

This Newsletter is intended to provide a general summary only and should not be relied on as a substitute for legal advice.

Our publications can be viewed on our web site - <http://www.deacons.com.au>

© Copyright 2001 - Deacons

digital signatures/pki

Understanding Digital Signatures & PKI

Public key infrastructure (PKI) is based on cryptography. The word cryptography comes from the Greek for “secret writing”. Cryptography is not new. It was used in the Hellenic wars. Even Julius Caesar is credited with inventing a cryptographic algorithm. Cryptography has developed in sophistication in parallel with developments in mathematics and information technology. Today, PKI is used to effect secure communications over open networks such as the Internet. PKI is also the enabling technology for many electronic payment systems. Accordingly, it is a technology that everyone engaged in e-commerce needs to be familiar with.

This paper aims to provide you with a general overview of the basic elements of the cryptography that underpins PKI. All cryptographic systems comprise the following 4 basic components:

1. Plain Text

This is the message before anything has been done to it. It is either human readable or in a format that anyone with the appropriate software can use.

2. Cipher Text

This is the plain text message after it has been modified in some way to obscure it, rendering it unreadable by a human. The process of converting plain text into cipher text is “encryption”. The process of converting cipher text into plain text is known as “decryption”.

3. Cryptographic Algorithm

This is the mathematical procedure used to convert plain text into cipher text, and vice versa.

4. Key

This is the secret key used to encrypt and/or decrypt the message. Each key transforms the same plain text into a different cipher text. If the cryptographic system works properly, only people who know the correct key can decrypt a piece of cipher text.

Cryptography is used to send cipher text (ie encrypted data) across insecure, public communications networks. If any cipher text is intercepted, it is useless to anyone who does not possess the decryption key. Before the advent of digital computers, plain text, cipher text and the key were generally in the form of human readable text. Now the three are, typically, streams of arbitrary binary information. In addition to text messages, video, sound and software can all be encrypted as easily as plain text.



Symmetric Cryptography

For many years, encryption algorithms were *symmetrical*. This means that the same secret key was used to both encrypt messages and decrypt cipher text (See Figure 1).

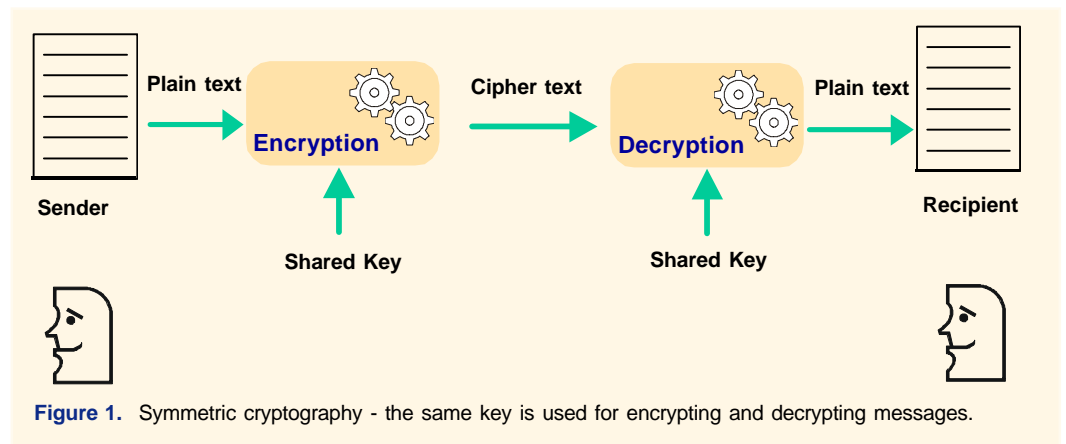


Figure 1. Symmetric cryptography - the same key is used for encrypting and decrypting messages.

However, *symmetric* key procedures present problems for the use on the Internet where parties frequently communicate remotely. Often these communications are unsolicited. This means that there will be no opportunity to exchange secret keys in advance.

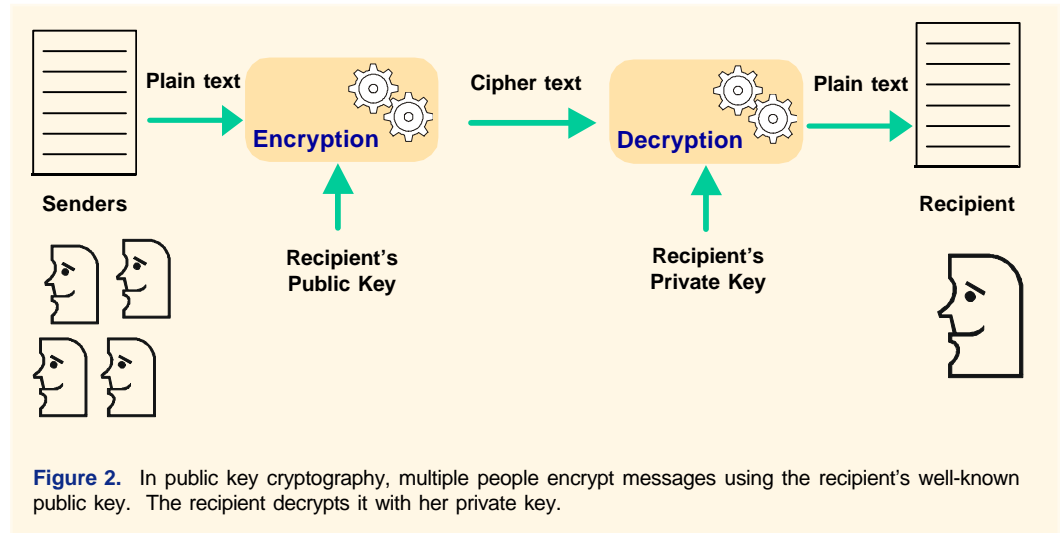
Also, symmetric key procedures are not flexible enough to provide a secure platform for one-to-many or many-to-one communications. Public key cryptography (or *asymmetric* cryptography) aims to overcome these problems.

Public Key Cryptography

Public key cryptography was invented in the mid-1970s. In public key systems, keys come in *asymmetric* pairs – one used for encryption and the other for decryption. Importantly, an encrypted message cannot be decrypted even if one knows the key that was used to encrypt it. Only the *asymmetric* decryption key can be used to retrieve the original message.

Everyone who participates in a public key cryptography system owns a unique pair of keys. One of the keys, called a public key is made publicly available. The public key is made available to anyone who requires it. The other key, called the private key, is a closely guarded secret. To send a secure message to someone, you look up the relevant person's public key and use it to encrypt the message. The message can now be sent over an insecure channel without fear of being read if intercepted. Provided the matching private key remains in the possession of its intended recipient, only the holder of the private key can decrypt and read that message.

Accordingly, PKI solutions are well suited to use on the Internet. You can send an encrypted message to anyone without making arrangements in advance. Multiple people can send messages to the same party without the need to share any secrets. Figure 2 represents the process for many one-to-one communications using a PKI solution.



While the mathematics underlying public key algorithms is extraordinarily complex, the concepts are quite simple. Public key algorithms rely for their security on computationally difficult problems such as the difficulty of deriving the prime factors of very large numbers. Barring fundamental breakthroughs in mathematics, solving these problems is very labour intensive, and the amount of labour required increases dramatically as the keys get longer. The longer the key length of key pair, the more computer time it takes to guess the private key. The keys typically used for Internet applications would take millions of years to crack using current technologies.

The main limitation of public key (or *asymmetric*) cryptography is speed. The fastest PKI solution available today is still a thousand times slower than a typical *symmetric* algorithm, making it impractical for encrypting long messages. In real world applications, public key and symmetric cryptography are usually combined in a way that takes advantage of their best features. This is called digital enveloping.

Digital Signatures

Before we examine digital envelopes it is important to be familiar with digital signatures. Digital signatures are one implementation of PKI. A central element of a digital signature is a "hash algorithm". When a user digitally signs a message, the clear text is processed by the hash algorithm and produces a unique "hash" or "fingerprint" of the message. This unique "fingerprint" is a small piece of data that serves to identify the complete message text. Once the hash of a message is calculated, it is signed using the sender's private key. When the recipient receives the message and the signed hash, she recalculates the hash of the message. She then decrypts the signed hash and compares the 2 values. If they match she knows the message came from the sender.



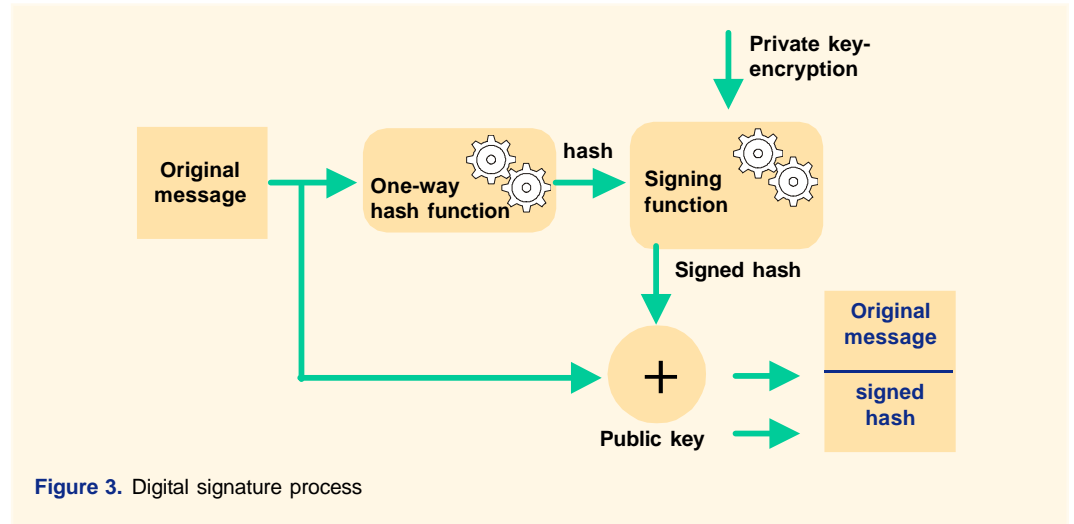


Figure 3. Digital signature process

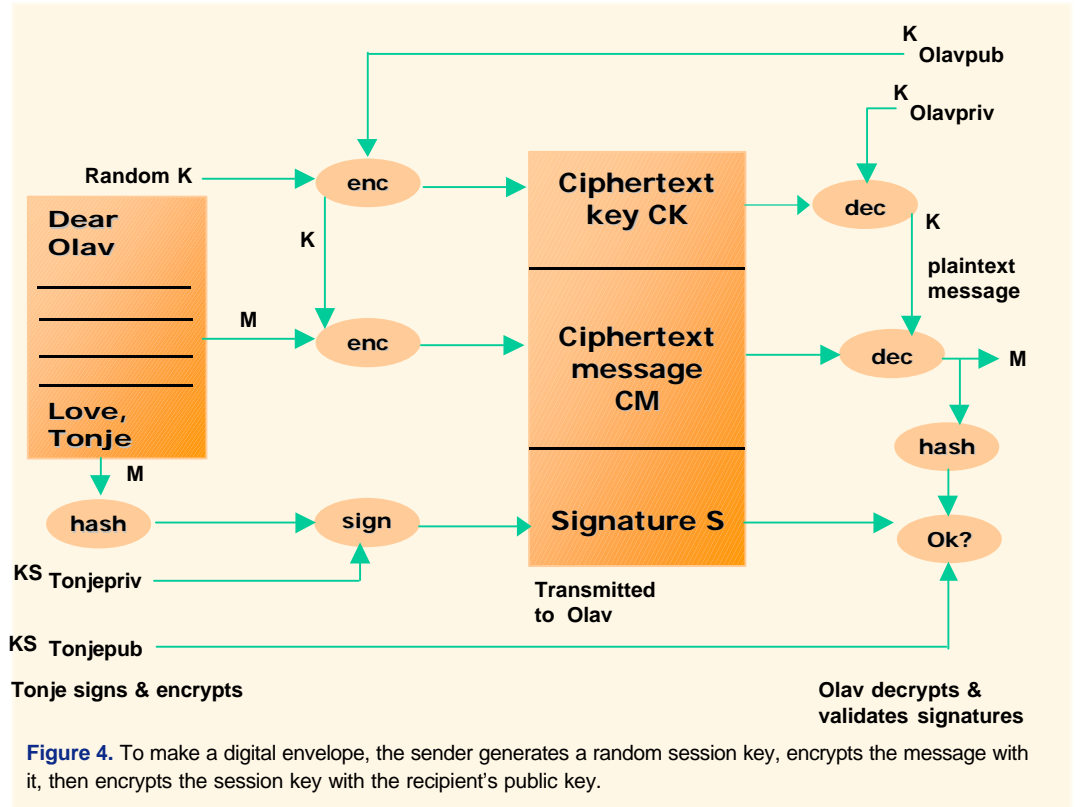
Digital Envelopes

Digital envelopes are used to overcome the high overheads associated with asymmetric cryptography. Digital envelopes combine the best aspects of both symmetric (ie, processing speed) and asymmetric (ie, high level security) cryptography. The process for creating digital envelopes is as follows:

- (1) Sender generates a random message key (K). Sender encrypts the message (M) with K , creating the cipher text message (CM).
- (2) Sender encrypts K with recipient's public key—encrypting key ($K_{Ola\text{vpub}}$), obtaining cipher text CK .
- (3) Sender computes a digital signature S using her private signature key $KS_{\text{Tonjepriv}}$
- (4) Sender sends CK , CM and S to recipient.
- (5) Recipient uses his private key encrypting key $K_{Ola\text{vpriv}}$ to decrypt CK and obtain K .
- (6) Recipient uses K to decrypt CM and get M .
- (7) Recipient uses sender's public signature key KS_{Tonjepub} to validate S .

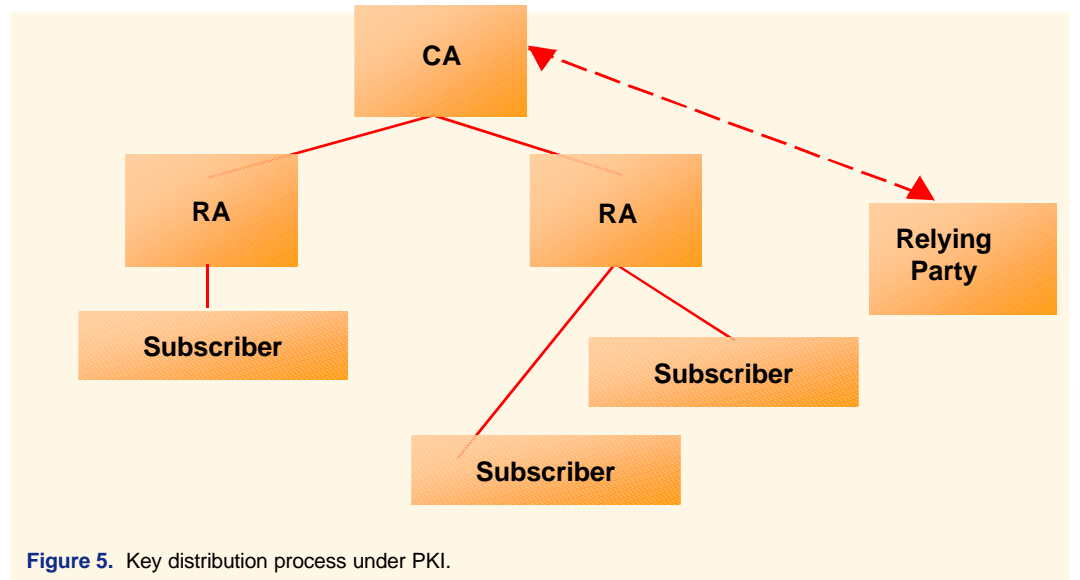
In practice, all of these steps will be automated by computer software (i.e. email clients) so that users will not have to perform any of these tasks. A diagrammatic representation of this process is set out below.





Key Distribution

The final components of a PKI are the Certification Authority (CA) and Registration Authority (RA). CAs basically act as a trusted third party which services as a distribution point for all digital certificates. The digital certificates which are publicly distributed contain a user's public key as well as other information such as the user's personal details and the expiry date of the key. RAs are the entities which verify a user's identity at the time the user applies for a digital certificate. In practice, often the CA and an RA are the same entities. Figure 5 outlines the certificate distribution processes under a PKI.





For further information,
contact:

Brisbane (07) 3309 0888
Phillip Hourigan
phillip.hourigan
@deacons.com.au

Matthew Hall
email: matthew.hall
@deacons.com.au

Melbourne (03) 9230 0411
Bernard O'Shea
email: bernard.o'shea
@deacons.com.au

Tony Cooke
email: anthony.cooke
@deacons.com.au

Perth (08) 9426 3222
John Groppoli
email: john.groppoli
@deacons.com.au

Chris Hewitt
email: chris.hewitt
@deacons.com.au

**Sydney /
Canberra
(02) 9330 8000**

John Grimes
email: John Grimes
@deacons.com.au

Leif Gamertsfelder
email: leif.gamertsfelder
@deacons.com.au

Andrew Sorensen
email: andrew.sorensen
@deacons.com.au

Under this model, a subscriber approaches an RA and requests a digital certificate. The RA will (under a robust system) request verification of the user's identity at the time of application. This is similar to the 100 point identity check that we go through when opening an account with a bank. If the RA satisfactorily verifies the identity of the subscriber a unique private and public key pair will be created for the subscriber and be signed by the CA. The public key will then be embedded in the digital certificate (along with other personal details of the subscriber), which will then be sent to the subscriber. The public key will then be made available online to relying parties. For a discussion about some of the possible problems with PKI download a copy of the publication entitled *Under Lock & Keyboard* at www.deacons.com.au.

Leif Gamertsfelder
Sydney

