

A photograph of a large wooden pigeon loft filled with many pigeons of various breeds. The loft has multiple levels with wooden perches and nesting boxes. Pigeons are seen on the top level, in the middle sections, and on the floor. The lighting is somewhat dim, and the overall tone is slightly greenish. The text 'RSA DATA SECURITY, INC.' is overlaid in the center, with 'RSA' and 'SECURITY, INC.' in a blue sans-serif font and 'DATA' in a large, stylized script font. Below it, 'A SECURITY DYNAMICS COMPANY' is written in a smaller blue sans-serif font.

RSA DATA SECURITY, INC.
A SECURITY DYNAMICS COMPANY



“Microsoft, Apple,
IBM and DEC
don’t agree on much,
but we all agree
RSA is the way to go.”

—*Nathan Myhrvold,*

VP Advanced Technology,

Microsoft Corp.



HAT are pigeons doing on the front of an RSA brochure?

Well, it's just our way of paying homage to a very special pigeon named *Cher Ami*.

*C*her Ami was a registered Black Check Cock carrier pigeon, one of 600 birds owned and flown by the U.S. Army Signal Corps in France during World War I. Carrier pigeons like Cher Ami were often the only means of secure communications available to forces actively engaged at the front lines in Verdun, France.

On his last mission, Cher Ami was shot through the breast by enemy fire, but still managed to return to his loft. Dangling from the ligaments of one of his legs, also shattered by enemy fire, was his last message capsule.

It was from Major Whittlesey's "Lost Battalion" of the 77th Infantry Division. They had been cutoff, and desperately required assistance. The message initiated a rescue operation, and just a few hours later, 194 survivors of the battalion were safe behind American lines.

Cher Ami was awarded the French Croix de Guerre with Palm for his heroic service between the Allied forts of Verdun. He died in 1919 from his wounds, and was later inducted into the Racing Pigeon Hall of Fame in 1931.

*S*o what do carrier pigeons and RSA have in common? Well, we just wanted to illustrate a point about the importance of secure communications. Just like Cher Ami, encryption and authentication technologies from RSA can "save the day" for you and your business. In today's battlefield of global electronic commerce, transaction security is essential. You need someone you can depend on. And nobody has the experience, the spirit or the drive of RSA.



100 MARINE PARKWAY
SUITE 500
REDWOOD CITY
CA 94065-1031

Dear Reader:

The invention of writing brought with it the need to prove messages to be genuine, so that a distant recipient might be assured of that message's authenticity. Throughout history, this has taken the form of a "seal" unique to each author, marked on the communications medium.

For centuries, the handwritten signature has been our traditional seal of authentication. Modern official seals — notary, government and corporate — still mark paper much as in ancient times. Envelopes emblazoned "personal and confidential" are still used to protect some of our most sensitive information. But all this is changing — and quickly.

Twenty-five years ago, the nascent ARPANET connected computers at about two dozen sites in the western United States. This tiny demonstration network grew into the global Internet, which is soon projected to link over one billion people all over the planet. It is clear that paper is rapidly becoming a presentation medium, as business worldwide shift their critical business transactions to media like E-mail, Electronic Commerce, EFT and EDI. Those who fail to embrace the technology will simply find themselves unable to compete.

This mass movement towards digital business transactions has forced changes in our traditional authentication and privacy assurance mechanisms. Handwritten signatures and notary seals, impossible to affix in the new non-tangible media, will be left behind with clay tablets and sealing wax. And much sooner than you think.

Elegant in construction, powerful in application, RSA digital signature and digital enveloping technologies are the sign and seal for the Information Age.

Sincerely,

D. James Bidzos
President
RSA Data Security

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

THE KEYS TO
PRIVACY AND
AUTHENTICATION

V I S I O N

*T*he RSA Public Key Cryptosystem was invented in 1977 at the Massachusetts Institute of Technology, and since then, has grown to become the most trusted encryption and authentication system in the world. It has undergone more scrutiny and withstood more MIPS-years of computer attack than any other encryption system. More academic studies have been published about RSA than any other cryptosystem. No other security technology is as well understood, or as well trusted, as RSA.

But while perhaps our company is most famous for our namesake technology, we have established ourselves by providing diverse cryptographic solutions across a broad client base. Today, RSA Data Security is the world's leading cryptography firm.

RSA's cryptographic technologies form the security core of hundreds of products, from Internet browsers and servers to realtime credit card authorization systems, from e-mail and workflow applications to phones, modems and satellite broadcast. Our encryption engines support products from virtually every leading vendor, including Netscape, Oracle, Microsoft and Sun.

But we're not one to rest on our laurels. RSA Laboratories, the research and development arm of RSA, performs basic research into mathematics, number theory, and application to cryptography. Labs' scientists continue to investigate and develop new security technologies, making it one of the world's leading centers of cryptographic expertise.

"RSA is undoubtedly the best choice for security in today's networked world, and it's a very important part of our future." — Bill Gates, Chairman & CEO, Microsoft.

"We considered doing this on our own ... for about ten minutes. There are some things you can roll on your own, but not this. It is a feature that will stand out. It shows people we're really concerned about the integrity of their systems." — Richard King, VP Software Development, Novell

"We have been convinced by user organizations that RSA will be a prerequisite for sales of security products." — Robert Follet, Standards Program Director, IBM

~1800 BC



An Egyptian scribe writes some unusual, unfamiliar hieroglyphs. Scientists later determine these to be the earliest known examples of written cryptography.

~1500 BC

A Mesopotamian pottery maker, eager to protect his glazing process, inscribes his formula onto a stone tablet using a secret, encrypted code.



~550 BC

Hebrew scribes write the book of Jeremiah using a reversed alphabet substitution cipher known as ATBASH — one of several Hebrew ciphers used within religious texts.



Privacy protection by conventional means such as DES (the government-sponsored Data Encryption Standard) is relatively easy in small networks, requiring the exchange of secret encryption keys with each party.

But as a network grows in size, using symmetric encryption techniques like DES by themselves becomes impractical. Arranging for the secure exchange of all those secret keys becomes expensive to administer. Moreover, DES requires secret sharing: each person must trust the other to not reveal (or lose) the key that they share.

Therefore, in practical implementations, secure communications can only take place between people with a prior relationship, such as employees of the same company. Finally, shared secret

keys prevent either party from proving what the other may have done with that key. Either party could forge a document using the shared key, and a third party would be unable to identify the culprit.

The 1976 theoretical work of Drs. Whitfield Diffie and Martin Hellman of Stanford came to fruition in 1977 with

then professors at the Massachusetts Institute of Technology.

RSA is, quite simply, a method of exchanging authenticated secret messages without exchanging secrets. Rather than using the same key to both encrypt and decrypt the data, the RSA system uses a matched pair of encryption and decryption keys. Each key performs a one-way transformation upon the data — what one encrypts, only the other can decrypt.

Since it is computationally infeasible to derive

one key from the other, one of the keys can be made “Public” while the other is kept “Private”, or secret. To send someone a private message, one simply encrypts the message using the intended

THE RSA PUBLIC KEY CONCEPT



Anything encrypted with someone's RSA public key can only be decrypted with the corresponding RSA private key, and vice-versa.

their development of the Diffie-Hellman Key Agreement technique, and the invention of the RSA Public Key Cryptosystem by Drs. Ronald Rivest, Adi Shamir, and Len Adleman,

~300 BC

In “Elements,” Euclid describes the method for computing the Greatest Common Divisor (GCD) of two numbers. History records it as the Euclidean Algorithm.



~150 BC

Greek historian Polybius introduces a method of substituting each letter of the alphabet with two-digit numbers by distributing all the letters into a matrix with numbered rows and columns.



The Greeks, using a device called the scytale, create cyphertext by wrapping a long, thin strip of leather around a wooden staff. A similar sized staff was needed by the recipient to decipher the script.

~100 BC

~50 BC



Julius Caesar was known to cipher his important communications by using a very simple alphabet shifting scheme.

C R Y P T O G R A P H Y



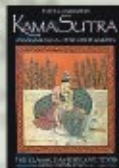
~200 AD

The Leiden papyrus uses a secret key cipher to hide secret potions and recipes for magic.



~400 AD

The Kama Sutra of Vatsyana lists cryptography as one of the 64 yogas (arts) for men and women to practice: "The art of understanding writing in cipher, and the writing of words in a peculiar way. The art of speaking by changing the forms of words."



790 AD

Abu 'Abd Yahmadi writes the first known book on cryptology (now lost).



1379 AD

Pope Clement VII commissions the creation of a combination substitution alphabet and small code, which remains in use among diplomats and some civilians for 450 years.



TAKING FLIGHT:

THE RSA PUBLIC

recipient's public key, confident in the fact that only the recipient's private key could decrypt it. This forms the basis for the RSA Digital Envelope.

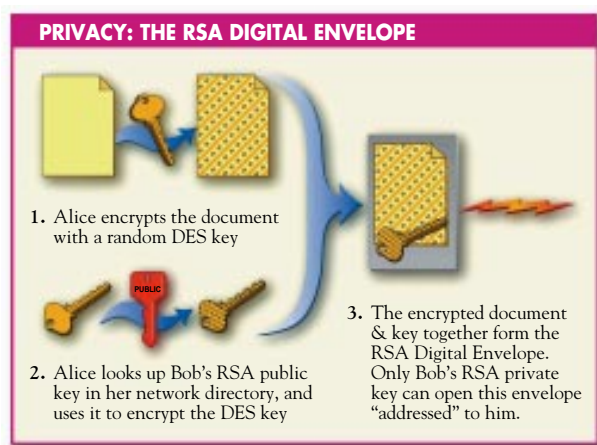
The RSA Digital Envelope provides an encryption solution that gives the user the best of both worlds: the speed of secret key algorithms, like DES, combined with the security of RSA. Conversely, when a message is encrypted with a private key it provides the basis for a "digital signature" — a scrambled message that only one person could produce, but everyone could verify with that person's public key.

But handwritten signatures do more than just identify the author of a document — they in effect must vouch for the document's integrity. A manager's signature on a letter typed by

a secretary says "I have reviewed this page, and the information it contains is the information that I do, in fact, wish to send." The RSA algorithm can accomplish even this.

change. And the hashing algorithm is a one-way function: the document content cannot be reconstructed from the bits of the message digest. With RSA's MD family of algorithms — featuring 128-bit

message digests — the probability that different documents will have the same digest by coincidence is less than 1 in a trillion *trillion*, effectively ensuring that two message digests will only match if their source documents are bit-for-bit identical.



The RSA Digital Signature employs a cryptographic "hashing" algorithm to create a message digest that is unique to each document, much like a fingerprint. If even a single bit of the document is changed, roughly 50% of the bits in the corresponding message digest will

So while the RSA Digital Signature is easy to produce and check, it is impossible to forge, and therefore positively identifies the author. And, unlike a handwritten signature, it also verifies the contents of a document.

1466 AD



Italian architect Leon Battista Alberti invents the first polyalphabetic cipher, designing a disk device which produced a new substitution alphabet with every turn of the wheel. His cipher was apparently not broken until the 1800's.

1473-1490 AD

Crucial instructions for making a "philosopher's stone" — a principle element in alchemy — are enciphered within a manuscript by Arnaldus de Bruxella.



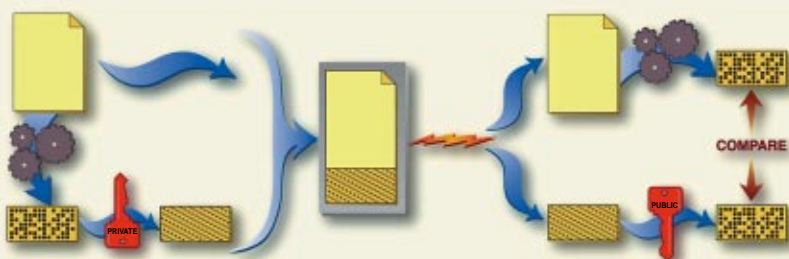
1518 AD

Johannes Trithemius writes the first printed book of cryptology; he also invents a steganographic cipher in which each letter is represented by words in successive columns of text designed to hide inconspicuously as a legitimate prayer.



K E Y C R Y P T O S Y S T E M

AUTHENTICATION: THE RSA DIGITAL SIGNATURE



Alice passes her document through a hashing algorithm to produce the message digest, then encrypts the digest with her RSA private key (forming an RSA Digital Signature) and transmits the signed document to Bob.

After receiving Alice's transmission, Bob uses the same hashing algorithm to create another message digest, and also decrypts the signature using Alice's RSA public key. The two resulting message digests are then compared.

↓ 1553 AD

The concept of using a passphrase as the key for a repeated polyalphabetic cipher is brought forth by Giovan Battista Belaso.

↓ 1563 AD

Giovanni Battista Porta writes a text on ciphers, in which he introduces the diagraphic cipher, and suggests the use of misspellings and synonyms to confuse the cryptanalyst.



↓ 1585 AD

In his "Traicté des Chiffres" Blaise de Vigenère uses a Trithemius table but changes the key system. One technique uses the plaintext as its own key; another uses the ciphertext. This is known as key scheduling, and is an integral part of the current Data Encryption Standard (DES).



↓ 1623 AD

Sir Francis Bacon invents a cipher which now bears his name — a biliteral cipher, known today as 5-bit binary encoding. The cipher uses a variation in type to carry each bit of the encoding.



B I R D S O F A F E A T H E R :

S T A N D A

The Genuine RSA Encryption Engine logo identifies OEM software and hardware products featuring RSA's powerful cryptography technology. The logo's two central keys represent the patented RSA Public Key Cryptography system, recognized by industry experts as the most secure approach to cryptography. It is also the industry's most widely accepted method of ensuring security and authentication in electronic messaging. Companies displaying the Genuine RSA Encryption Engine logo have shown their commitment to data security by utilizing technology from the most trusted name in cryptography. The Genuine RSA brand is your assurance that the security features in the product you are buying were designed by the very best in the business.

Standards are an important — if maddening — part of any discussion concerning telecommunications, and the field of cryptography is certainly no exception. Luckily, though, you don't have to pick and choose among a myriad telecommunications specs to find RSA. RSA technologies are literally everywhere you look.

ISO 9796 cites RSA, for instance, as does the ITU X.509 international digital certificate standard. RSA is truly the standard for the world-wide financial community, included in such diverse standards as France's ETEBAC 5 and Australia's AS2805.6.5.3 digital signature and electronic funds transfer specifications.



Probably the most widely known RSA standard is Netscape's Secure Sockets Layer (SSL), the most popular method for securing online shopping sessions on the World Wide Web.

Profiled on the next pages are some more important standards that allow disparate systems to interoperate securely. Of course, RSA Data Security offers developers toolkits that support all of them — and others besides. For more detailed technical information on any of these standards, or RSA products which let you build applications that comply to them, visit RSA's website at <www.rsa.com>.

↓ 1640 AD



Pierre de Fermat publishes his "Little Theorem" concerning exponentiation with a prime modulus.

↓ ~1740 AD

Leonhard Euler describes his "phi-function," shows it is multiplicative and uses it to generalize Fermat's Little theorem to include exponentiation with a modulus of a product of two primes.



↓ 1790's

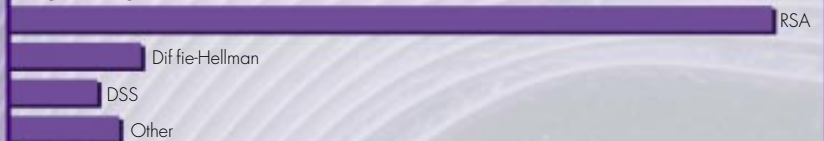
Thomas Jefferson, possibly aided by U. Penn. mathematician Dr. Robert Patterson, invents the wheel cipher. This same device is later used in WWII by the U.S. Navy as the Strip Cipher.



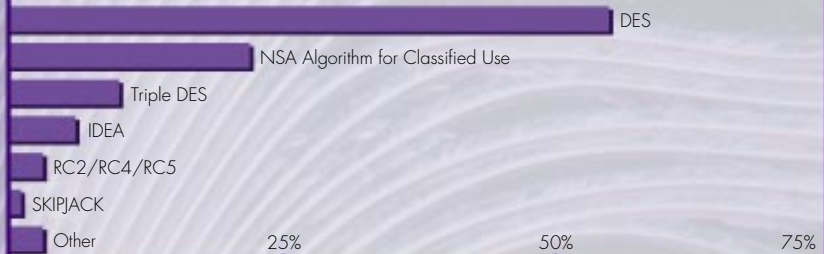
R D S & P A R T N E R S

ALGORITHM USAGE IN SECURED APPLICATIONS

PUBLIC KEY



SINGLE KEY



RSA is by far the most popular technology in Internet security and electronic commerce solutions.

↓ 1854

The Playfair cipher is invented by Charles Wheatstone. This cipher uses a keyed array of letters to make an easy-to-use diagrammatic cipher.



↓

1861-1865

During the US Civil War, the Confederacy is put at a disadvantage by its use of the Vigenère cipher — the solution of which had just been published by Kasiski.



↓

1917

AT&T employee Gilbert S. Vernam invents the one-time pad, a totally random and nonrepetitive cipher which is the only provably secure cipher as yet known.



B I R D S O F A *F* E A T H E R :

S T A N D A

S/MIME is the standard for secure, interoperable electronic mail over the Internet. Using secure e-mail used to mean settling on one e-mail package, company-wide. Now S/MIME allows different vendors to independently develop interoperable RSA-based

S/WAN's goal is to use the IETF's proposed Internet Security Protocols (IPSec) specifications to ensure secure interoperability among firewall, network equipment and TCP/IP stack vendors. In the past, implementing Virtual Private Networks in an organi-

THE S/WAN INITIATIVE

Secure, vendor-neutral virtual private networking

- Checkpoint Software
- FTP Software
- Gemini
- IBM
- Morningstar
- NIST
- Raptor
- RSA Data Security
- Secure Computing
- SOS
- TimeStep
- Trusted Information Systems



S/MIME INDUSTRY SUPPORT

Secure, interoperable electronic mail

- Attachmate
- Banyan
- ConnectSoft
- Deming Software
- EIT
- Frontier Technology
- FTP Software
- Globalkey
- IBM
- JetForm
- Lotus
- Microsoft
- NCD
- Netscape
- Northern Telecom
- OpenSoft
- Pemail
- Premenos
- RSA Data Security
- QUALCOMM
- V-One
- VeriFone
- VeriSign



security for their various e-mail platforms. And since it's based on the popular Internet MIME standard, S/MIME users can peacefully co-exist with their friends who still use older, non-secured MIME mailers.

*T*he RSA-based SET standard was developed by MasterCard and Visa International to define a specific suite of security measures for electronic bank card authori-

zation meant tying yourself down to a single-vendor solution. Not anymore. S/WAN allows customers to mix-and-match the best firewall and TCP/IP stack products to build secure VPN's.

zations transmitted over the Internet. SET is based on the Public Key Cryptography Standards, and has separate components for merchants, cardholders and member banks. Keep your eye on this one — scores of RSA/SET electronic commerce applications are coming online from your favorite vendors soon.

THE SET INITIATIVE

Secure, interoperable Internet bankcard transactions

- CommerceNet
- GTE Mobilnet
- IBM
- MasterCard
- Microsoft
- Netscape
- RSA Data Security
- SAIC
- Terisa Systems
- VeriFone, Inc.
- VeriSign, Inc.
- Visa International



1919

Cher Ami, a carrier pigeon flown by the U.S. Army Signal Corps during World War I, is shot through the breast on his last mission. Miraculously, he manages to return and deliver a message from Major Whittlesey's "Lost Battalion" that would save 194 men.



1922

During the Washington Naval Conference of 1921-22, U.S. Secretary of State Charles Evans Hughes uses information obtained by code cracker Herbert O. Yardley, to obtain a more favorable agreement on naval capital ships. He appears to be outsmarting the Japanese, but actually he is reading their negotiating position every day before he begins the negotiations.



R D S & P A R T N E R S

The most widely implemented and basic specifications for certificate-based encryption and authentication are PKCS — the Public Key Cryptography Standards. The PKCS were established in 1991 by a consortium of RSA and some of world's most important computer concerns, including Microsoft, Apple, Lotus, Sun, Northern Telecom, Digital and (of course!) M.I.T. PKCS provides systems designers with a low-level framework for building secure, interoperable applications that are platform independent.

↓ 1927–1933

Prohibition encourages international smuggling, and with it a growth in the use of cryptography by and against criminals. The FBI to this day runs a cryptanalytic office to deal with criminal cryptography.



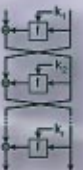
↓ 1941



British and Americans crack the infamous Enigma Machine. The code-breakers are assisted by an actual full-size reconstructed machine, requiring over 2,000 parts that were piece by piece stolen out of Germany, Poland and France by resistance forces.

↓ 1970, 1976

Dr. Horst Feistel, working for IBM, develops the Lucifer cipher, which would later inspire the whole family of so-called "Feistel ciphers". In 1976 an IBM design based on the Lucifer cipher is modified by the NSA and chosen as the US Data Encryption Standard (DES).

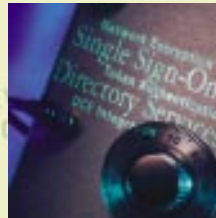


B I R D S O F

A

FEATHER:

S T A N D A



One of RSA's original licensees, **LOTUS DEVELOPMENT CORP.** has garnered rave reviews for *Notes*,[®] a product that quite literally coined the term "Workgroup Computing." Lotus Notes provides users with full RSA encryption and digital signature capabilities, and from the very beginning Lotus' security concept was certificate-based — even before the industry came together to establish the Public Key Cryptography Standards.

Other forms and workgroup computing packages that use RSA technology include Delrina PerForm Pro, F3 Software's Forms Automation System, Fischer International WorkFlow.2000, and WordPerfect InForms.

ORACLE CORPORATION has become the undisputed database juggernaut, partly due to the importance they place upon security. Their many product lines all utilize a common RSA-based security architecture. Oracle uses RSA's encryption technologies to build standards-based security mechanisms such as secure mail using S/MIME, web security with SSL and digital identities with X.509, and also provides cryptographic APIs to support RSA digital signatures and encryption. Products like Advanced Networking Option use the RSA RC4 encryption algorithm for end-to-end data protection of all network traffic. Oracle Mobile Agents uses public key technologies to provide a secure mobile data communications environment. Oracle's WebServer and PowerBrowser use RSA toolkits to implement the Secure Sockets Layer (SSL) protocol and protect web communications.

NETSCAPE is the undisputed leader in Internet browsers and servers, and from the very beginning has leveraged RSA security technologies to give them a competitive edge. Netscape's RSA-enabled *Secure Sockets Layer* (SSL) was the first protocol for secure electronic commerce on the expanding web scene, allowing Netscape users to buy products and send sensitive personal and financial information over the Internet. It proved to be an unbeatable competitive advantage, and though virtually all web browsers and servers now support RSA-SSL, Netscape has never lost its lead, dominating the worldwide market for browsers and servers.

1976 ↓



Stanford Professors Whitfield Diffie and Martin Hellman publish "New Directions in Cryptography," introducing to the world the idea of public key cryptography.

1977 ↓



Inspired by the Diffie-Hellman paper, MIT professors Ronald Rivest, Adi Shamir and Leonard Adleman (at the time complete novices in cryptography) discuss how to make a practical public key system. The result is the RSA algorithm: a practical public-key cipher for both confidentiality and digital signatures, based on the difficulty of factoring large numbers. It would lay the foundation of things to come.

1982 ↓



Kevin Mitnick breaks into the North American Air Defense Command (NORAD) computer.



R D S & P A R T N E R S



INTUIT is the leader in home banking and personal finance software. So when they wanted to expand their services to the Internet, naturally they called upon the leader in security. Intuit's *Quicken* offers advanced integrated banking solutions with participating financial institutions via the Internet featuring security based on state-of-the-art RSA encryption and authentication mechanisms. This also gives financial institutions working with Intuit an "instant Internet strategy" and the simplicity of a single link connecting them to customers who will be able to update and reconcile account activity, transfer funds and pay bills — with confidence. With advanced RSA-secured financial solutions like Intuit's, Internet banking is poised for an explosion.

MOTOROLA has always been active in the field of secure telecommunications. Their *Commercial Secure Telephone Units* (STU's) are available a variety of security levels and price points, and use several public and secret key algorithms, including RSA. Motorola's own internal Electronic Forms Routing and Approval project relies on implementations of RSA technology to provide private, tamper-proof electronic forms and document authorizations for tens of thousands of Motorola's employees. Other secure telephone and fax offerings using RSA technology are available from AT&T, Cycomm and ICTI/SCI.

Virtually every time you use a credit card, you use **VERIFONE**. Their credit-card "swipe" terminals are everywhere. And soon, a cyber-equivalent of those terminals will be available everywhere you can access the Internet, thanks to their partnership with RSA. VeriFone uses RSA's Secure Electronic Transaction (SET) security toolkits in its SET-compliant *vWALLET*, *vPOS* and *vGATE* Web software products for Internet-based electronic bankcard transactions. *vGATE* will enable acquiring banks and other payment processors to interface with the Internet, *vPOS* will enable merchant Web servers to process purchases, and *vWALLET* will allow consumers to interact with electronic payment systems via the World Wide Web. VeriFone's leadership in electronic payment systems and RSA's expertise in cryptography and tools allow customers to receive secure, robust, and tested SET solutions.

1982

RSA Data Security, Inc. is founded by Rivest, Shamir and Adleman, the inventors of its revolutionary algorithm.



1983

On Sept. 20, U.S. Patent #4,405,829 for "Cryptographic Communications System And Method" is issued to RSA.



1985

A brokerage firm margin clerk alters computer records to transform 1,700 shares of Loren Industries' stock into shares for another company, Long Island Lighting — which sold for more than ten times the price.

1986



Cliff Stoll, a systems administrator at Lawrence Berkeley Labs, uncovers intrusions into the Labs' computer network while investigating a 75-cent billing anomaly.

STRENGTH IN NUMBERS

R S A

In 1990, RSA Laboratories was split off from RSA Data Security as a completely independent division of the Company with three goals in mind: first, to provide a productive environment for RSA's top mathematicians, away from the distractions of the product development and marketing activities of the commercial arm of RSA. Second, to maintain the Company's reputation at the top of the fields of cryptographic research and algorithmic development. And third, to provide a purely technical (i.e. non-sales-oriented) resource for clients needing custom algorithms, optimizations, or security reviews and development.

The resources and services available through RSA Laboratories were originally conceived to be unique in the

industry—a “crypto shop for the rest of us”—to provide access to personnel and expertise that heretofore were only available at the best universities, the very largest computer corporations or the most impenetrable intelligence agencies. RSA Laboratories continues in this vision through its research program, its publications and seminars, and its expert assistance to RSA Data Security and its customers.

Research Program. RSA Laboratories is active in a wide range of areas in today's cryptography, with ties to research at universities and laboratories throughout the world. Its scientists have a strong academic profile both as members and chairs of conference program committees and as participants in international research programs. RSA Laboratories also coordinates the development of the

popular intervendore Public-Key Cryptography Standards.

Publications and Seminars. Bringing the latest research to the development community, RSA Laboratories' Cryptobytes newsletter features invited articles from researchers throughout the world. The annual Seminar Series does the same interactively, gathering leading researchers and leading developers for strategic interactions that will shape cryptographic R & D for years to come.

Expert Assistance. RSA Laboratories leads the design of new cryptographic technology for RSA Data Security, and offers similar critical advice to customers. RSA Laboratories' assistance covers a wide range of services, from architecture design to cryptanalysis to optimized software implementation.

↓ 1988

First National Bank of Chicago loses \$70 million in a computerized heist.

FIRST CHICAGO NBD

↓ 1989

After a 17-month investigation, US Officials confront French diplomats with evidence of espionage operations against IBM, Texas Instruments and Corning.

↓ 1990

An International Data Encryption Algorithm (IDEA) is proposed by Xuejia Lai and James Massey as a successor to DES. IDEA utilizes a 128-bit key and is more efficient than DES.

↓ 1990

Charles H. Bennett, Giles Brassard, et al. release their research findings on Quantum Cryptography, based on the laws of quantum physics. This system would provide secrecy as well as a positive indication of eavesdropping, with an indication of how much information may have been captured by the eavesdropper.

L A B O R A T O R I E S

The RSA Public Key Cryptosystem is recognized worldwide as one of the most secure cryptographic technique commercially available. To understand why RSA is so strong, you need to understand a bit more about the math. RSA public and private keys are actually each made up of two numbers: an exponent and a modulus (which is the product of two large prime numbers). The best course for an attacker to take is to attempt to factor the modulus back into its two component primes, thereby enabling him to derive the private key. But factoring is one of the most fundamentally difficult mathematical tasks. For example, using the best available techniques, factoring a single typical 768-bit RSA modulus would require 100 million MIPS years of computer time. And because of the nature of the RSA algorithm, advances in computer speed actually make RSA more secure — since larger keys can be used more efficiently than they can be factored.

↓ 1993



Grass-roots outrage over the government's proposed Clipper Chip forces the administration to back pedal on its encryption policy.

↓ 1995

RSA releases the fastest and most robust algorithm of its kind, the RC5 symmetric block cipher.



↓ 1995

SATAN, an automated hacking program, is released into the public domain. Thousands of Internet sites are attacked in the subsequent weeks, sending systems administrators into a panic.



T H E S C I E N T I S T S O F R S A



DR. BURTON S. KALISKI, JR.

CHIEF SCIENTIST

Dr. Kaliski received B.S., M.S., and Ph.D. degrees in Computer

Science from MIT in 1984, 1987 and 1988 respectively. In 1989 he joined RSA Data Security. His research interests include cryptography and fast arithmetic techniques. Dr. Kaliski is a member of the IEEE Computer Society, the Internet Privacy and Security Research Group, Sigma Xi, and Tau Beta Pi. He is also chair of IEEE P1363, a working group developing standards for public key cryptography, and is program chair of CRYPTO '97.



DR. MATTHEW J. B. ROBSHAW

SENIOR RESEARCH SCIENTIST

Dr. Robshaw received his First Class Honours Degree in Pure Mathematics from St. Andrews University, Scotland, in 1988, and his Ph.D. from the University of London in 1992. In 1993, Dr.

Robshaw joined RSA Laboratories. His research interests are focused on symmetric encryption techniques and cryptanalysis. Dr. Robshaw is a member of the organizing committee for EUROCRYPT '91 and SEI '97, and also a member of the IEEE and the International Association for Cryptologic Research.



DR. YIQUN LISA YIN

RESEARCH SCIENTIST

Dr. Yiqun Lisa Yin received her B.S. in Applied Mathematics from Beijing University, P. R. China, in 1989, and her Ph.D. in Applied Mathematics from MIT in 1994. In summer 1994, Dr. Yin joined

RSA Laboratories as a research scientist. Her research interests include cryptography and related areas in theoretical computer science. Dr. Yin is a member of IEEE and the International Association for Cryptologic Research, and is co-editor of the IEEE P1363 working group.



DR. RAYMOND M. SIDNEY

RESEARCH SCIENTIST

Dr. Sidney received his A.B. in Mathematics from Harvard College in 1991 and his Ph.D. in Mathematics from MIT in 1995. After working briefly at Trusted Information Systems, Inc. and D. E. Shaw

& Co., L. P., he joined RSA Laboratories as a research scientist in the fall of 1996. His primary research interests are cryptography, complexity, and information theory.

↓ **Winter 1996**

RSA licensee list tops 200 companies; more than 75 million copies of RSA encryption engines are installed and in use worldwide.



RSA establishes Nihon RSA, a wholly-owned RSA subsidiary company in Tokyo, providing developers in Japan with access to RSA's full suite of encryption technology — including the BSAFE and TIPEM toolkits.

↓ **Spring 1996**

↓ **Summer 1996**

Security Dynamics agrees to acquire RSA in a stock swap valued at over 200 million dollars, bringing together two giants of the security industry.



SecurityDynamics.

LABORATORIES



DR. RONALD L. RIVEST
DISTINGUISHED ASSOCIATE

Dr. Rivest is the Webster Professor of Electrical Engineering

and Computer Science at the Massachusetts Institute of Technology, an associate director of MIT's Laboratory for Computer Science, and a leader of that lab's Cryptography and Information Security research group. He received a B.A. in Mathematics from Yale University in 1969, and a Ph.D. in Computer Science from Stanford University in 1974. He is a Fellow of the Association for Computing Machinery and of the American Academy of Arts and Sciences, and is also a member of the National Academy of Engineering. Dr. Rivest is an inventor of the RSA Public Key Cryptosystem and a founder and director of RSA Data Security, and has also served a director of the International Association for Cryptologic Research.



DR. LEONARD M. ADLEMAN
DISTINGUISHED ASSOCIATE

Dr. Adleman received a B.S. in Mathematics and a Ph.D. in Com-

puter Science from the University of California at Berkeley in 1968 and 1976, respectively. He was an assistant, then an associate professor at the Massachusetts Institute of Technology from 1977 to 1979, where he helped invent the RSA Public Key Cryptosystem. He has been the Henry Salvatori Professor of Computer Science at the University of Southern California since 1985, and has taught there with tenure since 1980. His research interests include computational complexity, number theory, molecular computation, molecular biology, immunology and computer viruses. Dr. Adleman is a member of the National Academy of Engineering.



PROF. CLAUD P. SCHNORR
DISTINGUISHED ASSOCIATE

Prof. Schnorr studied mathematics and physics at the Univer-

sity of Saarbruecken, receiving a Ph.D. in 1967 and a Habilitation in Mathematics in 1970. He was a professor at Saarbruecken in 1970, and at Erlangen in 1971. Since 1971 Prof. Schnorr has been a full professor of mathematics at University of Frankfurt a.M., and since 1986 also a professor of computer science. Prof. Schnorr has also been a visiting professor at several universities including Stanford, Berkeley, ENS Paris, and the University of Chicago. Prof. Schnorr has a number of notable contributions in cryptography, including the identification scheme bearing his name. He is also the recipient of the Gottfried Wilhelm Leibniz award.

↓ August 1997

RSA celebrates its
15th anniversary





RSA Data Security, Inc.
A Security Dynamics Company
100 Marine Parkway, Suite 500
Redwood City, CA 94065-1031

Tel. 415/595-8782
Fax: 415/595-1873
Internet: info@rsa.com
Web: <http://www.rsa.com>



SecurityDynamics