An Introduction to digital signatures

This document is an extract from the book *Ecommerce - Legal Issues* authored by Rohas Nagpal. This book is available as courseware for the **Diploma in Cyber Law** and **PG Program in Cyber Law** conducted by Asian School of Cyber Laws

www.asianlaws.org

2. Digital Signatures - technical issues

The Information Technology Act 2000 (IT Act) prescribes digital signatures as a means of authentication of electronic records. In short, a digital signature has the same function as that of a handwritten signature.

However, understanding how a digital signature is created and how it achieves the same functionality as that of a handwritten signature is by no means an easy task. This is because the technical concepts involved in creating a digital signature seem far removed from the realm of law, although the objective of affixing digital signature to an electronic record is purely legal!

Digital signatures are an application of asymmetric key cryptography. This chapter traces the roots of cryptography, discusses symmetric and asymmetric key cryptography and ends with a detailed discussion on how asymmetric key cryptography can be used to create a digital signature.

Cryptography has a long and interesting history[1].

Cryptography is primarily used as a **tool to protect national secrets and strategies**. It is extensively used by the military, the diplomatic services and the banking sector.

One of the landmark developments in the history of cryptography was the introduction of the revolutionary concept of **public-key cryptography**[2].

In 1978, **Ron Rivest, Adi Shamir and Leonard Adleman** discovered the first practical public-key encryption and signature scheme, now referred to as RSA (after the names of its inventors).

[1] Kahn's book titled *The Codebreakers* traces cryptography from its initial use by the Egyptians more than 4000 years ago, to its role in the World Wars in the 20th century.

[2] This concept was introduced in "New Directions in Cryptography" written by Whitfield Diffie and Martin Hellman (published in 1976).

2.1 How cryptography works

Cryptography is the **science of using mathematics to encrypt and decrypt data**. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

While cryptography is the science of securing data, **cryptanalysis** is the science of analyzing and breaking secure communication (breaching security measures).

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.

A cryptographic algorithm, or **cipher**, is a mathematical function used in the encryption and decryption process. This mathematical function works in combination with a **key** — a very large number — to encrypt the plaintext (the original message).

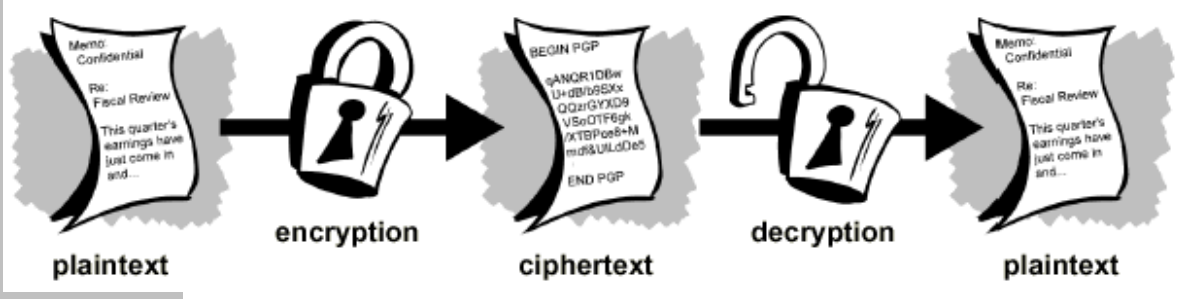
Data that can be read and understood without any special measures is called **plaintext** or clear text. Data which requires some special function to be performed on it before it can be read and understood, is called **cipher text**.

The same plaintext**,** encrypted by using different keys, will result in different cipher text. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a **cryptosystem**.

Encryption is used to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plaintext is called **decryption**.

The figure below illustrates the process of encryption and decryption.



The fundamental objective of cryptography is information security. Simply put, it is to ensure the following:

- ✓ **Confidentiality** is used to keep the content of information secret from unauthorized persons. This is achieved through symmetric and asymmetric encryption.

- ✓ **Data integrity** addresses the unauthorized alteration of data. This is addressed by hash functions.

- ✓ **Authentication** is related to identification. This function applies to both entities and information itself. This is achieved through digital signature certificates and digital signatures.

- ✓ **Non-repudiation** prevents someone from denying previous commitments or actions. This is achieved through digital signature certificates and digital signatures.

2.2 Keys

A key is a value that works with a cryptographic algorithm to produce a specific cipher text. Keys are basically **very, very, very big numbers**. Key size is measured in bits. In public key cryptography, the bigger the key, the more secure the cipher text. However, public key size and conventional cryptography's symmetric key size are totally unrelated.

The algorithms used for each type of cryptography are very different and are very difficult to compare.

Although the public and private keys are mathematically related, it is very difficult to derive the private key by analysing the public key (this is explained later in this chapter). Keys are stored by cryptographic software in an encrypted form. These files are called key rings.

The figure below illustrates a 512-bit RSA public key

```
3048 0241 00FC DBDF 80FA 0121 AD3F 8FFF B101 A19D
52E8 A4A4 E79D E9A2 BE37 EFED 8126 8A03 7130 F4E2
3644 1BE0 5CFE 613B 4400 CEE4 8E27 B971 ECCA 78C5
F714 FAE5 B2A2 1E01 FF02 0301 0001
```

A 512-bit RSA public key

The figures below illustrate a 1024 bit RSA key pair generated using the PGP (Pretty Good Privacy) digital signature and encryption software.

```
-----BEGIN PGP PRIVATE KEY BLOCK-----

lQHgBD5vDDEBBAC+UMHKr9YL1W0OYzL9gK/AERegEtzoFiveSzbeFQtNhxDIOSPJ
c60Y8v2nTecI0R5Y6Z55uzakcPBZmTJ+kWrFR4NZPApiOFXhUrkHF0DmrmEpa5Up
HjpO3sD+Hlvg84N6jHjAIRMlNMAyrg/e4i6ABGzAuxYbJCs6ax9mxdrFAQARAQABAw
vtDcK53Fr7j9Ss3v83ZR7g1DgFfY3oo97XWbmJ02BdRGy/C+aIuu3wMRNqmPo5w1I8
VVCjjM02eqSr0+8mbLLX0Dwqbn33QitGW34Upt6EI+fv0ObKbJRi2Hc628l3mi+jjsskxv
Q8oavtSJL2j/xTEtL+wvqObcFxllsyjpH5N1wY7xQ5BPSNjYLFZr99MXycFhee14V2Yd
Qv0iPZFrJnvCQFWXLAiX1L9AH5DgwmXLtNCPbIQnRwyLPyWSOT4yH8e6ibqIBvMh
pGe4WOAzuccHL6jjZrokVrBBu50Z6EqGFkzS8X6iygvSATOjr3L/X9EW7Fw098CcVK
3lDB93rpeXR+tU370nV+0FgXQqUzQ3SJ6vZwdlwy6cmjZOWmd/YrbGLOyyW+zFFS
ZFdiG480ELozMfMsqp3OJvElvhRgS/tbA/94jpOtzhWV9Du0pd7otCBBYmhpbmF2IEJo
YXR0IDxhYkBhc2lhbmxhd3Mub3JnPp0B4AQ+bwwyAQQAmkqdApHtWspZdNfqeER
OxctZKLxdvtXBnaO1J1sS6jKjx2qGj3yxLRnW+N4QUAgm+eNNsTrqZZjJUP526dOTK
8RmxV4QJeh2Q0bsLPs6SXTlPwfBWPpt+U/kfrSt8ZJF5lWR0jaiJG2hE3dBiuszPa+6cJ
UDuQnYCVCHZARCKLcAEQEAAQPT8PBQW4y8b4C7BvhjnGAATQliwRajv6uWmfU
FcI+DPdtAZh3yb9EKWmS8vSkSnz+pWG1dEkuURyvBGJMDxs/FB+CMouTQejhA11
Ho5tblas8HnoNPeQv1x9Xas+lrs1j2AmfrLWwKEQAuH9di+d9DRU6YHxy1ocIHZELXR
9ECsSP0C1iSeuJn+u4HLP3y4uBHcGRdihLRIUSCJ0tXd2meRAxw4dsZllDAeb21i2Tj
+l0SngTEzFj8fSuvAxoXRv30gq5VLbH5WDbJah5n688THMAUIUC5dlG8MMXMgmUe
887lwKEqSvLqCk5ymHmCdZiJQQEpAxVbXb9bkKs2UhxN1zRnug4OcR411XOqlvlBw
sk121yY7606mZ7r+icnXvLLEVezmegXsN8mlhAnb+p629HPZSMFOSHgX3CwhIwTK
DaMxZBft94Fk8w3l/NBuwQJYg===Emf5
-----END PGP PRIVATE KEY BLOCK-----
```

A 1024 bit RSA private key generated using the PGP (Pretty Good Privacy) digital signature and encryption software.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQCNBD5vDDEBBAC+UMHKr9YL1W0OYzL9gK/AERegEtzoFiveSzbeFQtNhxDIO
SPJc60Y8v2nTecl0R5Y6Z55uzakcPBZmTJ+kWrFR4NZPApiOFXhUrkHF0DmrmEp
a5UpHjpO3sD+Hlvg84N6jHjAIRMlNMAyrg/e4i6ABGzAuxYbJCs6ax9mxdrFAQARA
QABtCBBYmhpbmF2IEJoYXR0IDxhYkBhc2lhbmxhd3Mub3JnPokAtAQQAQIAHgU
CPm8MMQUJAeKFAAgLAwkIBwIBCgIZAQUbAwAAAAAKCRDRPtuuStKFCIJwA/9
t1Cjpi+hjVaWjJx1BZpoGv4b+t/Qb03J9ABFUatbypUX5jmMmCUT7h3TgiCgT5F4im
vijm4+uCDeoHz0Uj+nPfvW8guMd805s/+3oU+FT4R2qYvEX6MAQVex67TJ0pHvmi
V55Mn/apNvTdvgSXJbQfHuza9u1QPEUm+LlVdOZx7kAjQQ+bwwyAQQAmkqdAp
HtWspZdNfqeEROxctZKLxdvtXBnaO1J1sS6jKjx2qGj3yxLRnW+N4QUAgm+eNNsT
rqZZjJUP526dOTK8RmxV4QJeh2Q0bsLPs6SXTlPwfBWPpt+U/kfrSt8ZJF5lWR0jai
JG2hE3dBiuszPa+6cJUDuQnYCVCHZARCKLcAEQEAAYkAqAQYAQIAEgUCPm8
MMgUJAeKFAAUbDAAAAAAKCRDRPtuuStKFCADiA/0csZOSY9Ztyvw2iVSJqf9g4
u3z+ePmEcwy2RK5tuOXU2p7HvEBMKeLlG9Dxg0xwy7cVvHejjAn4LxMPG9j26Tin
LCAfqHs7C1og8an1tHstrM4Icw7pWx5fIRLiqQLqEc/RVFLBKU3nMAjgu0E9wjHicW
FwsxUfeF5qD9kAsI0Og===klTT
-----END PGP PUBLIC KEY BLOCK-----
```

A 1024 bit RSA public key generated using the PGP (Pretty Good Privacy) digital signature and encryption software.

2.3 Symmetric Cryptography

In conventional cryptography, also called secret-key or symmetric-key encryption, the **same key is used both for encryption and decryption**.

The figure below is an illustration of the conventional encryption process.

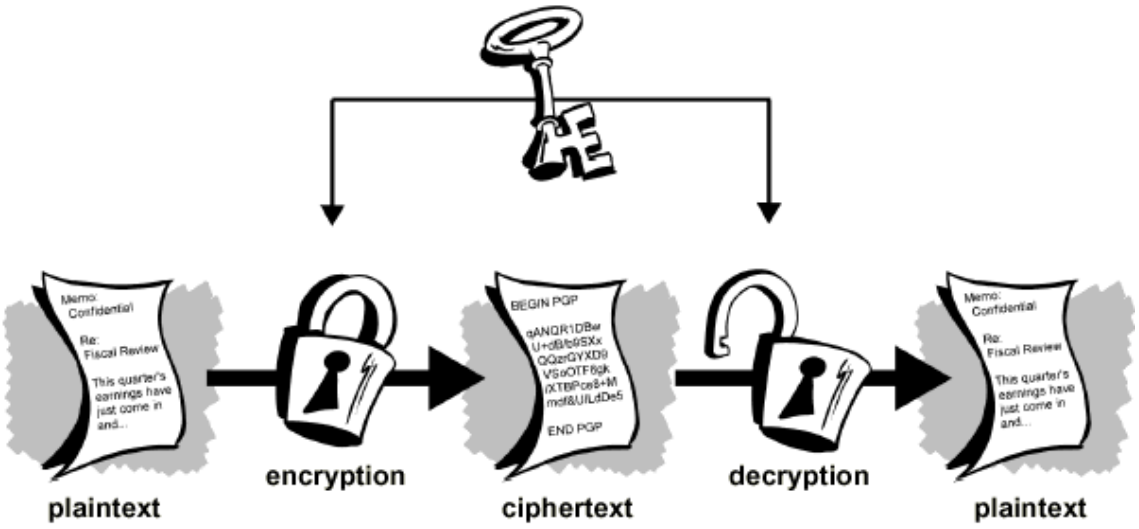


Figure 1 **Symmetric Cryptography**

Caesar's Cipher

When Julius Caesar sent messages to his generals, he didn't trust his messengers. So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the "shift by 3" rule could decipher his messages.

For example, if we want to encode the word "SECRET" using Caesar's key value of 3, we offset the alphabet so that the 3rd letter down, (D), begins the alphabet.

So starting with

ABCDEFGHIJKLMNOPQRSTUVWXYZ

and sliding everything up by 3, you get

DEFGHIJKLMNOPQRSTUVWXYZABC

where D=A, E=B, F=C, and so on.

Using this scheme, the plaintext, "SECRET" encrypts as "VHFUHW". To allow someone else to read the cipher text, you tell him or her that the key is 3. Obviously, this is exceedingly weak cryptography by today's standards, but it worked for Caesar, and it illustrates how conventional cryptography works.

Key management and conventional encryption

Conventional encryption has certain benefits. It is **very fast**. It is especially useful for encrypting data that is not to be transmitted anywhere. So, if you want to store information so that no one can read it without your authorization, it would be a good idea to use conventional encryption.

For a sender and recipient to communicate securely using conventional encryption, they must **agree upon a key and keep it secret** between themselves. If they are in different physical locations, they must trust a courier or some other **secure communication medium.**

This is to prevent the disclosure of the secret key during transmission. Anyone who overhears or intercepts the key in transit can later read, modify, and forge all information encrypted or authenticated with that key.

The persistent problem with conventional encryption is key distribution: how do you get the key to the recipient without someone intercepting it?

The problems of key distribution in conventional encryption are solved by public key cryptography, a concept that was introduced by Whitfield Diffie and Martin Hellman in the U.S.A.

2.4 Asymmetric Cryptography

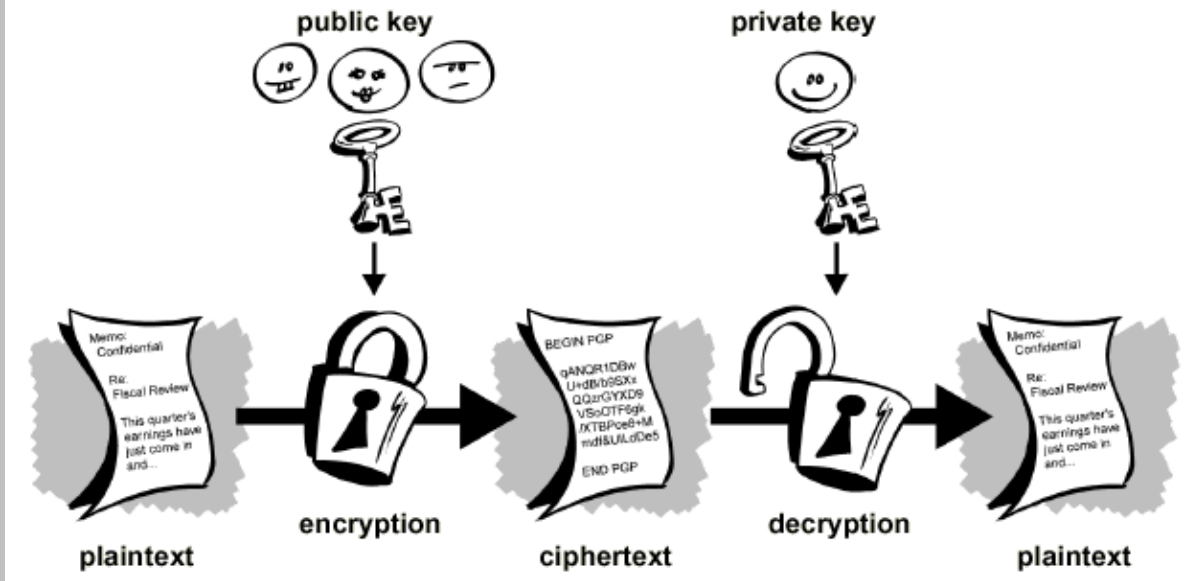
Public key cryptography is an asymmetric scheme that uses a pair of keys: a **public key**, which encrypts data, and a **corresponding private key**, or secret key for decryption.

Each user has a key pair given to him. The public key is published to the world while the private key is kept secret. Anyone with a copy of the public key can then encrypt information that only the person having the corresponding private key can read.

It is **computationally infeasible to deduce the private key from the public key**. Anyone who has a public key can encrypt information but cannot decrypt it.

Only the person who has the corresponding private key can decrypt the information.

The figure below illustrates the process of asymmetric encryption.



Public key encryption

The primary benefit of public key cryptography is that it allows people who have no pre-existing security arrangement to exchange messages securely.

The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared.

Some examples of public-key cryptosystems are ElGamal (named for its inventor, Taher ElGamal), RSA (named for its inventors, Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman), Diffie-Hellman (named for its inventors), and DSA, the Digital Signature Algorithm (invented by David Kravitz).

Because conventional cryptography was once the only available means for relaying secret information, the expense of secure channels and key distribution relegated its use only to those who could afford it, such as governments and large banks. Public key encryption is the technological revolution that provides **strong cryptography to the masses**.

The figure below illustrates a simple message.

Dear Sameer,

I am in town on the 11th of this month.

Will it be convenient for you to meet me at the Four Seasons restaurant for dinner?

Love,
Pooja

A simple message

The figure below illustrates the encrypted form of the message above.

hQCMAztC/6WmKod+AQQAiZmIDTpFg9nC5GmN4Azx
2+0JYo1C70Iux+IhhVvhGy9IA+BuURbxeqFroJPEl665fg
APrTHHdAHV112eTFieH7BW+LaA0Rt4sLzxb077GJEh+
e2wgMhKkymi6RXYQvlXaswMELm7xVz/F6Kh8Q0MwHI
t2jXUc8ayMpw6i7AWAqKkkb86t2XBUfQNw03ZfFG3z7E
ZKB+a772HGpM41MOYc7hY6rjwXHEwu5XtQC81SBAq
DBUK9A4gh9dWsCypB9y/k3LbpyhOGmmJJymG5PmbP
LSXXyi7b6Js6ZNk7Vtjv2zrBZYjhvRpxCIu7uwC41KKn7g
qsvD2fMXHqhgAyL/avwkOSREEw/dstAc94zUeowvBlLg
==tD2W

The encrypted form (using asymmetric encryption) of the message above.

2.5 Hash function

A one-way hash function takes variable-length input – say, a message of any length – and produces a fixed-length output; say, 160-bits. The hash function ensures that, if the information is changed in any way – even by just one bit – an entirely different output value is produced. The table below shows some sample output values using SHA (Standard Hash Algorithm)[3].

sanya	c75491c89395de9fa4ed29affda0e4d29cbad290
SANYA	33fef490220a0e6dee2f16c5a8f78ce491741adc
Sanya	4c391643f247937bee14c0bcca9ffb985fc0d0ba

It can be seen from the table above that the hash value for **sanya** is

c75491c89395de9fa4ed29affda0e4d29cbad290

while the hash value for **SANYA** is

33fef490220a0e6dee2f16c5a8f78ce491741adc

By changing the input from **sanya** to **SANYA**, an entirely different hash value is generated. What must be kept in mind is that irrespective of the size of the input, the hash output will always be of the same size.

Two things must be borne in mind with regard to one-way hash functions:

1. It is computationally infeasible to find two different input messages that will yield the same hash output.

2. It is computationally infeasible to reconstruct the original message from its hash output.

[3] To use SHA please visit http://www.asianlaws.org/sha

2.6 Digital Signatures

A major benefit of public key cryptography is that it provides a method for employing digital signatures.

Digital signatures enable the recipient of the information to verify the authenticity of the information's origin, and also verify that the information is intact. Thus, **digital signatures provide authentication and data integrity**.

A digital signature also provides **non-repudiation**, which means that it prevents the sender from claiming that he or she did not actually send the information. These features are every bit as fundamental to cryptography as privacy, if not more.

A digital signature serves the same purpose as a handwritten signature. However, a handwritten signature is easy to counterfeit. A **digital signature is superior to a handwritten signature** in that it is nearly impossible to counterfeit, plus it attests to the contents of the information as well as the identity of the signer.

Illustration

Sameer uses computer software to generate two keys, a public key and private key. These keys are nothing but extremely large numbers. Although the keys are mathematically related, it is almost impossible to obtain the private key by using the public key.

Sameer will give his public key to the whole world but will keep his private key to himself. Now Sameer wants to enter into a transaction with Pankaj. He composes an electronic document containing the words

> *I, Sameer owe Pankaj the sum of Rs. 500 only.*

Using his computer Sameer runs this document through a hash function.

The hash function software produces a fixed length of alphabets, numbers and symbols for any document. This is known as the hash result. However, the contents of this fixed length are never the same for two different documents.

If even one letter in the document is altered, an entirely different hash result will be generated.

When using a particular hash function, the length of the output is always the same, whether the input document is one word or 1-lakh words.

Moreover, the hash function software will always produce the same hash result for a particular message. It is practically impossible to reconstruct the original message from the hash result. That is why it is known as a one-way hash function.

Sameer now uses his computer to “sign” the hash result of his document. His computer software uses his private key to perform some calculations upon the hash result. This produces a signature, which consists of some digits. This set of digits is attached to the hash result.

Sameer now sends the original message and the signed message digest (hash result) to Pankaj. Pankaj has the same hash function software on his computer. He also has Sameer’s public key. When Pankaj receives Sameer’s email, he runs the original document through the hash function software and generates a hash result.

He compares this hash result with the one that was sent to him by Sameer. If the two hash results are the same, it means that the message is unaltered. Pankaj also verifies whether Sameer’s private key was actually used to sign the hash result. For this Pankaj’s computer uses Sameer’s public key. Only a message signed by Sameer’s private key can be verified using Sameer’s public key.

The public key and private key are basically two very large numbers that are mathematically related to each other. If a particular private key was used to “sign” a message, then only the corresponding public key will be able to verify the “signature”.

The digital signature creation and verification process achieves the following legal requirements:

1. **Signer authentication:** A person’s digital signature cannot be forged unless his private key is stolen. This means that if a digital signature can be verified by Sanya’s public key, then it must have been created by Sanya’s private key. The digital signature verification process thus authenticates the identity of the signer.

2. **Message authentication:** A digital signature is based upon the hash value (or message digest) of the actual message. Thus a digital signature is unique for each message and automatically authenticates the message.

3. **Affirmative act:** The process of digital signature creation requires the signer to use his private key (usually by entering a password). This overt act alerts the signer that he is initiating a transaction that may have legal consequences.

2.7 Digital Signature Certificates

Simply put, a digital signature certificate contains a public key as "certified" by a Certifying Authority (CA).

Let us take a simple illustration. Rohas Nagpal wants to digitally sign emails and electronic contracts. The first step he would take is to generate a private-public key pair. Once he has done that, he can use his private key to sign contracts etc. Anyone can use Mr. Nagpal's public key to verify his signature. That's where the problem begins.

How can anyone be sure which is Mr. Nagpal's public key? What if Mr. Nagpal denies that a particular public key is actually his? To solve this problem digital signature certificates are used.

Mr. Nagpal would apply to a licenced CA for a digital signature certificate. As part of the application process he would submit identification documents (such as passport, PAN card etc). He would also send his public key to the CA. The CA would then "certify" the public key as belonging to Mr. Nagpal and issue a digital signature certificate that contains Mr. Nagpal's public key along with information identifying him.

The digital signature certificate is digitally signed by the CA and is legally recognised under the law.

> **Note:** The detailed procedure for obtaining a digital signature certificate is discussed later in this book.

Let us now discuss the contents of a digital signature certificate in detail. For the purposes of this discussion we will discuss the **digital signature certificate issued to Mr. Rohas Nagpal** by the TCS CA.

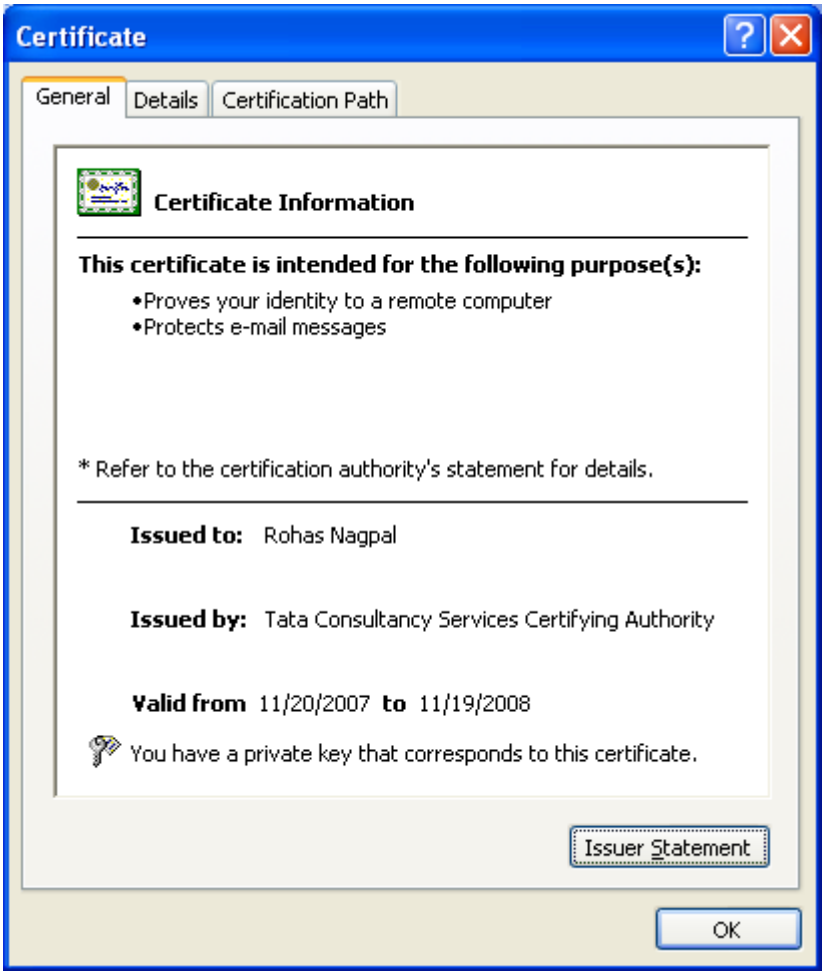
> To view digital signature certificates stored by default on your computer, you can open up the Microsoft Internet Explorer program and click on Tools → Internet Options → Content → Certificates option.

To make this section easy to understand, the language used is in the first person. References to "I", "me" etc refer to "Rohas Nagpal", the author of this book.

Let us discuss my digital signature certificate (DSC) in detail. I have been issued a DSC by TCS CA which is licenced by the Controller of Certifying Authorities of India. The DSC has been imported into my personal computer that also has the Microsoft Internet Explorer program installed.

To view my DSC, I first open up the Microsoft Internet Explorer program and click on Tools → Internet Options → Content → Certificates option.

Figure 1: General Information



The first view of the DSC displays the **Certificate Information** which contains the following basic information:

1. Purposes for which the certificate is intended.
2. Person to whom it is issued.
3. Issuer of the certificate.
4. Validity period of the certificate.

As can be seen from figure 1, the certificate is intended to do the following:

1. Prove my identity to another computer
2. Protect email messages

The certificate is issued to me by Tata Consultancy Services Certifying Authority (TCS CA) and is valid from 20th November 2007 to 19th November 2008.

It can be noticed that the DSC states that "**You have a private key that corresponds to this certificate**".

This is because the DSC is on my personal computer and my private key is also on this computer. If you were to download my DSC onto your computer, then this statement would not show up as your computer does not have my private key.

Clicking on the “Issuer Statement” button on the DSC opens up the **Relying Party Agreement** from the TCS website.

> The Relying Party Agreement is an agreement between TCS CA and the person relying on a DSC (or verifying a DSC).
>
> The agreement must be read along with the TCS-CA trust network certification practice statement (CPS) posted at the TCS-CA web site (https://www.tcs-ca.tcs.co.in) as amended from time to time.

Clicking on the **Details** tab, displays the certificate details.

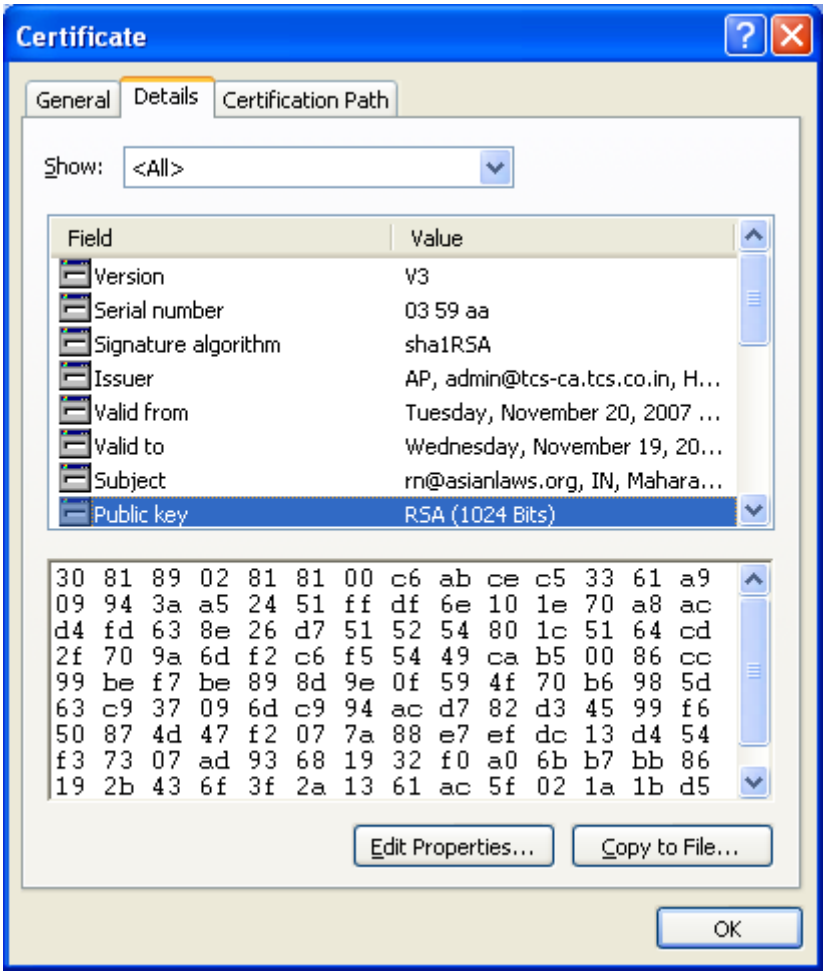


Figure 2: Details

The following are some of the details of the certificate:

1. **Version**
   This is stated as V3. This signifies that the DSC is based on the X509 version 3 technology standards.

2. **Serial number**
   The serial number is a positive integer assigned by the CA to each DSC issued by it. This number is unique for each DSC issued by the CA.

   Note: "03 59 aa" is a hexadecimal number that corresponds to the decimal number 50696362

3. **Signature Algorithm**
   This field identifies the mathematical algorithm used by the CA to sign the certificate [sha1RSA is this case].

   sha1 stands for Secure Hash Algorithm 1 while **RSA** stands for Rivest Shamir Adleman.

4. **Issuer**
   This field identifies the CA who has issued this DSC. The table below summarizes the information as contained in the DSC and the brief explanation of what that information stands for.

Information on DSC	Explanation
S = AP	State = Andhra Pradesh
E = admin@tcs-ca.tcs.co.in	Email = admin@tcs-ca.tcs.co.in
L = Hyderabad	Location = Hyderabad
CN = Tata Consultancy Services Certifying Authority	Common Name = Tata Consultancy Services Certifying Authority
OU = TCS CA	Organizational-unit = TCS CA,
O = India PKI	Organization = India PKI
C = IN	Country = India

5. **Valid From**
   This indicates that the DSC is valid from 11:31:07 AM on Tuesday, November 20, 2007.

6. **Valid To**
   This indicates that the DSC is valid till 11:31:07 AM on November 19, 2008.

7. **Subject**
   The subject field identifies the person to whom this DSC has been issued by the CA – Rohas Nagpal in this case. The table below

summarizes the information as contained in the DSC and the brief explanation of what that information stands for.

Information on DSC	Explanation
E = rn@asianlaws.org	Email = rn@asianlaws.org
C = IN	Country = India
S = Maharashtra	State = Maharashtra
L = Pune	Location = Pune
O = Tata Consultancy Services - Certifying Authority	Organisation = Tata Consultancy Services - Certifying Authority
OU = Class 3 Certificate	Organization Unit = Class 3 Certificate[4]
OU = Individual - Others	Organization Unit = Individual - Others[5]
OU = TCS-CA - Registration Authority	Organization Unit = TCS-CA - Registration Authority
CN = Rohas Nagpal	Common Name= Rohas Nagpal

8. Public Key

This field specifies my public key (see below), the algorithm used by me to generate the key (RSA) and the key size (1024 bits).

```
30 81 89 02 81 81 00 c6 ab ce c5 33 61 a9 09 94 3a a5 24 51 ff
df 6e 10 1e 70 a8 ac d4 fd 63 8e 26 d7 51 52 54 80 1c 51 64 cd
2f 70 9a 6d f2 c6 f5 54 49 ca b5 00 86 cc 99 be f7 be 89 8d 9e
0f 59 4f 70 b6 98 5d 63 c9 37 09 6d c9 94 ac d7 82 d3 45 99 f6
50 87 4d 47 f2 07 7a 88 e7 ef dc 13 d4 54 f3 73 07 ad 93 68 19
32 f0 a0 6b b7 bb 86 19 2b 43 6f 3f 2a 13 61 ac 5f 02 1a 1b d5
52 e5 70 24 16 fa 5d 83 79 02 03 01 00 01
```

9. CRL Distribution Points

A certificate revocation list (CRL) is a list of serial numbers of those digital signature certificates which should not be relied upon because they:

1. have been revoked, or
2. are no longer valid.

This field indicates the URL from where the relevant Certification Revocation List can be downloaded, which in this case is- http://www.tcs-ca.tcs.co.in/crl_2785.crl

[4] Class-3 Certificates are legally recognized digital signatures as per the IT Act, 2000.

[5] The basic options are Company user, Government user and Individual user. Under Individual user the options are Banking, Government and Others.

Clicking on the **Certification Path** tab, displays the certification path.

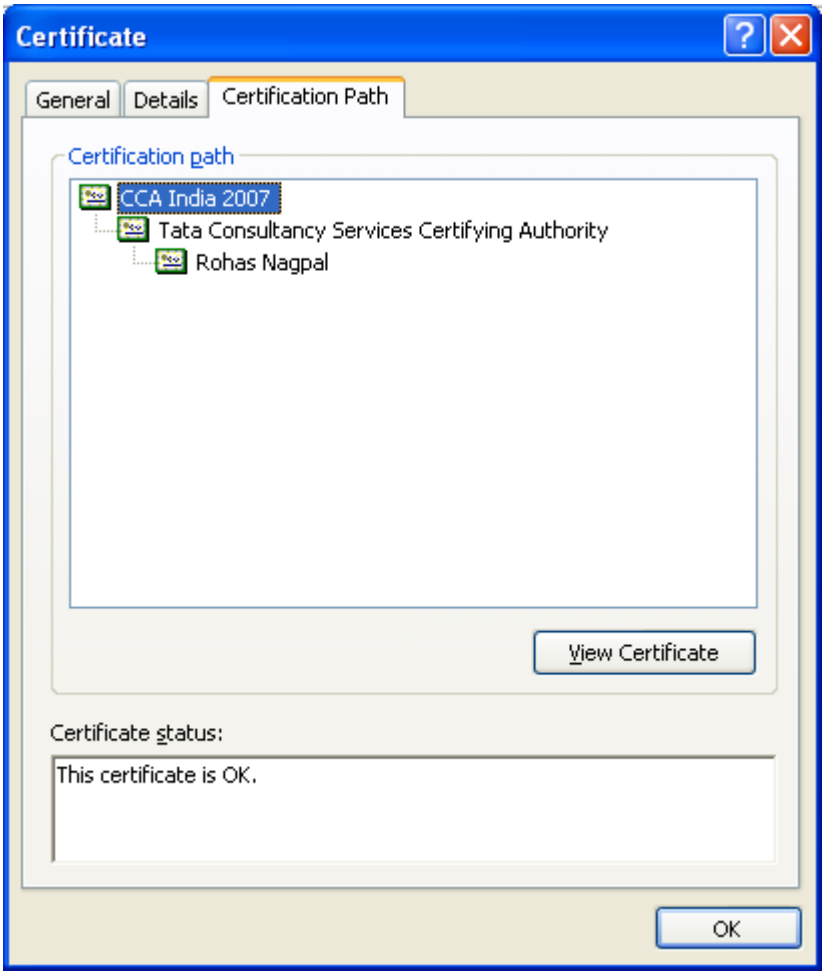


Figure 3: Certification Path

This shows that my digital signature certificate has been issued by TCS CA. It also shows that the TCS CA digital signature certificate has been issued by the Controller of Certifying Authorities.

www.asianlaws.org

Head Office

6th Floor, Pride Senate,

Behind Indiabulls Mega Store,

Senapati Bapat Road,

Pune - 411016.

India

Contact Numbers

+91-20-25667148

+91-20-40033365

+91-20-64000000

+91-20-64006464

Email: info@asianlaws.org

URL: www.asianlaws.org