**Overwiew of Cryptology (and This Book)**

This first chapter introduce us on the real meaning of Cryptography, this science is an old art, who the ancient Egypt used.

Since the beginig of the use of this art, another cultures start to use it as a method to hide the most important secret. Actually there are some old documents who are in anciente Greece, or the famous Caesar cipher in the ancient Rome.



We have to make an important statment the correct term is CRYPTOLOGY and not cryptography. The cryptography is the field.

Therefore cryptology split into two main branches :

**Cryptography**

* This is the science of secret writing with the goal of hiding the real meaning of a message.

**Cryptanalysis**

This is the science and sometimes art of breaking cryptosystems. You

might think that code breaking is for the intelligence community or perhaps or-

ganized crime, and should not be included in a serious classification of a scien-

tific discipline. However, most cryptanalysis is done by respectable researchers

in academia nowadays. Cryptanalysis is of central importance for modern cryp-

tosystems: without people who try to break our crypto methods, we will never

know whether they are really secure or not.

Cryptanalysis is the only way to assure that a cryptosystem is secure.

Cryptography have their own braches.

**Symmetric Algorithms**

are what many people assume cryptography is about:

two parties have an encryption and decryption method for which they share a

secret key. All cryptography from ancient times until 1976 was exclusively based

on symmetric methods. Symmetric ciphers are still in widespread use, especially

for data encryption and integrity check of messages

**Asymmetric (Public-Key) Algorithms**

In 1976 an entirely different type of

cipher was introduced by Whitfield Diffie, Martin Hellman and Ralph Merkle. In

public-key cryptography, a user possesses a secret key as in symmetric cryptog-

raphy but also a public key. Asymmetric algorithms can be used for applications

such as digital signatures and key establishment, and also for classical data en-

cryption

**Cryptographic Protocols**

Roughly speaking, crypto protocols deal with the application of cryptographic algorithms. Symmetric and asymmetric algorithms can be viewed as building blocks with which applications such as secure Internet communication can be realized. The Transport Layer Security (TLS) scheme, which is used in every Web browser, is an example of a cryptographic protocol

In the real world the use of this algorithms is mixed, i mean you use more than one to work, and this mixtures have a name “hybrid schemes”

**Symmetric Cryptography**

This section deals with the concepts of symmetric ciphers and it introduces the

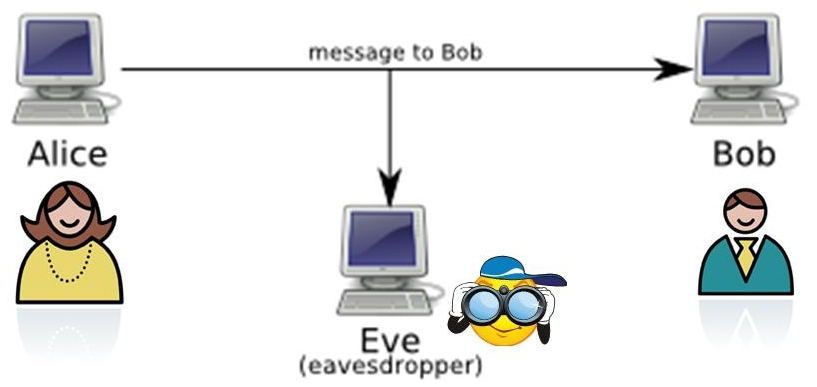
historic substitution cipher. Using the substitution cipher as an example, we will

learn the difference between brute-force and analytical attacks

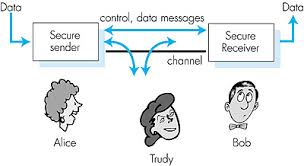
**Basics**

Symmetric cryptographic schemes are also referred to as symmetric-key, secret key and single-key schemes or algorithms, There are two users, Alice and Bob, who want to communicate over an insecure channel (channel might sound

a bit abstract but it is just a general term for the communication link: This can be the Internet, a stretch of air in the case of mobile phones or wireless LAN communica-tion, or any other communication media you can think of) The actual problem starts with the bad guy Oscar, who has acces to the channel, for instance, by hacking into an Internet router or by listening to the radio signals of a Wi-Fi communication. This kins of stuffs is called eavesdropping. Obviously, there are many situations in which Alice and Bob would prefer to communicate without Oscar listening. For instance, if Alice and Bob represent two offices of a car manufacturer, and they are transmitting documents containing the business strategy for the introduction of new car models in the next few years, these documents should not get into the hands of their competitors, or of foreign intelligence agencies for that matter.



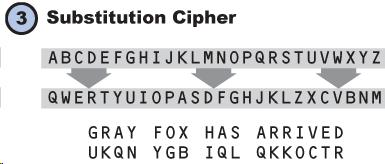
In this situation, symmetric cryptography offers a powerful solution: Alice encrypts her message x using a symmetric algorithm, yielding the ciphertext y. Bob receives the ciphertext and decrypts the message. Decryption is, thus, the inverse process of encryption. What is the advantage? If we have a strong encryption algorithm, the ciphertext will look like random bits to Oscar and will contain no information whatsoever that is useful to him.



As we can see in the second image, there is the explanation of what we just reed, this method work nicely with WPA (Wi-Fi Protected Access)

**Simple Symmetric Encryption: The Substitution**

This is one of the simplest methods for encrypting text, SUBSTITION, in the history of the man, this is an old technic whow has been used many times, and is a good way to show us the basic cryptography



**Brute-Force**

We hace the one attack, who use the brute-force

this means that the attacker has the ciphertext now he would try to descovered the message using all the keys, until he found the right key. In the real world maybe you can use this but the most common things to happen is that you can't find the right or maybe you just have false results

**Frequency Analysis**

The major wakness of the cipher os that each plaintext symbol always maps to the same ciphertext symbol. That means that the statistical properties of the plaintext are preserved in the ciphertext. Like we saw in the golden bug