The word Cryptology derives from the Greek 'cruptos', meaning hidden, and 'logos', meaning study or science, and literally implies the science of keeping secrets. Cryptography is an area within the field of cryptology, deriving from the Greek 'kryptós graphe', meaning secret writing. Cryptography is the science and study of creating and using systems for communicating in secret via communication channels that are not secure. A sender maintains this secrecy by transforming data, known as plaintext, into an unintelligible form, known as ciphertext, in a process known as encryption, or encipherment. The receiver recovers the original plaintext using the inverse process of converting ciphertext to plaintext; this procedure is known as decryption or decipherment. A cryptographic key controls both the encryption and decryption processes (Figure 1).
Figure 1: The cipher process

Current Digital Cryptography Requirements
In today's electronic age, the importance of digital cryptography in securing electronic data transactions is unquestionable. Every day, users electronically generate and communicate a large volume of information with others. This information includes medical, financial and legal files; automatic and Internet banking; phone conversations; pay-per-view television; and other e-commerce transactions. The following examples, as well as many other applications, require a great deal of security in the storage and transportation of this information. By using various digital-cryptography techniques, people and organizations can secure electronic information to protect economic interests, prevent fraud, and guarantee the privacy of individuals.

Voice Communications
There is a potentially significant market for high-strength encryption on VoIP, wireless phone, and land-line phone communications. The perceived threat of eavesdropping is a powerful market driver in the world of personal communications. Expect Nokia, Ericsson, Samsung, Motorola, TI, Casio, and the other major phone makers to move in, along with a cadre of startups that hope to provide the IP. Once one major vendor offers encryption on a popular phone then, rapidly, every other vendor will be forced to follow suit or lose business to competition. In the space of 18-24 months, encryption mode will become the default talk mode. Expect every VoIP system and land-line phone to gain this functionality as well.

Network Appliances
Another potentially large market for digital encryption is network appliances—anything electronic that is interactively hooked up to a network. As the number of non-PC and wireless devices accessing the Internet increases, the rate of cyber attacks on network infrastructure and service providers will increase. Critical functions such as power-grid management and water-distribution systems are shifting to the Web and need to be protected. Even simple appliances such as fire alarms or temperature alarms can be vulnerable to hacker attacks. There is great value in preventing a hacker from electronically yelling, “fire”.

Virtual Private Network (VPN)
VPNs protect direct connections between users and enterprise networks. The high cost of dedicated telecom links compels transition from software to hardware support for these links. Dedicated lease lines are relatively private and secure, but it's too expensive to give everyone a private line. Putting encrypted VPN traffic on public lines is less expensive. While few individual users require a dedicated connection at Gbit/sec speeds, the ballooning number of VPN users means a corporate
LAN will need to aggregate and process encrypted data streams in the gigabit range now, and in the multi-gigabit range in the near future.

**Secure Socket Layer (SSL)**
SSLs provide security using the Secure Socket Layer protocol for Internet browser-based transactions (in other words, SSL is Web specific). The presence of encryption on a Web site is often the deciding factor whether to make an online transaction; no company wants to lose business for lack of a secure connection. As bandwidth requirements go up, it is vital to include a resident SSL hardware accelerator in the data center to encode and decode traffic going in and out of the Web site.

Note that SSL processing currently works from a suite of algorithms including DES, 3-DES, IDEA, RC-2, and RC-4 (plus digital signature algorithms such as SHA and MD5). It is too early to tell whether AES will simply be added to SSL ciphers or used to replace the other algorithms altogether. It is important to realize that the NIST (National Institute of Standards and Technology) selection team decided against a multiple-algorithm AES. One of the primary reasons is that multiple AES key sizes provide increased levels of security. Another primary reason is that a single-algorithm AES decreases the complexity of implementations that will be built to comply with the AES specifications, thereby lowering costs and promoting interoperability.

**Introduction to Digital Cryptography**
Digital cryptography is a set of protocols, algorithms, and techniques providing security for digital information by encoding and decoding the information using a specific key. Digital cryptography methods have two basic objectives:

- **Privacy** to prevent the unauthorized disclosure of data
- **Authenticity** to prevent the unauthorized modification of data.

Encryption techniques use complicated algorithms to transform digital information from plaintext to ciphertext. Every time the encryption key is changed, the ciphertext will be different, although the algorithm stays the same. The relationship between the encryption and decryption keys classifies the encryption methods in one of two distinct categories: symmetric and asymmetric encryption.

**Symmetric Encryption**
Symmetric encryption is a traditional way of encrypting (also called Private Key Encryption), where the encryption and decryption keys are the same. This method is faster and easier to implement than asymmetric encryption, since the sender and the receiver use the same key to transmit and receive information. In addition, the key sizes are smaller in symmetric encryption compared to asymmetric algorithms. However, the private exchanging of the key between the sender and receiver is challenging. Both parties have to agree and trust on a communication medium such as a phone system to exchange the key. Examples of some common Private Key Encryption algorithms are:

- IDEA (International Data Encryption Algorithm)
- FEAL (Fast Data Encipherment Algorithm)
- DES (Data Encryption Standard)
Symmetric encryption is also divided into two groups: block and stream ciphers. Block ciphers work on blocks of data and are commonly used to encrypt the documents. You use stream ciphers to encrypt streams of data, such as chat programs.

**Asymmetric Encryption**
Asymmetric encryption is a method where the encryption and decryption keys are different. These systems are also called Public Key Encryption Systems, since the encryption key does not have to be a secret. The sender can publish the encryption key and anyone can encrypt messages going to the specific user. However, only the receiver can decrypt the message, since the decryption key cannot be generated with the knowledge of the encryption key. This method is slower and requires more computational power than symmetric encryption. Examples of some common Public Key Encryption algorithms are:

- **RSA (Rivest-Shamir-Adelman)**
- **Diffie-Hellman**

**Hacker Attacks and Cryptanalysis**
Cryptanalysis is the science and study of breaking ciphers. A cipher can be broken if it is possible to determine the plaintext or the key from the ciphertext, or if someone can determine the key from plaintext-ciphertext pairs. The attempt to find the key in encryption algorithms by brute force requires a very long time. The longer the key length, the more immune the key is against the brute force attacks. A cryptanalysis attack is an attack by an intruder trying to discover the contents of an encrypted message or the secret key by means other than a straightforward random attack. The three methods of attack are:

- Ciphertext-only
- Known-plaintext
- Chosen-plaintext

These methods have been successful against some of the different encryption algorithms such as: DES, FEAL-4, FEAL-8, FEAL-N, and LOKI. With the advances in today's computer power, some of the older algorithms are susceptible to variety of cryptanalysis attacks. Therefore Triple DES (3-DES) with 168-bit key length has become more popular. The 3-DES algorithm provides high security and has been proven to be immune to hacker attacks. However, this method requires a high computational complexity that makes it complicated to implement. For this reason, the Advanced Encryption Standard (AES), offering the same or higher level of security as 3-DES with more efficiency and less computational complexity, is replacing its encryption predecessors.

**Advanced Encryption Standard (AES)**
In September 1997, the NIST issued a request for possible candidates for a new AES to replace the DES. In August 1998, NIST selected 15 candidate algorithms and in August 1999, announced five
finalists: MARS, RC6, Rijndael, Serpent, and Twofish. On October 2, 2000, the NIST selected the
Rijndael algorithm\(^1\), developed by Joan Daemen and Vincent Rijmen, as the winner of the AES
development race. In performance comparison studies carried out on all five finalists\(^2\), Rijndael
proved to be the fastest algorithm and also achieved very efficient hardware utilization. Therefore, it
is believed that Rijndael can be used in many applications where a high level of security comparable
to 3-DES is desired but hardware and computational resources are limited.

**Rijndael Algorithm**

The Rijndael algorithm is a symmetric iterated block cipher. The block and key lengths can be 128,
192, or 256 bits. The NIST requested that the AES must implement a symmetric block cipher with a
block size of 128 bits. Due to this requirement, variations of Rijndael that can operate on larger
block sizes will not be included in the actual standard. Rijndael also has a variable number of
iterations or rounds: 10, 12, and 14 when the key lengths are 128, 192, and 256 respectively. The
transformations in Rijndael consider the data block as a four-column rectangular array of 4-byte
vectors. The key is also considered to be a rectangular array of 4-byte vectors \[\text{the number of}
columns is dependent on key length.}

**Figure 2:** Block diagram representing the Rijndael algorithm

Rijndael decryption comprises the inverse of the transformations that encryption uses, performed in
reverse order. Decryption commences with the inverse of the final round, followed by the inverses of
the rounds, and finishes with the initial data/key addition, which is its own inverse.

Industry AES Solutions

Due to the broad range of applications that Rijndael algorithm can support, it is important to have
multiple versions of Rijndael-based products. AES solutions are currently available in four different
versions:

- **Standard**
  The Standard version provides data rates of up to 500 Mbits/sec and is appropriate for applications
  such as VoIP.

- **Compact**
  The Compact AES products are perfect solutions for wireless applications, such as PDAs and cell
  phones, where power and area minimization are crucial.

- **Fast**
  The Fast version goes up to 2000 Mbits/sec and is suitable for VPN security products incorporated
  into broadband switches, routers, firewalls, and remote-access concentrators.

- **Very Fast**
  Very Fast AES products target applications with data rates faster than 2000 Mbits/sec.

**Figure 3** illustrates an application of Standard AES products needed to secure VoIP systems.
**Figure 4** demonstrates another practical example using Fast AES solutions in a secure wireless video-communication system.

**Figure 3:** Example of a secure VoIP system using AES

**Figure 4:** Example of a secure wireless video-communication system using Fast AES solutions

Digital cryptography has become a de facto standard for today’s electronic data transactions. AES has proven to be more secure and efficient than its encryption predecessors. Among AES algorithms, Rijndael has proven to be an extremely fast, state-of-the-art, easy to implement, and highly secure algorithm. Various AES products are available to cover the need for different applications based on their speed, size, and power consumption.

**Editor’s Note:**
Amphion offers four different sets of Rijndael AES cores—Standard, Compact, High Speed, and Ultra High Speed—for ASIC and programmable-logic implementations. You can design these cores into VPN chips for systems targeting broadband switches, routers, firewalls and remote access concentrators, along with chips for SSL applications.

Jim Lipman, Content Director, TechOnLine

About the Author
Faranak Nekoogar is Technical Marketing Manager for Amphion Semiconductor and is a PhD candidate in Wireless Communications at the University of California, Davis. Ms. Nekoogar is co-author of the upcoming book "From ASICs to SOCs—a Practical Approach to Design and Verification," Prentice Hall, 2001.