# Cryptography and the New Economy

Today, e-commerce occupies everyone's mind—merchants, programmers, bankers, and consumers. Three to five years

ago, the then-fledgling industry was struggling to convince the public to make purchases and do financial transactions online. A key element that the industry needed to address was the public's concern about the security of online processes and transactions. The science of modern cryptography-a field based on advanced mathematical concepts that include number theory and group theory—was identified as a vehicle for securing public confidence in the safety of e-

commerce transactions. The effective application of cryptographic mathematics to ecommerce has proved to be a key factor in its current level of acceptance.

Modern cryptography is a relatively new field. Before 1970, the world of encrypting and decrypting messages was primarily a black art practiced by government security agencies and the military without a consistent framework. The early to mid-1970s saw the emergence of mathematical cryptography, which provided a robust theoretical framework for encryption and decryption that enabled cryptographers to predict the security of messages.

## Classes of cryptography

Mathematical cryptography is categorized into two broad areas: symmetric key and public key. Symmetric-key cryptography assumes that two or more parties are privy to a common number or set of numbers for encrypting and decrypting information, which is known as the key. The best known example of symmetric-key cryptography is the Data Encryption Standard (DES), which is essentially an algorithm for scrambling information sent online, such as financial data. The advantages of DES are its simplicity and speed. The sender and

receiver use the same key to scramble and

unscramble a message, and DES can scram-

ble large amounts of information extremely

fast. The main problem of DES is the need

to tightly manage the distribution of the key

in multiparty networks. Clearly, the more

people who know the secret key, the greater

Public-key cryptography is a more recent

development that effectively addresses the

key-management issue. Unlike DES, this

technique requires two keys, a public one

for encryption and a private one for decryp-

tion. In a multiparty situation, such as an

internal network at a corporation, everyone

has his or her individual keys. The encryp-

tion, or public key, can be made available to

anyone; a person who wants to send confi-

dential information to someone else would

get that person's public key and use it to

encrypt a message. The decryption, or pri-

vate key, is intended for the recipient's use

only and is never disclosed. If a sender uses

the recipient's public key to encrypt the

message, then only the recipient can deci-

pher the information. This is because the

private key will recognize an individual's

the risk of a breach in security.

public key through a set of mathematical relationships that link the two.

The most commonly used public-key system is RSA (Rivest-Shamir-Adel-

man, named for the inventors of the technique). In the RSA system, the mathematical problem that one must solve to break the encryption is to factor a very large integer into its two prime numbers (integers used in RSA have only two prime factors). However, elliptic curve cryptosystems (ECCs) are an emerging and potentially dominant approach. Breaking an ECC requires determining the number of times

that a seed value, a known point on an elliptic curve, is multiplied in order to get to another point on the same elliptic curve. Both techniques are based on the branch of mathematics called number theory.

In practice, the symmetric-key and public-key systems are not in competition. Most cryptographic schemes on which ecommerce operations rely use a hybrid of the two systems to exploit the key-management flexibility of a public-key system and the fast scrambling speeds of symmetrickey systems. This hybrid approach is often called key wrapping.

During the past few years, computer protocols and application techniques have been developed that make the implementation of encryption mathematics more convenient for programmers. Protocols operate at a higher level of abstraction than DES or ECCs, and from these protocols, we get phrases now infiltrating the technology lexicon. These terms include *public-key infra structure* (PKI), which is a comprehensive way to manage the online identification and encryption processes of an entire organization; *digital signature*, an identifier unique

29 The Industrial Physicist

to an individual; and *certificate authority* (CA), which is the industry-established system that certifies to buyers that an online business is legitimate.

Until a few years ago, modern cryptography was the exclusive domain of pure mathematicians working for universities, the military, and government agencies. When the business world embraced encryption, we began hearing acronyms such as PKI and CA. In fact, cryptography has emerged as one of the hottest areas in so-called enterprise computing. Today, some of the largest conferences in mainstream computing are on cryptography. The RSA Conference, the Entrust SecureSummit Conference, and the Certicom Public Key Solutions Conference are examples of annual events at which thousands of people gather to discuss cryptography.

Many number theorists once boasted that they could see no possible way that the purity and beauty of their research area could ever be tainted by military or commercial applications. Unfortunately for them, the adoption of number theory to cryptography represents perhaps the most profound integration of abstract theory into everyday life in recent history.

## Everyday applications

To appreciate the impact of cryptography on daily life, one needs to better understand some of its key commercial applications. Internet sales and mobile commerce are two prominent examples.

Most reputable players in Web-based ecommerce share a common framework of cryptographic protocols. Many use a protocol known as the Secure Socket Layer (SSL), which Netscape pioneered for e-commerce. This particular protocol has enabled many transactions to take place online, from the simple purchasing of goods to banking and bill paying. Through SSL, users can positively identify a Web site as being reputable and know that they are sending confidential information, such as credit card numbers, through a secure, encrypted system.

SSL is a variation of public-key encryption. It uses RSA-based digital signatures, which are analogous to a personal signature, to identify online users. The software for SSL is typically embedded in computer browsers and the server software of e-commerce sites.

Supporting the RSA routines is the DES symmetric-encryption scheme, which performs the actual encryption of credit-card numbers or other data. In most of the world, the DES encryption strength is 56 bits (the number of bits indicates the size of the key; the more bits, the stronger the encryption power). However, the National Institute of Standards and Technology will soon announce a new standard called the Advanced Encryption Standard, which has a strength of 128, 192, or 256 bits.

A recent e-commerce phenomenon involves the convergence of Internet access with small and often wireless devices such

### USING YOUR CREDIT CARD ON THE WEB

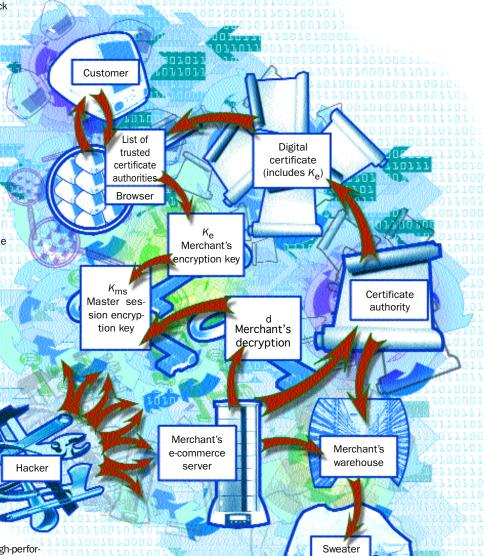
If you want to buy a sweater on the Web, the personal details you enter on your computer and send to the merchant are encrypted with a key number that is virtually impossible for a hacker to find.

**SETTING UP SHOP.** In a commonly used public key system called the RSA system, when a merchant sets up for e-commerce, two random large prime numbers, p and q, are chosen, and the product pq = n is calculated. The product n is used to generate a public encryption key number,  $K_e$ , and a private or secret decryption key number,  $K_d$ . In the next stage, an industry-trusted certificate authority endorses the merchant's identity by taking  $K_e$  and other merchant information, and digitally "signing" it. Mathematically, this step is roughly equivalent to raising the information to the power of the numerical value of  $K_d$ . This creates a "certificates, each one corresponding to a merchant. During a transaction, these certificates may be sought via the Web to positively identify a merchant.

**STARTING A TRANSACTION.** When a customer begins the checkout process at a Web site, his or her computer automatically sends information about the browser to the merchant's computer, which sends its certificate, signed by a certificate authority, to the customer. The certificate includes the merchant's  $K_e$ . The customer's computer checks the merchant's certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded collection of certificate and  $K_e$  against his browser's preloaded co

cates from recognized and trusted certificate authorities. If the merchant's particulars check out, the customer's computer mathematically encrypts its own identifying key information  $(n \text{ and } K_e)$  with the merchant's  $K_e$ , and the customer generates a secret number,  $K_{\rm s}$ . This is sent back to the merchant's computer, encrypted with the merchant's n and  $K_{e}$ . The merchant can decrypt the secret number using his K<sub>d</sub>. Both computers now share a common secret number,  $K_{\rm s}$ , that can be used as the master session key for the symmetric-encryption step. A secure channel is established. All information (e.g., the credit card number) is encrypted using this session key when entering the channel and is decrypted when leaving the channel. Once the transaction is completed, the session key is destroyed on both ends.

WHY WE ARE SAFE. To break the encryption, a hacker would need to access the data channel at particular steps of the process, understand and perform the complex mathematical backtracking to expose the product n = pq, factor n, and then derive the merchant key  $K_{d}$ , which would allow him to recover the session key and retrieve sensitive information. The problem for the hacker is that the successful factoring of *n* is virtually impossible. A recent empirical test-the Certicom Challenge (Hayward, California)-showed that cracking even a single test or simple encryption required performing hundreds of trillions



of iterations of the mathematics on 9,500 high-performance computers from 40 countries running in a coordinated fashion over four months. These test encryptions are considered 100 million times weaker than commercial grade encryption. Thus, with today's technology and knowledge, there are not enough accessible computers and personnel to manage efficient cracking of commercial-grade encryption. However, if unauthorized people get access to some of this information, there is a vulnerability.

01 00 00

Chris Gregor

as mobile phones, hand-held computers with modems, two-way pagers, and hybrids that embody two or more of these technologies. Inexpensive, useful information services are now available to help people look up telephone numbers, buy and sell stocks, and carry out other time-critical tasks anywhere that is served by appropriate wireless services. In some respects, the need for cryptographic security is even greater for these uses because wireless channels are less secure than wired channels.

Protocols based on ECC are becoming the standard for the information-authenticating step for wireless devices. Functionally, ECC is similar to the more established RSA system. However, commercial versions of ECC offer key sizes that are an order of magnitude smaller than an RSA of equivalent strength, and thus, they provide shorter computation times for some operations. This greater efficiency is critical for bandwidth-limited and battery-operated devices. Certicom (Hayward, CA) is the commercial leader in ECC implementations, although other companies are beginning to offer their own versions. Companies that have deployed ECC-based security in their products include 3Com's Palm Computing division in its Palm VII device, and Research in Motion's Blackberry pager system, which is offered through partnerships with service providers such as Bell South.

Cryptography will form the foundation for e-commerce security in the foreseeable future. Confidence in cryptographic theory and technology is high, and we should not expect to see fundamental changes. The most interesting developments are likely to come on the applications side. As advanced cryptography becomes easier to implement and manage, more companies and organizations will take advantage of its benefits.

### For further reading

Schneier, B. Applied Cryptography; Wiley: New York, 1995; 784 pp.; ISBN 0-471-12845-7.

Menezes, A. J.; Van Oorschot, P. C.; Vanstone, S. A. *Handbook of Applied Cryptogra phy*; CRC Press: Boca Raton, FL, 1996; 816 pp.; ISBN 0-849-38523-7. A number companies, such as Certicom (www.certicom.com) and RSA Security (www.rsa.com) offer white papers on various aspects of cryptography. The more adventurous may wish to try implementing some of the algorithms. An ideal platform is a comprehensive interactive mathematics package such as Maple 6. The Maple 6 Application Center (which is online at www.maplesoft.com/apps) also offers several good examples of using this package for cryptographic applications.