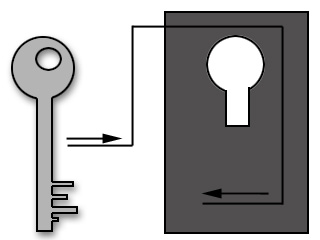
**CRYPTOGRAPHY**

***ABSTRACT***

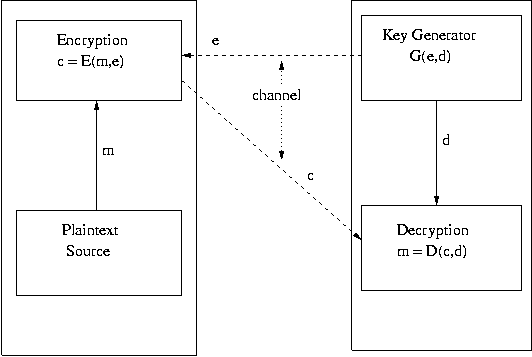
**In the real world, to provide securities**

**The following four areas have been identified as the framework for secure E-commerce:**

* **Confidentiality: Protecting the data from all but the intended receiver(s).**
* **Authentication: Proving one's identity.**
* **Integrity: Ensuring no unauthorized alteration of data.**
* **Non-repudiation: Preventing an entity from denying previous commitments or actions.**
* **The universal technique for providing confidentiality of transmitted data is cryptography. Cryptography is the one branch that deals with encryption and decryption.**

**The basic functionality of cryptography is to hide information. Its operation typically includes two processes:**

* **Encryption as the process of transforming information so that it is unintelligible to an intruder, and**
* **Decryption as the process of transforming the encrypted information so that it is intelligible again.**



**FIG: it is 2 way process dependent on each other..**

* **The information in its original form is known as plain text, and the encrypted message is called cipher text.**
* **Exchanging or choosing a key pair (e, d) secretly does secure communication between two persons.**
* **The security lies in the fact that the mathematical function and the key are only bound to the sender and receiver, not to anybody else.**
* **Keys are very critical to the functionality of cryptographic algorithms and it is sound cryptographic practice to change keys frequently.**

**There are two types of hash algorithms. . There are two types of hash algorithms. They are:**

**. MD5**

**SHA-1**

* **Due to the advancement in computing power and hash function crypt-analysis have led to the decline in the popularity of MD4 and MD5, two very popular hash functions. In response, newer hash algorithms have been developed with longer hash code length and with features designed to resist specific crypt-analytic attacks**

**SHA-1 LOGIC:**

**The algorithm takes as input a message with a maximum length of less than 264 bits and produces as output a 160-bit message digest. length and chaining variable length of 160 bits. The processing consists of the following steps:**

* **Append padding bits :**

* **Append length :**

**Initialize MD buffer :**

**These registers are initialized as:**

**A=67452301**

B=EFCDAB89

**C=98BADCFE**

D=10325476

##### **E=C3D2E1F0**

**These values are stored in big-endian format, which is the most significant byte of a word in the low-address byte position.**

**As 32-bit strings, the initialization values appears as follows:**

**Word A: 67 45 23 01**

#### Word B: EF CD AB 89

## Word C: 98 BA DC FE

**Word D: 10 32 54 76**

Word E: C3 D2 E1 F0

# MD5 MESSAGE DIGEST ALGORITHM

# MD5 LOGIC

**The algorithm takes as input a message of arbitrary length and produces as output a 128-bit message digest. The input is processed in 512-bit blocks.**

**The processing consists of the following steps:**

* **Append padding bits :**
* **Append length :**

* **Initialize MD buffer :**

**The buffer can be represented as four 32-bit registers (A, B, C, and D). These registers are initialized as**

A=67452301

**B=EFCDAB89**

## C=98BADCFE

**D=10325476**

**As 32-bit strings, the initialization values appear as follows:**

**Word A: 01 23 45 67**

**Word B: 89 AB CD EF**

#### Word C: FE DC BA 98

## Word D: 76 54 32 10

Applications of cryptography include

[ATM cards](http://en.wikipedia.org/wiki/Automated_teller_machine), [computer passwords](http://en.wikipedia.org/wiki/Password), and [electronic commerce](http://en.wikipedia.org/wiki/Electronic_commerce).

## Modern cryptography

### 1:Symmetric-key cryptography

### 2:Public-key cryptography

***LIFE AND CARRIER IN CRYPTOGRAPHY***

**1:DNA cryptography is a new born cryptographic field emerged with the research of DNA computing, in which DNA is used as information carrier and the modern biological technology is used as implementation tool.**

**2: Quantum cryptography with continuous variables is an emerging field that ... using the quadrature components of electromagnetic fields as quantum carriers**

**And on root level…**

**It is one ..where peole don’t show their intrest because it is associated with devotion and experience….**

**Conclusion:**

**There is no gain saying the fact that cryptography plays an essential role in protecting the privacy of electronic information against threats from a variety of potential attackers. Public key cryptography, is the most important technology in modern cryptographic schemes to address issues like key management, authentication, non-repudiation and digital signature cryptosystems with smaller key lengths offer virtually no security. Symmetric-key systems offer an advantage over the public-key systems. Private keys in public-key systems are much larger.**

**REFERENCES:**

* **Cryptography and Network security William Stalling**

#### Applied Cryptography

###### **Bruce Schneie**