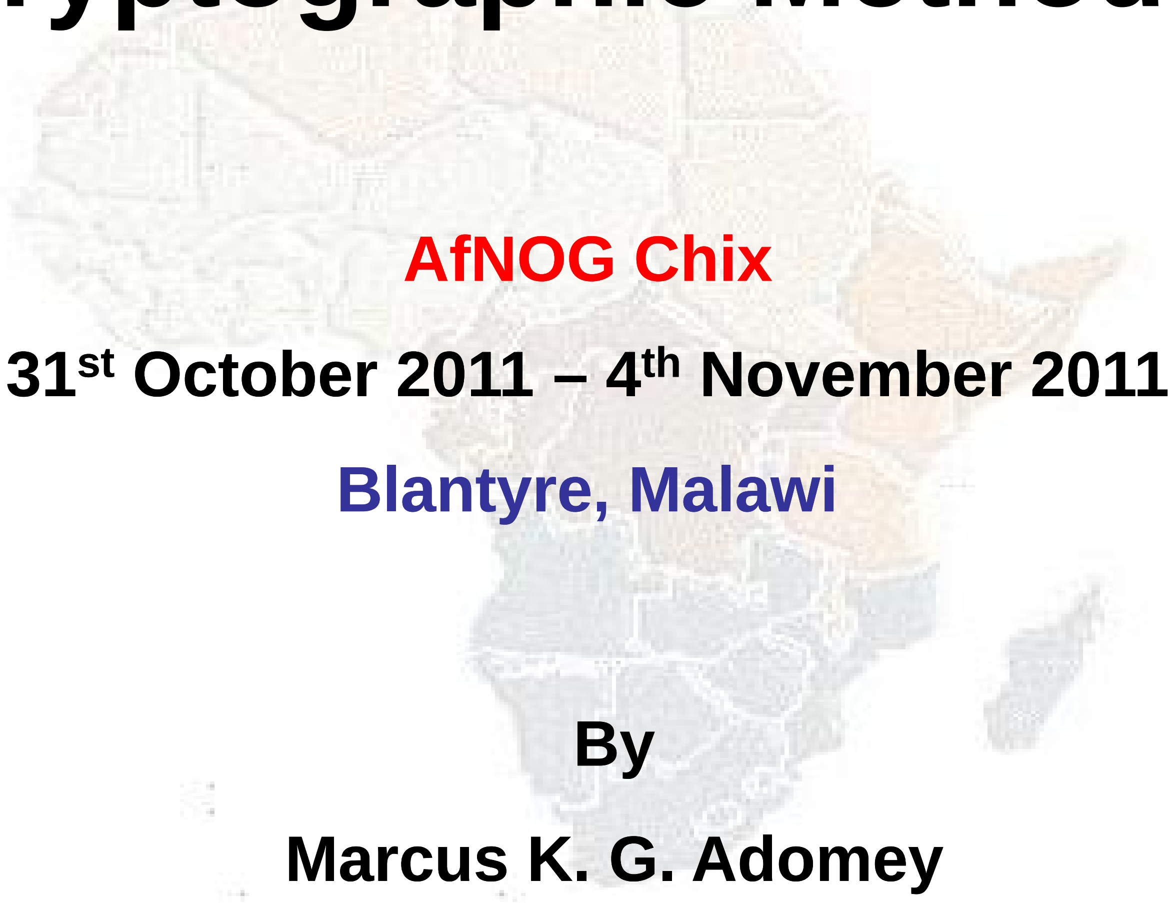
Cryptographic Methods



AfNOG Chix

31st October 2011 – 4th November 2011

Blantyre, Malawi

By

Marcus K. G. Adomey

OVERVIEW

1. Cryptography
    a. Definition
    b. Terminology
    c. History
    d. Goal of Cryptography
    e. Services of Cryptography
2. Types of Cryptography
    1. Symmetric Cryptography
    2. Asymmetric Cryptography
    3. Hash Function
3. Use of Cryptography
4. Some Cryptographic Tools
5. Useful Resources

1 - CRYPTOGRAPHY

Definition

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

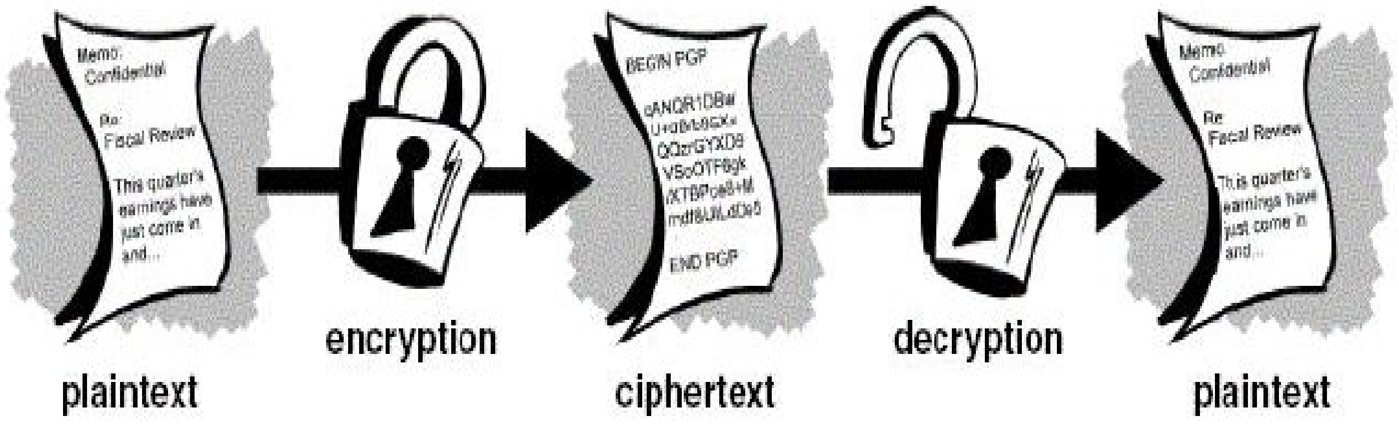
Phil Zimmermann

Cryptography is the art and science of keeping messages secure.

Bruce Schneier

TERMINOLOGY

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***.



TERMINOLOGY (cont.)

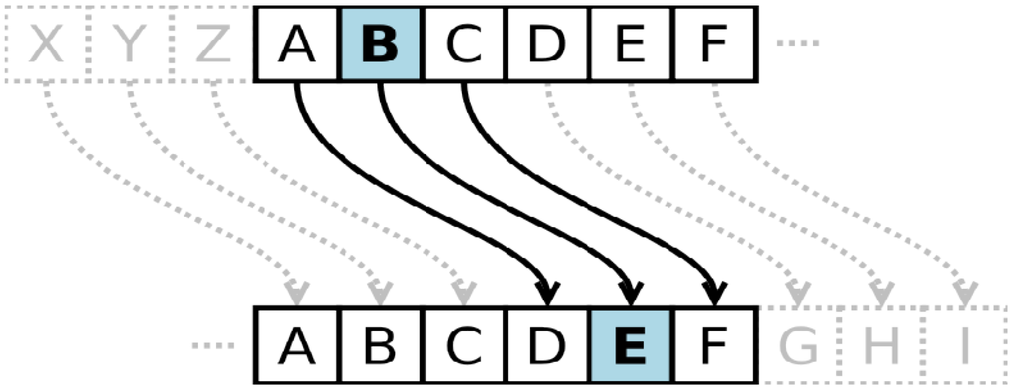
While cryptography is the science of securing data, ***cryptanalysis*** is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and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

Visit http://www.giac.org/resources/whitepaper/cryptography/57.php
For various attack

Cryptology embraces both cryptography and cryptanalysis.

Caesar's Cipher

- The Caesar cipher is named after Julius Caesar, who used it with a shift of three to protect messages of military significance.
- It is based on the substitution of one piece of information for another. This is done by offsetting letters of the alphabet.
- Using Caesar's key value of 3, we offset the alphabet so that the 3rd letter down (D) begins the alphabet



Plaintext

ABCDEFGHIJKLMNOPQRSTUVWXYZ

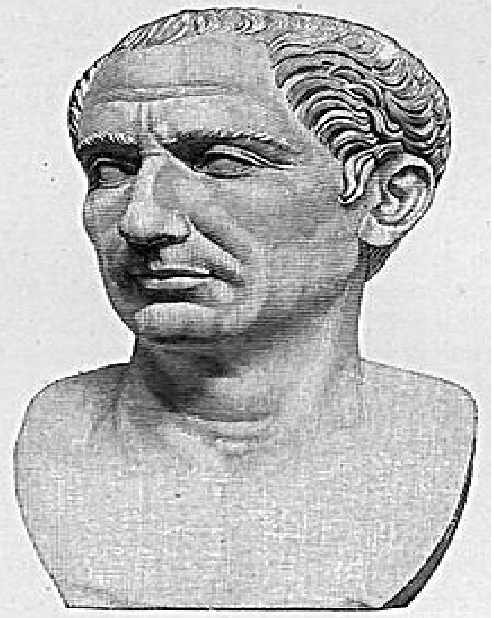
Ciphertext

DEFGHIJKLMNOPQRSTUVWXYZABC

where A=D (A encrypts as D) , B=E, C=F, and so on.

Example: With n = 3

Plaintext	**AFNOG SUCCESS**
Ciphertext	**DIQRJ VXFFHVV**



**Gaius Julius Caesar
(13 July 100 BC – 15 March 44 BC)**

HISTORY

Visit the following websites for more information

http://www.cypher.com.au/crypto_history.htm
http://en.wikipedia.org/wiki/History_of_cryptography
http://all.net/BOOKS/IP/cHAP2-1.HTML
http://www.slideshare.net/guest9006ab/a-brief-history-of-cryptography
http://www.billthelizard.com/2009/05/brief-history-of-cryptography.html
http://www.ridex.co.uk/cryptology/

Cryptography: 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.

Cryptography: Services

Cryptography can provide one or more of the following services:

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

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.

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

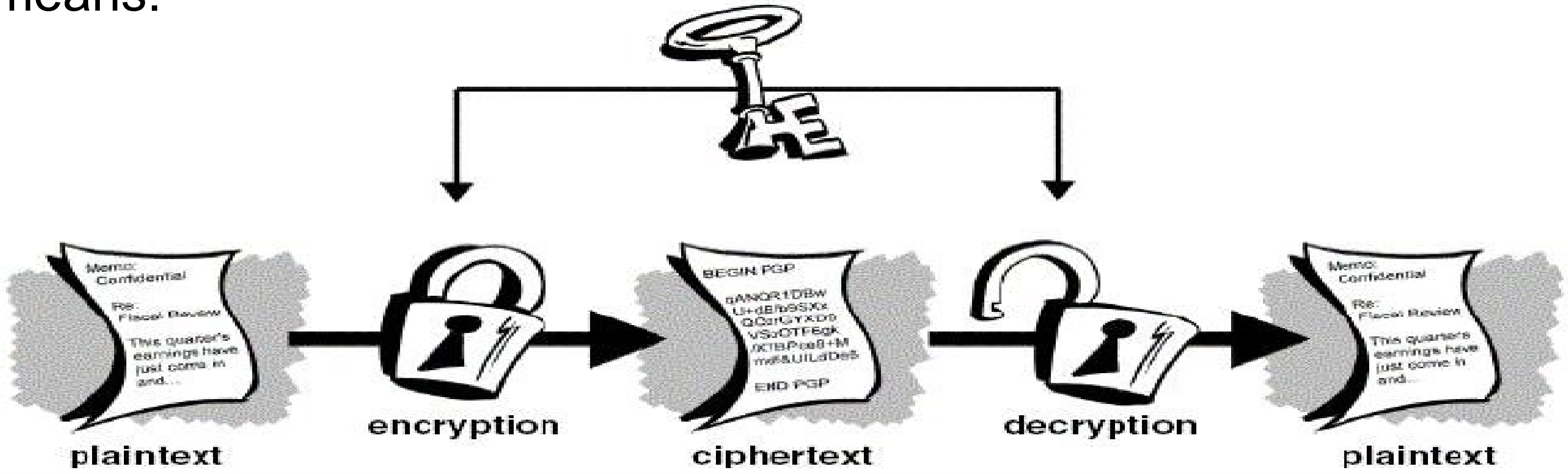
- A mechanism to prove that the sender really sent this message

Type of Cryptography

- ❑ Conventional Cryptography
  - ➢ Secret Key Cryptography
  - ➢ Symmetric Key Cryptography
- ❑ Public Key Cryptography
  - ➢ Asymmetric Key Cryptography

Conventional Cryptography

- In conventional cryptography, the key used for encryption and decryption of the message is the same. Since there is only one key for decryption as well as encryption, it is also called as “**Symmetric Cryptography**” or “**Symmetric Key Cryptography”**.
- This key (=“password”) for decrypting the file had to be known to all the recipients. Else, the message could not be decrypted by conventional means.



Examples of Symmetric Algorithms

Data Encryption Standard (DES)

The Data Encryption Standard was published in 1977 by the US National Bureau of Standards and became an ANSI standard subsequently. 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, the key size is indeed one of the most controversial aspects of this algorithm.

Examples of Symmetric Algorithms (Cont.)

Triple DES (3DES)

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.

Examples of Symmetric Algorithms (Cont.)

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).

Examples of Symmetric Algorithms (Cont.)

IDEA - International **D**ata **E**ncryption **A**lgorithm

- The IDEA 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.

Other Symmetric Algorithms

Lucifer - Madryga

FEAL - REDOC

LOKI - GOST

Blowfish - Towfish

Safer - Crab

RC5 - CAST

Problems with Conventional Cryptography

Key Management

Key Management caused nightmare for the parties using the conventional 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.

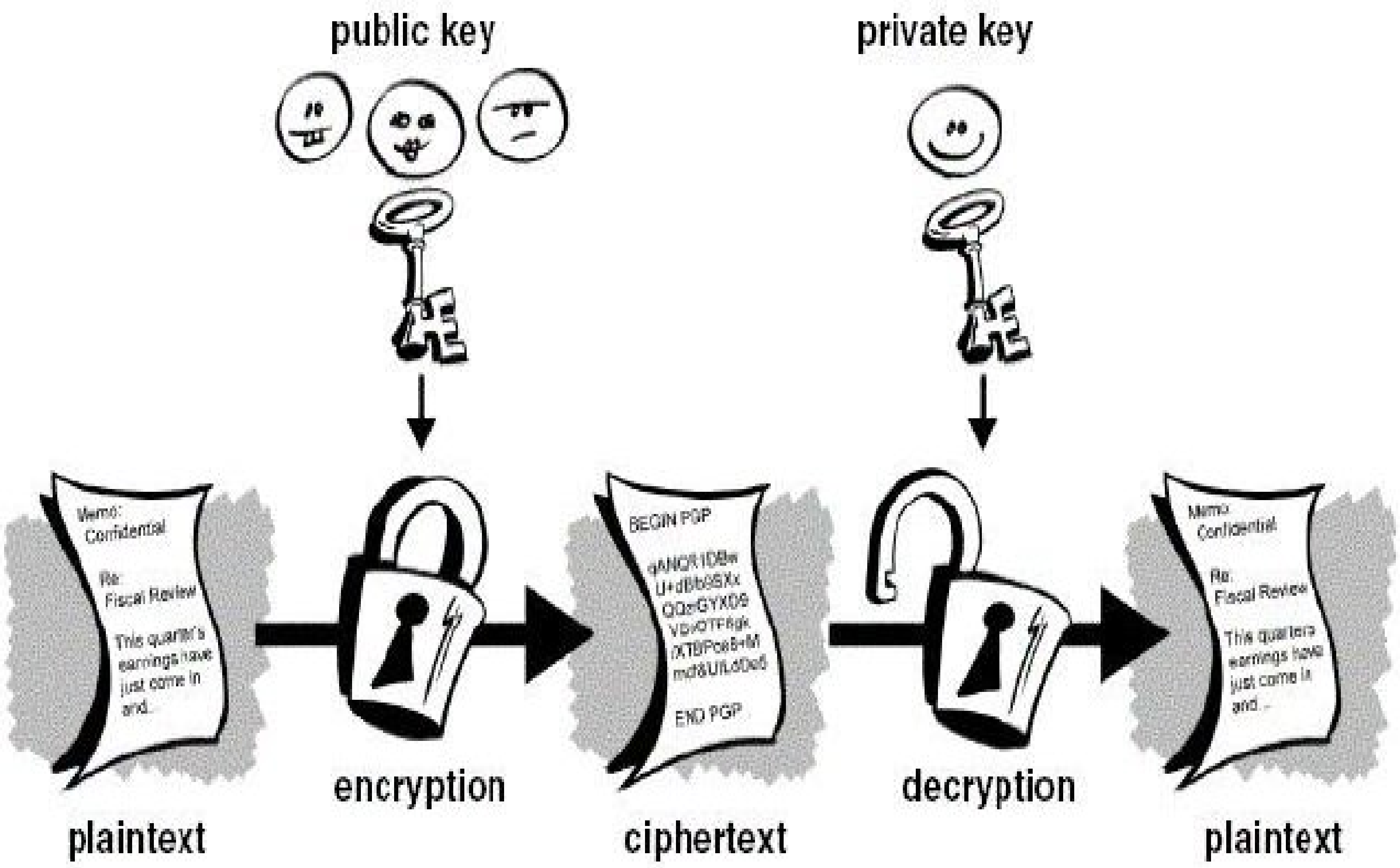
Public Key Cryptography

Invented in 1975 Whitfield Diffie, Ralph Merkle, and Martin Hellman.

The basic technique of public key cryptography was first discovered in 1973 by Clifford Cocks of CESG (part of the British GCHQ) but this was a secret until 1997.

It employs the use of two keys: one key is used to encrypt the message and the other one is used to decrypt the message. These two keys are referred to as the “public key” and the “private key” respectively.

Since this method employs the use of two different keys, it is also known as “Asymmetric Cryptography”. The pictorial description of the public key encryption system is given in the next slide.


public key
private key
Memo:
Confidential
Re:
Fiscal Review
This quarter's
earnings have
just come in
and...
BEGIN PGP
qANQR1DBw
U+dBb0SXx
QQsGYXD9
VDvOTF8gk
iXTBPos8+M
md8UfLdDe6
END PGP
encryption
decryption
plaintext
ciphertext
plaintext

Examples of public Key Algorithm

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.

Examples of public Key Algorithm (Cont.)

Summary of RSA Algorithm

- ✓ n = pq, where p and q are distinct primes.
- ✓ phi, φ = (p-1)(q-1)
- ✓ e < n such that gcd(e, phi)=1
- ✓ d = e-1 mod phi.
- ✓ c = me mod n, 1<m<n.
- ✓ m = cd mod n.

- n is known as the *modulus*.
- e is known as the *public exponent* or *encryption exponent* or just the *exponent*.
- d is known as the *secret exponent* or *decryption exponent*.

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

RSA Cryptanalysis (Cont.)

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.

Left to Right - Adi Shamir, Ron Rivest, Len Adleman, Ralph Merkle, Martin Hellman, and Whit Diffie on August 21 at Crypto 2001

Hash Function

Hash functions are algorithms that take a variable-size input and returns a fixed-size string, which is called the hash value

The ideal hash function has four main properties:

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

Examples of Hash Function

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		

In an attack on MD5 published in December 2008, a group of researchers used this technique to fake SSL certificate validity. U. S. Department of Homeland Security said MD5 "should be considered cryptographically broken and unsuitable for further use," and most U.S. government applications will be required to move to the SHA-2 family of hash functions by 2010.

Examples of Hash Function (Cont.)

SHA

- The **S**ecure **H**ash **A**lgorithm (**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.

- The three SHA algorithms are structured differently and are distinguished as SHA-0, SHA-1, and SHA-2.

Collusion Discovery

By Xiaoyun Wang and Hongbo Yu

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
```

Collusion Discovery

By Xiaoyun Wang and Hongbo Yu

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
```

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

Department of Homeland Security stated that MD5 "should be considered cryptographically broken and unsuitable for further use," and most U.S. government applications were required to move to the SHA-2 family of hash functions by 2010.

A new hash standard, SHA-3, is currently under development — the function will be selected via an open competition running between fall 2008 and 2012.

3 - Use of Cryptography

- Digital Signature
- Digital Certificate
- SSL
- SSH

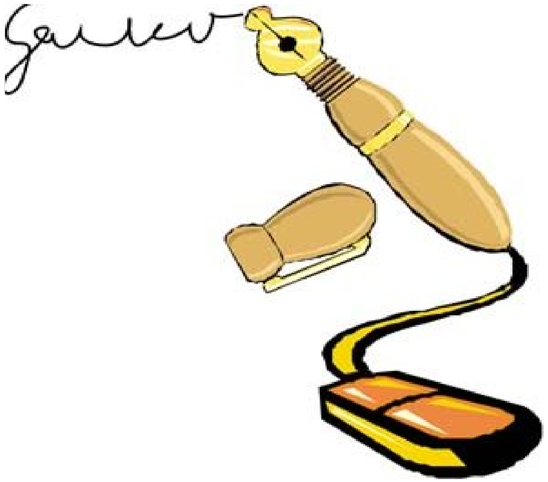
Secure Digital Signature

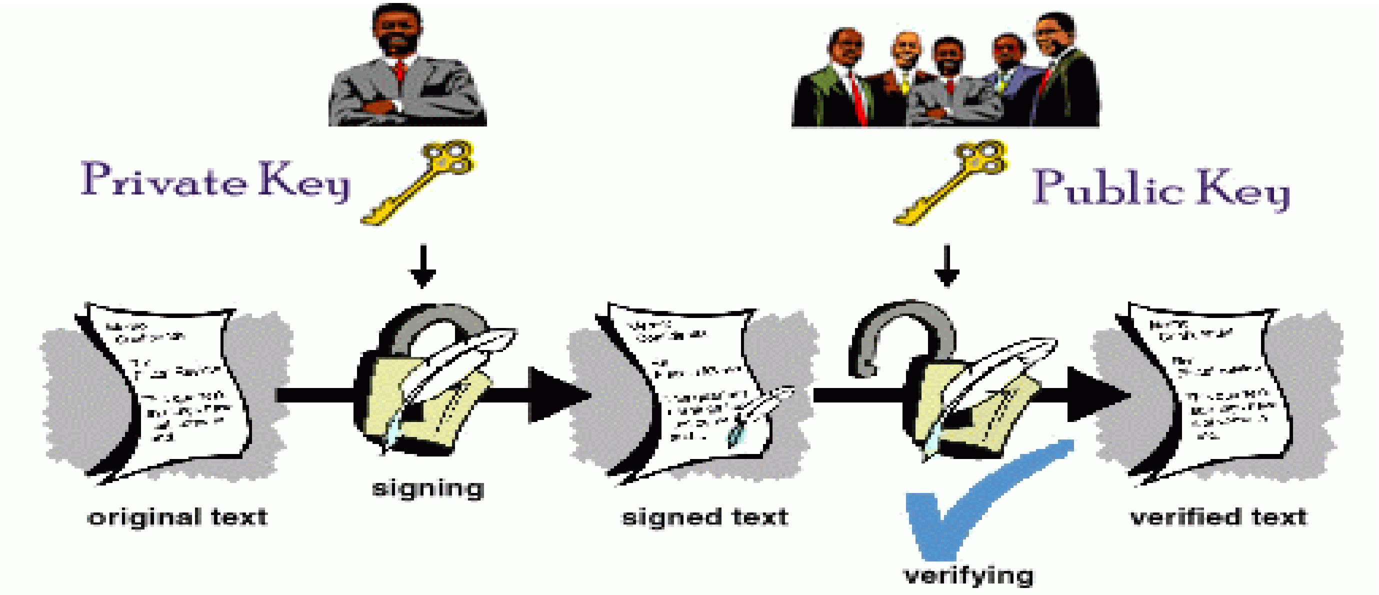
A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged.

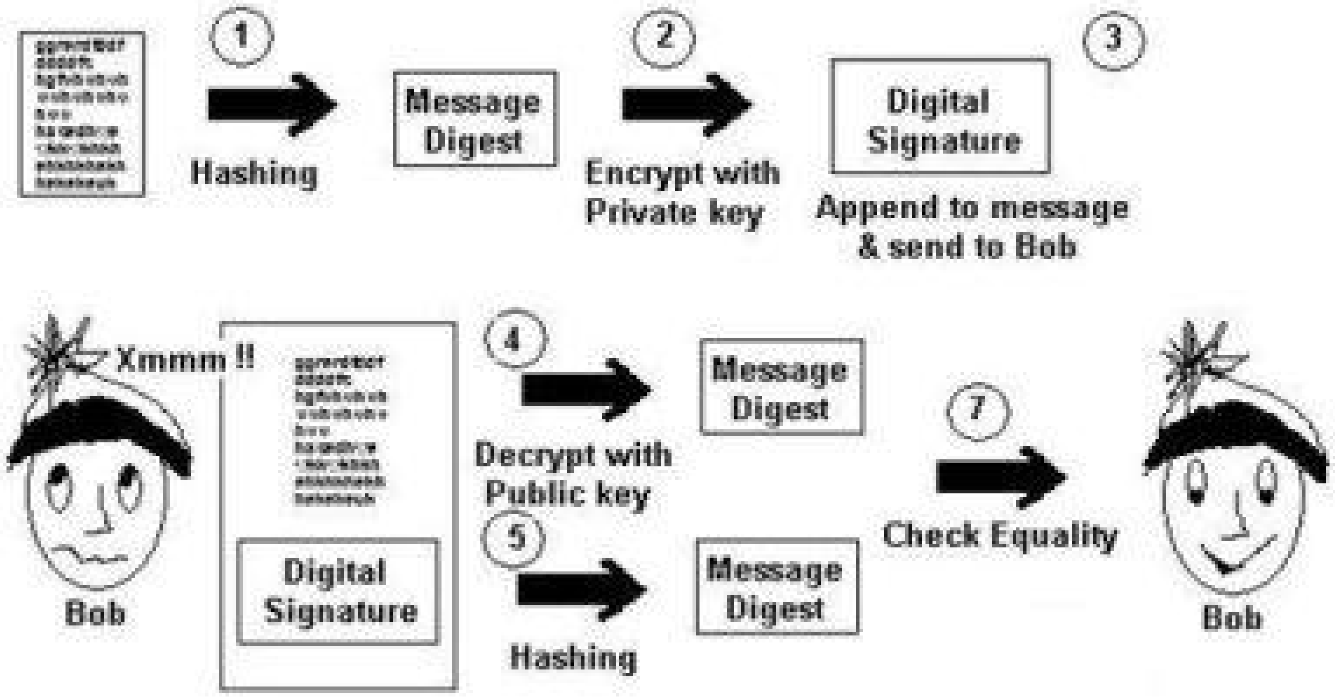
Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

Secure Digital Signature Cont.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact.




Private Key
Public Key
original text
signing
signed text
verifying
verified text


1
Hashing
Message Digest
2
Encrypt with Private key
Digital Signature
3
Append to message & send to Bob
Xmmm !!
Bob
Digital Signature
4
Decrypt with Public key
Message Digest
5
Hashing
Message Digest
7
Check Equality
Bob

Physical Signature vs Digital Signature

Physical Signature	Digital Signature
Physical Signature is just a writing on paper	Digital Signature encompasses crucial parameters of identification
Physical Signature can be copied	It is IMPOSSIBLE to copy a Digital signature
Physical Signature does not give privacy to content	Digital Signature also enables encryption and thus privacy
Physical Signature cannot protect the content	Digital Signature protects the content

Digital Certificate

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web.

It is issued by a ***certification authority*** (CA).

It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

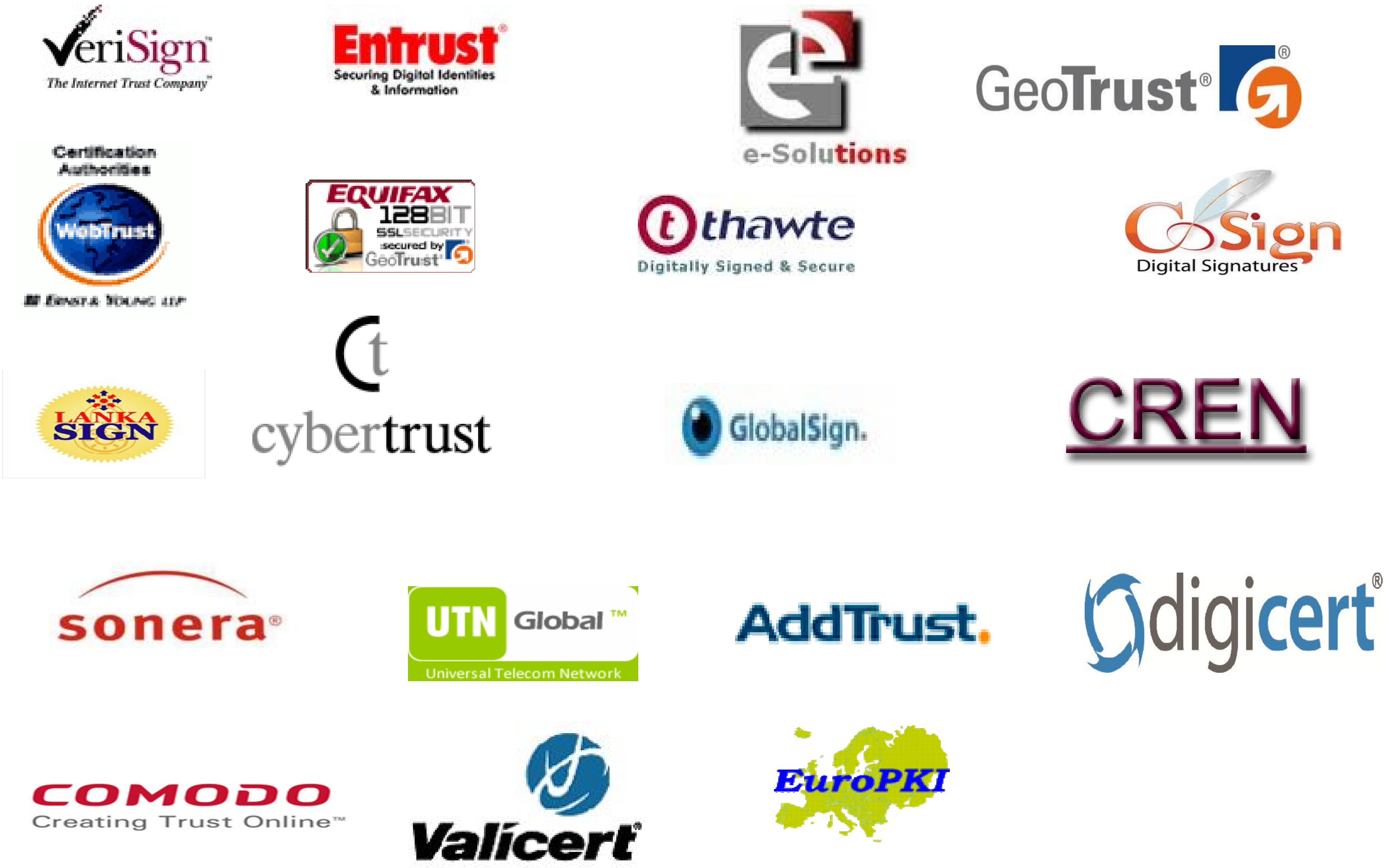
Certificate Authority

A certificate authority (CA) is an authority in a network that issues and manages security credentials and public keys for message encryption.

A CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate.

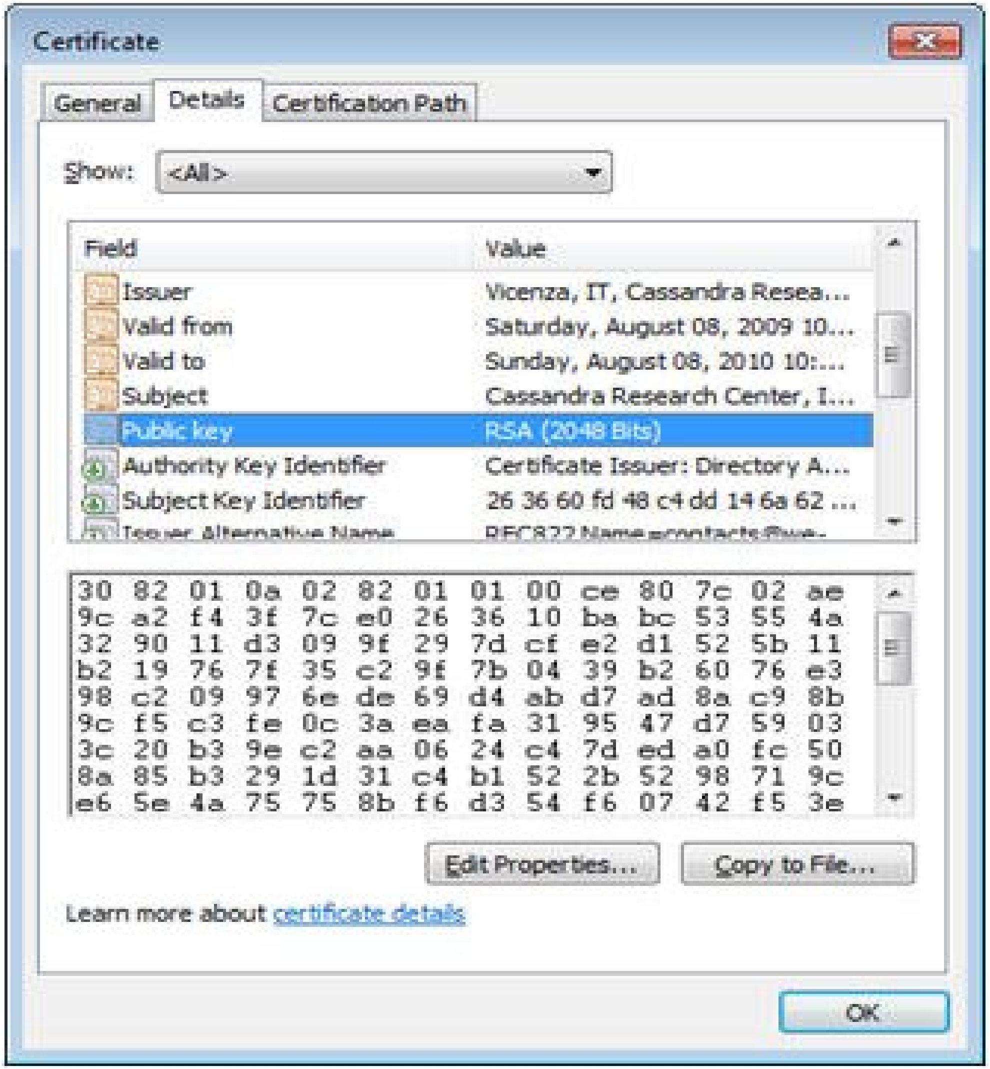
If the RA verifies the requestor's information, the CA can then issue a certificate.

Some Certificate Authorities



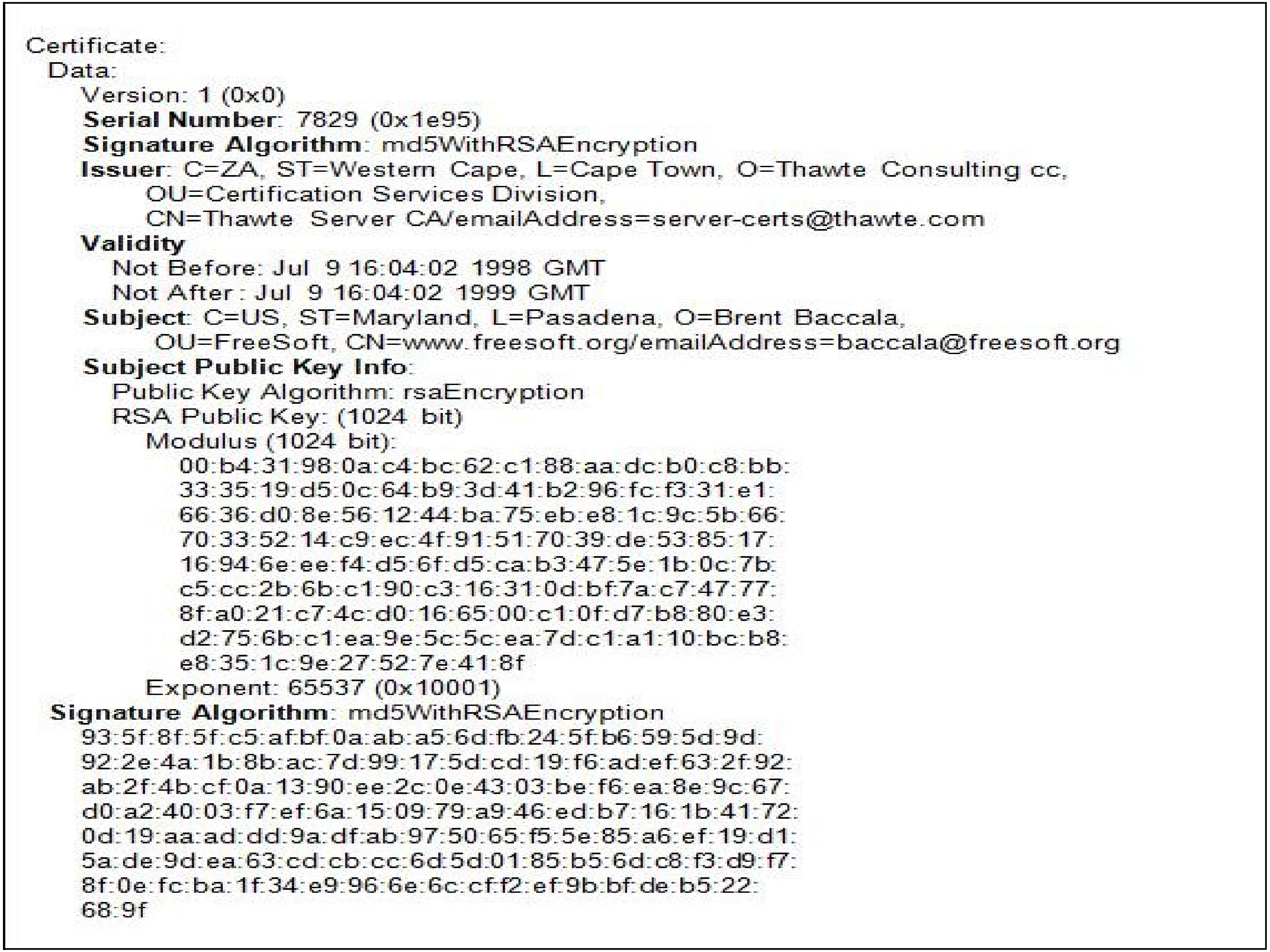
Examples of Digital Certificate

certmgr.msc



Field	Value
Issuer	Vicenza, IT, Cassandra Resea...
Valid from	Saturday, August 08, 2009 10...
Valid to	Sunday, August 08, 2010 10:...
Subject	Cassandra Research Center, I...
Public key	RSA (2048 Bits)
Authority Key Identifier	Certificate Issuer: Directory A...
Subject Key Identifier	26 36 60 fd 48 c4 dd 14 6a 62 ...
Issuer Alternative Name	RFC822 Name=contacts@we-

```
30 82 01 0a 02 82 01 01 00 ce 80 7c 02 ae
9c a2 f4 3f 7c e0 26 36 10 ba bc 53 55 4a
32 90 11 d3 09 9f 29 7d cf e2 d1 52 5b 11
b2 19 76 7f 35 c2 9f 7b 04 39 b2 60 76 e3
98 c2 09 97 6e de 69 d4 ab d7 ad 8a c9 8b
9c f5 c3 fe 0c 3a ea fa 31 95 47 d7 59 03
3c 20 b3 9e c2 aa 06 24 c4 7d ed a0 fc 50
8a 85 b3 29 1d 31 c4 b1 52 2b 52 98 71 9c
e6 5e 4a 75 75 8b f6 d3 54 f6 07 42 f5 3e
```



```
Certificate:
  Data:
      Version: 1 (0x0)
      Serial Number: 7829 (0x1e95)
      Signature Algorithm: md5WithRSAEncryption
      Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
              OU=Certification Services Division,
              CN=Thawte Server CA/emailAddress=server-certs@thawte.com
      Validity
         Not Before: Jul  9 16:04:02 1998 GMT
         Not After : Jul  9 16:04:02 1999 GMT
      Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
               OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@freesoft.org
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (1024 bit)
            Modulus (1024 bit):
               00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
               33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
               66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
               70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
               16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
               c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
               8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
               d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
               e8:35:1c:9e:27:52:7e:41:8f
            Exponent: 65537 (0x10001)
  Signature Algorithm: md5WithRSAEncryption
      93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
      92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
      ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
      d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
      0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
      5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
      8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
      68:9f
```

Applications of Digital Signature and Certificate

E-commerce

E-Banking

E-Health

…

Secure Shell (SSH)

Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

SSH was designed as a replacement for Telnet and other insecure remote shells, which send information, notably passwords, in plaintext, rendering them susceptible to packet analysis.

The encryption used by SSH provides confidentiality and integrity of data over an insecure network, such as the Internet.

SSH program enables users

- to log into another computer over a network,
- to execute commands in a remote machine, and
- to move files from one machine to another.

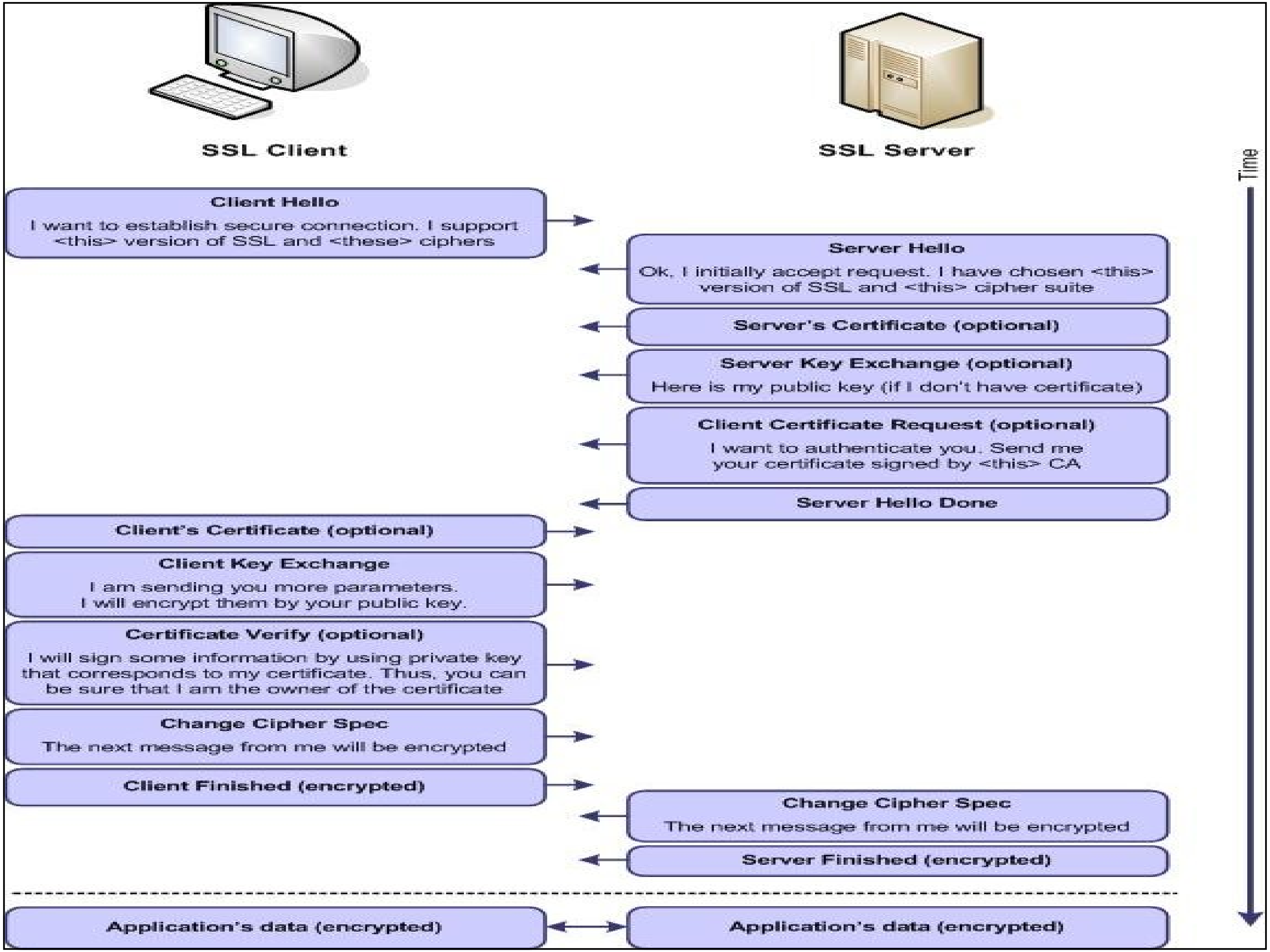
It provides strong authentication and secure communications over unsecure channels. It is intended as a replacement for rlogin, rsh, and rcp.

TLS/SSL

Transport Layer Security (TLS) /Secure Sockets Layer (SSL) is the most widely known protocol that offers privacy and good reliability for client-server communication over the Internet.

It negotiates the cryptography algorithms and keys between two sides of a communication, and establishes an encrypted tunnel through which other protocols (like HTTP) can be transported.

Since invention of SSL v1.0 (which has never been released, by the way) there have been at least five protocols: SSL v2.0, PCT v1.0, SSL v3.0, TLS v1.0 (also known as SSL v3.1) and WTLS



Client Hello

I want to establish secure connection. I support <this> version of SSL and <these> ciphers

Server Hello

Ok, I initially accept request. I have chosen <this> version of SSL and <this> cipher suite

Server's Certificate (optional)

Server Key Exchange (optional)

Here is my public key (if I don't have certificate)

Client Certificate Request (optional)

I want to authenticate you. Send me your certificate signed by <this> CA

Server Hello Done

Client's Certificate (optional)

Client Key Exchange

I am sending you more parameters.
I will encrypt them by your public key.

Certificate Verify (optional)

I will sign some information by using private key that corresponds to my certificate. Thus, you can be sure that I am the owner of the certificate

Change Cipher Spec

The next message from me will be encrypted

Client Finished (encrypted)

Change Cipher Spec

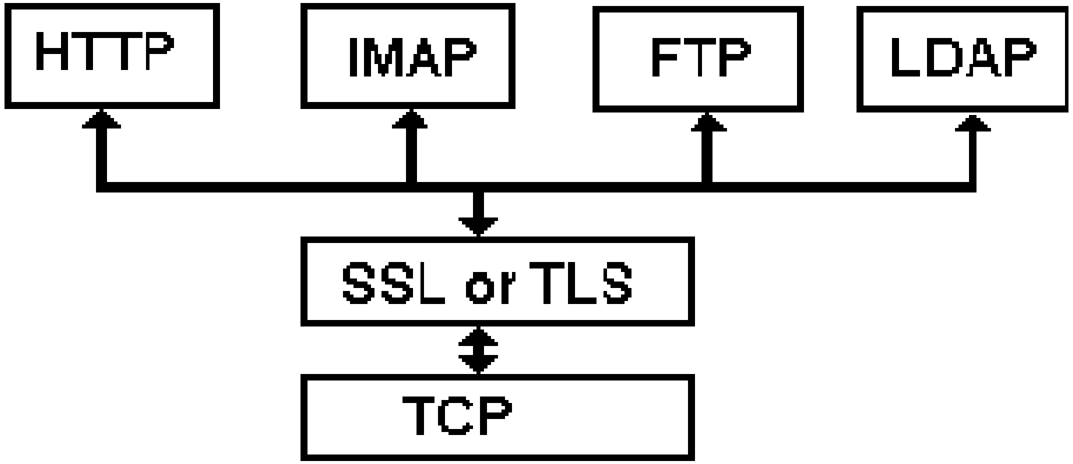
The next message from me will be encrypted

Server Finished (encrypted)

Application's data (encrypted)

Application's data (encrypted)

The position of the TLS/SSL protocols according to the TCP/IP model has been illustrated on the following diagram in the figure below:



HTTP + SSL/TLS + TCP = HTTPS

How does SSL work?

Some Cryptographic Tools

- OpenSSH
- OpenSSL
- PGP

OpenSSH

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network usin

protocol. It enables users

- to log into another computer over a network,
- to execute commands in a remote machine, and
- to move files from one machine to another.

It provides strong authentication and secure communications over unsecure channels. It is intended as a replacement for rlogin, rsh, and rcp.

Some OpenSSH Commands

Useful Link to visit

http://rcc.its.psu.edu/user_guides/remote_connectivity/ssh/

OpenSSL

OpenSSL is an open source implementation of the SSL and TLS protocols. The core library (written in the C programming language) implements the basic cryptographic functions and provides various utility functions. Wrappers allowing the use of the OpenSSL library in a variety of computer languages are available.

Some OpenSSL Commands

Useful Link to Visit

http://www.madboa.com/geek/openssl/

PGP - Pretty Good Privacy

Pretty Good Privacy (PGP) is a computer program that provides cryptographic privacy and authentication. PGP is often used for signing, encrypting and decrypting e-mails to increase the security of e-mail communications. It was created by Philip Zimmermann in 1991.

PGP and similar products follow the OpenPGP standard (RFC 4880) for encrypting and decrypting data.

Some pgp/GnuPG Commands

Useful Links to visit

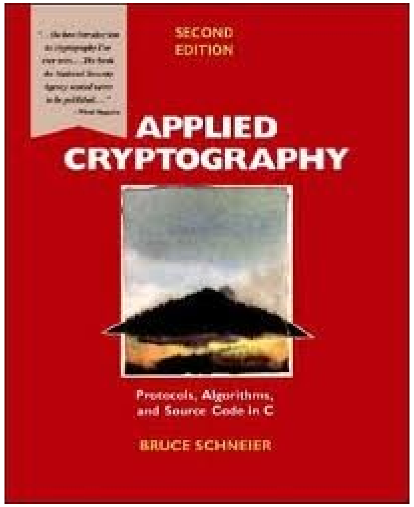
http://dewinter.com/gnupg_howto/english/GPGMiniHowto.html

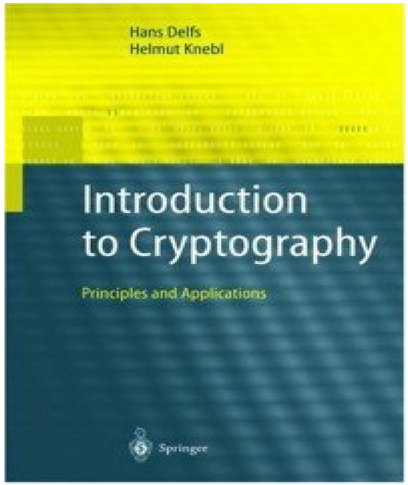
http://www.queen.clara.net/pgp/art3.html

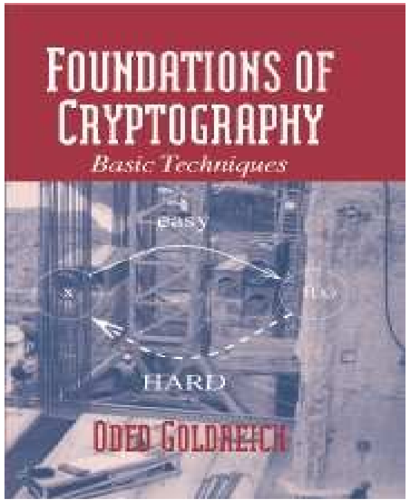
http://www.gnupg.org/documentation/manuals/gnupg/GPG-Commands.html

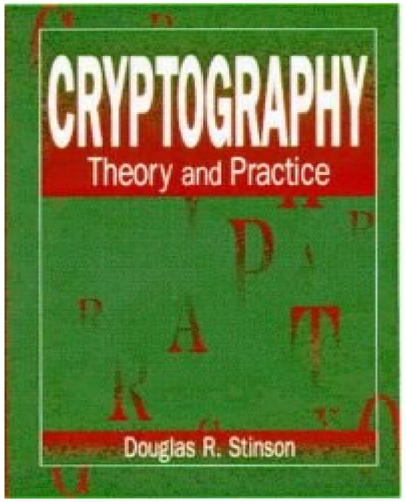
http://www.queen.clara.net/pgp/pgp.html

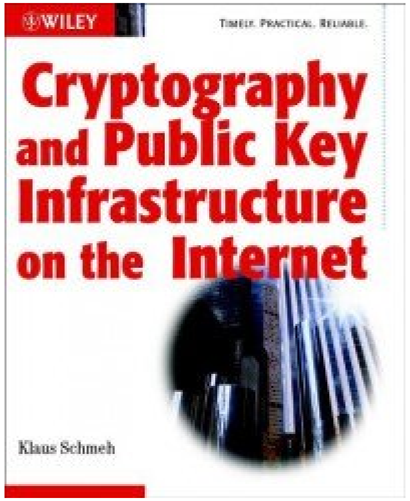
Useful Books

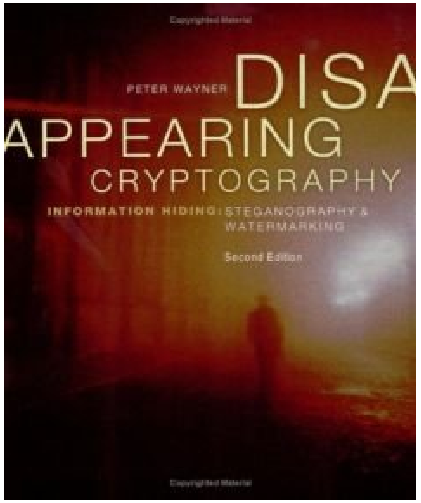


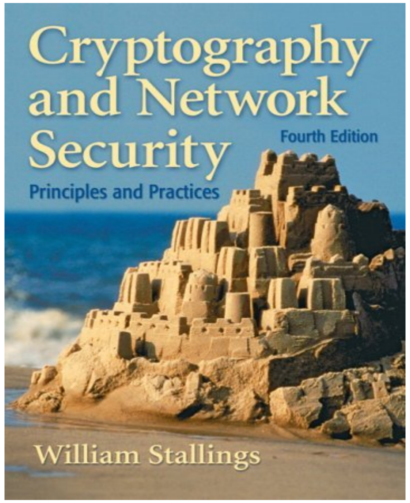


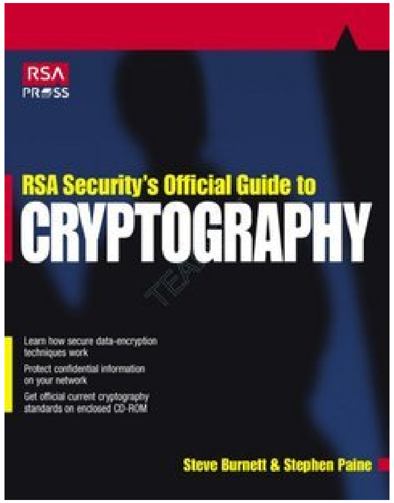


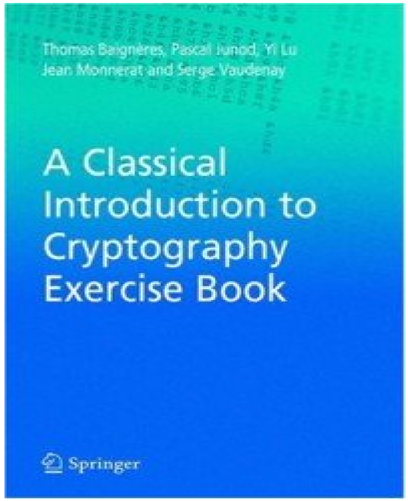


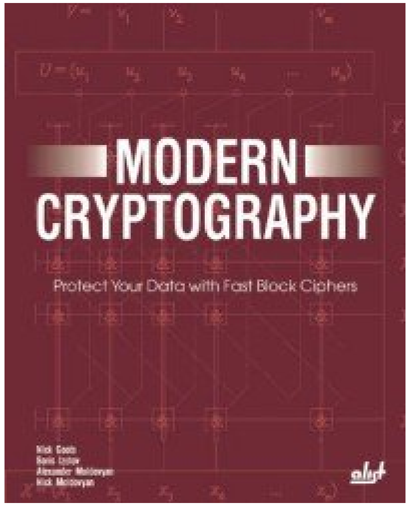

WILEY
TIMELY. PRACTICAL. RELIABLE.
Cryptography and Public Key Infrastructure on the Internet
Klaus Schmeh

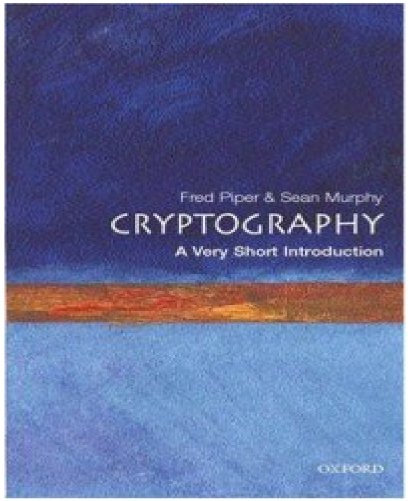

PETER WAYNER
DISAPPEARING CRYPTOGRAPHY
INFORMATION HIDING: STEGANOGRAPHY & WATERMARKING
Second Edition

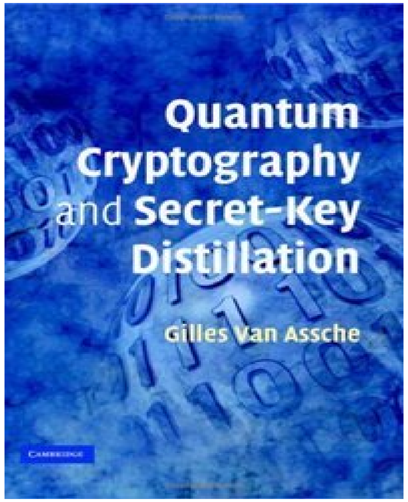


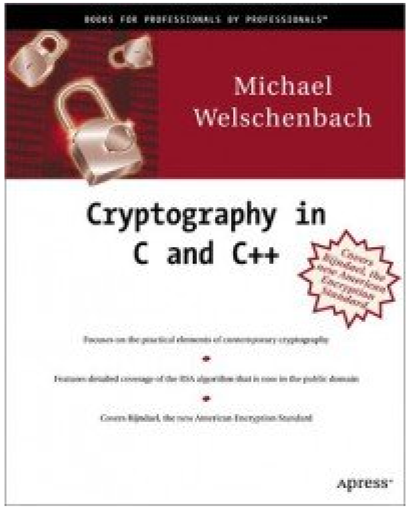

RSA PRESS
RSA Security's Official Guide to CRYPTOGRAPHY
Learn how secure data-encryption techniques work
Protect confidential information on your network
Get official current cryptography standards on enclosed CD-ROM
Steve Burnett & Stephen Paine

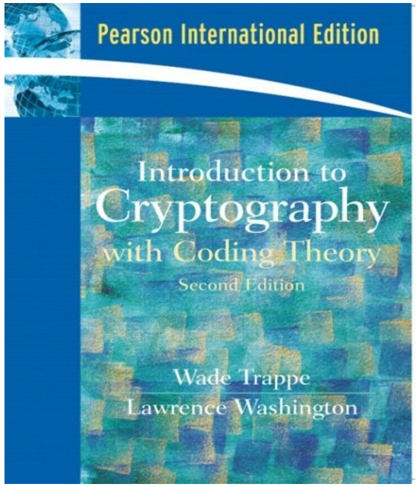

Thomas Baignères, Pascal Junod, Yi Lu
Jean Monnerat and Serge Vaudenay
A Classical Introduction to Cryptography Exercise Book
Springer

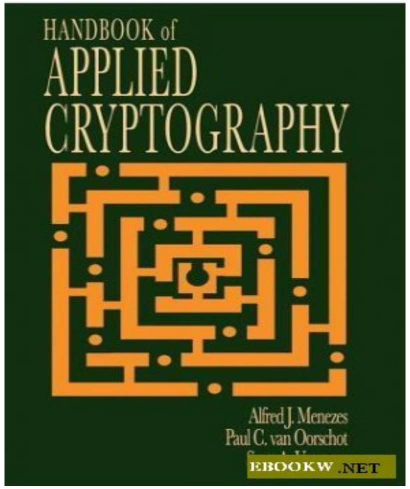

MODERN CRYPTOGRAPHY
Protect Your Data with Fast Block Ciphers
Nick Goots
Boris Izotov
Alexander Moldovyan
Nick Moldovyan
alist

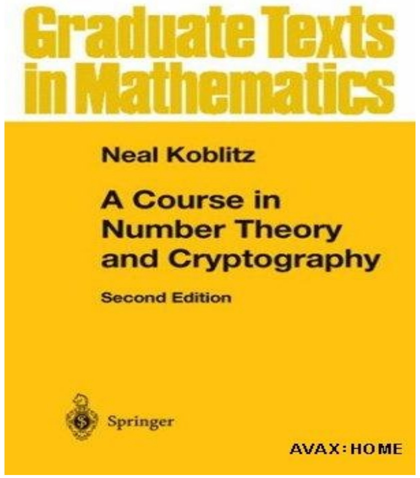

Fred Piper & Sean Murphy
CRYPTOGRAPHY
A Very Short Introduction
OXFORD


Quantum Cryptography and Secret-Key Distillation
Gilles Van Assche
CAMBRIDGE


BOOKS FOR PROFESSIONALS BY PROFESSIONALS™
Michael Welschenbach
Cryptography in C and C++
Covers Rijndael, the new American Encryption Standard
Focuses on the practical elements of contemporary cryptography
Features detailed coverage of the IDEA algorithm that is now in the public domain
Covers Rijndael, the new American Encryption Standard
Apress®


Pearson International Edition
Introduction to Cryptography with Coding Theory
Second Edition
Wade Trappe
Lawrence Washington


HANDBOOK of APPLIED CRYPTOGRAPHY
Alfred J. Menezes
Paul C. van Oorschot
EBOOKW .NET


Graduate Texts in Mathematics
Neal Koblitz
A Course in Number Theory and Cryptography
Second Edition
Springer
AVAX:HOME

Thanks!
ne©

THE END

bye-bye