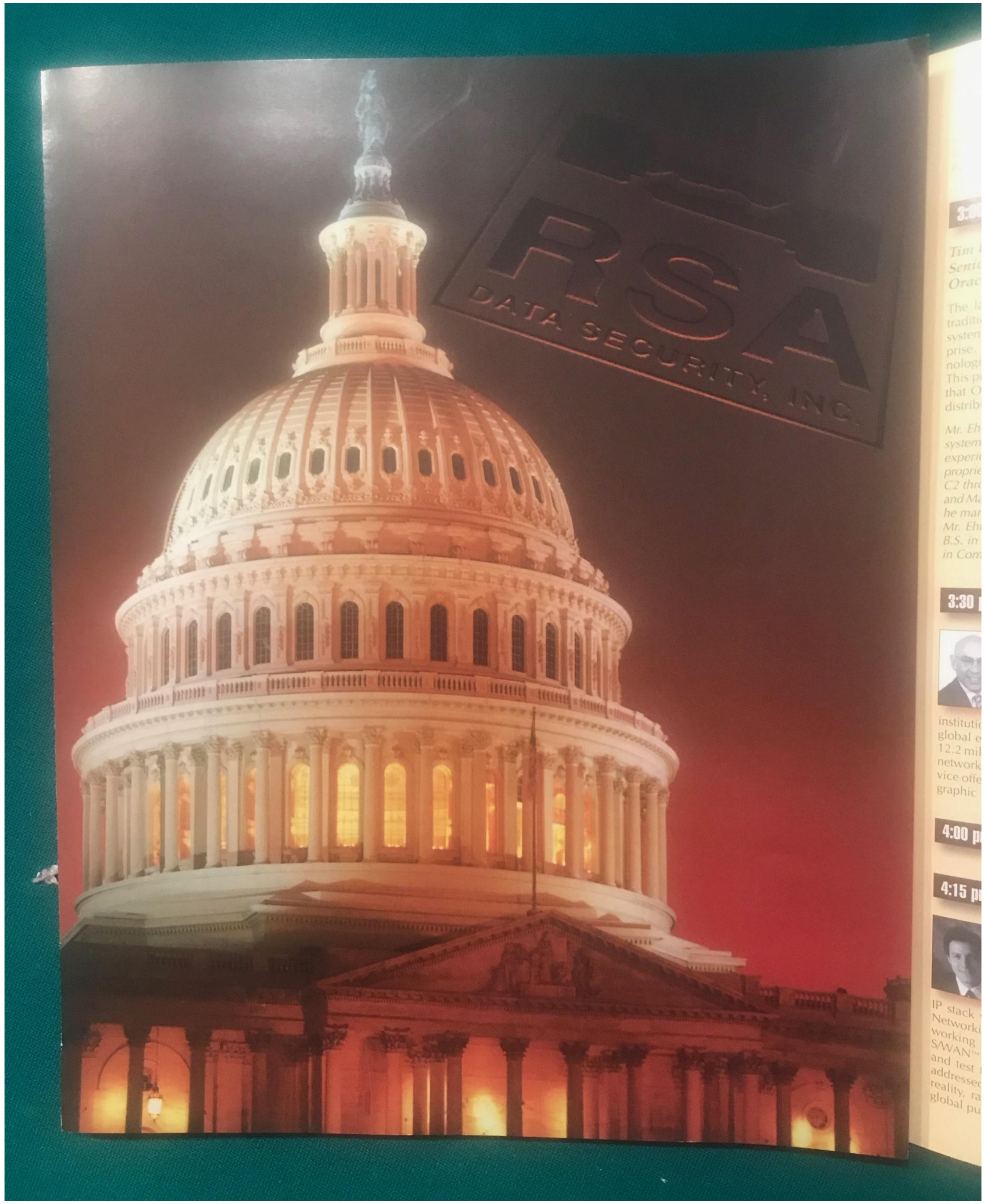
Intel reported flat first-quarter earnings Monday, acknowledging that the Christmas slowdown in personal computer sales growth extended into the first three months of this year.

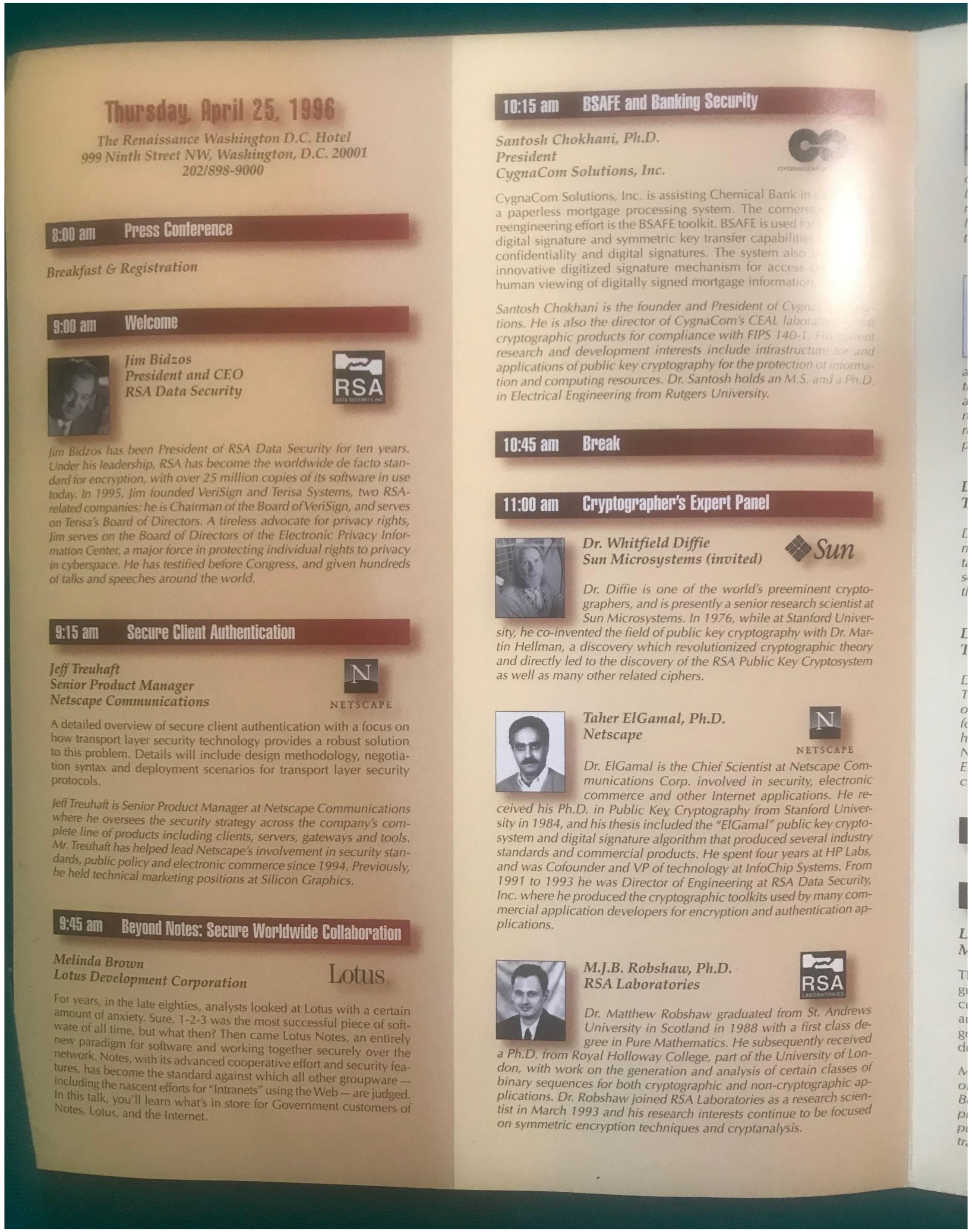
But the widely anticipated report came as a relief to many in the chip and computer industries because the results at the world's largest chip maker beat Wall Street's downbeat expectations and matched Intel's own forecast in January. Moreover, Chief Financial Officer Andy Bryant said the company could generate second-quarter sales equal to the first quarter's.

"Expectations were low for Intel," said Jonathan Joseph, analyst at Montgomery Securities in San Francisco. "But it's clear the PC market has not collapsed, especially when you look at worldwide numbers."

Revenues for the quarter were $4.64 billion, up 31 percent from $3.56 billion in the first quarter of 1995. Earnings were $894 million, up slightly from $889 million. Earnings per share were flat at $1.02. First-quarter revenue was slightly higher than Intel expected, but it was offset by higher-than-expected write

See ***INTEL*** *, Page 2*


RSA
DATA SECURITY, INC.
3:00
3:30 p
4:00 p
4:15 p



Thursday, April 25, 1996

The Renaissance Washington D.C. Hotel
999 Ninth Street NW, Washington, D.C. 20001
202/898-9000

8:00 am Press Conference

Breakfast & Registration

9:00 am Welcome

Jim Bidzos
President and CEO
RSA Data Security

Jim Bidzos has been President of RSA Data Security for ten years. Under his leadership, RSA has become the worldwide de facto standard for encryption, with over 25 million copies of its software in use today. In 1995, Jim founded VeriSign and Terisa Systems, two RSA-related companies; he is Chairman of the Board of VeriSign, and serves on Terisa's Board of Directors. A tireless advocate for privacy rights, Jim serves on the Board of Directors of the Electronic Privacy Information Center, a major force in protecting individual rights to privacy in cyberspace. He has testified before Congress, and given hundreds of talks and speeches around the world.

9:15 am Secure Client Authentication

Jeff Treuhaft
Senior Product Manager
Netscape Communications

A detailed overview of secure client authentication with a focus on how transport layer security technology provides a robust solution to this problem. Details will include design methodology, negotiation syntax and deployment scenarios for transport layer security protocols.

Jeff Treuhaft is Senior Product Manager at Netscape Communications where he oversees the security strategy across the company's complete line of products including clients, servers, gateways and tools. Mr. Treuhaft has helped lead Netscape's involvement in security standards, public policy and electronic commerce since 1994. Previously, he held technical marketing positions at Silicon Graphics.

9:45 am Beyond Notes: Secure Worldwide Collaboration

Melinda Brown
Lotus Development Corporation

For years, in the late eighties, analysts looked at Lotus with a certain amount of anxiety. Sure, 1-2-3 was the most successful piece of software of all time, but what then? Then came Lotus Notes, an entirely new paradigm for software and working together securely over the network. Notes, with its advanced cooperative effort and security features, has become the standard against which all other groupware — including the nascent efforts for "Intranets" using the Web — are judged. In this talk, you'll learn what's in store for Government customers of Notes, Lotus, and the Internet.

10:15 am BSAFE and Banking Security

Santosh Chokhani, Ph.D.
President
CygnaCom Solutions, Inc.

CygnaCom Solutions, Inc. is assisting Chemical Bank in [illegible] a paperless mortgage processing system. The [illegible] reengineering effort is the BSAFE toolkit. BSAFE is used [illegible] digital signature and symmetric key transfer capabilities [illegible] confidentiality and digital signatures. The system also [illegible] innovative digitized signature mechanism for access [illegible] human viewing of digitally signed mortgage information [illegible]

Santosh Chokhani is the founder and President of [illegible] tions. He is also the director of CygnaCom's CEAL laboratory to test cryptographic products for compliance with FIPS 140-1. His current research and development interests include infrastructure for and applications of public key cryptography for the protection of information and computing resources. Dr. Santosh holds an M.S. and a Ph.D. in Electrical Engineering from Rutgers University.

10:45 am Break

11:00 am Cryptographer's Expert Panel

Dr. Whitfield Diffie
Sun Microsystems (invited)

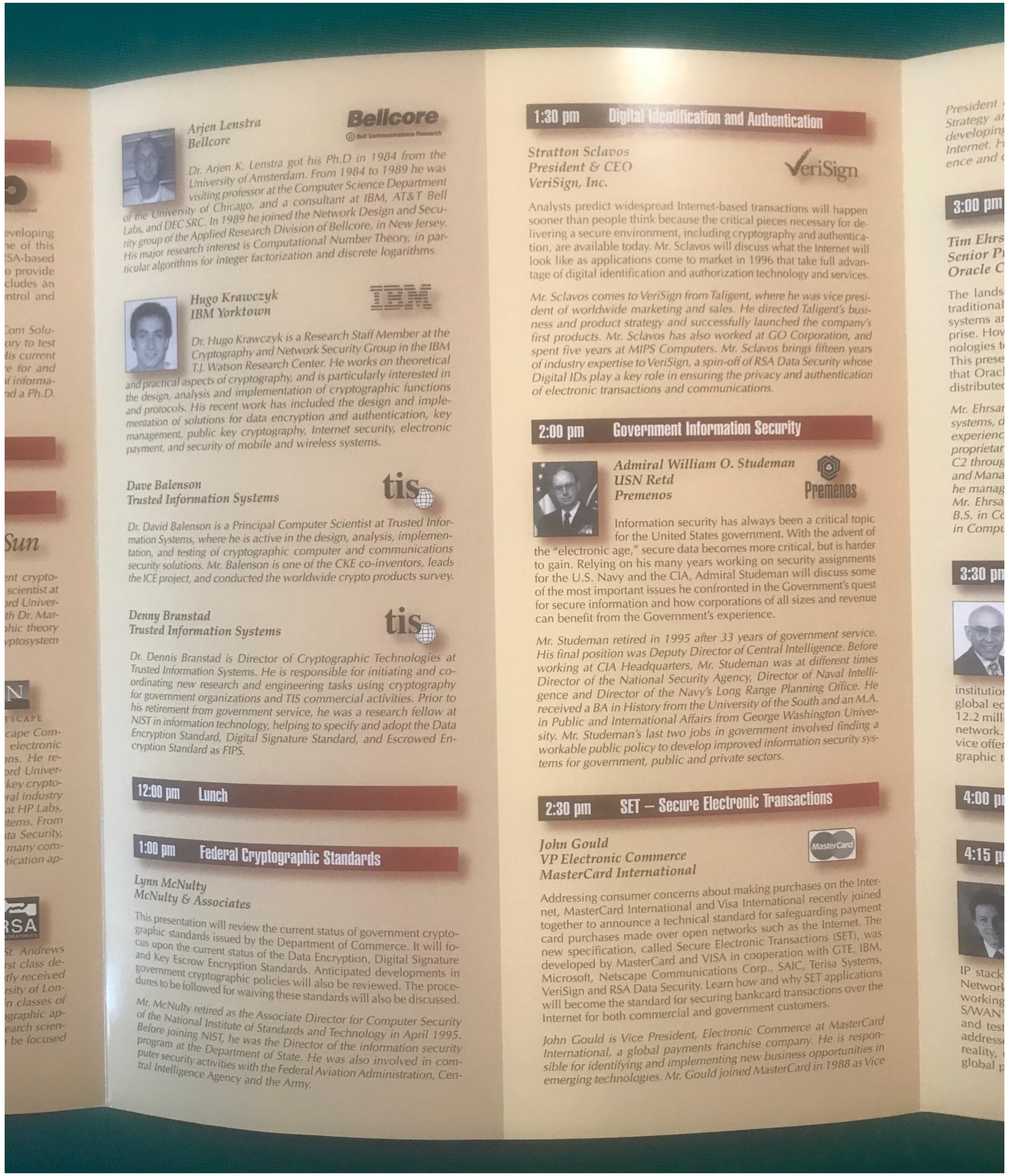
Dr. Diffie is one of the world's preeminent cryptographers, and is presently a senior research scientist at Sun Microsystems. In 1976, while at Stanford University, he co-invented the field of public key cryptography with Dr. Martin Hellman, a discovery which revolutionized cryptographic theory and directly led to the discovery of the RSA Public Key Cryptosystem as well as many other related ciphers.

Taher ElGamal, Ph.D.
Netscape

Dr. ElGamal is the Chief Scientist at Netscape Communications Corp. involved in security, electronic commerce and other Internet applications. He received his Ph.D. in Public Key Cryptography from Stanford University in 1984, and his thesis included the "ElGamal" public key cryptosystem and digital signature algorithm that produced several industry standards and commercial products. He spent four years at HP Labs, and was Cofounder and VP of technology at InfoChip Systems. From 1991 to 1993 he was Director of Engineering at RSA Data Security, Inc. where he produced the cryptographic toolkits used by many commercial application developers for encryption and authentication applications.

M.J.B. Robshaw, Ph.D.
RSA Laboratories

Dr. Matthew Robshaw graduated from St. Andrews University in Scotland in 1988 with a first class degree in Pure Mathematics. He subsequently received a Ph.D. from Royal Holloway College, part of the University of London, with work on the generation and analysis of certain classes of binary sequences for both cryptographic and non-cryptographic applications. Dr. Robshaw joined RSA Laboratories as a research scientist in March 1993 and his research interests continue to be focused on symmetric encryption techniques and cryptanalysis.



Arjen Lenstra
Bellcore

Dr. Arjen K. Lenstra got his Ph.D in 1984 from the University of Amsterdam. From 1984 to 1989 he was visiting professor at the Computer Science Department of the University of Chicago, and a consultant at IBM, AT&T Bell Labs, and DEC SRC. In 1989 he joined the Network Design and Security group of the Applied Research Division of Bellcore, in New Jersey. His major research interest is Computational Number Theory, in particular algorithms for integer factorization and discrete logarithms.

Hugo Krawczyk
IBM Yorktown

Dr. Hugo Krawczyk is a Research Staff Member at the Cryptography and Network Security Group in the IBM T.J. Watson Research Center. He works on theoretical and practical aspects of cryptography, and is particularly interested in the design, analysis and implementation of cryptographic functions and protocols. His recent work has included the design and implementation of solutions for data encryption and authentication, key management, public key cryptography, Internet security, electronic payment, and security of mobile and wireless systems.

Dave Balenson
Trusted Information Systems

Dr. David Balenson is a Principal Computer Scientist at Trusted Information Systems, where he is active in the design, analysis, implementation, and testing of cryptographic computer and communications security solutions. Mr. Balenson is one of the CKE co-inventors, leads the ICE project, and conducted the worldwide crypto products survey.

Denny Branstad
Trusted Information Systems

Dr. Dennis Branstad is Director of Cryptographic Technologies at Trusted Information Systems. He is responsible for initiating and coordinating new research and engineering tasks using cryptography for government organizations and TIS commercial activities. Prior to his retirement from government service, he was a research fellow at NIST in information technology, helping to specify and adopt the Data Encryption Standard, Digital Signature Standard, and Escrowed Encryption Standard as FIPS.

12:00 pm Lunch

1:00 pm Federal Cryptographic Standards

Lynn McNulty
McNulty & Associates

This presentation will review the current status of government cryptographic standards issued by the Department of Commerce. It will focus upon the current status of the Data Encryption, Digital Signature and Key Escrow Encryption Standards. Anticipated developments in government cryptographic policies will also be reviewed. The procedures to be followed for waiving these standards will also be discussed.

Mr. McNulty retired as the Associate Director for Computer Security of the National Institute of Standards and Technology in April 1995. Before joining NIST, he was the Director of the information security program at the Department of State. He was also involved in computer security activities with the Federal Aviation Administration, Central Intelligence Agency and the Army.

1:30 pm Digital Identification and Authentication

Stratton Sclavos
President & CEO
VeriSign, Inc.

Analysts predict widespread Internet-based transactions will happen sooner than people think because the critical pieces necessary for delivering a secure environment, including cryptography and authentication, are available today. Mr. Sclavos will discuss what the Internet will look like as applications come to market in 1996 that take full advantage of digital identification and authorization technology and services.

Mr. Sclavos comes to VeriSign from Taligent, where he was vice president of worldwide marketing and sales. He directed Taligent's business and product strategy and successfully launched the company's first products. Mr. Sclavos has also worked at GO Corporation, and spent five years at MIPS Computers. Mr. Sclavos brings fifteen years of industry expertise to VeriSign, a spin-off of RSA Data Security whose Digital IDs play a key role in ensuring the privacy and authentication of electronic transactions and communications.

2:00 pm Government Information Security

Admiral William O. Studeman
USN Retd
Premenos

Information security has always been a critical topic for the United States government. With the advent of the "electronic age," secure data becomes more critical, but is harder to gain. Relying on his many years working on security assignments for the U.S. Navy and the CIA, Admiral Studeman will discuss some of the most important issues he confronted in the Government's quest for secure information and how corporations of all sizes and revenue can benefit from the Government's experience.

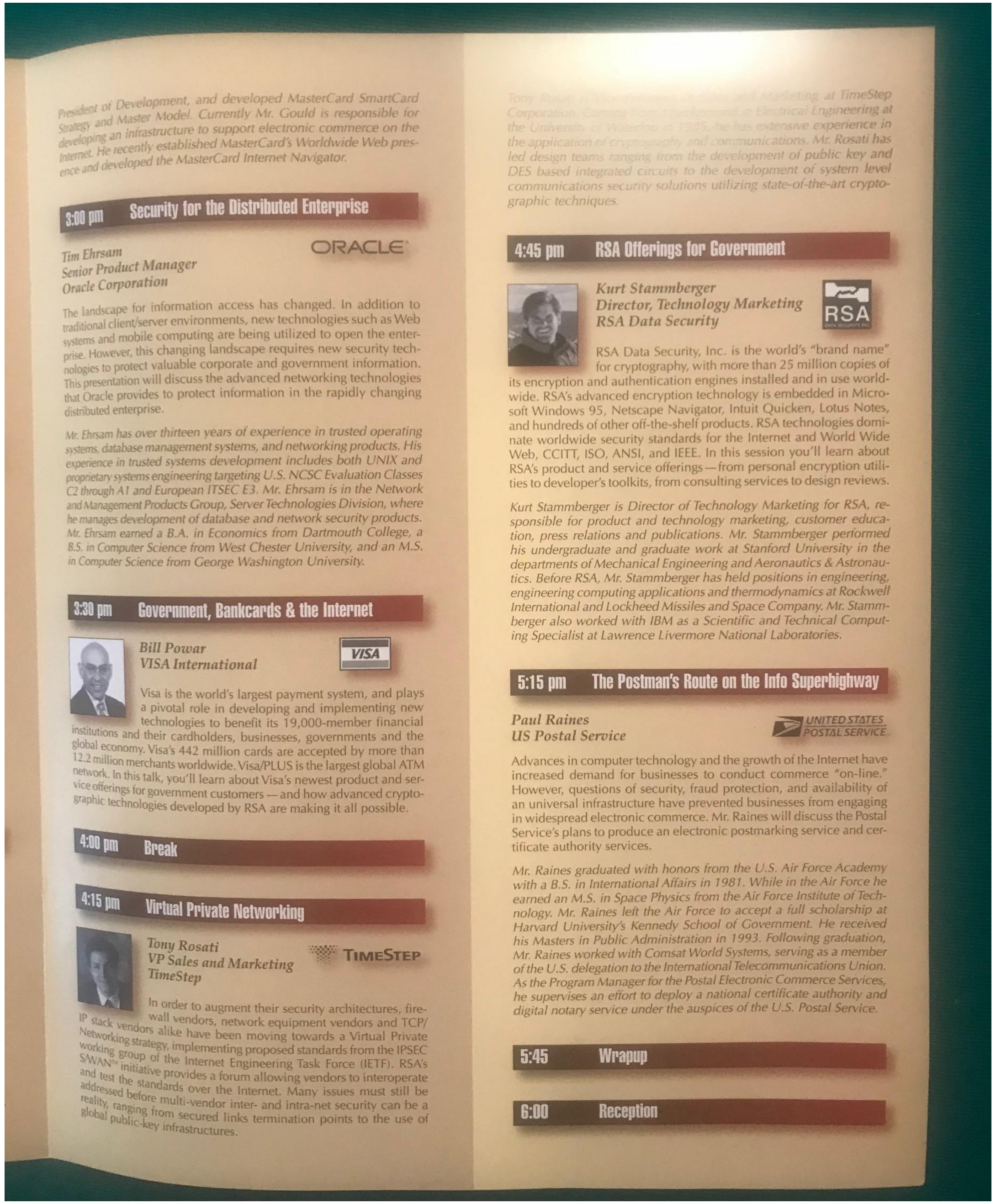
Mr. Studeman retired in 1995 after 33 years of government service. His final position was Deputy Director of Central Intelligence. Before working at CIA Headquarters, Mr. Studeman was at different times Director of the National Security Agency, Director of Naval Intelligence and Director of the Navy's Long Range Planning Office. He received a BA in History from the University of the South and an M.A. in Public and International Affairs from George Washington University. Mr. Studeman's last two jobs in government involved finding a workable public policy to develop improved information security systems for government, public and private sectors.

2:30 pm SET – Secure Electronic Transactions

John Gould
VP Electronic Commerce
MasterCard International

Addressing consumer concerns about making purchases on the Internet, MasterCard International and Visa International recently joined together to announce a technical standard for safeguarding payment card purchases made over open networks such as the Internet. The new specification, called Secure Electronic Transactions (SET), was developed by MasterCard and VISA in cooperation with GTE, IBM, Microsoft, Netscape Communications Corp., SAIC, Terisa Systems, VeriSign and RSA Data Security. Learn how and why SET applications will become the standard for securing bankcard transactions over the Internet for both commercial and government customers.

John Gould is Vice President, Electronic Commerce at MasterCard International, a global payments franchise company. He is responsible for identifying and implementing new business opportunities in emerging technologies. Mr. Gould joined MasterCard in 1988 as Vice



President of Development, and developed MasterCard SmartCard Strategy and Master Model. Currently Mr. Gould is responsible for developing an infrastructure to support electronic commerce on the Internet. He recently established MasterCard's Worldwide Web presence and developed the MasterCard Internet Navigator.

3:00 pm Security for the Distributed Enterprise

ORACLE

Tim Ehrsam
Senior Product Manager
Oracle Corporation

The landscape for information access has changed. In addition to traditional client/server environments, new technologies such as Web systems and mobile computing are being utilized to open the enterprise. However, this changing landscape requires new security technologies to protect valuable corporate and government information. This presentation will discuss the advanced networking technologies that Oracle provides to protect information in the rapidly changing distributed enterprise.

Mr. Ehrsam has over thirteen years of experience in trusted operating systems, database management systems, and networking products. His experience in trusted systems development includes both UNIX and proprietary systems engineering targeting U.S. NCSC Evaluation Classes C2 through A1 and European ITSEC E3. Mr. Ehrsam is in the Network and Management Products Group, Server Technologies Division, where he manages development of database and network security products. Mr. Ehrsam earned a B.A. in Economics from Dartmouth College, a B.S. in Computer Science from West Chester University, and an M.S. in Computer Science from George Washington University.

3:30 pm Government, Bankcards & the Internet

Bill Powar
VISA International

VISA

Visa is the world's largest payment system, and plays a pivotal role in developing and implementing new technologies to benefit its 19,000-member financial institutions and their cardholders, businesses, governments and the global economy. Visa's 442 million cards are accepted by more than 12.2 million merchants worldwide. Visa/PLUS is the largest global ATM network. In this talk, you'll learn about Visa's newest product and service offerings for government customers — and how advanced cryptographic technologies developed by RSA are making it all possible.

4:00 pm Break

4:15 pm Virtual Private Networking

Tony Rosati
VP Sales and Marketing
TimeStep

TIMESTEP

In order to augment their security architectures, firewall vendors, network equipment vendors and TCP/IP stack vendors alike have been moving towards a Virtual Private Networking strategy, implementing proposed standards from the IPSEC working group of the Internet Engineering Task Force (IETF). RSA's S/WAN™ initiative provides a forum allowing vendors to interoperate and test the standards over the Internet. Many issues must still be addressed before multi-vendor inter- and intra-net security can be a reality, ranging from secured links termination points to the use of global public-key infrastructures.

Tony Rosati is Vice President of Sales and Marketing at TimeStep Corporation. Coming from a background in Electrical Engineering at the University of Waterloo in 1985, he has extensive experience in the application of cryptography and communications. Mr. Rosati has led design teams ranging from the development of public key and DES based integrated circuits to the development of system level communications security solutions utilizing state-of-the-art cryptographic techniques.

4:45 pm RSA Offerings for Government

Kurt Stammberger
Director, Technology Marketing
RSA Data Security

RSA
DATA SECURITY INC

RSA Data Security, Inc. is the world's "brand name" for cryptography, with more than 25 million copies of its encryption and authentication engines installed and in use worldwide. RSA's advanced encryption technology is embedded in Microsoft Windows 95, Netscape Navigator, Intuit Quicken, Lotus Notes, and hundreds of other off-the-shelf products. RSA technologies dominate worldwide security standards for the Internet and World Wide Web, CCITT, ISO, ANSI, and IEEE. In this session you'll learn about RSA's product and service offerings — from personal encryption utilities to developer's toolkits, from consulting services to design reviews.

Kurt Stammberger is Director of Technology Marketing for RSA, responsible for product and technology marketing, customer education, press relations and publications. Mr. Stammberger performed his undergraduate and graduate work at Stanford University in the departments of Mechanical Engineering and Aeronautics & Astronautics. Before RSA, Mr. Stammberger has held positions in engineering, engineering computing applications and thermodynamics at Rockwell International and Lockheed Missiles and Space Company. Mr. Stammberger also worked with IBM as a Scientific and Technical Computing Specialist at Lawrence Livermore National Laboratories.

5:15 pm The Postman's Route on the Info Superhighway

Paul Raines
US Postal Service

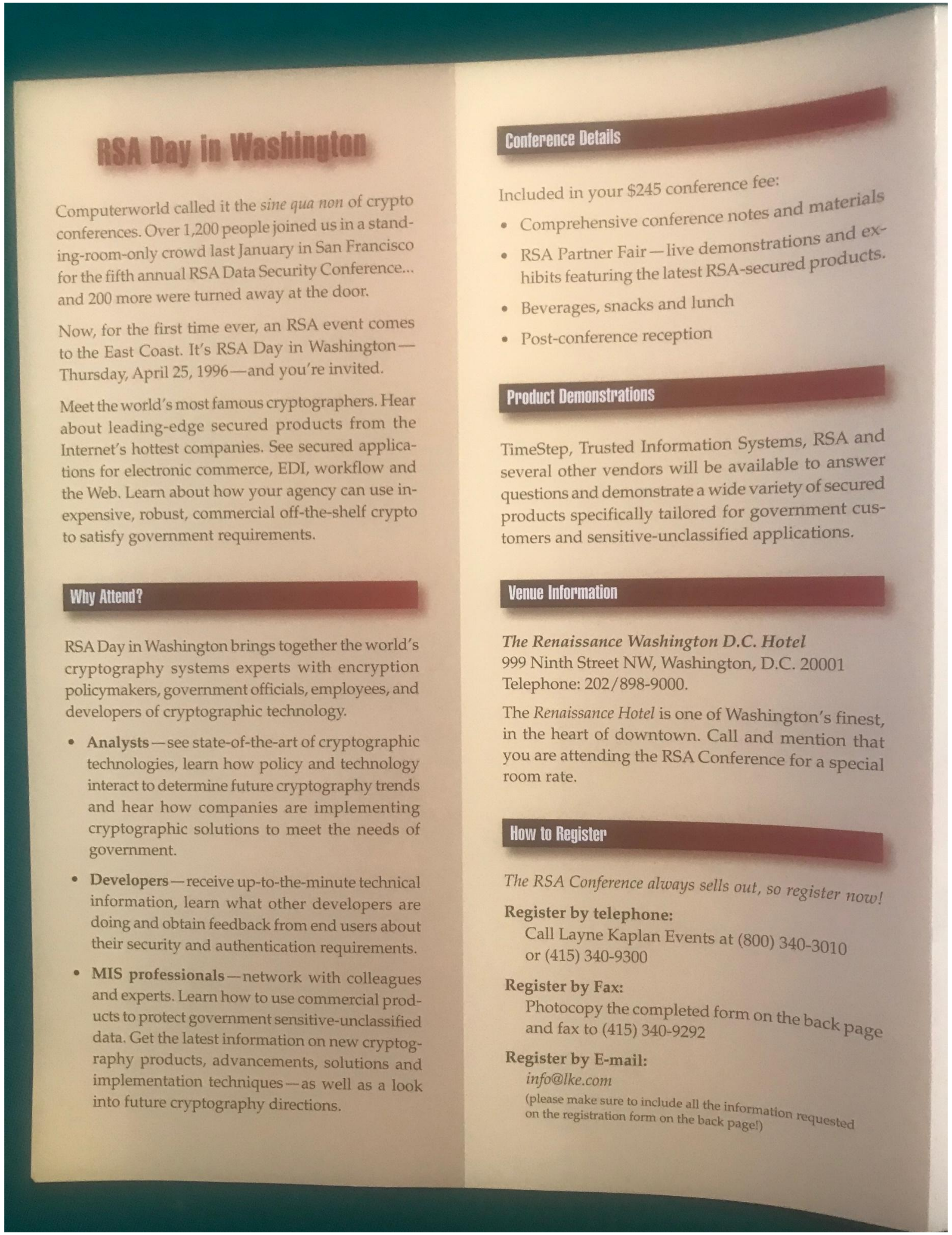
UNITED STATES POSTAL SERVICE

Advances in computer technology and the growth of the Internet have increased demand for businesses to conduct commerce "on-line." However, questions of security, fraud protection, and availability of an universal infrastructure have prevented businesses from engaging in widespread electronic commerce. Mr. Raines will discuss the Postal Service's plans to produce an electronic postmarking service and certificate authority services.

Mr. Raines graduated with honors from the U.S. Air Force Academy with a B.S. in International Affairs in 1981. While in the Air Force he earned an M.S. in Space Physics from the Air Force Institute of Technology. Mr. Raines left the Air Force to accept a full scholarship at Harvard University's Kennedy School of Government. He received his Masters in Public Administration in 1993. Following graduation, Mr. Raines worked with Comsat World Systems, serving as a member of the U.S. delegation to the International Telecommunications Union. As the Program Manager for the Postal Electronic Commerce Services, he supervises an effort to deploy a national certificate authority and digital notary service under the auspices of the U.S. Postal Service.

5:45 Wrapup

6:00 Reception



RSA Day in Washington

Computerworld called it the *sine qua non* of crypto conferences. Over 1,200 people joined us in a standing-room-only crowd last January in San Francisco for the fifth annual RSA Data Security Conference... and 200 more were turned away at the door.

Now, for the first time ever, an RSA event comes to the East Coast. It's RSA Day in Washington—Thursday, April 25, 1996—and you're invited.

Meet the world's most famous cryptographers. Hear about leading-edge secured products from the Internet's hottest companies. See secured applications for electronic commerce, EDI, workflow and the Web. Learn about how your agency can use inexpensive, robust, commercial off-the-shelf crypto to satisfy government requirements.

Why Attend?

RSA Day in Washington brings together the world's cryptography systems experts with encryption policymakers, government officials, employees, and developers of cryptographic technology.

- **Analysts**—see state-of-the-art of cryptographic technologies, learn how policy and technology interact to determine future cryptography trends and hear how companies are implementing cryptographic solutions to meet the needs of government.
- **Developers**—receive up-to-the-minute technical information, learn what other developers are doing and obtain feedback from end users about their security and authentication requirements.
- **MIS professionals**—network with colleagues and experts. Learn how to use commercial products to protect government sensitive-unclassified data. Get the latest information on new cryptography products, advancements, solutions and implementation techniques—as well as a look into future cryptography directions.

Conference Details

Included in your $245 conference fee:

- Comprehensive conference notes and materials
- RSA Partner Fair—live demonstrations and exhibits featuring the latest RSA-secured products.
- Beverages, snacks and lunch
- Post-conference reception

Product Demonstrations

TimeStep, Trusted Information Systems, RSA and several other vendors will be available to answer questions and demonstrate a wide variety of secured products specifically tailored for government customers and sensitive-unclassified applications.

Venue Information

The Renaissance Washington D.C. Hotel
999 Ninth Street NW, Washington, D.C. 20001
Telephone: 202/898-9000.

The *Renaissance Hotel* is one of Washington's finest, in the heart of downtown. Call and mention that you are attending the RSA Conference for a special room rate.

How to Register

The RSA Conference always sells out, so register now!

Register by telephone:
Call Layne Kaplan Events at (800) 340-3010
or (415) 340-9300

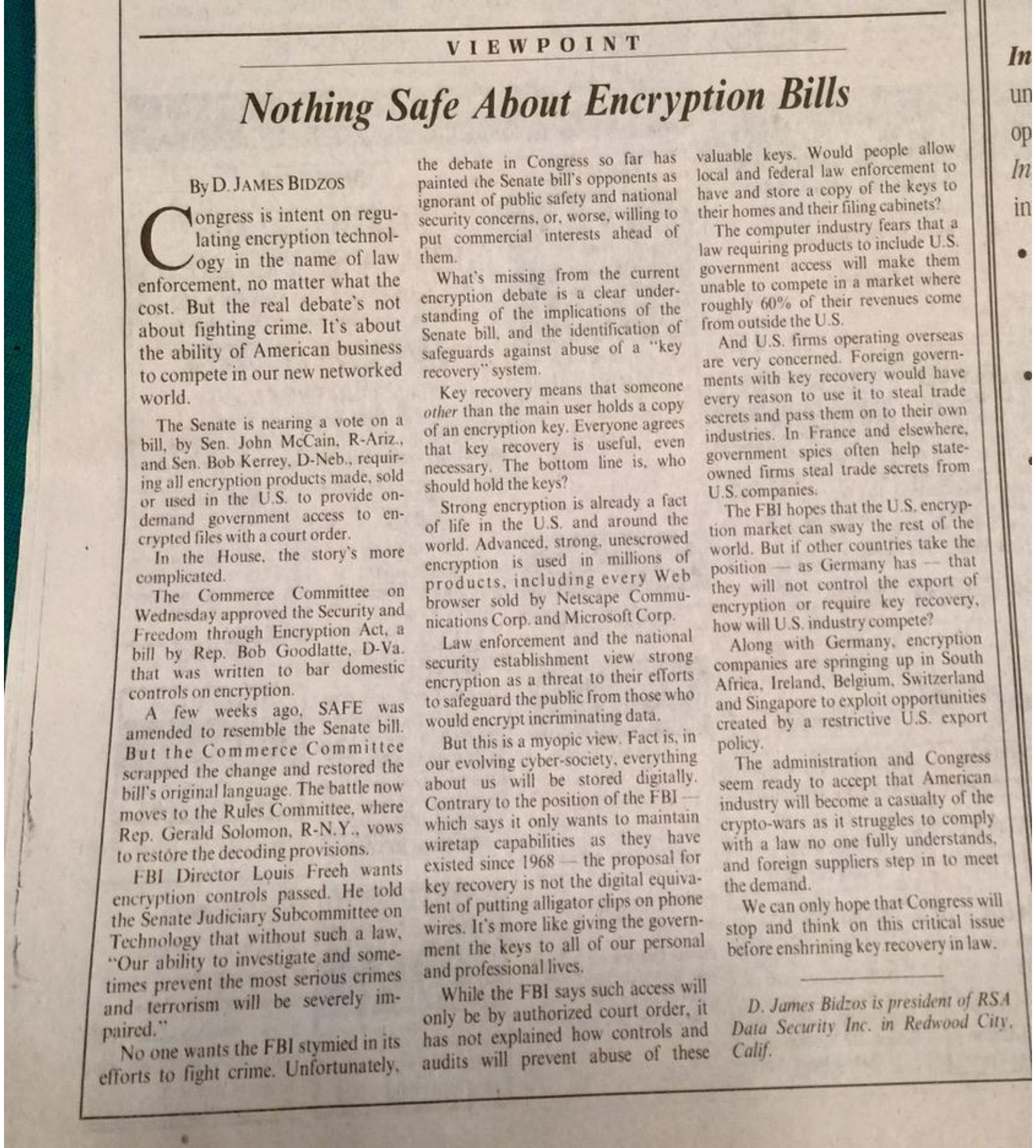
Register by Fax:
Photocopy the completed form on the back page and fax to (415) 340-9292

Register by E-mail:
info@lke.com
(please make sure to include all the information requested on the registration form on the back page!)

Unstoppable Growth, 1995-2000

The WWW explodes; a new company is created (and one is dissolved); allies help secure a major policy win.

1995: The Internet becomes the WWW with 100MM browsers in use as Microsoft follows with IE.
Verisign formed to be independent CA; PKP dissolved after lengthy arbitration.
1996: RSA merges with SDI, becomes a public company. SAFE Act attempted ambush.
RSA Day in Washington. B settles some old family business.
NIST point person for crypto standards (Lynn McNulty) and NSA Deputy
Director for InfoSec (Ed Hart) both join RSA/Verisign. As do many others.
1997 B meets with Pres. Clinton on crypto export policy.



VIEWPOINT

Nothing Safe About Encryption Bills

By D. JAMES BIDZOS

Congress is intent on regulating encryption technology in the name of law enforcement, no matter what the cost. But the real debate's not about fighting crime. It's about the ability of American business to compete in our new networked world.

The Senate is nearing a vote on a bill, by Sen. John McCain, R-Ariz., and Sen. Bob Kerrey, D-Neb., requiring all encryption products made, sold or used in the U.S. to provide on-demand government access to encrypted files with a court order.

In the House, the story's more complicated.

The Commerce Committee on Wednesday approved the Security and Freedom through Encryption Act, a bill by Rep. Bob Goodlatte, D-Va. that was written to bar domestic controls on encryption.

A few weeks ago, SAFE was amended to resemble the Senate bill. But the Commerce Committee scrapped the change and restored the bill's original language. The battle now moves to the Rules Committee, where Rep. Gerald Solomon, R-N.Y., vows to restore the decoding provisions.

FBI Director Louis Freeh wants encryption controls passed. He told the Senate Judiciary Subcommittee on Technology that without such a law, "Our ability to investigate and sometimes prevent the most serious crimes and terrorism will be severely impaired."

No one wants the FBI stymied in its efforts to fight crime. Unfortunately, the debate in Congress so far has painted the Senate bill's opponents as ignorant of public safety and national security concerns, or, worse, willing to put commercial interests ahead of them.

What's missing from the current encryption debate is a clear understanding of the implications of the Senate bill, and the identification of safeguards against abuse of a "key recovery" system.

Key recovery means that someone *other* than the main user holds a copy of an encryption key. Everyone agrees that key recovery is useful, even necessary. The bottom line is, who should hold the keys?

Strong encryption is already a fact of life in the U.S. and around the world. Advanced, strong, unescrowed encryption is used in millions of products, including every Web browser sold by Netscape Communications Corp. and Microsoft Corp.

Law enforcement and the national security establishment view strong encryption as a threat to their efforts to safeguard the public from those who would encrypt incriminating data.

But this is a myopic view. Fact is, in our evolving cyber-society, everything about us will be stored digitally. Contrary to the position of the FBI — which says it only wants to maintain wiretap capabilities as they have existed since 1968 — the proposal for key recovery is not the digital equivalent of putting alligator clips on phone wires. It's more like giving the government the keys to all of our personal and professional lives.

While the FBI says such access will only be by authorized court order, it has not explained how controls and audits will prevent abuse of these valuable keys. Would people allow local and federal law enforcement to have and store a copy of the keys to their homes and their filing cabinets?

The computer industry fears that a law requiring products to include U.S. government access will make them unable to compete in a market where roughly 60% of their revenues come from outside the U.S.

And U.S. firms operating overseas are very concerned. Foreign governments with key recovery would have every reason to use it to steal trade secrets and pass them on to their own industries. In France and elsewhere, government spies often help state-owned firms steal trade secrets from U.S. companies.

The FBI hopes that the U.S. encryption market can sway the rest of the world. But if other countries take the position — as Germany has — that they will not control the export of encryption or require key recovery, how will U.S. industry compete?

Along with Germany, encryption companies are springing up in South Africa, Ireland, Belgium, Switzerland and Singapore to exploit opportunities created by a restrictive U.S. export policy.

The administration and Congress seem ready to accept that American industry will become a casualty of the crypto-wars as it struggles to comply with a law no one fully understands, and foreign suppliers step in to meet the demand.

We can only hope that Congress will stop and think on this critical issue before enshrining key recovery in law.

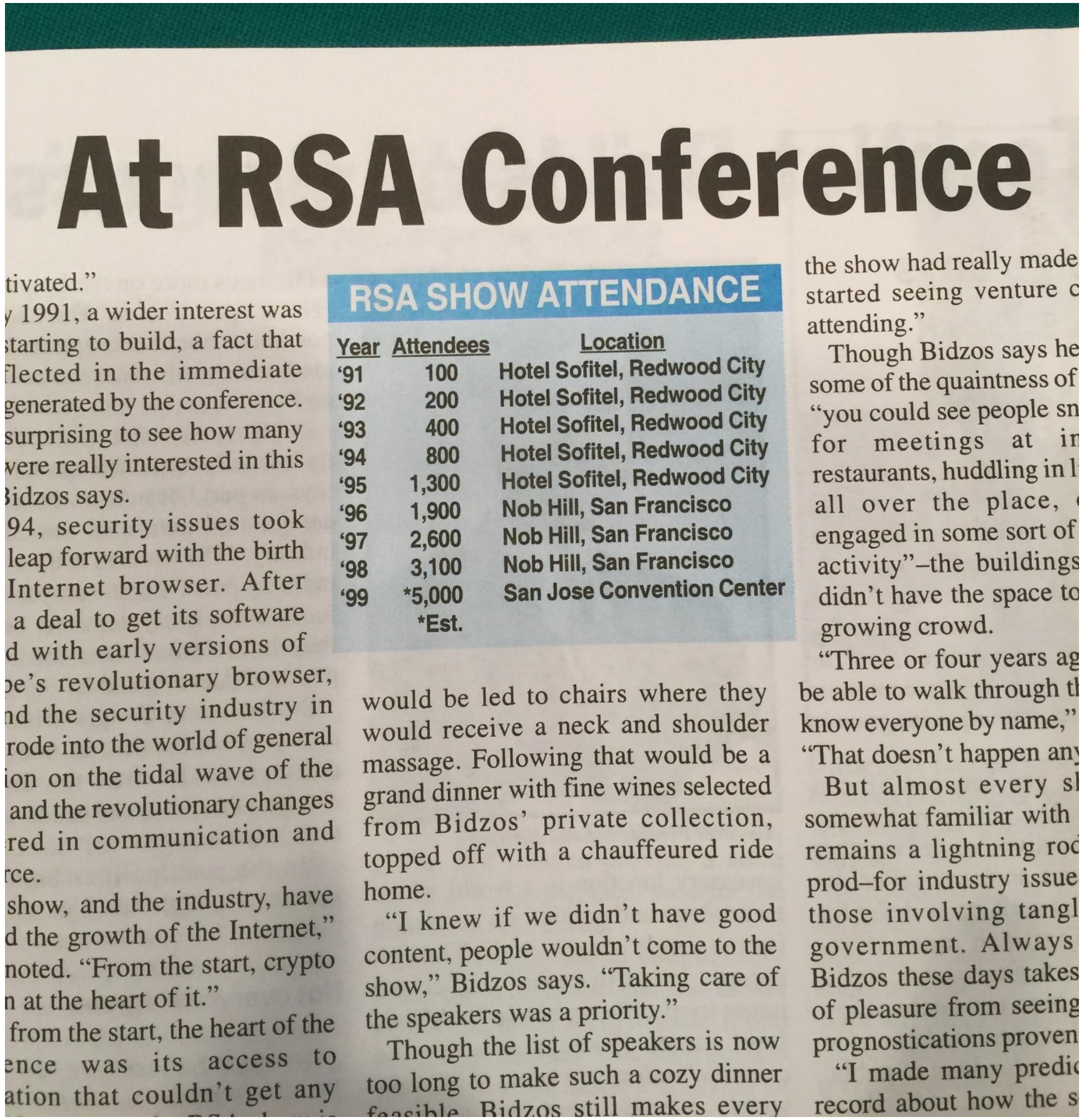
D. James Bidzos is president of RSA Data Security Inc. in Redwood City, Calif.

"While the FBI says such access <to escrowed keys> will only be granted by court order, it has not explained how controls and audits will prevent abuse of these valuable keys. Would people allow local and federal law enforcement to have and store a copy of the keys to their homes and their filing cabinets?"

Unstoppable Growth, 1995-2000

The WWW explodes; a new company is created (and one is dissolved); allies help secure a major policy win.

1995: The Internet becomes the WWW with 100MM browsers in use as Microsoft follows with IE.
Verisign formed to be independent CA; PKP dissolved after lengthy arbitration.
1996: RSA merges with SDI, becomes a public company. SAFE Act attempted ambush.
RSA Day in Washington. B settles some old family business.
NIST point person for crypto standards (Lynn McNulty) and NSA Deputy
Director for InfoSec (Ed Hart) both join RSA/Verisign. As do many others.
1997 B meets with Pres. Clinton on crypto export policy
1998: Big guns join the lobby team. Senate Commerce Cmte hearings – Microsoft,
Netscape, others testify. Nob Hill is the place to be as RSAC grows. Verisign IPO. Aspen.



At RSA Conference

tivated."
y 1991, a wider interest was
starting to build, a fact that
flected in the immediate
generated by the conference.
surprising to see how many
were really interested in this
idzos says.
94, security issues took
leap forward with the birth
Internet browser. After
a deal to get its software
d with early versions of
pe's revolutionary browser,
nd the security industry in
rode into the world of general
ion on the tidal wave of the
and the revolutionary changes
red in communication and
rce.
show, and the industry, have
d the growth of the Internet,"
noted. "From the start, crypto
n at the heart of it."
from the start, the heart of the
ence was its access to
ation that couldn't get any

RSA SHOW ATTENDANCE

Year	Attendees	Location
'91	100	Hotel Sofitel, Redwood City
'92	200	Hotel Sofitel, Redwood City
'93	400	Hotel Sofitel, Redwood City
'94	800	Hotel Sofitel, Redwood City
'95	1,300	Hotel Sofitel, Redwood City
'96	1,900	Nob Hill, San Francisco
'97	2,600	Nob Hill, San Francisco
'98	3,100	Nob Hill, San Francisco
'99	*5,000	San Jose Convention Center

*Est.

would be led to chairs where they would receive a neck and shoulder massage. Following that would be a grand dinner with fine wines selected from Bidzos' private collection, topped off with a chauffeured ride home.

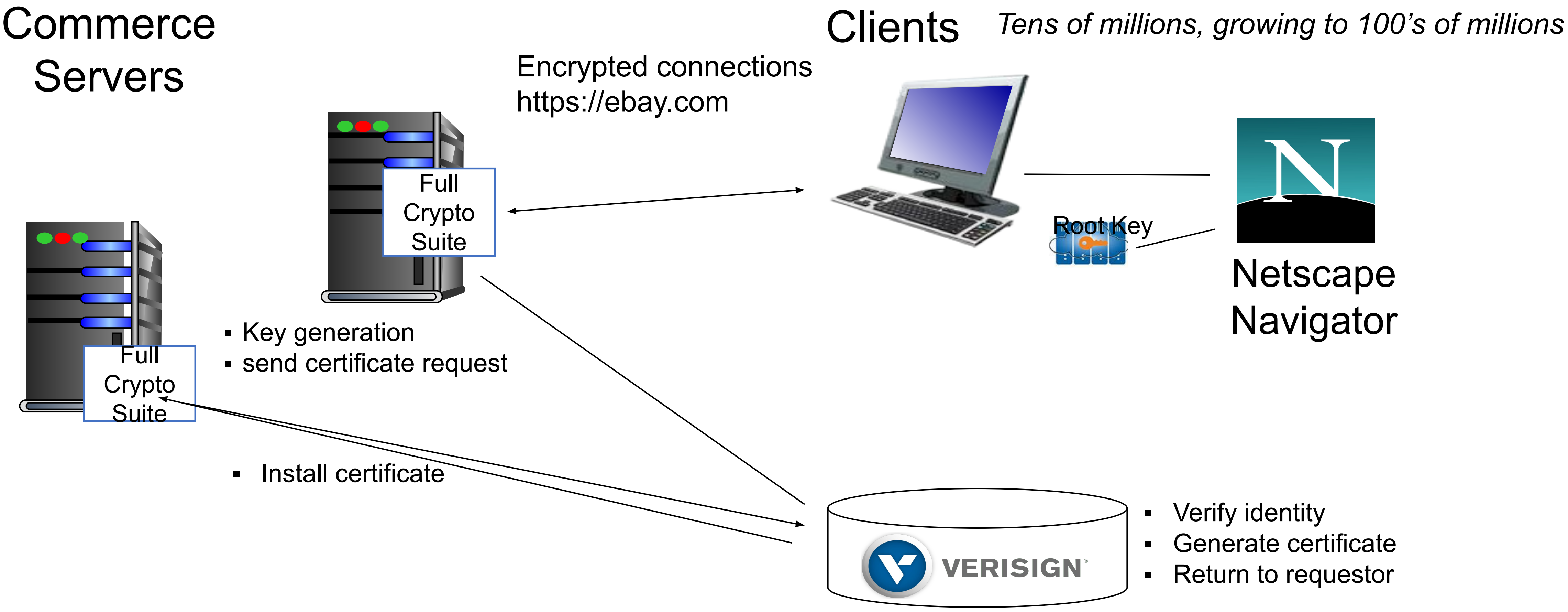
"I knew if we didn't have good content, people wouldn't come to the show," Bidzos says. "Taking care of the speakers was a priority."

Though the list of speakers is now too long to make such a cozy dinner feasible, Bidzos still makes every

the show had really made
started seeing venture c
attending."
Though Bidzos says he
some of the quaintness of
"you could see people sn
for meetings at in
restaurants, huddling in l
all over the place,
engaged in some sort of
activity"–the buildings
didn't have the space to
growing crowd.
"Three or four years ag
be able to walk through th
know everyone by name,"
"That doesn't happen any
But almost every sl
somewhat familiar with
remains a lightning roc
prod–for industry issue
those involving tangl
government. Always
Bidzos these days takes
of pleasure from seeing
prognostications proven
"I made many predic
record about how the s

onference 2000
111

Netscape 1994 (followed by Microsoft in 1995)



Commerce Servers

Clients *Tens of millions, growing to 100's of millions*

Encrypted connections
https://ebay.com

- Key generation
- send certificate request

- Install certificate

- Verify identity
- Generate certificate
- Return to requestor

Verisign in April 1995 at time of incorporation

- IP: Established, defended, respected –VALUABLE
- Brand: RSA, endorsed, proven over years of scrutiny –VERY VALUABLE
- Product (BSAFE): Mature, proven, distributed – EXTREMELY VALUABLE
- Control of Distributed and Enabled Root keys in BSAFE - PRICELESS

Verisign in April 1995 at time of incorporation

- Technology: Mature, tested and proven, widely standardized:

* PKCS #1

* DOCSYS
* ANSI X9.31 part 4 (draft)
* Privacy-Enhanced Mail
* Australian Standard AS2805.5.3
* ISO/IEC 9796 (almost)
* ANSI X9.31 part 1 (draft)
* ISO/IEC JTC1 SC27/WG2 (work in progress)
* CCITT X.509 (informative)
* Australian Standard AS2805.6.5.3 (draft)
* CFONB ETEBAC-5
* ISO CD 11666 (draft)
* IEEE P1363 (work in progress)

Unstoppable Growth, 1995-2000

The WWW explodes; a new company is created (and one is dissolved); allies help secure a major policy win.

1995: The Internet becomes the WWW with 100MM browsers in use as Microsoft follows with IE.
Verisign formed to be independent CA; PKP dissolved after lengthy arbitration.

1996: RSADSI merges with SDI, becomes a public company. SAFE Act ambush.
In Their Face: RSA Day in Washington. 64-24=40 is horrible math. B settles some old family business. NIST point person crypto standards (Lynn McNulty) and NSA Deputy Director for InfoSec (Ed Hart) both join RSA/Verisign. As do many others.

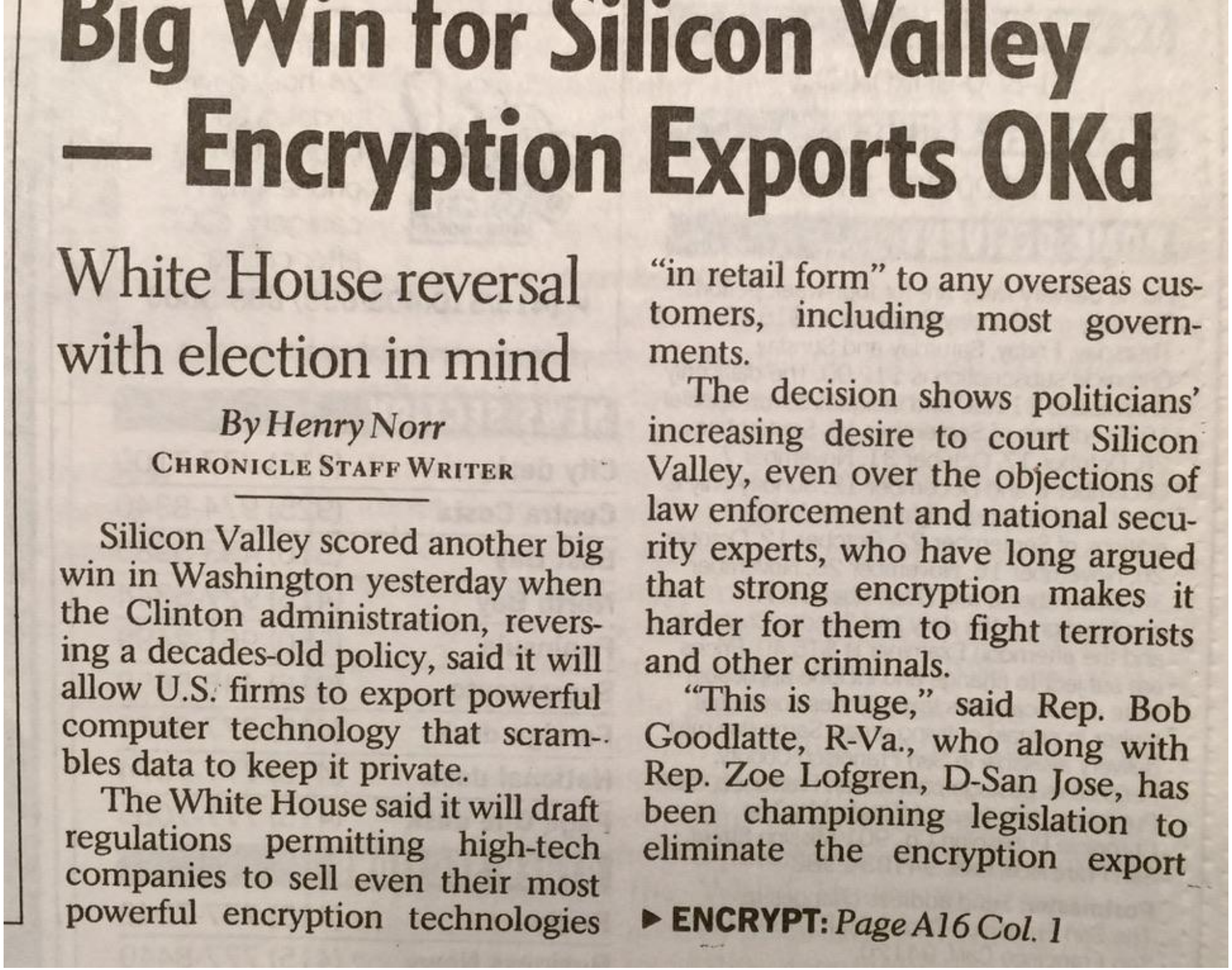
1997 B meets with Pres. Clinton on crypto export policy

1998: Big guns join the lobby team. Senate Commerce Cmte hearings – Microsoft, Netscape, others testify. Nob Hill is the place to be as RSAC grows. Verisign IPO. Aspen.

1999: Internet (and RSA) explosive growth continues, companies pile on for policy change

2000: January – USG announces mass-market software with strong encryption to be commoditized under export rules. B announces retirement.

JIM



Big Win for Silicon Valley — Encryption Exports OKd

White House reversal with election in mind

By Henry Norr
CHRONICLE STAFF WRITER

Silicon Valley scored another big win in Washington yesterday when the Clinton administration, reversing a decades-old policy, said it will allow U.S. firms to export powerful computer technology that scrambles data to keep it private.

The White House said it will draft regulations permitting high-tech companies to sell even their most powerful encryption technologies "in retail form" to any overseas customers, including most governments.

The decision shows politicians' increasing desire to court Silicon Valley, even over the objections of law enforcement and national security experts, who have long argued that strong encryption makes it harder for them to fight terrorists and other criminals.

"This is huge," said Rep. Bob Goodlatte, R-Va., who along with Rep. Zoe Lofgren, D-San Jose, has been championing legislation to eliminate the encryption export

▶ ENCRYPT: *Page A16 Col. 1*

White House to draft new, relaxed export regs

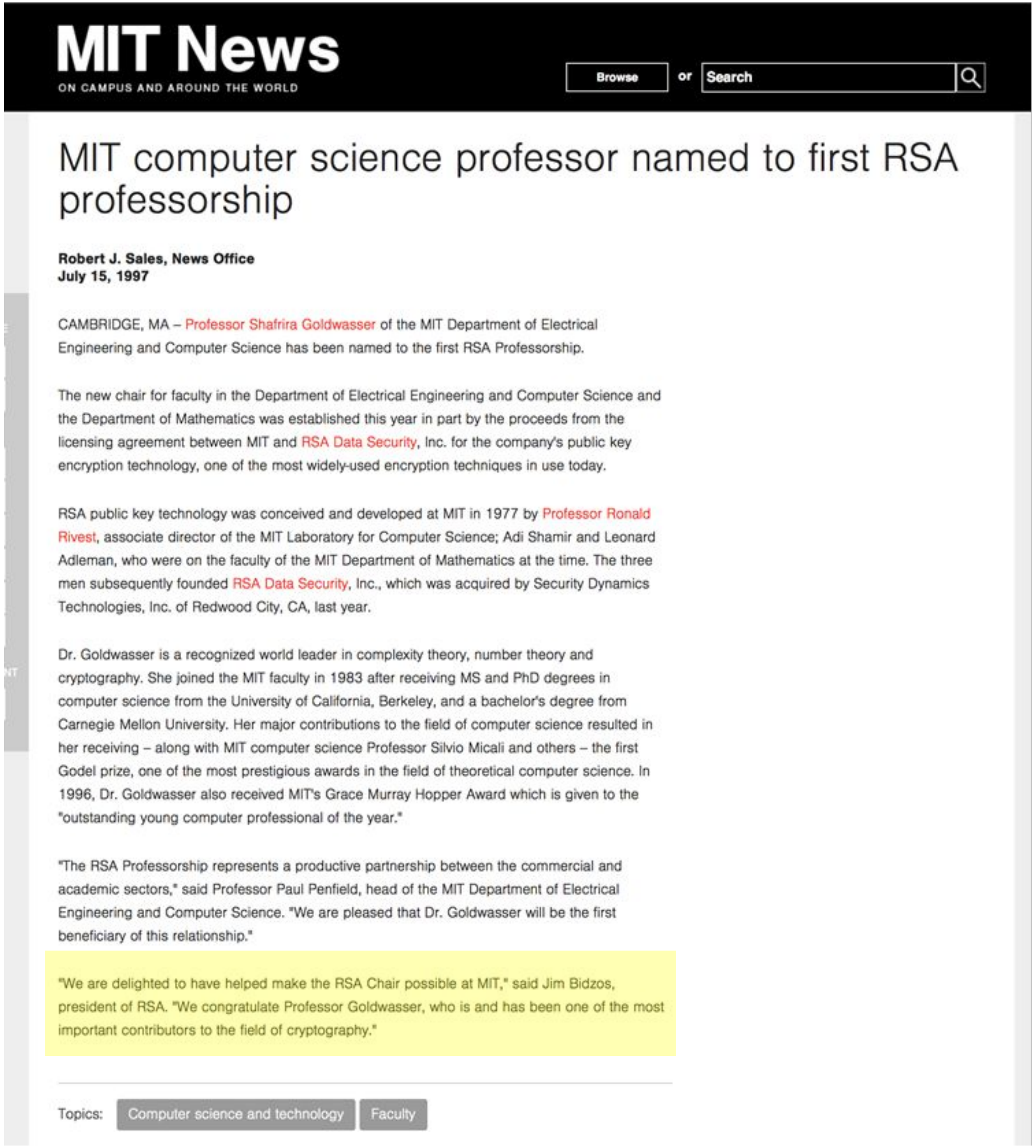
"This is huge," said Bob Goodlatte, R-Va.

LESSONS LEARNED

- You never know how things can happen!
- Naiveté can be a good thing.
- How to dance with elephants and not get crushed.
- Compartmentalize. Don’t let things you can’t influence consume you.
- It’s never as bad as it seems. Don’t let your imagination run wild.
- Never lose sight of your goal!
- Surround yourself with great people.

EPILOGUE

- R, S, and A receive Turing Award 2002, Diffie and Hellman in 2015
- R still MIT faculty, Institute Professor
- S faculty at Weizmann, A faculty at USC
- All continue to teach and make substantial research contributions
- MIT shares in RSADSI Endowed RSA Chair of EECS, and more
- RSA patent (through RSADSI shares) most lucrative for MIT in its history at the time in 1997, exceeding penicillin and core memory
- B retires from the RSA in 2000, RSA board in 2002, from RSAC in 2004
- RSA sold to EMC 2006, EMC bought by DELL 2016, RSAC bought by PE 2022
- B came back in 2008 to restructure Verisign, still Chairman & CEO today



MIT computer science professor named to first RSA professorship

Robert J. Sales, News Office
July 15, 1997

CAMBRIDGE, MA – Professor Shafrira Goldwasser of the MIT Department of Electrical Engineering and Computer Science has been named to the first RSA Professorship.

The new chair for faculty in the Department of Electrical Engineering and Computer Science and the Department of Mathematics was established this year in part by the proceeds from the licensing agreement between MIT and RSA Data Security, Inc. for the company's public key encryption technology, one of the most widely-used encryption techniques in use today.

RSA public key technology was conceived and developed at MIT in 1977 by Professor Ronald Rivest, associate director of the MIT Laboratory for Computer Science; Adi Shamir and Leonard Adleman, who were on the faculty of the MIT Department of Mathematics at the time. The three men subsequently founded RSA Data Security, Inc., which was acquired by Security Dynamics Technologies, Inc. of Redwood City, CA, last year.

Dr. Goldwasser is a recognized world leader in complexity theory, number theory and cryptography. She joined the MIT faculty in 1983 after receiving MS and PhD degrees in computer science from the University of California, Berkeley, and a bachelor's degree from Carnegie Mellon University. Her major contributions to the field of computer science resulted in her receiving – along with MIT computer science Professor Silvio Micali and others – the first Godel prize, one of the most prestigious awards in the field of theoretical computer science. In 1996, Dr. Goldwasser also received MIT's Grace Murray Hopper Award which is given to the "outstanding young computer professional of the year."

"The RSA Professorship represents a productive partnership between the commercial and academic sectors," said Professor Paul Penfield, head of the MIT Department of Electrical Engineering and Computer Science. "We are pleased that Dr. Goldwasser will be the first beneficiary of this relationship."

"We are delighted to have helped make the RSA Chair possible at MIT," said Jim Bidzos, president of RSA. "We congratulate Professor Goldwasser, who is and has been one of the most important contributors to the field of cryptography."

Topics: Computer science and technology Faculty

THANK YOU.