Introduction to Cryptography

By

Marcus K. G. Adomey

Chief Operations Manager
AfricaCERT
Email: marcus.adomey@africacert.org

OVERVIEW

- Cryptography
    - *Definition*
    - *Terminology*
    - *History*
    - *Goal and Services*
- Types of Cryptography
    - *Symmetric Key Cryptography*
    - *Asymmetric Key Cryptography*
    - *Hash Functions*

CRYPTOGRAPHY

- □ *Definition*
- □ *Terminology*
- □ *History*
- □ *Goal and Services*

Cryptography

Definition

Cryptography is the science of using mathematics to encrypt and decrypt data.

Phil Zimmermann

Cryptography is the art and science of keeping messages secure.

Bruce Schneier

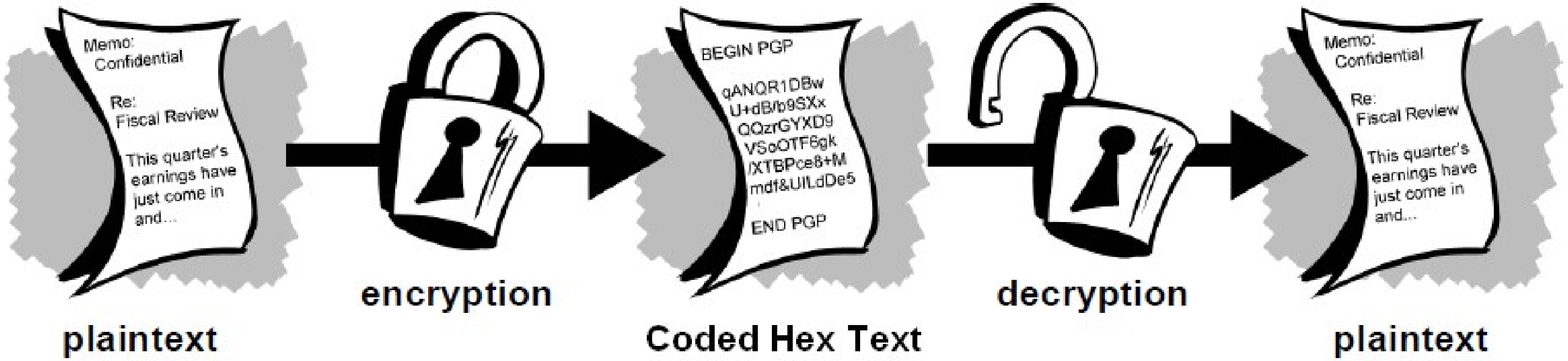
The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography.

Cryptography

Terminologies

A message is **plaintext** (sometimes called **cleartext**). The process of disguising a message in such a way as to hide its substance is **encryption**. An encrypted message is **ciphertext**. The process of turning ciphertext back into plaintext is **decryption**.

A **cipher** (or **cypher**) is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure.



Cryptography

Terminology

A **cryptosystem** is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system. The various components of a basic cryptosystem are as follows –

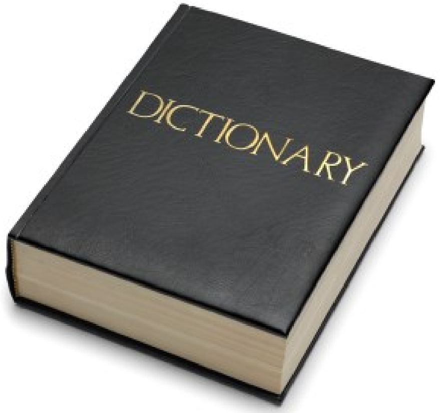
- Plaintext
- Encryption Algorithm
- Ciphertext
- Decryption Algorithm
- Encryption Key
- Decryption Key

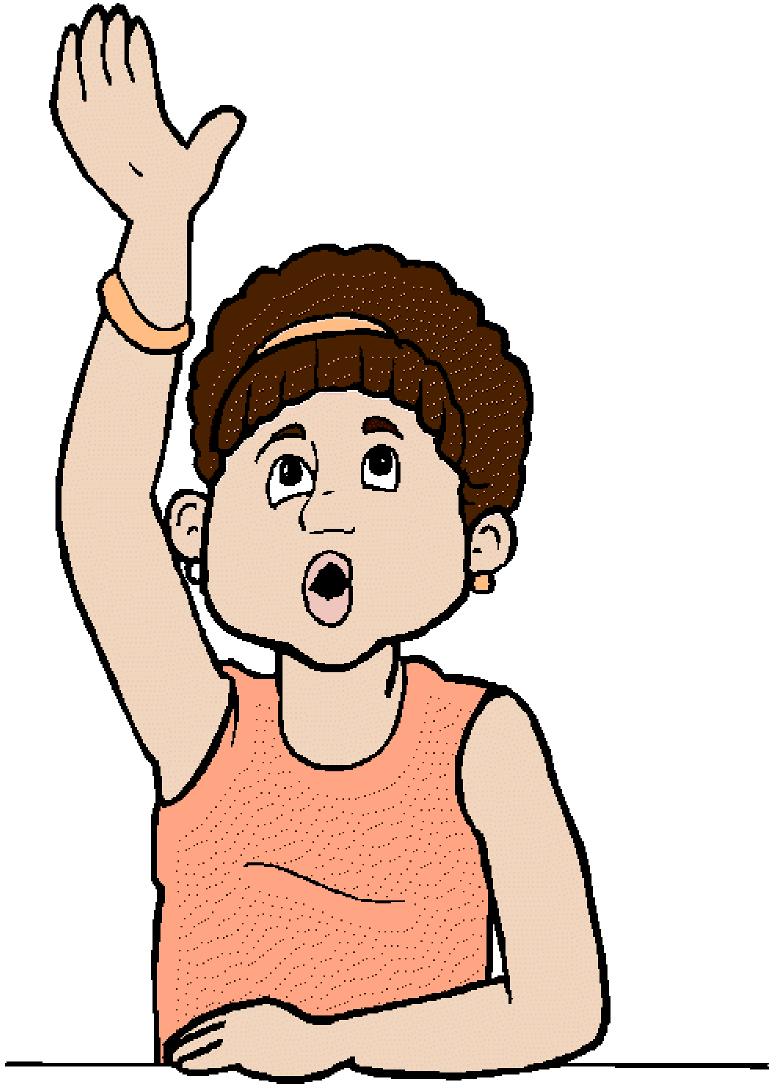
Cryptography

Terminology

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.





History of Cryptography

History of Cryptography

History of Cryptography

As civilizations evolved, human beings got organized in tribes, groups, and kingdoms.

This led to the emergence of ideas such as power, battles, supremacy, and politics.

These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well.

The roots of cryptography are found in Roman and Egyptian civilizations.

History of Cryptography

Hieroglyph

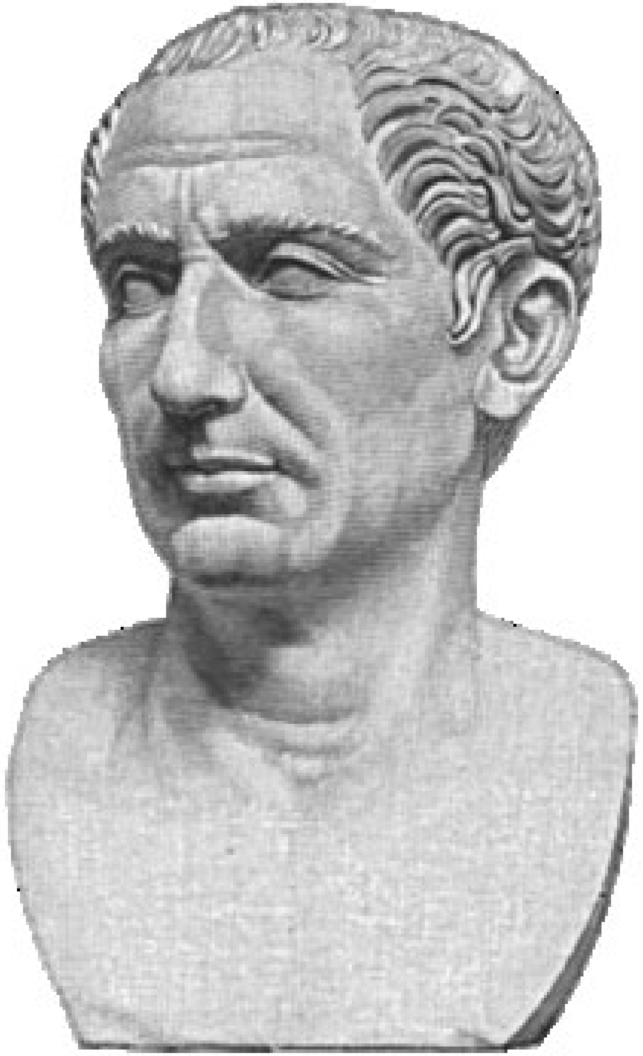
The first known evidence of cryptography can be traced to the use of ‘hieroglyph’. Some 4000 years ago, the Egyptians used to communicate by messages written in hieroglyph.

History of Cryptography

Caesar Shift Cipher

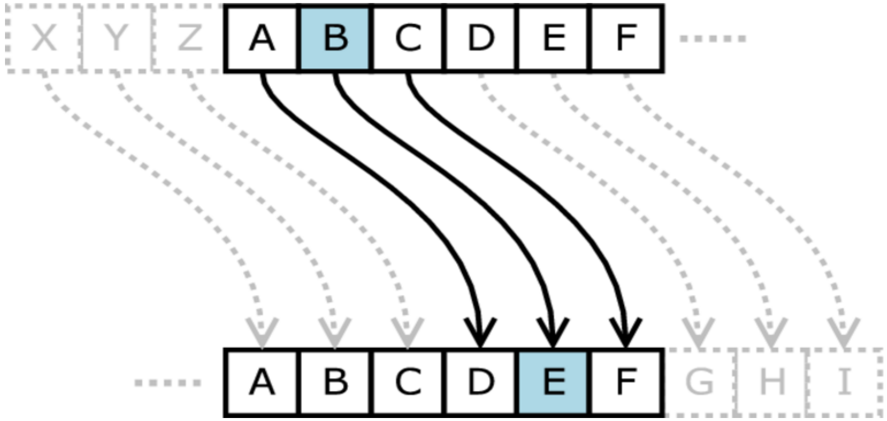
Caesar Shift Cipher, relies on shifting the letters of a message by an agreed number (three was a common choice), the recipient of this message would then shift the letters back by the same number and obtain the original message.

The Caesar cipher is named after Julius Caesar , who used it with a shift of three to protect messages of military significance.

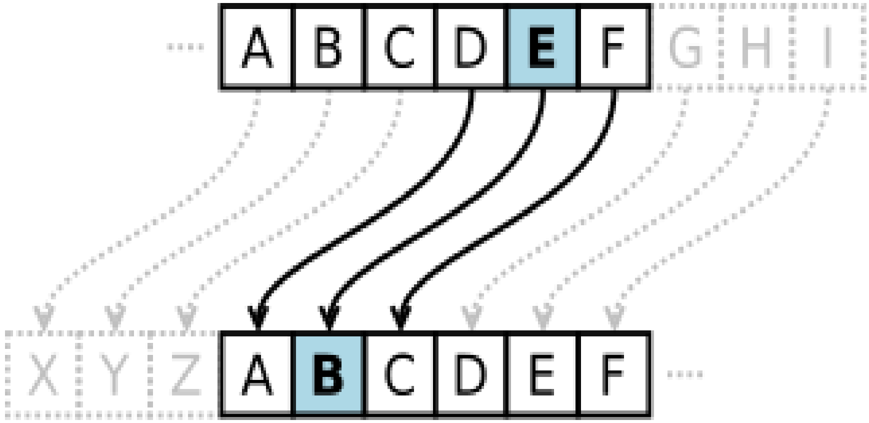


History of Cryptography

Caesar Shift Cipher



Encryption



Decryption

PLAINTEXT	**:**	**internet society ghana chapter**
CYPHERTEXT	**:**	**lqwhuqhw vrflhwb jkdqd fkdswhu**

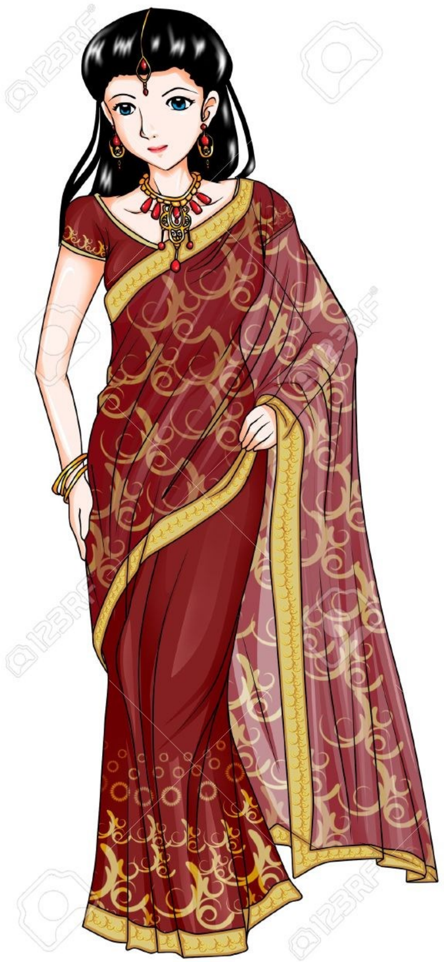
History of Cryptography

Kamasutra Cipher

The Kamasutra cipher is one of the earliest known substitution methods.

It is described in the Kamasutra around 400 BC.

The purpose was to teach women how to hide secret messages from prying eyes.



History of Cryptography

Kamasutra Cipher

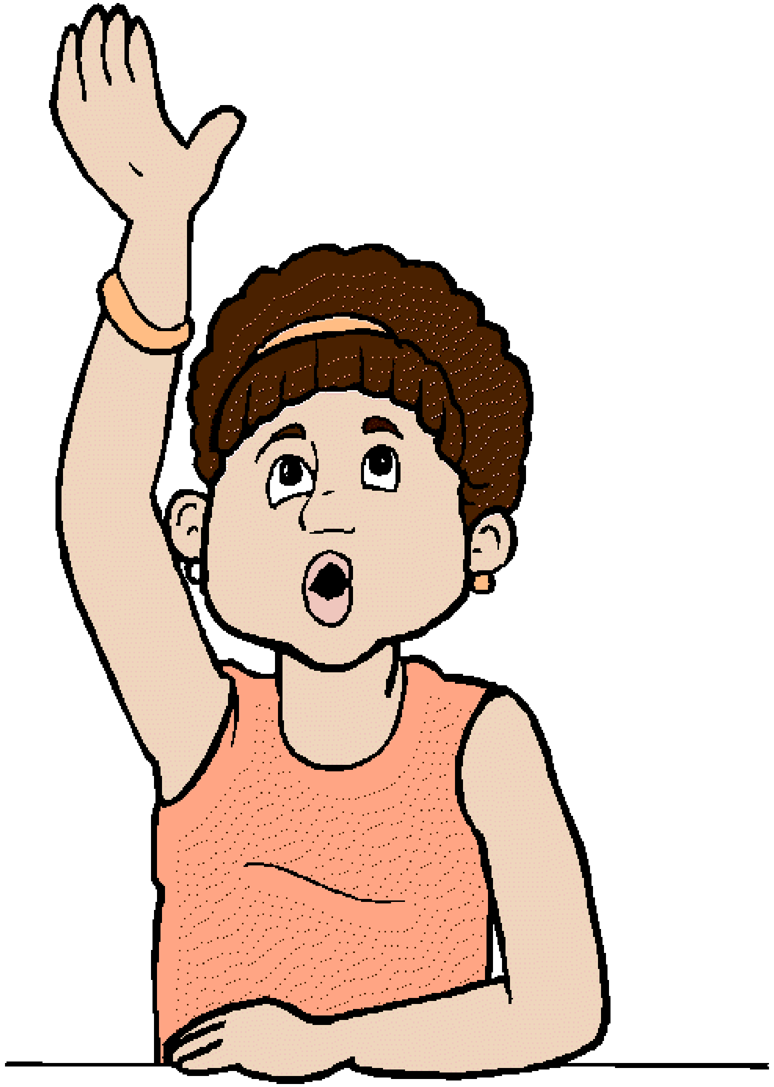
The techniques involves randomly pairing letters of the alphabet, and then substituting each letter in the original message with its partner.

UPPER HALF	W	Z	V	P	O	F	D	E	A	B	R	M	Y
LOWER HALF	N	H	G	X	K	S	I	C	J	U	T	Q	L

The key is the permutation of the alphabet.

INTERNET SOCIETY GHANA CHAPTER

DWRCTWCR FKEDCRL VZJWJ EZJXRCT



Goal and Services

Cryptography

Goal and Services

Goal: The primary goal of cryptography is to secure important data on the hard disk or as it passes through a medium that may not be secure itself. Usually, that medium is a computer network.

Services: Cryptography can provide the following services:

- ***Confidentiality (secrecy)***
- ***Integrity (anti-tampering)***
- ***Authentication***
- ***Non-repudiation.***

Goal and Services

Confidentiality (secrecy)

- Ensuring that no one can read the message except the intended receiver
- Data is kept secret from those without the proper credentials, even if that data travels through an insecure medium

Integrity (anti-tampering)

- Assuring the receiver that the received message has not been altered in any way from the original.

Cryptography

Goal and Services

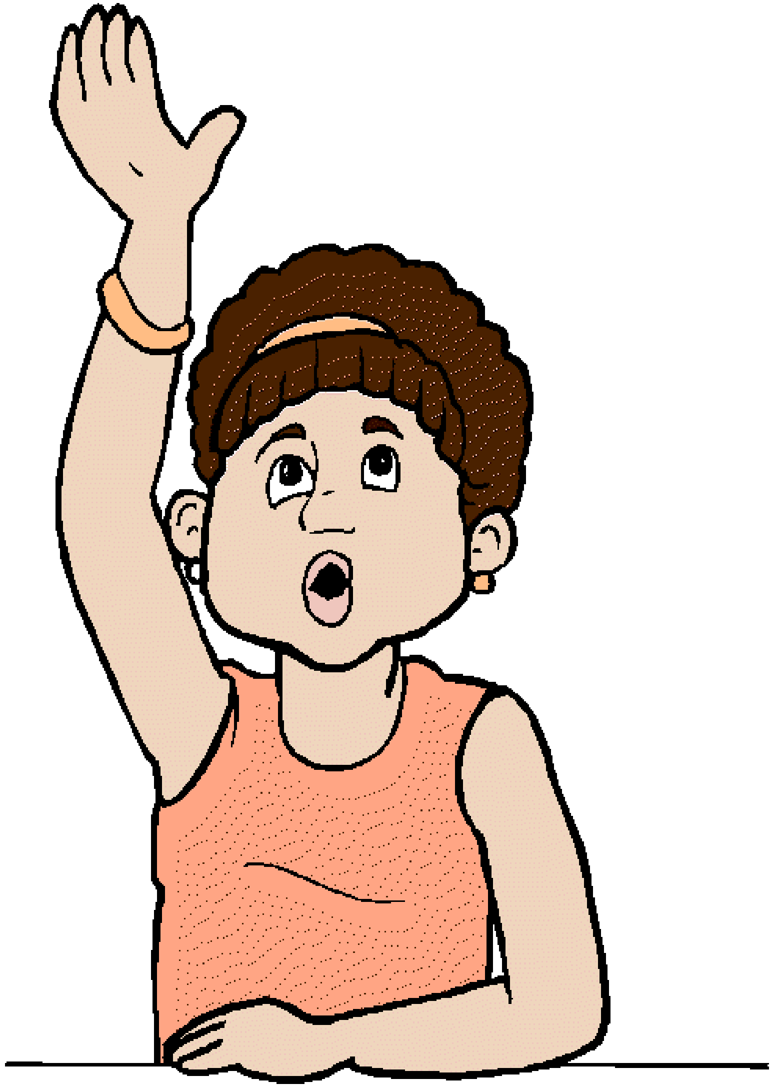
Authentication

Cryptography can help establish identity for authentication purposes

The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)

Non-repudiation

A mechanism to prove that the sender really sent this message



Types of Cryptography

- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Hash Functions

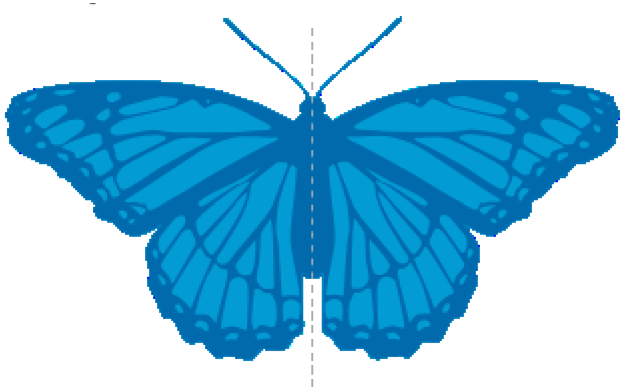
Types of Cryptography

Symmetric Key Cryptography

Also known as Secret Key Cryptography or Conventional Cryptography, Symmetric Key Cryptography is an encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message.

The Algorithm use is also known as a secret key algorithm or sometimes called a symmetric algorithm

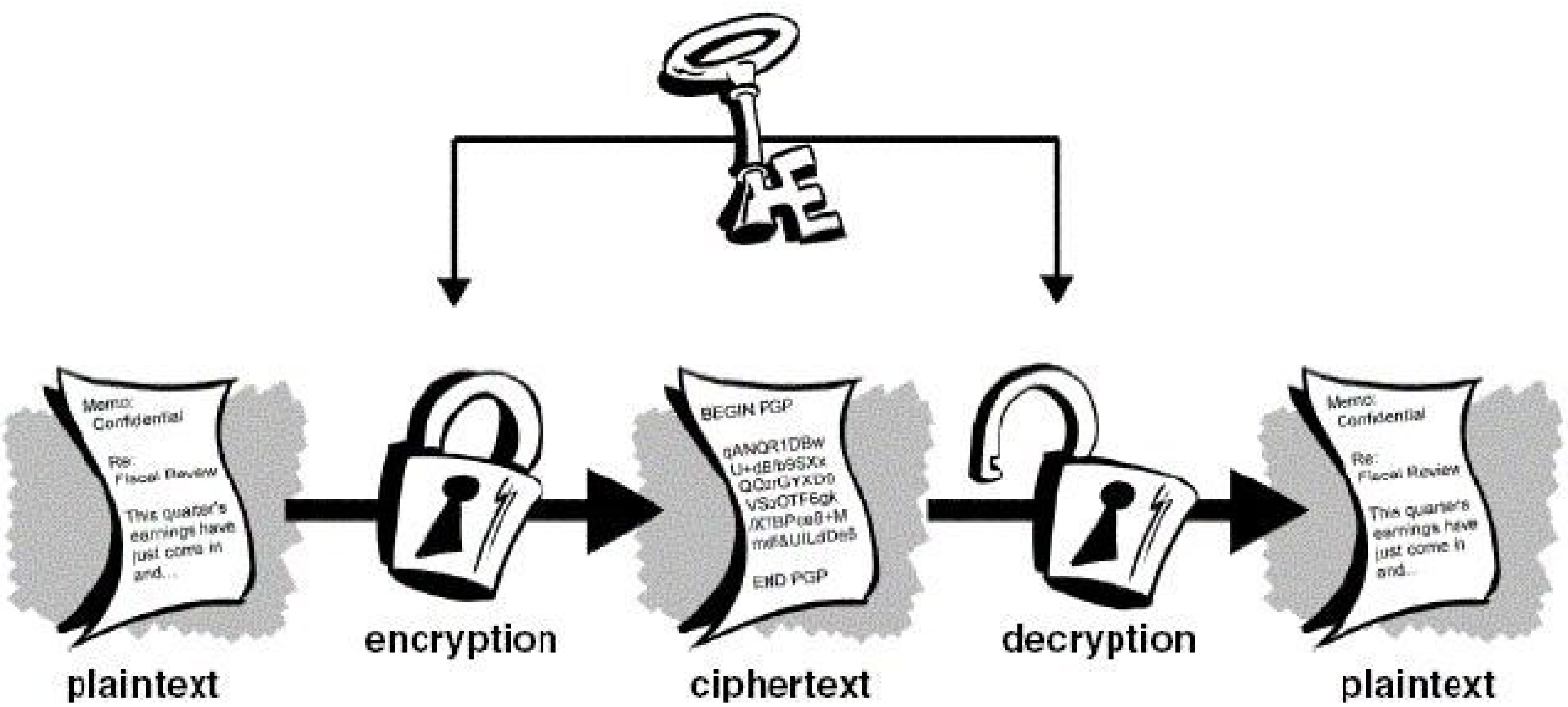
A key is a piece of information (a parameter) that determines the functional outp cryptographic algorithm or cipher.



Types of Cryptography

Symmetric Key Cryptography

The key for encrypting and decrypting the file had to be known to all the recipients. Else, the message could not be decrypted by conventional means.



Types of Cryptography

Symmetric Key Cryptography - Examples

Data Encryption Standard (DES)

The Data Encryption Standard was published in 1977 by the US National Bureau of Standards.

DES uses a 56 bit key and maps a 64 bit input block of plaintext onto a 64 bit output block of ciphertext. 56 bits is a rather small key for today's computing power.

Triple DES

Triple DES was the answer to many of the shortcomings of DES. Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES.

Types of Cryptography

Symmetric Key Cryptography - Examples

Advanced Encryption Standard (AES) (RFC3602)

Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael.

Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES).

Types of Cryptography

Symmetric Key Cryptography

IDEA:- The International Data Encryption Algorithm was developed in 1991.

It uses a 128 bit key to encrypt a 64 bit block of plaintext into a 64 bit block of ciphertext.

IDEA's general structure is very similar to DES, it performs 17 rounds, each round taking 64 bits of input to produce a 64 bit output, using per-round keys generated from the 128 bit key.

Types of Cryptography

Symmetric Key Cryptography - Examples

Lucifer - Madryga

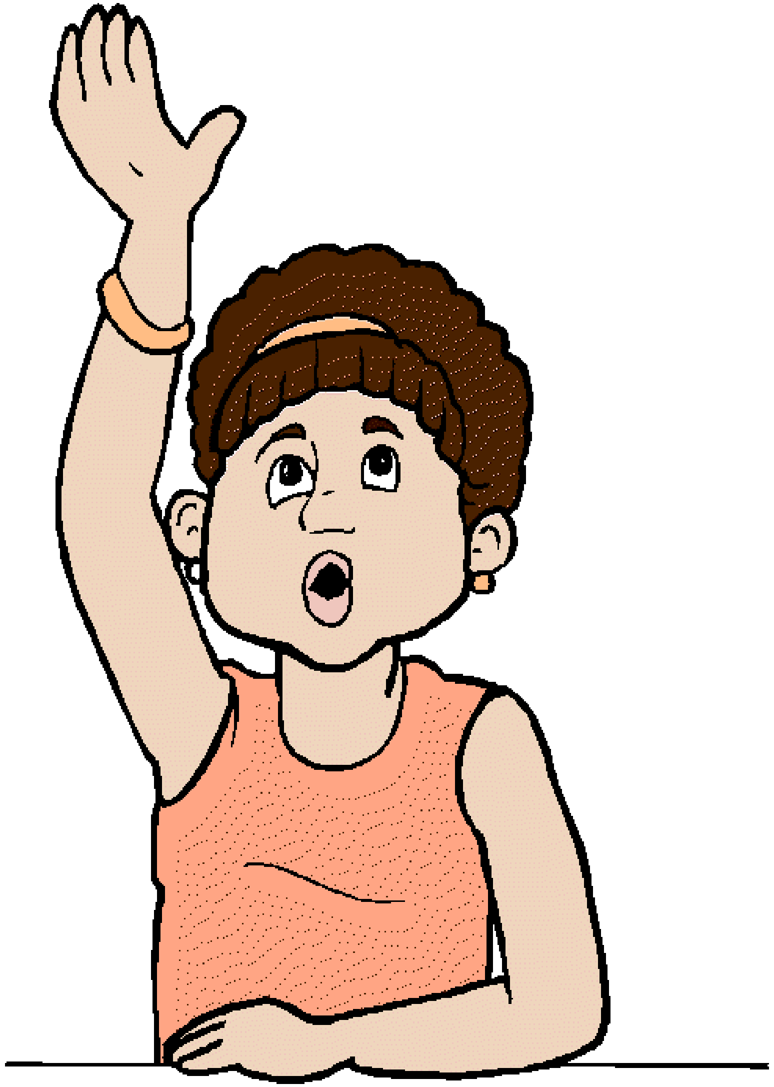
FEAL - REDOC

LOKI - GOST

CAST - Blowfish

Safer - Crab

RC5 -



Types of Cryptography

Problems with Conventional Cryptography

Key Management

Symmetric-key systems are simpler and faster; their main drawback is that the two parties must somehow exchange the key in a secure way and keep it secure after that.

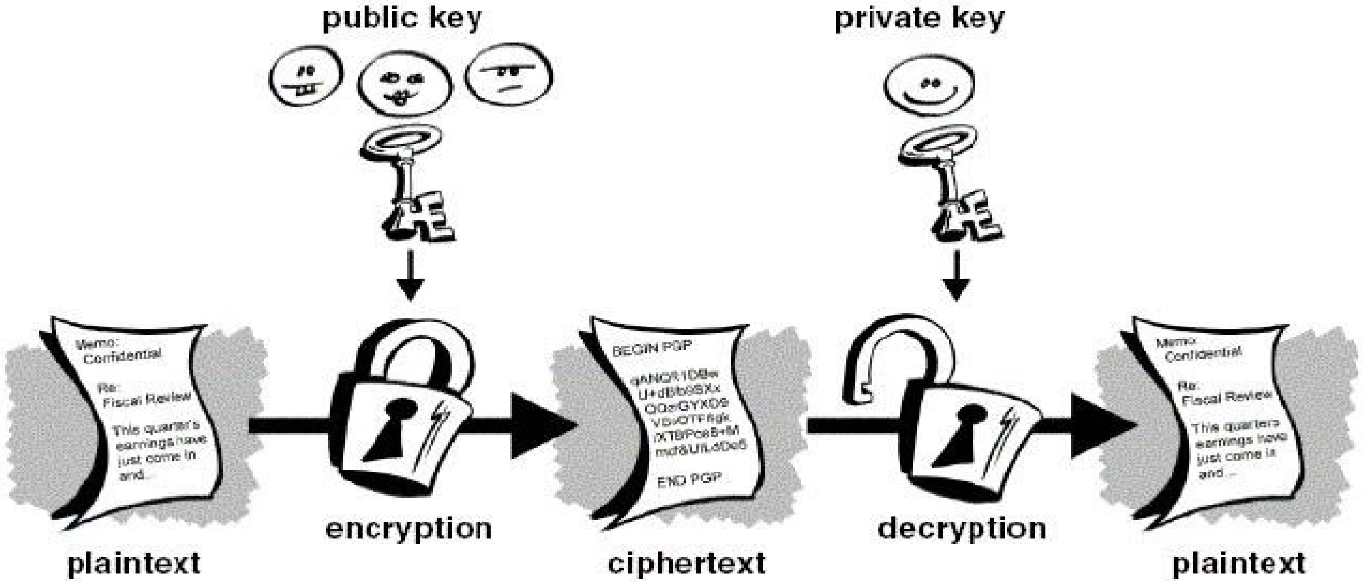
Key Management caused nightmare for the parties using the symmetric key cryptography. They were worried about how to get the keys safely and securely across to all users so that the decryption of the message would be possible. This gave the chance for third parties to intercept the keys in transit to decode the top-secret messages. Thus, if the key was compromised, the entire coding system was compromised and a “Secret” would no longer remain a “Secret”.

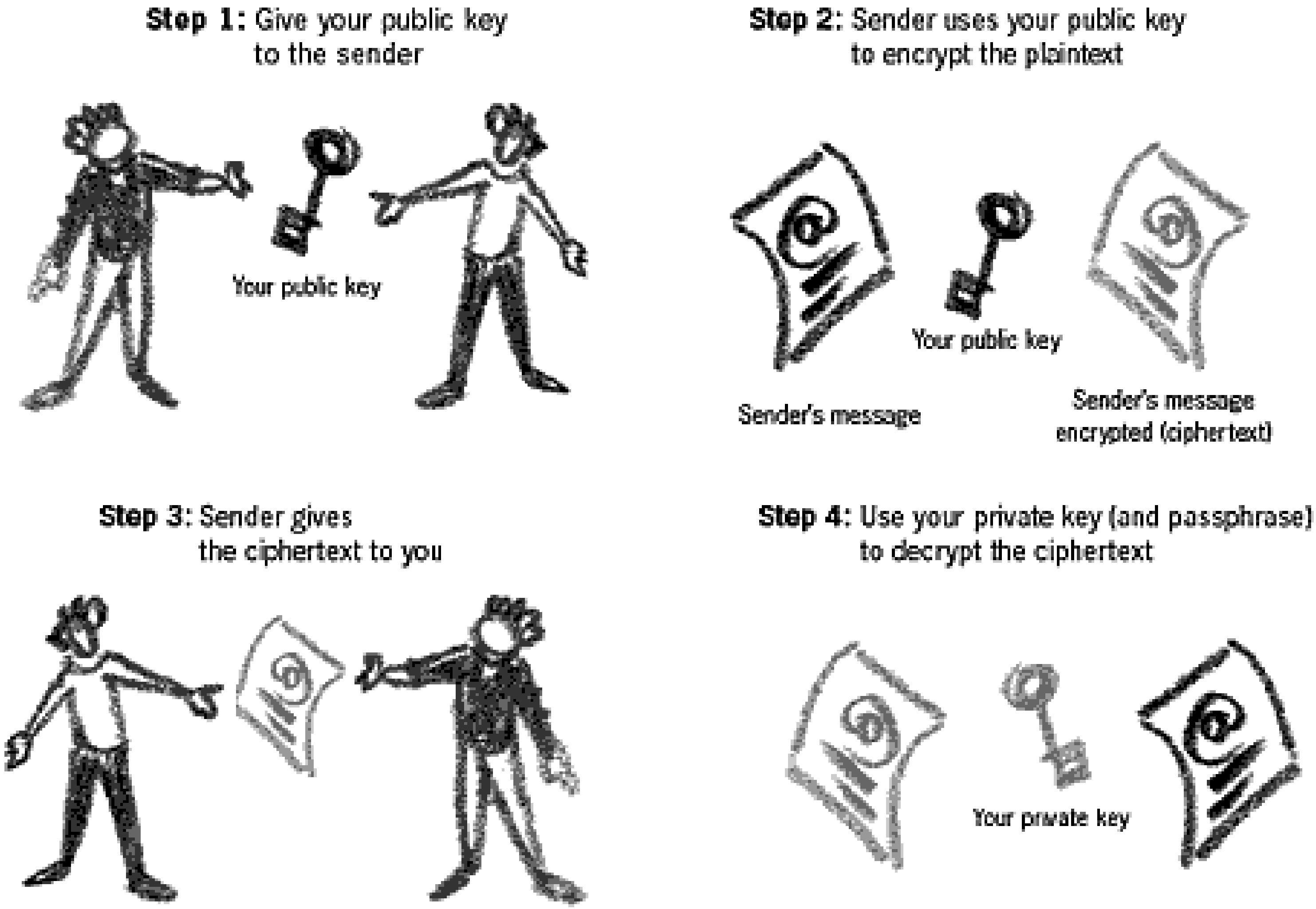
This is why the “Public Key Cryptography” came into existence.

Types of Cryptography

Asymmetric Key Cryptography

Asymmetric cryptography , also known as Public-key cryptography, refers to a cryptographic algorithm which requires two separate keys, one of which is private and one of which is public. The public key is used to encrypt the message and the private one is used to decrypt the message.





Step 1: Give your public key to the sender

Step 2: Sender uses your public key to encrypt the plaintext

Step 3: Sender gives the ciphertext to you

Step 4: Use your private key (and passphrase) to decrypt the ciphertext

Types of Cryptography

Asymmetric Key Cryptography

Public Key Cryptography is a very advanced form of cryptography.

Officially, it was invented by Whitfield Diffie and Martin Hellman in 1975.

The basic technique of public key cryptography was first discovered in 1973 by the British Clifford Cocks of Communications-Electronics Security Group (CESG) of (Government Communications Headquarters - GCHQ) but this was a secret until 1997.

Types of Cryptography

Asymmetric Key Cryptography - Examples

Digital Signature Standard (DSS)

Digital Signature Standard (DSS) is the digital signature algorithm (DSA) developed by the U.S. National Security Agency (NSA) to generate a digital signature for the authentication of electronic documents. DSS was put forth by the National Institute of Standards and Technology (NIST) in 1994, and has become the United States government standard for authentication of electronic documents. DSS is specified in Federal Information Processing Standard (FIPS) 186.

Types of Cryptography

Asymmetric Key Cryptography - Examples

Algorithm - RSA

RSA (Rivest, Shamir and Adleman who first publicly described it in 1977) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography.

RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

Types of Cryptography

Asymmetric Key Cryptography - Examples

RSA Cryptanalysis

Rivest, Shamir, and Adelman placed a challenge in Martin Gardner’s column in Scientific American (journal) in which the readers were invited to crack.

C=114,381,625,757,888,867,669,235,779,976,146,612,010,218,296,721,242,362,562,561,842,935,706,935
,245,733,897,830,597,123,563,958,705,058,989,075,147,599,290,026,879,543,541

Types of Cryptography

Asymmetric Key Cryptography - Examples

RSA Cryptanalysis

This was solved in April 26, 1994, cracked by an international effort via the internet with the use of **1600 workstations, mainframes, and supercomputers attacked the number for eight months before finding its Public key and its private key**.

Encryption key = **9007**

The message "**first solver wins one hundred dollars**".

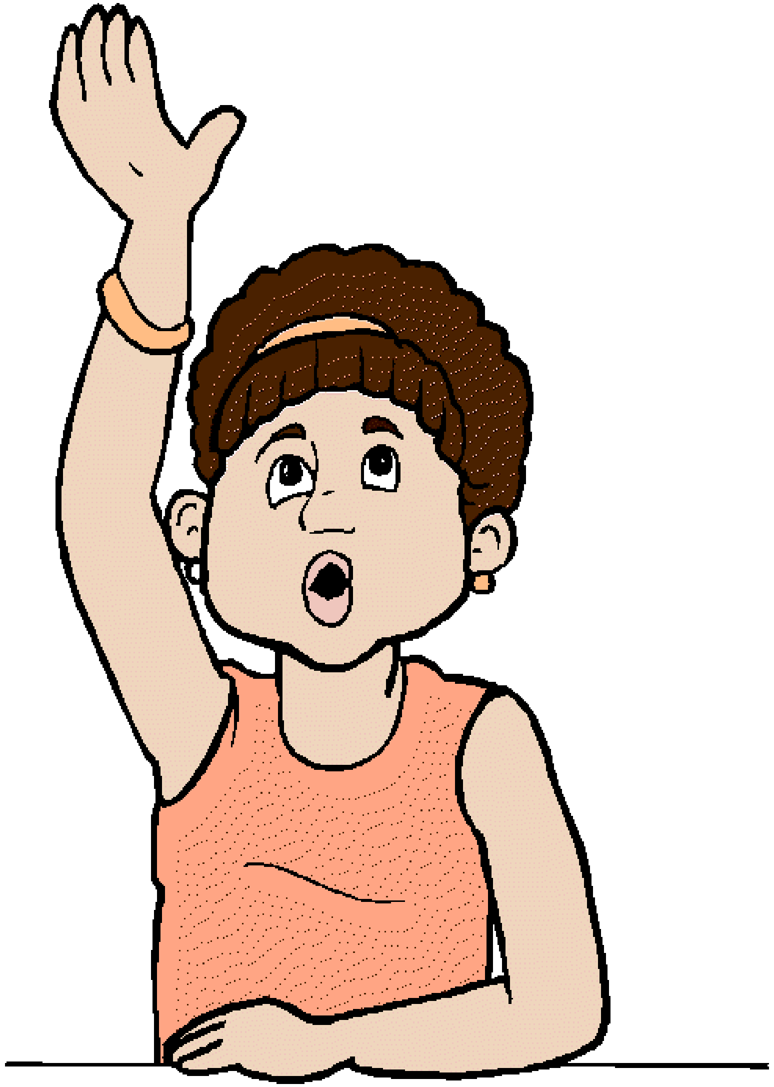
Of course, the **RSA** algorithm is safe, as it would be incredibly difficult to gather up such international participation to commit malicious acts.

Types of Cryptography

Asymmetric Key Cryptography - Examples

ElGamal

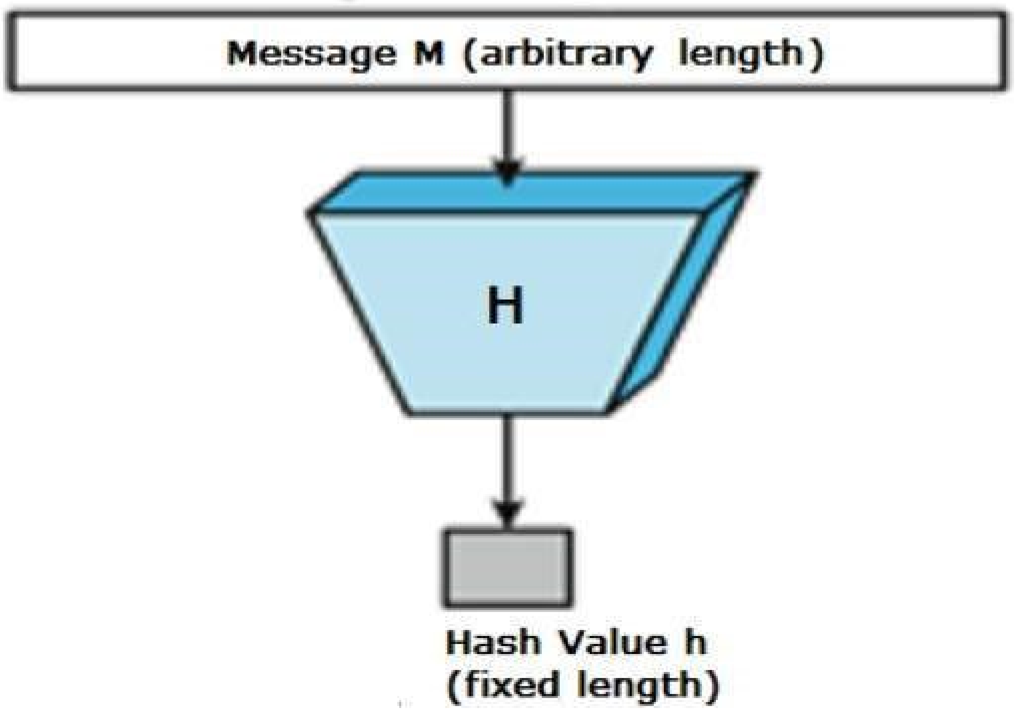
- ElGamal is a public key method that is used in both encryption and digital signing.
- The encryption algorithm is similar in nature to the Diffie-Hellman key agreement protocol
- It is used in many applications and uses discrete logarithms.
- ElGamal encryption is used in the free GNU Privacy Guard software



Hash Functions

What is a Hash Function

A cryptographic hash function is a hash function that takes an arbitrary block of data and returns a fixed-size bit string, the cryptographic hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded are often called the message, and the hash value is sometimes called the message digest or simply digest.

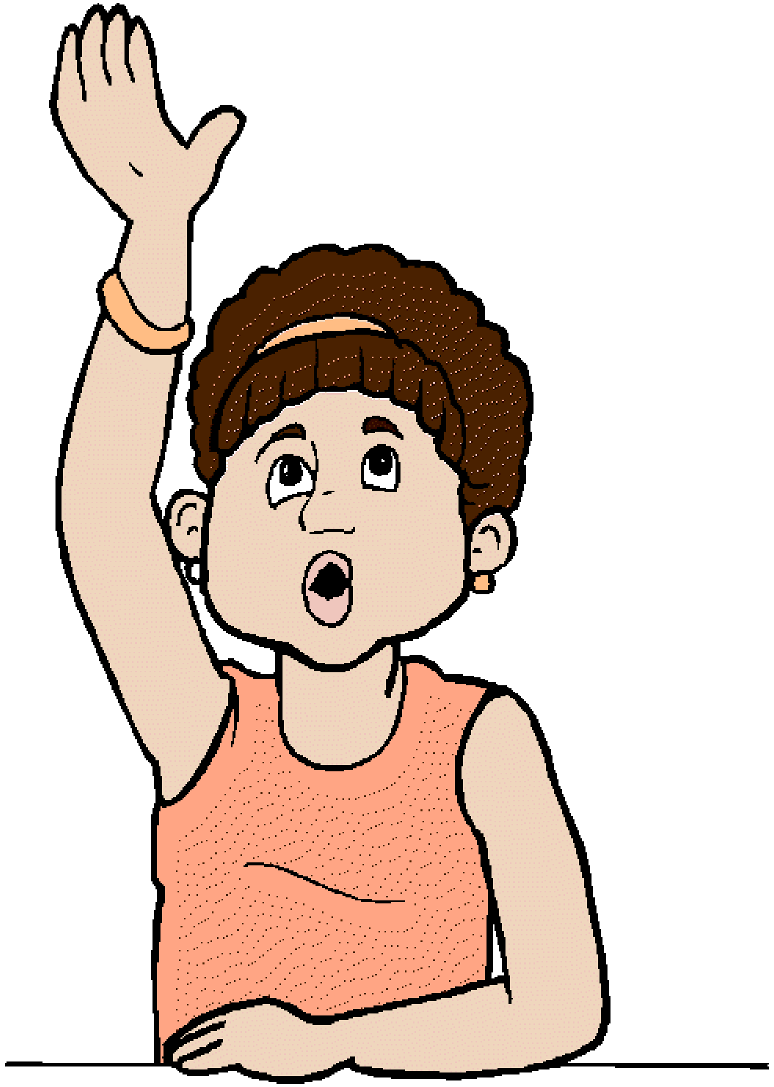


Hash Functions

What is a Hash Function

The ideal cryptographic hash function has four main properties:

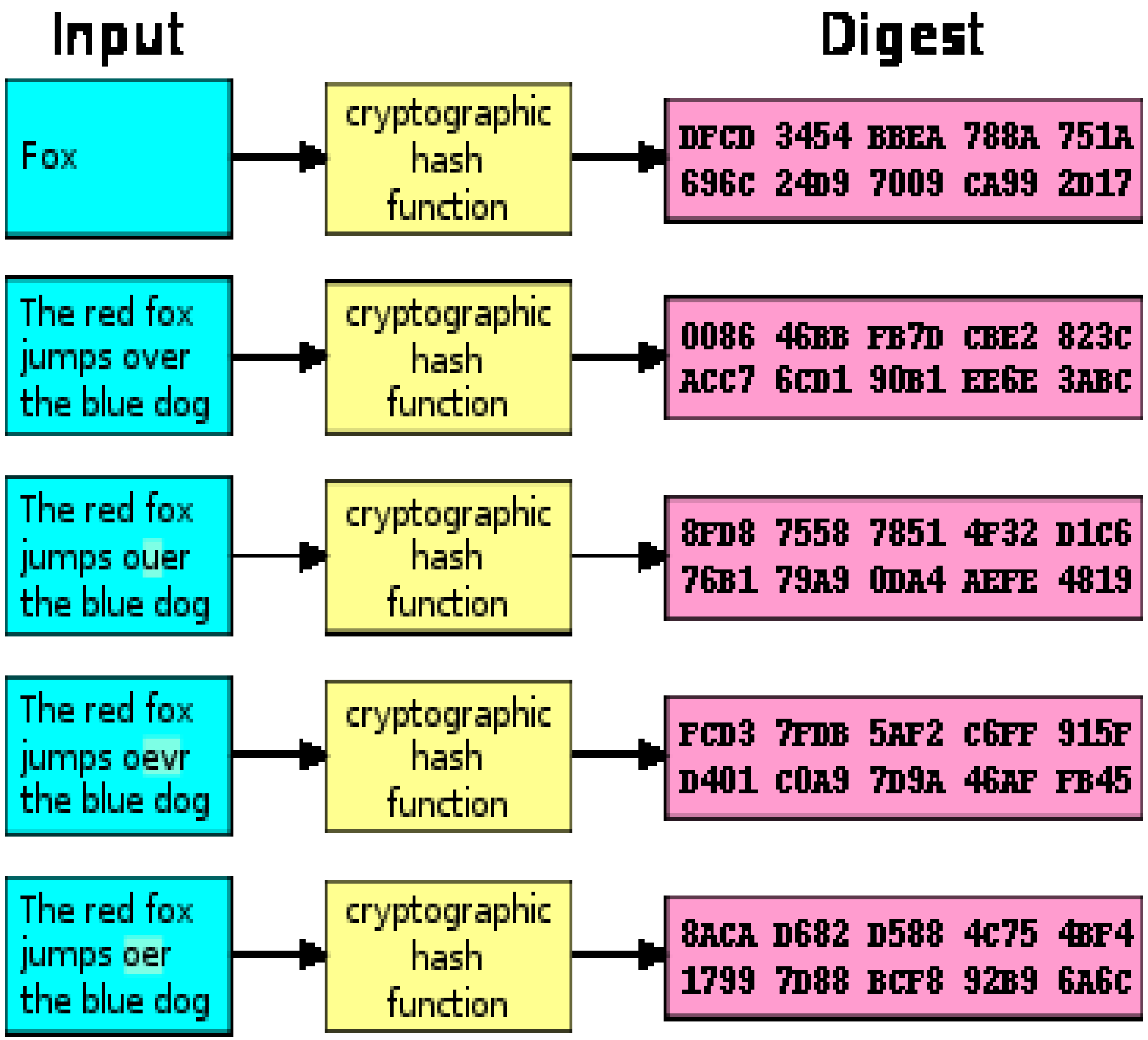
- it is easy to compute the hash value for any given message
- it is infeasible to generate a message that has a given hash
- it is infeasible to modify a message without changing the hash
- it is infeasible to find two different messages with the same hash.



Hash Functions

Hash Function - Examples

Snefru		Ralph Merkle	
N-Hash		Nippon T.T.	
Message Digest	MD2	(RFC 1115)	B. Kaliski
	MD4	(RFC1320)	Ron Rivest
	MD5	(RFC 1321)	Ron Rivest
	MD6		
SHA1			
SHA2			



Input		Digest
Fox	cryptographic hash function	DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog	cryptographic hash function	0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog	cryptographic hash function	8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog	cryptographic hash function	FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog	cryptographic hash function	8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

DATA INPUT	=	MD5 HASH VALUE
"Superman"	=	527D60CD4715DB174AD56CDA34AB2DCE
"A mind needs books as a sword needs a whetstone, if it is to keep its edge." *(Game of Thrones)*	=	7CE452645B7DF2549C02AECD26CA7E67
Shopping List.txt	=	B5DA1ACF7885741738508ABC704E519F
 Watermelon Man.mp3	=	6B4CB3F6963CAE53A2F23347A5680AD7

Hash Functions

Collusion Discovery

In March 2005 Xiaoyun Wang and Hongbo Yu of Shandong University in China created a pair of files that share the same MD5 checksum hence prove that there is a collusion when using MD5

Hash Functions

By Xiaoyun Wang and Hongbo Yu

Collusion Discovery

file1.dat

```
00000000 d1 31 dd 02 c5 e6 ee c4 69 3d 9a 06 98 af f9 5c
00000010 2f ca b5 87 12 46 7e ab 40 04 58 3e b8 fb 7f 89
00000020 55 ad 34 06 09 f4 b3 02 83 e4 88 83 25 71 41 5a
00000030 08 51 25 e8 f7 cd c9 9f d9 1d bd f2 80 37 3c 5b
00000040 96 0b 1d d1 dc 41 7b 9c e4 d8 97 f4 5a 65 55 d5
00000050 35 73 9a c7 f0 eb fd 0c 30 29 f1 66 d1 09 b1 8f
00000060 75 27 7f 79 30 d5 5c eb 22 e8 ad ba 79 cc 15 5c
00000070 ed 74 cb dd 5f c5 d3 6d b1 9b 0a d8 35 cc a7 e3
```

file2.dat

```
00000000 d1 31 dd 02 c5 e6 ee c4 69 3d 9a 06 98 af f9 5c
00000010 2f ca b5 07 12 46 7e ab 40 04 58 3e b8 fb 7f 89
00000020 55 ad 34 06 09 f4 b3 02 83 e4 88 83 25 f1 41 5a
00000030 08 51 25 e8 f7 cd c9 9f d9 1d bd 72 80 37 3c 5b
00000040 96 0b 1d d1 dc 41 7b 9c e4 d8 97 f4 5a 65 55 d5
00000050 35 73 9a 47 f0 eb fd 0c 30 29 f1 66 d1 09 b1 8f
00000060 75 27 7f 79 30 d5 5c eb 22 e8 ad ba 79 4c 15 5c
00000070 ed 74 cb dd 5f c5 d3 6d b1 9b 0a 58 35 cc a7 e3
```

Hash Functions

Collusion Discovery

file1.dat

```
00000000 d1 31 dd 02 c5 e6 ee c4 69 3d 9a 06 98 af f9 5c
00000010 2f ca b5 87 12 46 7e ab 40 04 58 3e b8 fb 7f 89
00000020 55 ad 34 06 09 f4 b3 02 83 e4 88 83 25 71 41 5a
00000030 08 51 25 e8 f7 cd c9 9f d9 1d bd f2 80 37 3c 5b
00000040 96 0b 1d d1 dc 41 7b 9c e4 d8 97 f4 5a 65 55 d5
00000050 35 73 9a c7 f0 eb fd 0c 30 29 f1 66 d1 09 b1 8f
00000060 75 27 7f 79 30 d5 5c eb 22 e8 ad ba 79 cc 15 5c
00000070 ed 74 cb dd 5f c5 d3 6d b1 9b 0a d8 35 cc a7 e3
```

file2.dat

```
00000000 d1 31 dd 02 c5 e6 ee c4 69 3d 9a 06 98 af f9 5c
00000010 2f ca b5 07 12 46 7e ab 40 04 58 3e b8 fb 7f 89
00000020 55 ad 34 06 09 f4 b3 02 83 e4 88 83 25 f1 41 5a
00000030 08 51 25 e8 f7 cd c9 9f d9 1d bd 72 80 37 3c 5b
00000040 96 0b 1d d1 dc 41 7b 9c e4 d8 97 f4 5a 65 55 d5
00000050 35 73 9a 47 f0 eb fd 0c 30 29 f1 66 d1 09 b1 8f
00000060 75 27 7f 79 30 d5 5c eb 22 e8 ad ba 79 4c 15 5c
00000070 ed 74 cb dd 5f c5 d3 6d b1 9b 0a 58 35 cc a7 e3
```

Hash Functions

Collusion Discovery

Checking

```
$ md5sum file1.dat
MD5 Sum = a4c0d35c95a63a805915367dcfe6b751
$ md5sum file2.dat
MD5 Sum = a4c0d35c95a63a805915367dcfe6b751
```

By Xiaoyun Wang and Hongbo Yu of Shandong University in China - March 2005

Visit the following websites for more information

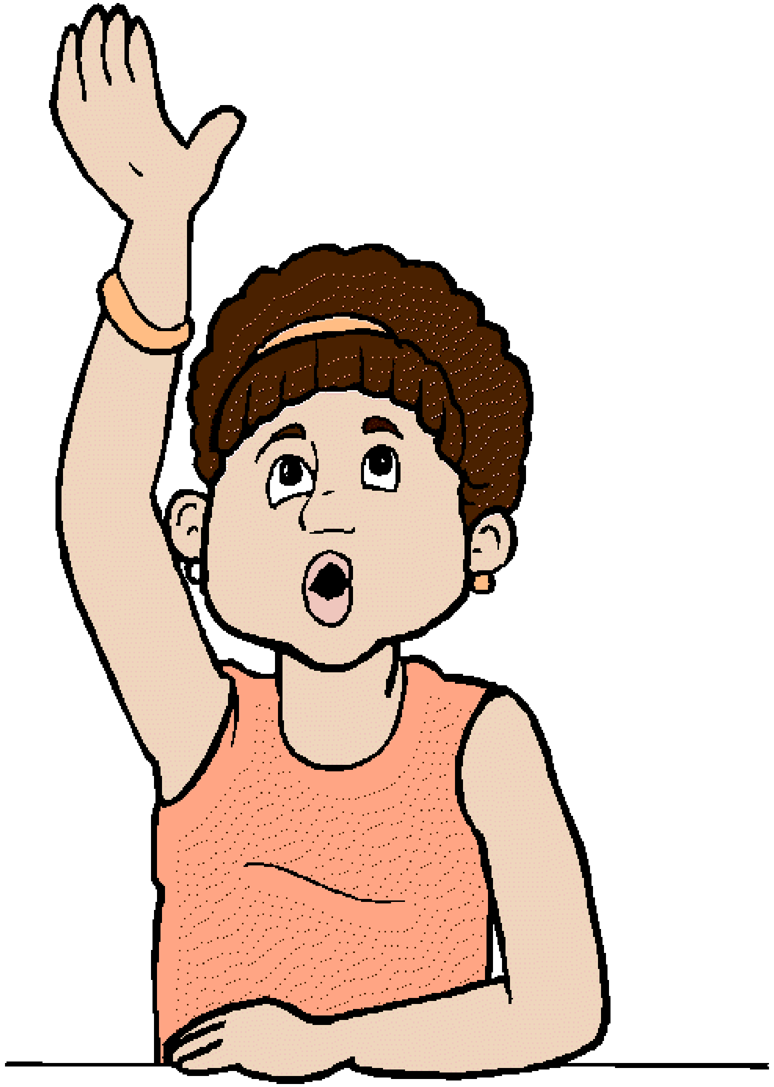
http://www.mscs.dal.ca/~selinger/md5collision/
http://www.x-ways.net/md5collision.html

Examples of Hash Function

SHA

The Secure Hash Algorithm (**SHA**) hash functions are a set of cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard.

- SHA stands for Secure Hash Algorithm.
- Because of the successful attacks on MD5, SHA-0 and theoretical attacks on SHA-1, NIST perceived a need for an alternative, dissimilar cryptographic hash, which became SHA-3.
- In October 2012, the National Institute of Standards and Technology (NIST) chose the **Keccak** algorithm as the new SHA-3 standard.



Thank you