

Auditors need a working knowledge of encryption to provide assurance that it is helping secure data.

Encryption Essentials

Albert J. Marcella Jr.

Encryption is essential to establishing strong security and internal controls in an increasingly wired and privacy-conscious world. The principles, dynamics, functionality, and the art and science of encryption may cause auditors who aren't familiar with it to dread and avoid examining their organization's implementation and application of encryption, as one element of an overall defense-in-depth strategy.

Internal audits of an organization's encryption policies, practices, and procedures are an important step in assessing its procedures and internal controls for protecting data. If implemented and used appropriately and proactively as part of its data management and security structure, encryption can enable greater defense in depth and strengthen internal controls over critical enterprise data.

When examining encryption policies, practices, and procedures, internal auditors should review both encryption's technical and nontechnical aspects. To do this, auditors must have a complete understanding and working knowledge of the basics of encryption—the theory, concepts, and terminology of the various components—and how the encryption process works. Such an understanding will enable auditors to recommend to management the most appropriate,

logical, and technically correct solution to this important aspect of enterprise-wide security.

BEHIND THE JARGON

The discussion of encryption involves terms that are important to understanding how it works. *Cryptology* is the scientific study of cryptography. *Cryptography* is the process of converting plain text into a cipher or encrypted text using an algorithm, making the resulting text unreadable without a decoding key. A *cipher* is a way to make a word or message secret by changing or rearranging the letters in the message.

The process of converting a plain text message to its cipher text form is called *enciphering* (see “Enciphering Plain Text Into Cipher Text” on this page). Reversing the process, converting enciphered text into plain text, is called *deciphering*. The intended recipient must use a decoding key to un-encrypt the text and convert it back into plain, comprehensible text. There is a low probability that anyone without the decoding key would be able to un-encrypt the original plain text.

Public Key Infrastructure (PKI) is a framework that enables various services related to cryptography to be integrated. PKI enables organizations and users to manage keys and certificates, which are used for identification,

entitlements, verification, and privacy. By managing keys and certificates through a PKI, an organization establishes and maintains a secure and trustworthy networking environment that allows information and money to be exchanged safely and securely. The aim of PKI is to provide confidentiality, integrity, access control, authentication, and nonrepudiation over transactions, email, and communications enacted by, between, and through discrete users.

ELEMENTS OF ENCRYPTION

The quickest, easiest, and most straightforward way to gain an understanding of encryption is to examine each component of the encryption process. These components and the definitions represent the essential elements that an auditor will typically encounter when working with encryption and decryption systems. Moreover, a review of these elements will better enable auditors to correctly answer the encryption challenge (see “The Encryption Challenge” on page 57).

Authentication. Assurance that a message has not been modified in transit or while stored on a computer. NetAction’s Guide to Using Encryption Software refers to this as message authentication code or the message’s data integrity.


TO COMMENT
 on this article,
EMAIL the
author at
 albert.marcella@
 theiia.org

ENCIPHERING PLAIN TEXT INTO CIPHER TEXT

Plain Text	This is a secret message that I only want to share with authenticated recipients
Cipher Text	ATRCiekINIUCGF6S3bzPf6JTiaVQCf05+z+p+cHrdMI4TCQePWtdaxHPXAIEdBz4A+eOOWF/IWuXHzNmqb3M0wSDEshgYYtwjSq01X+aiH1yeeRQajB1nqYRIWhNXSobse9FPT+KB7Zzwm66aAafkQYbMp/AeyTtbMfr-vOeWoRg=

Encrypted Secure Sockets Layer network traffic doubled in North America and quadrupled in Europe in the past year, according to a report from Canadian broadband company Sandvine.

Certificate. Proves the identity of a user or device seeking to access the network. It ensures that the entity has provided correct information and is the owner of the public key, according to the Oracle 9i Security Overview. A certificate is created when an entity's public key is signed by a trusted identity, such as a certificate authority. It contains information such as:

- The certificate user's name.
- An expiration date.
- A unique serial number assigned by the certificate authority.
- The user's public key.
- Information about the rights and uses associated with the certificate.
- The name of the certificate authority that issued the certificate.
- The certificate authority's signature.
- An algorithm identifier that identifies which algorithm was used to sign the certificate.

Certificate Authority. An authority in a network that issues and manages security credentials and public keys for message encryption, according to SearchSecurity.com. A certificate authority consults with a registration authority to verify information provided by the requestor of a digital certificate. Once the information is verified, the certificate authority can issue a certificate. The certificate includes the owner's public key, the expiration date of the certificate, the owner's name, and other information about the public key owner.

Confidentiality. Provides assurance that only owners of a shared secret key can decrypt a computer file that has been encrypted with the shared secret key. Confidentiality is ensured because only individuals who know the key will be able to read the encrypted message.

Cryptographic Keys. U.S. National Institute of Standards and Technology Special Publication 800-57 (July

THE ENCRYPTION CHALLENGE

A **corporate requirement** in the form of securing email transmissions illustrates the essential components and process of encryption. A user wants to send an email from point A to an intended recipient at point B. The user requires that the email's contents remain confidential and viewed only by the recipient, while the recipient expects to be able to authenticate the sender and ensure that the sender cannot deny having sent the email.

The internal auditor's challenge is to recommend a solution that identifies all necessary elements in their appropriate order, sequence, and relationship. This solution must allow the sender and recipient to achieve confidentiality, integrity, authentication, and nonrepudiation of any email exchanged between them.

See "Solving the Encryption Challenge" on page 59 for an answer to the challenge.

2012), Recommendation for Key Management—Part 1, General (Revision 3), identifies 19 different cryptographic keys, each used for a different purpose. In asymmetric key systems, there are a pair of keys that work in tandem: a private key and a public key. The most commonly used key types are:

- Private signature key—used by public-key algorithms to generate digital signatures with possible long-term implications. Private signature keys are used to authenticate the source of a key, protect its integrity, and ensure nonrepudiation of messages, documents, or stored data.
- Public signature-verification key—verifies digital signatures.
- Private authentication key—provides assurance of the originating entity's identity when executing an authentication mechanism as part of an authentication protocol run or when establishing an authenticated communication session.
- Public authentication key—provides assurance of the originating

entity's identity when executing an authentication mechanism as part of an authentication protocol run or when establishing an authenticated communication session.

Digital Certificate. A document signed by a trusted third party that is the preferred way to securely deliver public keys. The top part of a digital certificate contains plain text identifying the issuer (signer), subject (whose public key is attached), the subject's public key, and the expiration date of the certificate. The bottom part contains the issuer's signed hash of the top part.

Digital Signature. A small piece of code created by encryption software that is used to authenticate the data sender. A private key creates a digital signature, and a corresponding public key verifies that the signature was really generated by the holder of the private key.

Hashing. Used to encrypt and decrypt digital signatures. The hash function



VISIT InternalAuditor.org for additional encryption practice scenarios

SOLVING THE ENCRYPTION CHALLENGE

To answer the encryption challenge correctly, internal auditors must consider several essential elements of encryption, specifically digital signatures, hashing, and private and public keys.

The specific steps the sender should take are:

1. Create an initial message.
2. Calculate a hash value for the message.
3. Encrypt the hash with his or her private key.
4. Attach the hash to the message.
5. Sign the message with his or her digital signature.
6. Encrypt the message with the recipient's public key.
7. Send the message to the recipient.



The recipient of the email should:

1. Open the message by decrypting it using the recipient's private key.
2. Calculate a new hash value.
3. Decrypt the sender's hash using the sender's public key.
4. Compare the hashes. This provides assurance that the sender sent the message, as the sender's digital signature is attached to the message, which "binds" the sender as its originator. If there are any discrepancies in the hash values, the recipient cannot rely on the message's integrity.

This provides the recipient assurance that the message came from the sender, as the sender's signature is on the file, thus establishing nonrepudiation.

transforms the digital signature into a hashed value called the message digest; both the message digest and the signature are sent in separate transmissions to the receiver. Using the same hash function as the sender, the receiver derives a message digest from the signature and compares it with the message digest it also received to ensure their contents are the same.

Integrity (or message authentication). Assurance that a file was not changed during transit.

Key. A piece of data used for encryption and decryption. Keys typically look like alphanumeric gibberish and are not human-readable.

Nonrepudiation. Assurance that the data sender has received proof of delivery and the recipient has proof of the sender's identity, so neither can later deny having processed the data. For


example, if a person has a digital signature that verifies with public key "K," then he or she knows that the associated private key was used to make that signature. Cryptographic nonrepudiation is provably achieved by all practical public-key cryptosystems.

Registration Authority. An authority in a PKI that verifies user requests for a digital certificate and instructs the certificate authority to issue it.

Secure Sockets Layer Authentication (SSL). Provides authentication, data encryption, and data integrity in a PKI through the exchange of certificates, which are verified by trusted certificate authorities. Authentication is performed using digital certificates and a public/private key pair. SSL typically is used to establish digital identities and to protect data and messages from eavesdropping, tampering, or forging.

PROTECTING CRITICAL ASSETS

A working knowledge of encryption definitions, concepts, and methodologies alone is not sufficient to assess internal controls for securing an organization's critical data assets. As part of a comprehensive internal controls review of enterprisewide data management and security procedures, auditors should examine encryption implementation procedures, policies, enforcement measures, general access controls, and access rights management procedures.

In today's always-on, globally connected society, it is imperative that organizations develop resilient information management strategies to protect their critical data assets. A robust, proactive cryptographic strategy and platform is an essential piece of a well-controlled and secure enterprise. 

ALBERT J. MARCELLA JR., PHD, CISA, CISM, is president of Business Automation Consultants LLC in Saint Louis.