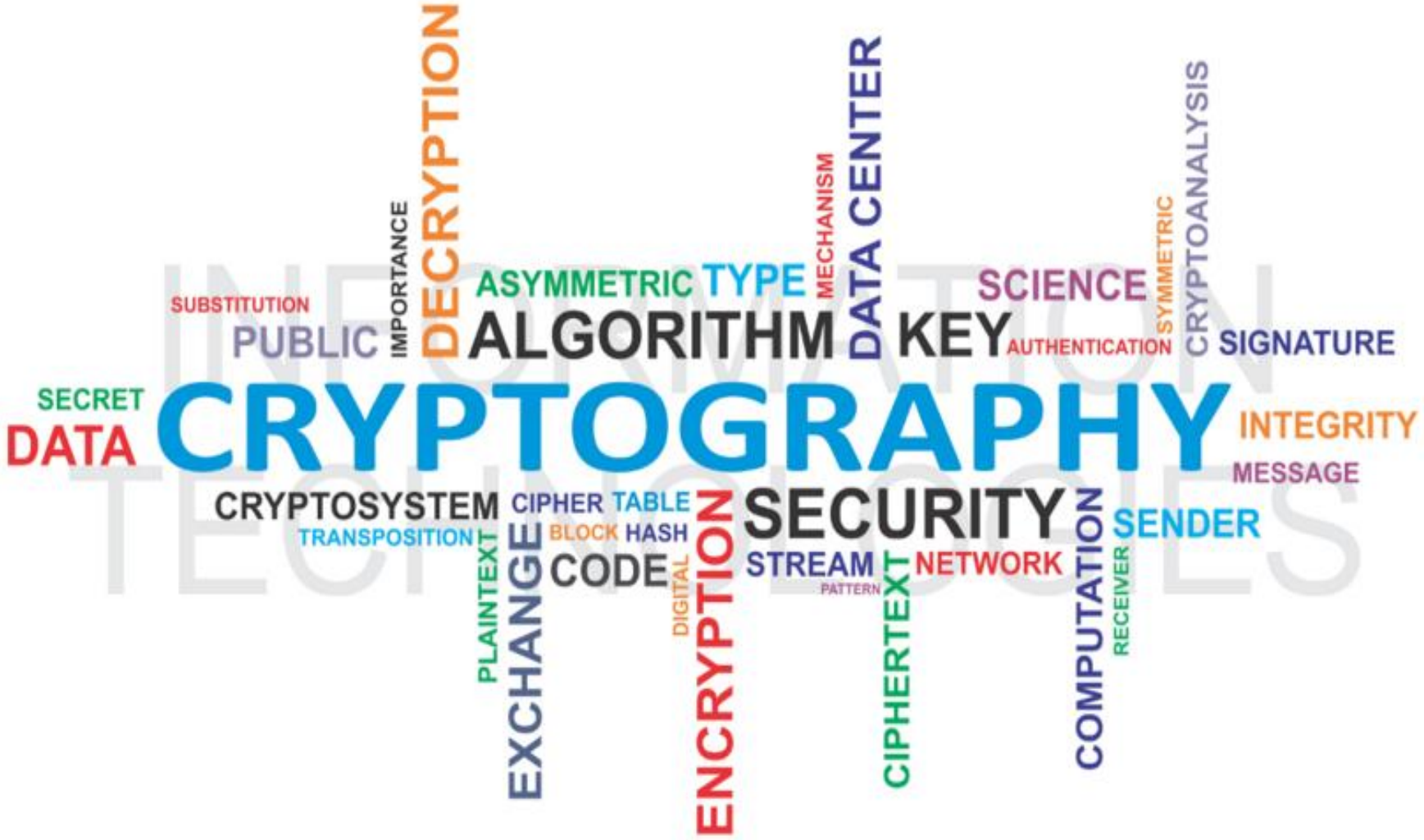

CRYPTOGRAPHY
DATA
SECRET
ALGORITHM
KEY
PUBLIC
SUBSTITUTION
IMPORTANCE
DECRYPTION
ASYMMETRIC
TYPE
MECHANISM
DATA CENTER
SCIENCE
SYMMETRIC
CRYPTOANALYSIS
AUTHENTICATION
SIGNATURE
INTEGRITY
MESSAGE
CRYPTOSYSTEM
CIPHER TABLE
TRANSPOSITION
BLOCK HASH
SECURITY
SENDER
PLAINTEXT
EXCHANGE
CODE
DIGITAL
ENCRYPTION
STREAM
NETWORK
PATTERN
CIPHERTEXT
COMPUTATION
RECEIVER

CHAPTER 1: INTRODUCTION TO CRYPTOGRAPHY

Terminologies

- **Cryptography:**
  - **branch of knowledge discussing about technique of concealing & scrambling sensitive data**

- **Encipherment:**
  - **a security mechanism for covering the content of data to provide confidentiality**

- **Encryption:**
  - **mathematical processes to scramble an original data to unreadable data**
- **Decryption:**
  - **mathematical process to unscramble the encrypted data and recover the original data**
  - **reverse process of encryption**
- **Key:**
  - **parameter used in encryption and decryption**

- **Plaintext:**
  - **Original/decrypted data (readable)**

- **Ciphertext:**
  - **encrypted data (unreadable)**

- **Cipher:**
  - **encryption-decryption algorithm**

- **Cryptosystem:**
  - **cryptography-system**
  - **combination of cipher, plaintext, ciphertext and keys.**

- **Sender:**
  - **an authorized party who sends data**

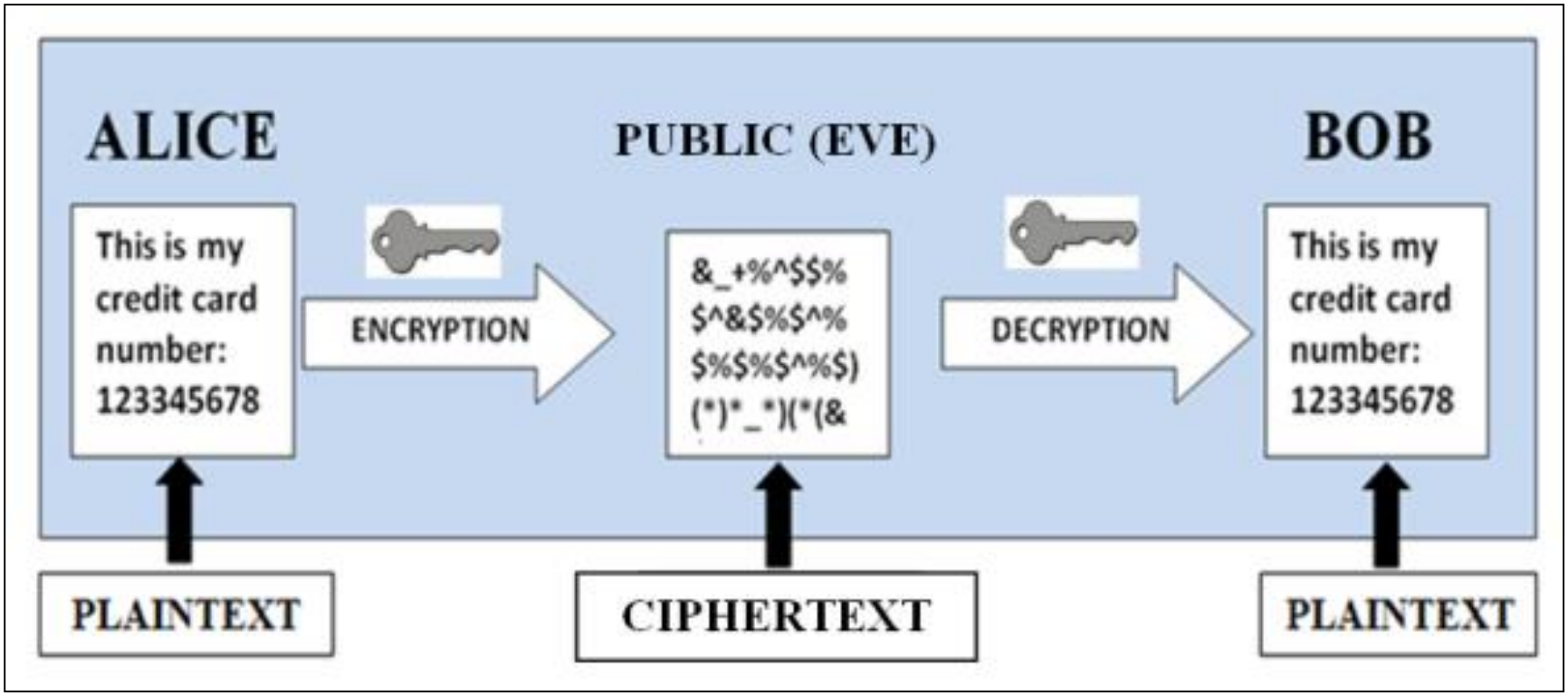
- **Recipient / Receiver:**
  - **an authorized party who receives data**

- **Eavesdropper/ Attacker/ Adversary:**
  - **an unauthorized party who interested to read and understand the content of transmitted data between Sender and Recipient**

- **Cryptanalysis:**
  - **technique of breaking the security of cryptosystem**

- **Cryptology:**
  - **branch of knowledge that contains cryptography and cryptanalysis**

- **Overview:**


ALICE
PUBLIC (EVE)
BOB
This is my credit card number: 123345678
ENCRYPTION
&_+%^$$%$^&$%$^%$%$%$^%$)(*)*_*)(*(&
DECRYPTION
This is my credit card number: 123345678
PLAINTEXT
CIPHERTEXT
PLAINTEXT

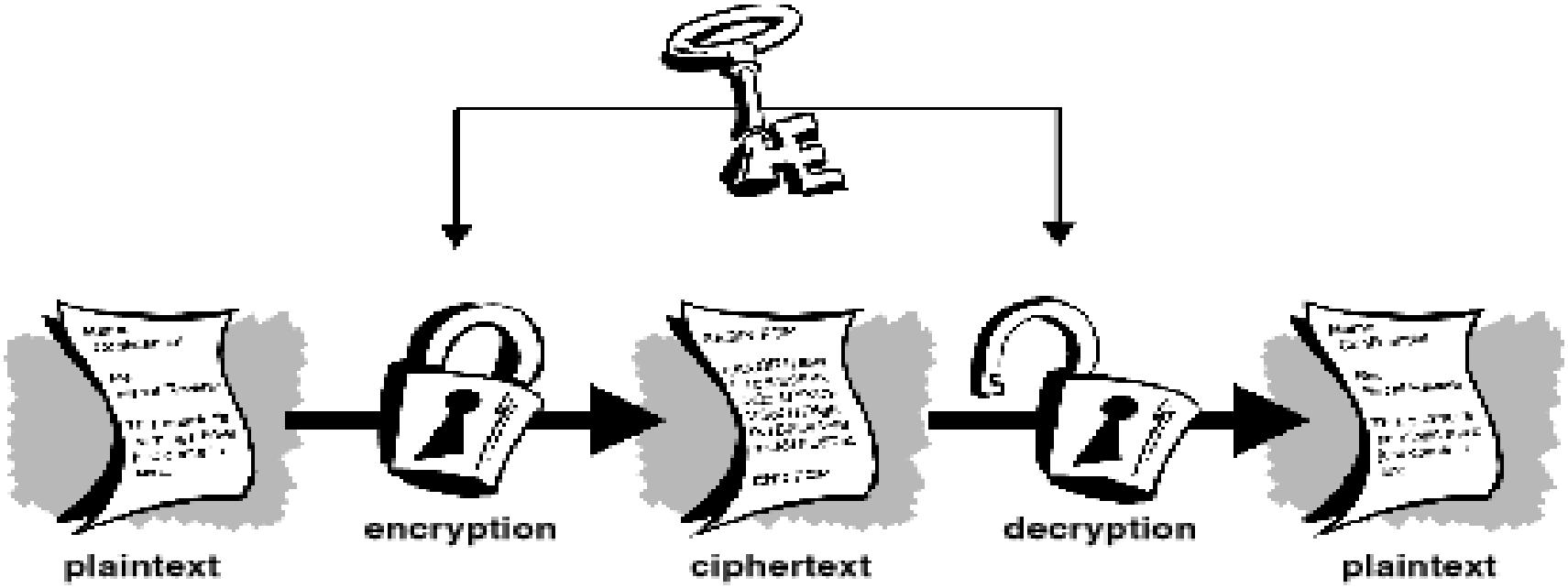
Cryptography:

- can be referred to as the science of transforming messages to make them secure and immune to attacks

- based on keys, 2 major classes:
  i. Secret key / Symmetric key
  ii. Private key / Asymmetric key

Symmetric-Key Cryptography

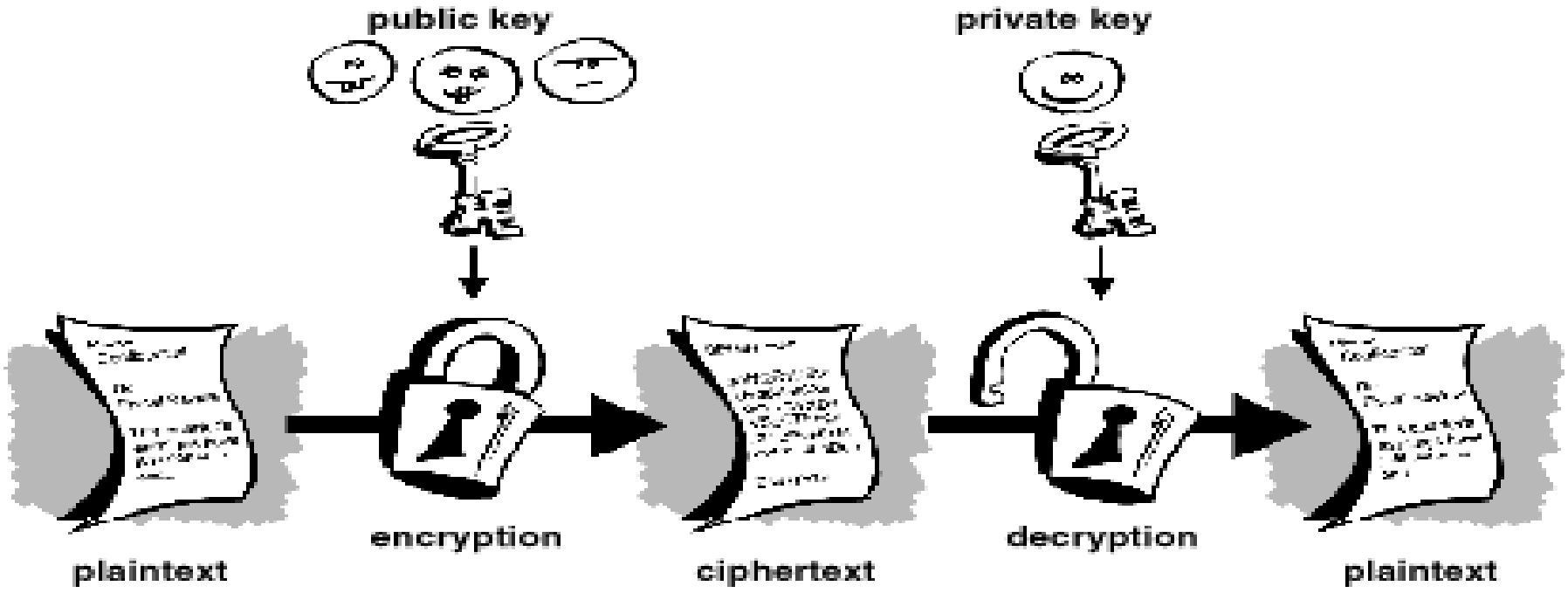
- **uses a single secret key for both encryption and decryption**



Source: http://www.gpgtools.org/intro.html

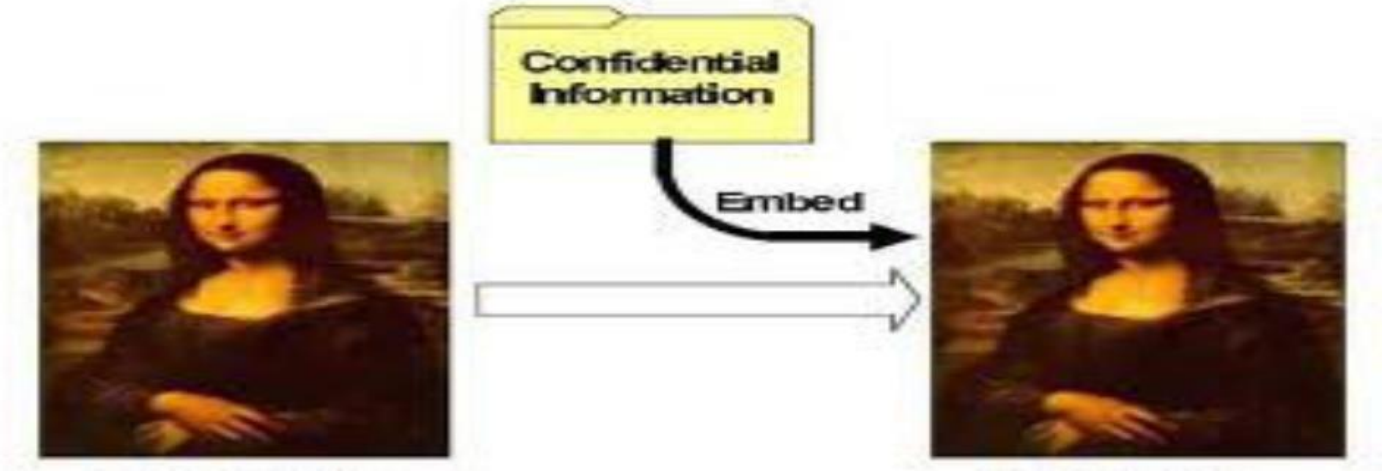
Asymmetric-Key Cryptography

- involves **two keys** instead of one: **private key and public key**



Source: http://www.gpgtools.org/intro.html

- **Steganography:**
  - **comes from Greek word means covered writing**
  - **in China, war messages were written on thin pieces of silk and rolled into a small ball and swallowed by the messenger.**
  - **hide the data & does not change (scramble) the data**
  - **other example: shaving head, invisible ink etc**


Confidential Information
Embed


NEED A CHANGE?
HEAD DOWN TO
NEW ZEALAND
airnewzealand.com

- today, any form of data such as text, image, audio and video can be digitalized

- it is possible to insert secret binary information into the data during digitalization process

- Steganography vs Cryptography:

Steganography	*Cryptography*
Hides the whole data	Does not hide the data
Does not change the content of data	Scramble the content of data via encryption
Makes the data invisible to unauthorized party	Unauthorized party still able to access and see the data but do not understand the content of the data

Hard Mathematical Problems

- **Mathematics is the backbone of cryptography**

- **There are rigorous mathematical processes behind cryptography, especially the asymmetric-key encipherment**

- **Underlying each asymmetric - key encipherment is a hard mathematical problem**

- **The hard mathematical problem assumed only can be solved by authorized party who has the secret information (encryption-decryption keys)**

- **Without the secret information, hard mathematical problem can be assumed (hopefully) cannot be solved by unauthorized party**

- **The best known hard mathematical problems:**

Cryptosystem	*Hard Mathematical Problem*
RSA	**Integer Factorization Problem (IFP)**
ElGamal	**Discrete Logarithm Problem (DLP)**
Elliptic Curve Cryptography (ECC)	**Elliptic Curve Discrete Logarithm Problem (ECDLP)**

Security Goals

- We need to keep **information** about every aspect of our lives

- **Information** is an **asset** that has a value like any other asset and needs to be secured from unauthorized party

- **To be secured, information content need to be**
  - **hidden from unauthorized access (confidentiality)**
  - **protected from unauthorized change (integrity)**
  - **available to an authorized access when it is needed (availability)**

- **Until a few decades ago, the information collected by an organization was stored in physical files.**

- **With the advent of computers, information storage became electronic**

- **The files stored in computers require confidentiality, integrity and availability**

- **During the last two decades, computer networks created a revolution in the use of information where information now can be easily distributed.**

- **Authorized people can send and retrieve information from a distance using computer networks**

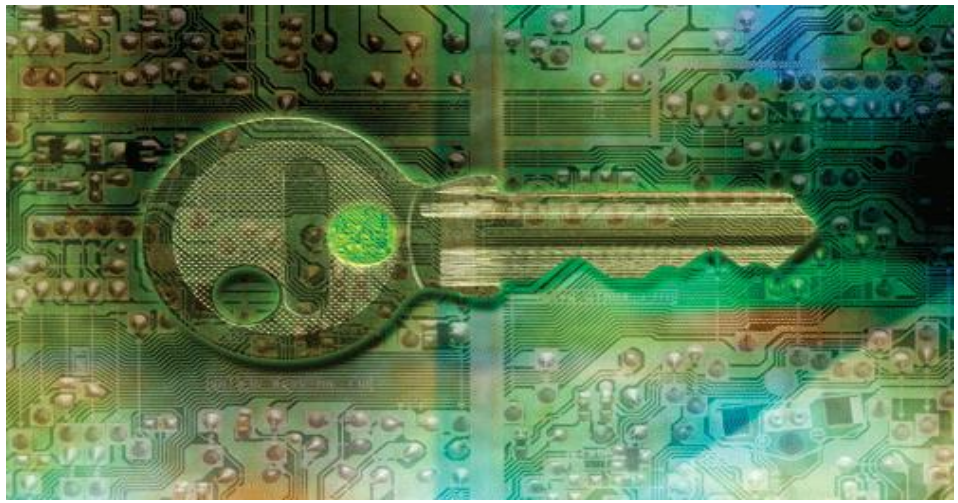
- **Although the three requirements (confidentiality, integrity and availability) have not changed, they now have some new dimensions.**

- **Not only should information be confidential when it is stored in a computer, there should also be a way to maintain its confidentiality when it is transmitted from one computer to another**

- **Confidentiality:**
  - **in military, concealment of sensitive information is the major concern**
  - **in industry, hiding some information from competitors is crucial to the operation of the organization**
  - **in banking, customers' accounts need to be kept secret**
  - **can be provided via encryption-decryption techniques (encipherment)**

- **Integrity:**
  - **information needs to be changed constantly**
  - **in a bank, when a customer deposits or withdraw money, the balance of his/her account needs to be changed**
  - **integrity means that changes need to be done only by authorized entities and through authorized mechanisms.**
  - **can be provided by using hash function**

- **Availability:**
  - **information created and stored by an organization needs to be available to authorized entities**
  - **information need to be constantly changed, which means it must be accessible to authorized party**



References:

Farouzan, B. A. 2008. *Introduction to Cryptography and Network Security*. McGraw-Hill.

Hoffstein, J. Pipher, J. Silverman, J. H. 2004. *An Introduction to Mathematical Cryptography.* Springer.