Encryption and Decryption techniques.

Data that can be read and understood without any special measures is called *plaintext* or *cleartext*. The method of disguising plaintext in such a way as to hide its substance is called *encryption.* Encrypting plaintext results in unreadable gibberish called *ciphertext*. You use encryption to ensure that
information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plaintext is called *decryption*.

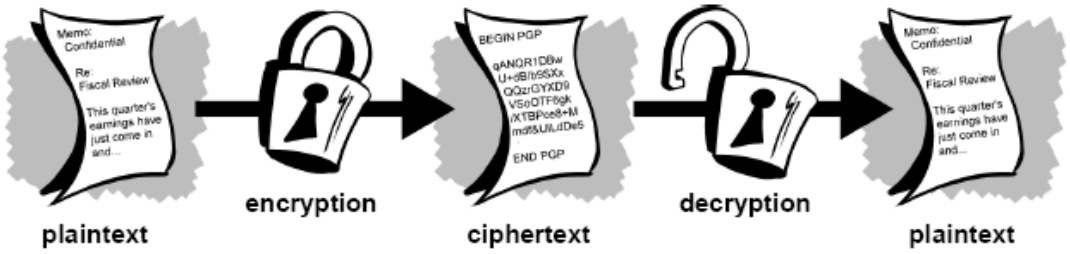

Figure 1. Encryption and Decryption.

What is cryptography?.

Cryptography is the science of using the mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across the insecure networks(like the internet) so that cannot be read by anyone except the intend recipient.

While cryptography is the science of securing data, *cryptanalysis* is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck.
Cryptanalysts are also called ***attackers***.
Cryptology embraces both cryptography and cryptanalysis.

How does cryptography work?.

A *cryptographic algorithm*, or *cipher*, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a *key*—a word, number, or phrase—to encrypt the plaintext. The same plaintext encrypts to different ciphertext with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a *cryptosystem.*

Conventional Cryptography.

In conventional cryptography, also called *secret-key* or *symmetric-key* encryption, one key is used both for encryption and decryption. The Data Encryption Standard (DES) is an example of a conventional cryptosystem that is widely employed by the Federal Government. Figure 2 is an illustration of the conventional encryption process.

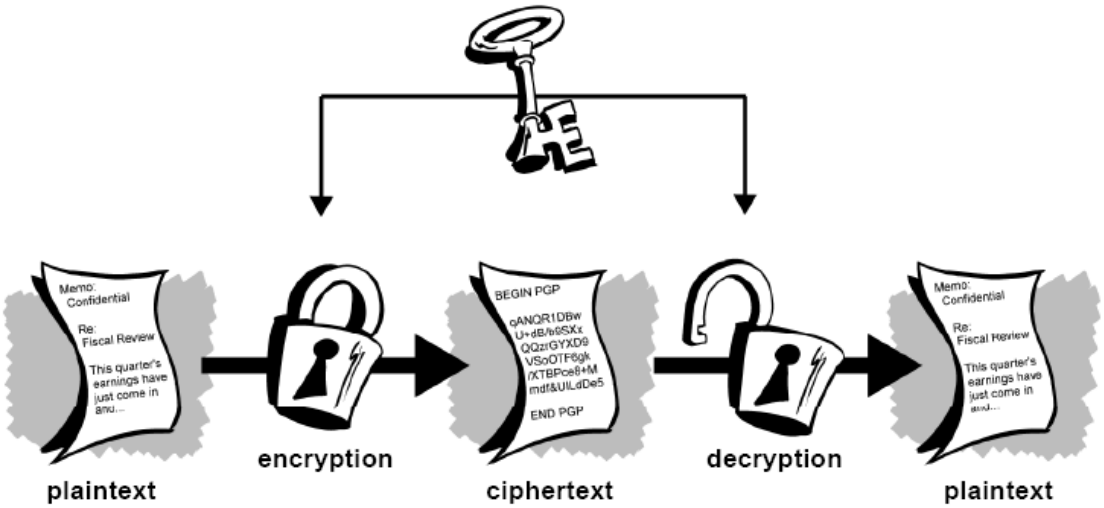

Figure 2. Conventional Encryption.

Conventional encryption has benefits. It is very fast. It is especially useful for encrypting data that is not *going* anywhere. However, conventional encryption alone as a means for transmitting secure data can be quite expensive simply due to the difficulty of secure key distribution. Recall a character from your favorite spy movie: the person with a locked briefcase handcuffed to his or her wrist.What is in the briefcase, anyway? It's probably not the missile launch code/biotoxin formula/invasion plan itself.
It's the *key* that will decrypt the secret data. For a sender and recipient to communicate securely using conventional encryption, they must agree upon a key and keep it secret between themselves. If they are in different physical locations, they must trust a courier, the Bat Phone, or some other secure communication medium to prevent the disclosure of the secret key during transmission. Anyone who overhears or intercepts the key in transit can later read, modify, and forge all information encrypted or authenticated with that key. From DES to Captain Midnight's Secret Decoder Ring, the persistent problem with conventional encryption is *key distribution*: how do you get the key to the recipient without someone intercepting it?

- **DES** (Data Encryption Standard) is a symmetric cipher defined in Federal Information Processing (FIPS) Standard Number 46 in 1977 as the federal government approved encryption algorithm for sensitive but non-classified information. DES was developed by IBM and was based upon IBM's earlier Lucifer cipher. DES utilizes a 56-bit key. This key size is vulnerable to a brute force attack using current technology.

- **Triple DES** is a variant of DES, Triple DES, provides significantly enhanced security by executing the core DES algorithm three times in a row. The effect of making the DES encryption much more difficult to brute force. Triple-DES is estimated to be 2 to the 56th times more difficult to break than DES. Triple DES can still be considered a secure encryption algorithm. Triple DES is also written as 3-DES or 3DES.

- **AES** (Advanced Encryption Standard) is a symmetric cipher defined in Federal Information Processing (FIPS) Standard Number 197 in 2001 as the federal government approved encryption algorithm. The NSA has approved 128-bit AES for use up to SECRET level and 192-bit AES for use up to TOP SECRET level. AES is based upon the Rijndael algorithm, which was invented by Joan Daemen and Vincent Rijmen. AES specifies three approved key lengths: 128-bits, 192-bits and 256-bits.

Public Key Cryptography.

The problems of key distribution are solved by *public key cryptography.* Public key cryptography is an asymmetric scheme that uses a *pair* of keys for encryption: a *public key*, which encrypts data, and a corresponding *private,* or *secret key* for decryption. You publish your public key to the world while keeping your private key secret. Anyone with a copy of your public key can then encrypt information that only you can read. Even people you have never met.

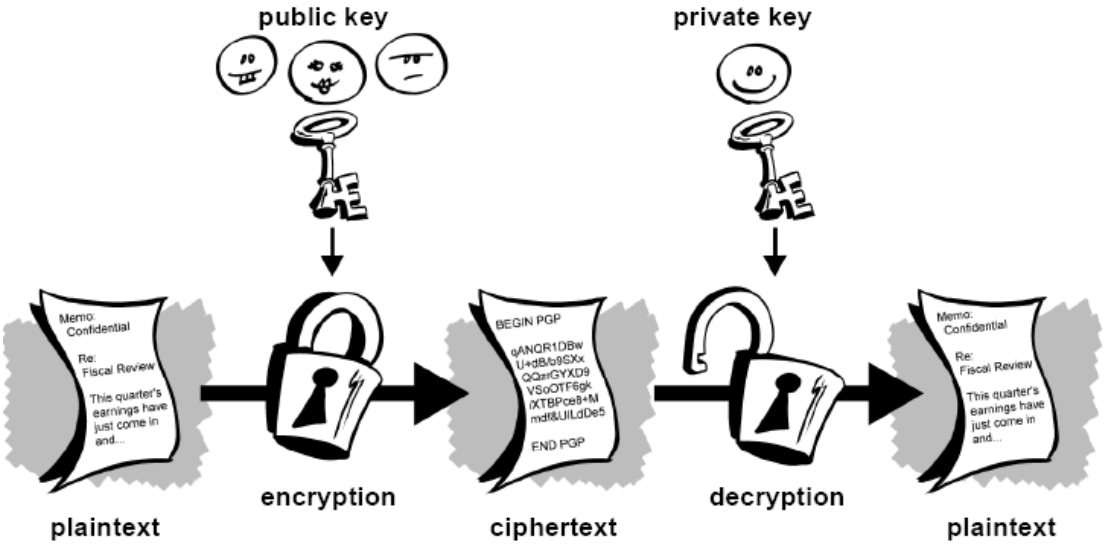

Figure 3. Public key encryption.

The primary benefit of public key cryptography is that it allows people who have no preexisting security arrangement to exchange messages securely. The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. Some examples of public-key cryptosystems are Elgamal (named for its inventor, Taher Elgamal), RSA (named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman), Diffie-Hellman (named, you guessed it, for its inventors), and DSA, the Digital Signature
Algorithm (invented by David Kravitz). Because conventional cryptography was once the only available means for relaying secret information, the expense of secure channels and key distribution relegated its use only to those who could afford it, such as governments and large banks (or small children with secret decoder rings). Public key encryption is the technological revolution that provides strong cryptography to the adult masses. Remember the courier with the locked briefcase handcuffed to his wrist? Public-key encryption puts him out of business (probably to his relief).

- **RSA** is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. It's also part of Lotus Notes, Intuit's Quicken, and many other products. The encryption system is owned by RSA Security. The company licenses the algorithm technologies and also sells development kits. The technologies are part of existing or proposed Web, Internet, and computing standards.

- **Elliptic curve cryptography (ECC)** is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The use of elliptic curves in cryptography was suggested independently by Neal Koblitz and Victor S. Miller in 1985. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization.

- **ElGamal encryption system** is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key agreement. It was described by Taher Elgamal in 1985. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm is a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption.