Data Encryption

Module 4

Simplifying Security.

Certified Secure Computer User

Module 4: Data Encryption

Exam 112-12

Module Objective

Personal computers and portable computing devices often contain **confidential data** such as payment information, personal files, bank account details, and more, which must be shielded from prying eyes in the event of theft or loss of the device. This module teaches you how to protect the data with **encryption** to maintain confidentiality. This module will familiarize you with:

- Common Terminologies
- What is Encryption?
- Objectives of Encryption
- Types of Encryption
- Encryption Standards
- Symmetric vs. Asymmetric Encryption
- Usage of Encryption
- Digital Certificates
- How to Work Digital Certificates
- Digital Signature
- How Digital Signature Works
- Cryptography Too

Module Flow

Encryption

Types of Encryption

Encryption Standards

Digital Certificates

Digital Signature

Cryptography Tools

Common Terminologies

Plaintext:

In cryptography, plaintext is the ordinary, readable text from before being encryption into cipher text and is the result of decryption.

Cipher Text:

Cipher text is encrypted text that is unreadable until it has been decrypted to plaintext with a key. It is used to securely send messages over the Internet.

Encryption Key:

A key is a piece of information that can encrypt, decrypt, or perform both functions, depending on the type of encryption being used.

What is Encryption?

Encryption is the process of converting information, programs, images, and other data into an **unreadable** cipher text to prevent **unauthorized access** by applying a set of complex algorithms that transform the data into blocks or streams of random alphanumeric characters.

How Encryption Works

If Bob desires to send a secret message to Alice, he searches for Alice's **public key** in a directory, uses it to encrypt the message, and sends it to Alice. Alice then uses her **private key** to decrypt the message and reads it. No one else can decrypt the message. So, cryptography **secures the data against eavesdropping** or betrayal.

Anyone can send an encrypted message to Alice, but only Alice can read the message. Thus, although many people may know Alice's public key, and use it to verify Alice's signatures, they cannot discover Alice's private key and use it to forge digital signatures. This is referred to as the principle of "**irreversibility**."

Bob does a computation involving both his private key and the message to sign it. The outcome of this process is called a digital signature, which is attached to the message. The message is then sent to Alice. If Alice wants to check whether the given signature is genuine or fraudulent, she carries out a computation involving the message, the purported signature, and Bob's public key. If the result holds properly through the simple mathematical relation, the signature is genuine and the message has not been tampered with. However, if the signature is not genuine, it is likely that somebody has eavesdropped and altered it.

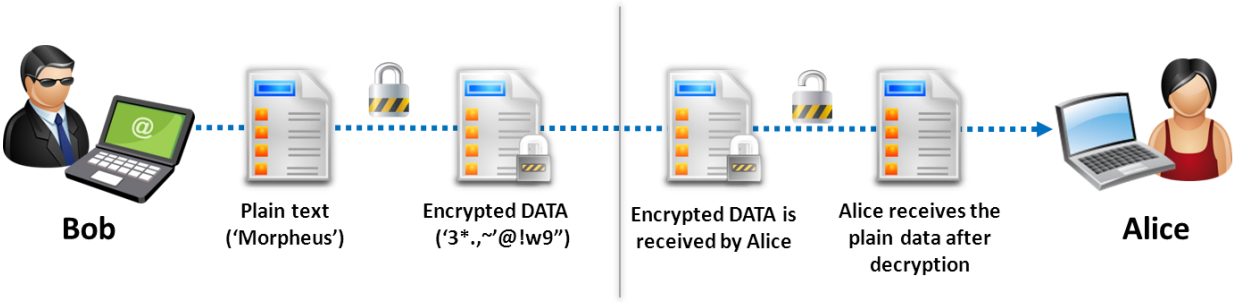

Figure 04-01: Example of Encryption

Objectives of Encryption

Data Integrity:

This requires the recipient to ensure that, accidentally or deliberately or because of third-party activity, the message has not been:

- Lost or changed during the transmission
- Prevented from reaching the recipient
- Reached the recipient twice

Data integrity can be verified by using a message digest that acts as a **digital fingerprint** of the message.

Authentication:

Verifying the origin of the message is required. It assures the sender that the message is sent to the intended recipient, and the recipient can be sure that the message is sent by a legitimate sender and not an imposter. Sender authentication is accomplished through a **digital certificate** and **digital signature**.

Non-repudiation:

Non-repudiation is also referred to as data accountability and refers to the evidence that a message exchange took place. The sender cannot deny that the message was sent and the recipient cannot deny that the message was received. Data accountability is accomplished through digital signatures.

Usage of Encryption

Usage of encryption includes:

- Encryption is used to **protect user credentials** such as user names and passwords

- It helps to safely **store sensitive information** on a computer or external storage media
- Encryption provides a **secure medium** for users to connect to their friends or employees' networks from outside the home or office
- It provides a **higher level of trust** when receiving files from other users by ensuring that the source and contents of the message are trusted
- Encryption is used as a resource for web-based **information exchange** to protect important information such as credit card numbers
- It provides assurance of a sender's **identity**
- Encryption helps avoiding attention to a confidential email

Types of Encryption

Based on the number of keys that are employed for encryption and decryption, cryptography algorithms are classified as:

- ### Symmetric Encryption:

  Symmetric encryption is also called private key or **secret key encryption** and ensures privacy and confidentiality. Secret key is used for both encryption and decryption in which a sender encrypts the plaintext and the receiver decrypts the message. Both the sender and receiver must know the secret key.

  Secret key cryptography is classified as two ciphers. One is **stream ciphers** and the other is **block ciphers**. Using stream ciphers, the same plaintext using the same key will encrypt different cipher text, whereas using the block cipher, the same plaintext using the same key will encrypt the same cipher text.

- ### Asymmetric Encryption:

  Asymmetric encryption is also called **public-key cryptography** and ensures non-repudiation and user authentication. In asymmetric encryption, the user uses two keys: public key and a private key. One key is used for encryption and other key is used for decryption. One of the two keys must be kept secret.

- ### Hash Function:

  Hash function ensures integrity, which is also referred to as **one-way encryption** and message digest. Hash functions are used by the operating systems to encrypt the passwords and ensure that files are not altered by unauthorized users.

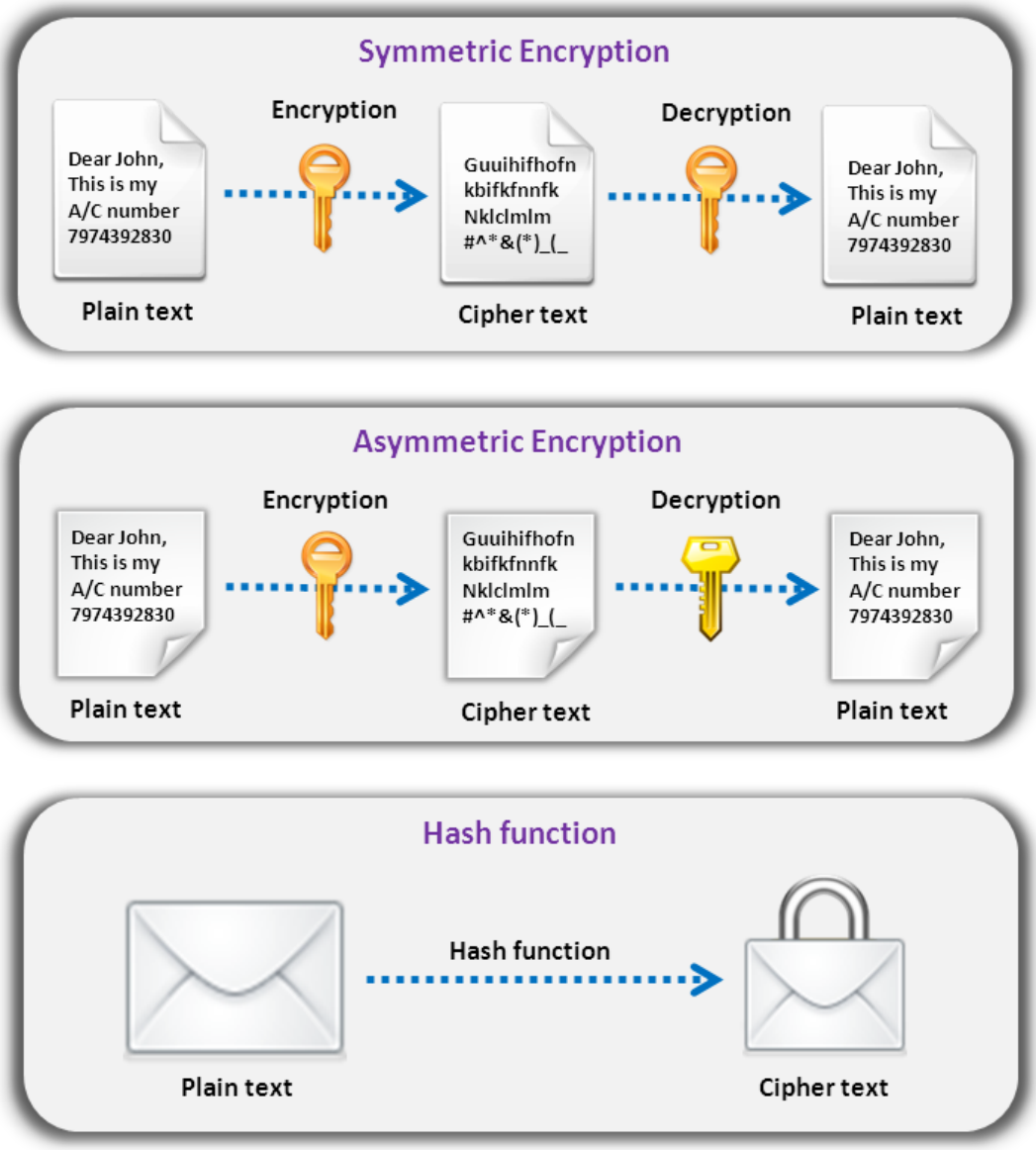

Figure 04-02: Types of Encryption

Symmetric vs. Asymmetric Encryption

Symmetric Encryption:

- Symmetric encryption uses only **one key** for both encryption and decryption.
- The key cannot be shared freely.
- Symmetric encryption requires that the sender and the receiver of the data know the secret key.

- The algorithm is less complex and faster; thus, data encryption is faster.
- The key length is fixed.
- It is used for bulk encryption, which means encrypting files and communication paths.
- Symmetric encryption ensures confidentiality and integrity.

Asymmetric Encryption:

- Asymmetric encryption uses a **public key** for encryption and a **private key** for decryption.
- In asymmetric encryption, the public key can be freely shared, which eliminates the risk of compromising the secret key.
- Only the public key is known; the secret key is kept undisclosed by its owner.
- The algorithm is **slower** and more **complex**.
- The key length is variable.
- It is used for key encryption and distributing keys.
- Asymmetric encryption ensures confidentiality, integrity, authentication, and non-repudiation.

Encryption Standards

DES

The data encryption standard (DES) is the name of the **Federal Information Processing Standard (FIPS) 46-3**, which describes the data encryption algorithm (DEA). The DES has a **64-bit block size** and during execution it uses a **56-bit key**. When it is used for communication, both the sender and the receiver must know the secret key that is used to encrypt and decrypt the message, or to generate and verify a message authentication code (MAC). It is a symmetric cryptosystem originally designed to be implemented in hardware. It is used for single-user encryption such as storing encrypted files on a hard disk.

AES

The advanced encryption standard (AES) is an **iterated symmetric block** cipher defined in FIPS, which means that it works by repeating the same defined steps multiple times. It is a secret key encryption algorithm, and operates on a fixed number of bytes. AES-128, AES-192, and AES-256 are the three block ciphers present in AES. These block ciphers are taken from the Rijndael. AES-128 bit is used for the **SECRET** level, whereas 192-bit is used for the **TOP SECRET** level by the National Security Association (NSA).

Digital Certificates

A digital certificate is an **electronic card** that provides credential information while doing business or other online transactions on the web. It contains the name, expiration date, signature information and serial number, copy of the owner's public key, and digital signature of the certificate-issuing authority that enables the recipient to verify that the certificate is authentic. It is used to verify one's identity and can be used in various ways such as to **control access** on websites, to secure email, to create virtual private networks, and to assure the authenticity of downloaded software. Digital certificates can be personal certificate, software publisher certificates, server certificates, or certificate authority certificate. Digital certificates are used:

Identification: To verify that individuals are connected with a particular server that enables business partners and co-workers to securely communicate using public communication protocols

Authentication: To assure that the signed code is safe to execute and that it is from trusted software vendor, found most in software publisher certificates

Security: To validate HTTPS-based websites and to guarantee the user that all communication, particularly e-commerce related information, is secure

How Digital Certificates Work

The function of the certification authority is to guarantee that, when a user downloads a file or opens a sent message, the sender is genuine and not someone who has forged a signature. The **certification authority** verifies the identity and sends a digital certificate, which contains information about the sender's identity, and a copy of the public key. The certificate in turn is encrypted by the certification authority's private key. The following steps illustrates the working of digital certificates

- A user applies for a certificate with the **registration authority** (RA).
- The RA receives the request from the user, verifies the applicant, and requests that the **certification authority** (CA) issues a certificate to the user.
- The CA issues a public key certificate to the user and sends the updated information to the **validation authority** (VA).
- When a user makes a transaction, the user duly signs the message digitally in the public key certificate and sends the message to the client.
- The client verifies the authenticity of the user by inquiring about the user's public key certificate validity with the VA.
- The VA compares the public key certificate of the user with that of the updated information provided by the CA and determines the result.

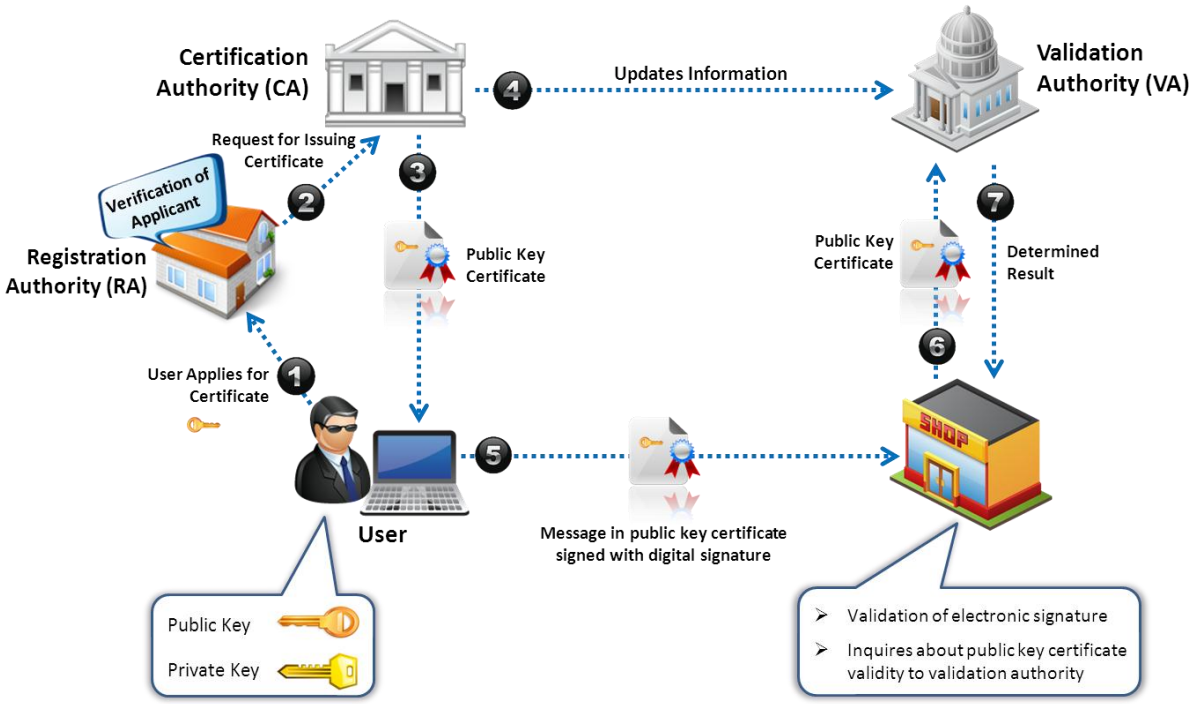

Figure 04-03: How Digital Certificates Work

Digital Signature

A digital signature is a cryptographic means of authentication. Public key cryptography, which uses an **asymmetric key algorithm**, is used to create the digital signature. The two types of keys in public key cryptography are the private key (which is known only to the signer and is used to create the digital signature) and the public key (which is more widely known and is used by a relying party to verify the digital signature). "Hash function" is a process, or an algorithm, which is used when creating and verifying a digital signature. This algorithm creates a **digital representation** of a message, which is also known as a "fingerprint." This fingerprint or "hash value" is of a standard length, which is much smaller than the message, but is still unique. If any change is made to the message, it will automatically produce a different hash result; it is not possible to derive the original message from the hash value in case of a secure hash function, which is also known as the "**one-way hash function**."

The hash result of the original message and the hash function that is used to create the digital signature are required to verify the digital signature. With the help of the public key and the new result, the verifier checks:

- If the digital signature is created with the related private key
- If the new hash result is the same as the original hash result, which was converted into a digital signature during the signing process

To **correlate the key pair** with the respective signer, the certification authority presents a certificate that is an electronic record of the public as the subject of the certificate, and

confirms the identity of the signer as the related private key owner. The future signer is called the **subscriber**. The main function of a certificate is to bind a pair of public and private keys to a particular subscriber. The recipient of the certificate relies on a digital signature created by the subscriber named in the certificate. The public key listed can be used to verify that the private key is used to create the related digital signature.

The certification authority digitally signs the certificate to assure the **authenticity** of both the public key and the subscriber's identity. The authority's digital signature on the certificate can be verified with the help of the public key of the certification authority recorded in another certificate, which belongs to another certification authority. This certificate can be authenticated with the help of another public key recorded in another certificate and so on.

The **repository** can be made to publish the certificate; the public key and its identity are available for verification of the certificate. The retrieval and verification of the digital signature is made with the help of online databases called repositories, which holds the certificates and other information. The certification authority may suspend or revoke the certificate.

How Digital Signature Works

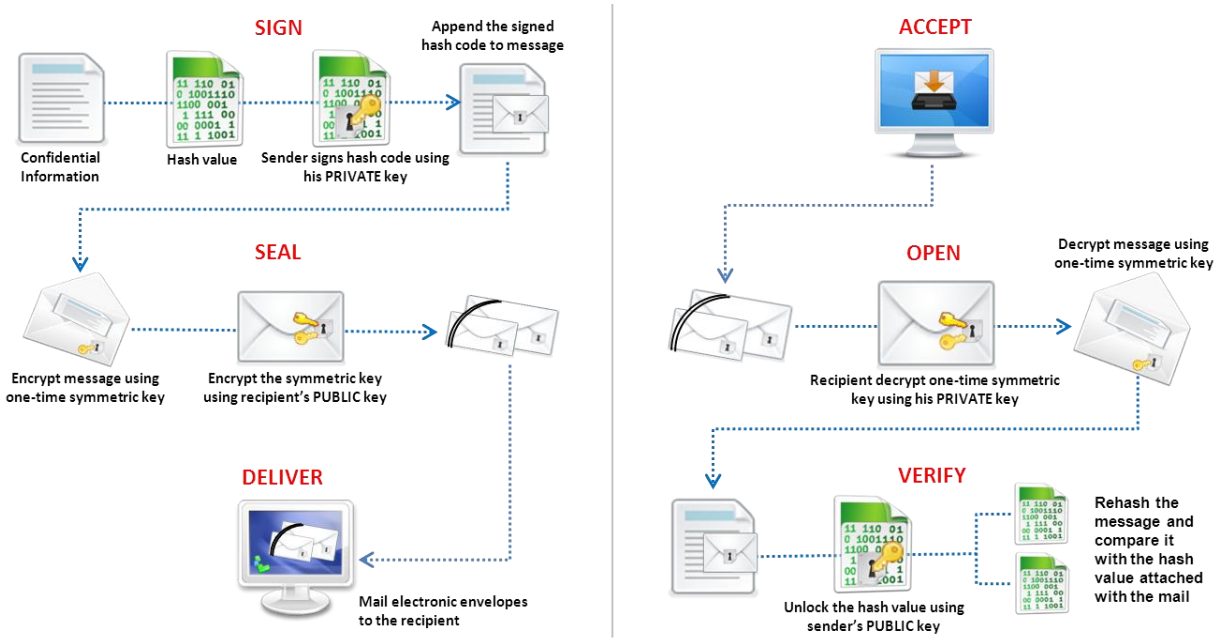

Figure 04-04: The working of Digital Signature

Cryptography Tool: TrueCrypt

Source: http://www.truecrypt.org

Free open-source disk encryption software for Windows 7/Vista/XP, Mac OS X, and Linux

Features:

- It creates a **virtual encrypted disk** within a file and mounts it as a real disk.
- It **encrypts an entire partition or storage device** such as a USB flash drive or a hard drive.
- It encrypts a partition or drive where Windows is installed (pre-boot authentication).
- Encryption is automatic, real-time (**on-the-fly**), and transparent.
- Parallelization and pipelining allow data to be read and written as fast as if the drive were not encrypted.
- The encryption can be hardware-accelerated on modern processors.
- It provides plausible deniability in case an adversary forces you to reveal the password—hidden volume (steganography) and hidden operating system.

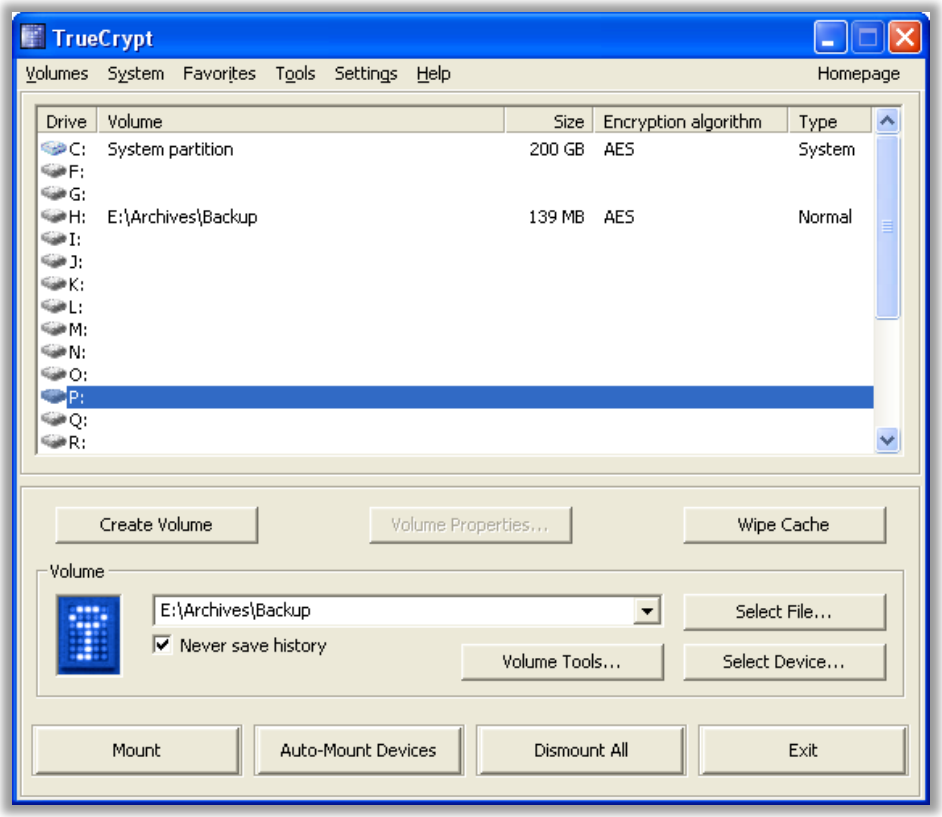

Figure 04-05: Selecting the Drive to Encrypt in TrueCrypt Tool

Cryptography Tools

Secret Data Manager

Source: http://www.secretdata.info

Secret Data Manager enables computer users to keep their secret files encrypted to protect data from being stolen. It integrates encryption, compression, hiding files and folders, a file shredder, smart open and automatic updates, and intelligent close through an easy Windows-style user interface.

AxCrypt

Source: http://www.axantum.com

AxCrypt is file encryption software for Windows. It integrates with Windows to compress, encrypt, decrypt, store, send, and work with individual files.

File Waster

Source: http://www.jcmatt.com

File Waster protects the files from prying eyes with secure encryption technology. It can encrypt and decrypt files while securely wiping the originals, recurse sub-directories, and compress files before encryption.

MAXA Text2Exe

Source: http://www.maxa-tools.com

MAXA Text2Exe hides serial numbers, passwords, phone numbers, and everyday notes in a safe place with a 256-bit AES encryption algorithm. It allows for saving text encrypted as an executable file.

PixelCryptor

Source: http://www.codegazer.com

PixelCryptor offers an easy-to-use wizard to guide users through the process of encryption and decryption.

EncryptOnClick

Source: http://www.2brightsparks.com

EncryptOnClick enables keeping data secure. The encryption and decryption method used is 256-bit AES encryption. It will encrypt, decrypt, compress, and decompress files that can also be opened and decrypted using third-party programs like WinZip 9.

Encrypt Files

Source: http://www.encryptfiles.net

Encrypt Files is free encryption desktop computer software that protects your files and folders from unauthorized viewing. Some of its features include encrypting entire folders, shredding original files, and hiding files after encryption.

Zero Footprint Crypt

Source: http://www.baroufasoft.net

Zero Footprint Crypt allows users to view encrypted image files without having to decrypt them to the hard disk. This allows for maximum security as the file remains in its encrypted state on the hard disk (leaving no footprint on the drive). It allows users to choose either "decrypt to file" or "decrypt to memory."

Module Summary

Encryption is the process of converting data into a cipher text that cannot be understood by unauthorized people.

Symmetric encryption uses only one key for both encryption and decryption, whereas asymmetric encryption uses a public key for encryption and a private key for decryption.

Encryption provides a higher level of trust when receiving files from other users by ensuring that the source and contents of the message are trusted.

A digital certificate is an electronic card that provides credential information when doing online transactions on the web.

A digital signature implements asymmetric cryptography to simulate the security properties of a signature in digital rather than written form.

This page is intentionally left blank.