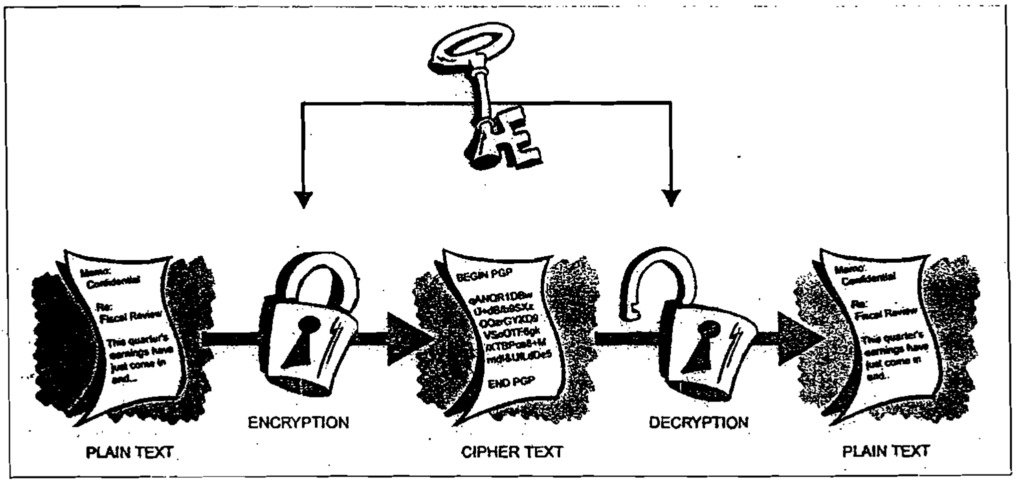

Fig. 2: Private key cryptography

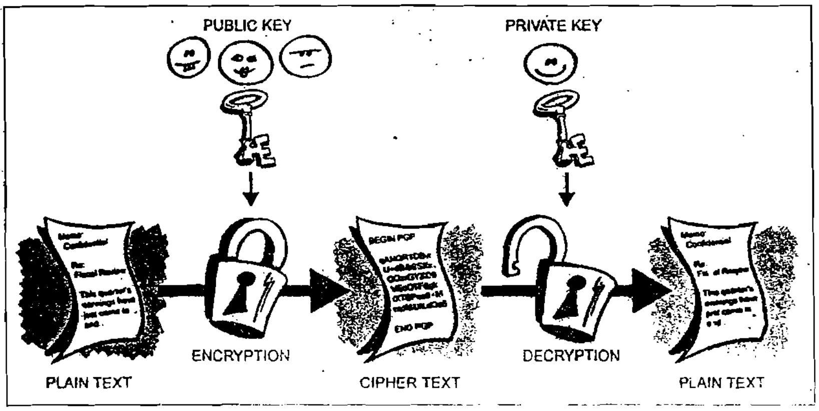

Fig. 3: Public key cryptography

security would be provided through the use of passwords. This meant that the decryption technique or the password first of all had to be mutually agreed upon and then had to be transmitted securely to the recipient. This again created the same problems: How to send this data securely in the first place, and how to engender trust if the two parties did not have any pre-established relationship?

This kind of mechanism was called private key cryptography or symmetric cryptography. Both the parties had identical 'keys,' which were nothing but sophisticated passwords. A message that was encrypted (scrambled) by one key could only be decrypted (unscrambled) using the copy of the same key present with the recipient.

This method is very fast and especially useful for encrypting data that is not going anywhere. However, conventional encryption alone as a means for transmitting secure data can be quite expensive simply due to the difficulty of secure key distribution. 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, the bat phone or some other secure communication medium to prevent disclosure of the secret key during transmission.

Asymmetric or public key cryptography

A mechanism that enables two parties to establish a secret key for secure communications without the need for a separate trusted channel is called public key cryptography or asymmetric cryptography. It is based on a pair of keys, one of which is made public and accessible to anyone. The other remains private and is kept with the recipient.

The sender uses the public key to encrypt a message. This message can be decrypted only by using the private key of the key pair. Since this private key exists only with the recipient, the sender is assured that his message can be viewed only by the person for whom it is intended. Thus parties can establish secure communications with each other dynamically, and without the need to form a prior relationship.

Subsequent advances in public key cryptography led to other systems that used the same idea of a public and private key. Systems such as RSA (named after its creators Rivest, Shamir and Adelman) were developed that enabled secure exchange of secret keys.

A very popular public-key encryption utility is called 'pretty good privacy' (PGP), which allows you to encrypt almost anything.

How PGP works

PGP combines some of the best features of both conventional and public key cryptography. In other words, it is a hybrid cryptosystem. When a user encrypts plain text with PGP, PGP first compresses the plain text. Data compression saves modem transmission time and disk space and, more importantly, strengthens cryptographic security.

Most cryptanalysis techniques exploit patterns found in the plain text to crack the cipher. Compression reduces these patterns in the plain text, thereby greatly enhancing resistance to cryptanalysis. (Files that are too short to compress or which don't compress well aren't compressed.)

PGP then creates a session key, which is a one-time-only secret key. The session key is a random number generated from the random movements of your mouse and the keystrokes you type. It works with a very secure, fast conventional encryption algorithm to encrypt the plain text. The result is cipher text. Once the data is encrypted, the session key is encrypted to the recipient's public key. This public key-encrypted session key is transmitted along with the cipher text to the recipient.

Decryption works in the reverse way. The recipient's copy of PGP uses his private key to recover the temporary session key, which PGP then uses to decrypt the conventionally encrypted cipher text.

The combination of the two encryption methods combines the convenience of public key encryption with the speed of conventional encryption. Conventional encryption is around 1000 times faster than public key encryption. Public key encryption, on the other hand, provides a solution to key distribution and data transmission issues. Used together, performance and key distribution are improved without any sacrifice in security.

Public key infrastructure

Public key infrastructure (PKI) makes use of public key cryptography for authenticating a message sender or encrypting and decrypting a message. It is a combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on the Internet.

Enterprises take advantage of the speed and immediacy of the Internet while protecting business-critical information from interception, tampering and unauthorised access. The data is securely and privately exchanged through the use of a public-private cryptographic key pair that is obtained and shared through a trusted authority.

Use of PKI

A PKI offers the following:

1. Secure e-business. Companies can offer customers and business partners the confidence to purchase their goods and services on the Web as well as conduct various other transactions online. They can also provide secure and controlled access to an intranet for HR data, secure e-mail and applications to their employees. For example, a company employee at a remote location can access (after being verified) statistics or files needed to show a client from the intranet. A PKI also lets you create secure extranets that give select partners easy access to business-critical information stored on your internal network. This is an invaluable aid for enhancing e-business.

2. Integration of supply chain. A PKI provides a protected environment for safe information exchange at every stage of your manufacturing process. For example, a document that is confidential can be encrypted using the public key of only the authorised person to prevent leakage of information.

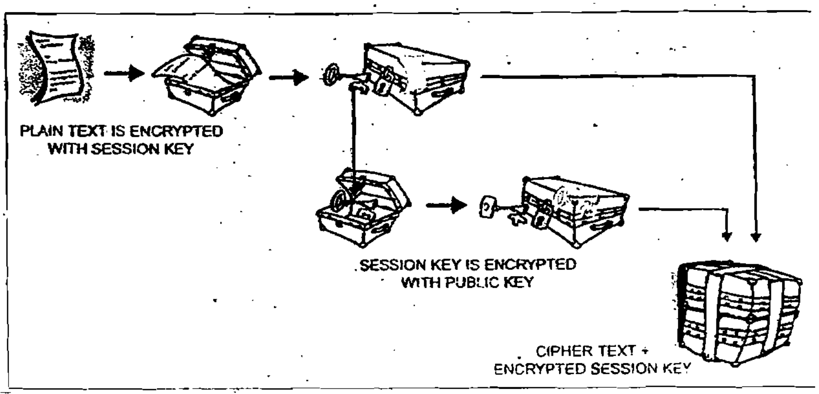
PLAIN TEXT IS ENCRYPTED WITH SESSION KEY
SESSION KEY IS ENCRYPTED WITH PUBLIC KEY
CIPHER TEXT + ENCRYPTED SESSION KEY

Fig. 4: PGP encryption

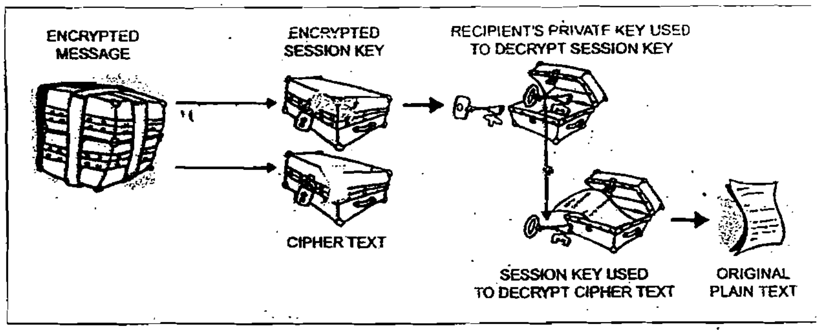
ENCRYPTED MESSAGE
ENCRYPTED SESSION KEY
RECIPIENT'S PRIVATE KEY USED TO DECRYPT SESSION KEY
CIPHER TEXT
SESSION KEY USED TO DECRYPT CIPHER TEXT
ORIGINAL PLAIN TEXT

Fig. 5: PGP decryption

3. Identity authentication. Digital certificates issued as part of PKI allow individual users, organisations and Website operators to confidently validate the identity of each party in an Internet transaction.

4. Integrity verification. A digital certificate ensures that the message or document that the certificate 'signs' has not been changed or corrupted in transit online. It can also alert the user if the document has been tampered.

5. Privacy: Information is protected from interception during Internet transmission.

6. Access authorisation. PKI digital certificates replace easily guessed and frequently lost user identifications (IDs) and passwords to streamline the intranet log-in security and reduce the MIS overhead.

7. Transaction authorisation. Enterprises can control access privileges for specified online transactions.

8. Non-repudiation. Digital certificates validate their users' identities, making it nearly impossible to later repudiate a digitally 'signed' transaction, such as a purchase made on a Website.

Components of a PKI

A PKI consists of certificate authority, registration authority, directories, certificate management system, certificates and certificate revocation list.

Certificate authority (CA). Public key cryptography works fine between individuals. If you want to send us encrypted information, you give us your public key and we give you ours. And thus we can encrypt any message meant for you using your public key and rest assured that no one but you can decipher or decrypt it. Similarly, if you want to securely communicate with us, you would encrypt the message using my public key.

However, this process gets more difficult as more people become involved. There must be a mechanism to obtain a key from someone you don't know and still be assured of its authenticity.

In traditional business interactions, this is the role of a notary or letter of introduction. Some trusted third-party vouches for the identities of correspondents to their mutual satisfaction.

In an electronic environment, the CA performs this role. Each participant is issued a public key certificate. This certificate contains the identity and affiliation of the individual, and that person's public key. This certificate is bound together with the digital signature of the certificate authority. Thus, the CA vouches for the identity of the certificate's owner and binds the owner's public key to that identity. The authentisity of the certificate is verifiable through the mechanism of digital signatures.

Thus CA is an entity that acts as a trusted third party by confirming the identities of organisations and individuals. It can be an authority in a network that issues and manages security credentials and public keys for message encryption and decryption, or it can be an independent organisation that takes on this onus.

As part of a public key infrastructure, a CA checks with a registration authority to verify the information provided by the requester of a digital certificate. If the registration authority verifies the requester's information, the CA can issue a certificate. A certificate includes the public key or information about the public key.

Registration authority (RA). In the case of large organisations spread across different geographic locations, it becomes difficult for a centralised CA to manage all the functions related to the issuance of certificates.

A number of RAs are created differentiated on the basis of certain characters like common name, country, organisation, organisation unit, state, location and e-mail. These collect details about the people or organisations that are requesting certificates from the CA. The RA will verify the validity of these details and pass on a request to the CA that the certificates be issued. RAs thus act as verifiers for the CA before a digital certificate is issued to a requester.

Directories. A user's public key certificate is stored in a special directory that acts much like an electronic phone book. The sender of a message looks up the recipient's certificate in this directory. The message can then be encrypted using the key embedded in the certificate.

Public key cryptography works fine between individuals. If you want to send us encrypted information, you give us your public key and we give you ours. And thus we can encrypt any message meant for you using your public key and rest assured that no one but you can decipher it.

Traditionally, to send a letter to someone, you look up the recipient's address in an address book. This may be your own compilation, a published phone book or a reference given to you by someone you trust. The degree of trust you place in the directory listing is related to your trust in the creator of that directory and your judgment of whether or not it is likely to be out of date.

The analogous electronic directory contains addresses and subscriber certificates. It is kept current, taking into account certificate expirations and revocations. The contents of the directory can be trusted because they are packaged and signed by your trusted CA.

Certificate management system. This refers to the software that helps in issuing, validating and managing the certificates. Example of this could be Microsoft Certificate Server (MSCS). These provide customisable services for issuing and managing digital certificates used in software security systems employing public-key cryptography. Certificate servers perform a central role in the management of software security systems to enable secure communications across the Internet, corporate intranets and other non-secure networks.

Certificates. A digital certificate can be likened to the electronic version of a passport or an identity card. It is used to positively identify a person or organisation, and establishes their credentials when doing business or conducting other transactions on the Web.

The digital certificate is issued by a certificate authority (CA). It contains the name of the person or organisation to which it is issued, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures) and the digital signature of the certificate-issuing authority. This is so that the recipient can verify that the certificate is real. Some digital certificates conform to a standard called X.509. Digital certificates can be kept in directories, so authenticated users can look up other users' public keys.

Certificate revocation list. To make a public key and its identification with a specific subscriber readily available for use in verification, the certificate may be published in a repository or made available by other means. Repositories are online databases of certificates and other information available for retrieval and use in verifying digital signatures. Retrieval can be accomplished automatically by having the verification program directly inquire of the repository to obtain certificates as needed.

This is necessary because a certificate may prove to be unreliable, such as in situations where the subscriber misrepresents his identity to the CA. Also, in a place like the Internet, which is ever changing, some information that might have been true when the certificate had been applied for, may have become out of date and untrue in a short time.

If the subscriber loses control of the private key ('compromise' of the private key), the certificate becomes unreliable, and the CA (with or without the subscriber's request depending on the circumstances) may suspend or revoke (permanently invalidate) the certificate. Immediately upon suspending or revoking a certificate, the CA must publish a notice of the revocation (called 'certificate revocation list') or suspension, or notify persons who inquire or who are known to have received a digital signature verifiable by reference to the unreliable certificate.

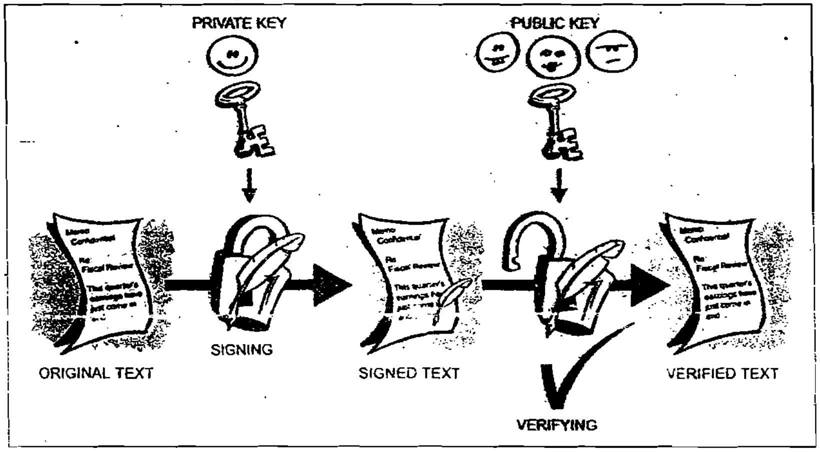

Fig. 6: Simple digital signatures

Types of PKI

Before an organisation can begin implementing PKI and acting as a CA by issuing certificates, it needs to be able to issue certificates that contain company-specific identifying information, and must be able to control who is issued a certificate. There are two main PKI options: closed PKI and open PKI.

Closed PKI. With proprietary PKI software, one can issue digital certificates to a limited, controlled community of users. Applications, including those of extranet users and anyone else outside the enterprise with which employees need to communicate securely, need a special software interface from the PKI vendor to work with the certificates. Closed PKI systems require additional training, hardware, software and maintenance.

Open PKI. Applications interface seamlessly with certificates issued under an open PKI, the roots of which are already embedded. Open PKI systems allow enterprises to become their own CA while taking advantage of the PKI vendor's service and support.

One does not have to depend on proprietary PKI systems, since the security features are based on MSCrypto API, which is present in most computers by default. If a computer has Microsoft Internet Explorer version 4.01 and above, the computer has MS Crypto API installed as well. Therefore there are no fears of future obsolescence or incompatibility with other PKI systems. Since Microsoft provides MS Internet Explorer free, cost overheads are less too.

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 information to verify the authenticity of the information's origin and also that the information is intact. Thus, public key digital signatures provide authentication and data integrity. A digital signature also provides non-repudiation, which means it prevents the sender from claiming that he did not actually send the information. These features are 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 to the identity of the signer.

Some people tend to use signatures more than they use encryption. For example, you may not care if anyone knows that you just deposited Rs 1000 in your account, but you do want to be darn sure that it was the bank teller you were dealing with.

The basic manner in which digital signatures are created is shown in Fig. 6. Instead of encrypting information using someone else's public key, you encrypt it with your private key. If the information can be decrypted with your public key, it must have originated with you.

Hash functions

The digital signature system described above has some problems. It is slow and produces an enormous volume of data—at least double the size of the original information. An improvement on the above scheme is the addition of a one-way hash function in the process. A one-way hash function takes variable-length input—in this case, a message of any length, even thousands or millions of bits—and produces a fixed-length output; say, 160-bit. 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.

PGP uses a cryptographically strong hash function on the plain text the user is signing. This generates a fixed-length data item known as a 'message digest.' (Again, any change to the information results in a totally different digest.)

Then PGP uses the digest and the private key to create the 'signature.' PGP transmits the signature and the plain text together. Upon receipt of the message, the recipient uses PGP to re-compute the digest, thus verifying the signature. PGP can encrypt the plain text or not; signing plain text is useful if some of the recipients are not interested in or capable of verifying the signature.

As long as a secure hash function is used, there is no way to take someone's signature from one document and attach it to another, or to alter a signed message in any way. The slightest change in a signed document will cause the digital signature verification process to fail.

Digital signatures play a major role in authenticating and validating other PGP users' keys.

Use of digital signatures

1. Signer authentication. If a public and private key pair is associated with an identified signer, the digital signature binds the message to the signer. The digital signature cannot be forged, unless the signer loses his private key through corruption of the media or if being divulged to someone else compromises the key.

2. Message authentication. The digital signature also identifies the signed message. Verification reveals any tampering, since comparison of hash results shows whether the message is the same as when signed. This authentication is typically far better than in the case of a paper-based signature, since in the case of a signature on paper, it is easier to add something or alter the pre-existing document without the signer's consent. Once an e-document is digitally signed, it is virtually impossible to make any alteration howsoever minute without being detected.

3. Affirmative act. Creating a digital signature requires the signer to use the signer's private key. This act can perform the 'ceremonial' function of alerting the signer to the fact that the signer is consummating a transaction with legal consequences.

4. Efficiency. The process of creating and verifying a digital signature is usually completely automated and transparent to the user, who does not need to know the details of the processes being carried out. Digital signing software eliminates the overheads and tedium associated with authenticating paper-based signatures such as checking specimen signature cards. Such methods are extremely labour-intensive and rarely used in practice—digital signatures yield a high degree of assurance that the digital signature is genuinely the signer's without adding greatly to the resources required for processing.

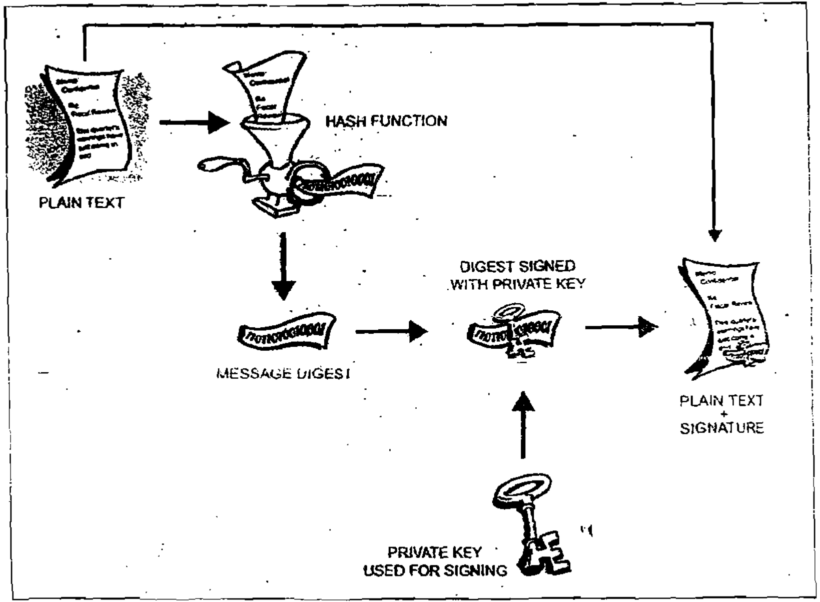

Fig. 7: Secure digital signatures

Thus digital signing techniques not only provide for sender authentication of e-documents and check for data integrity but also go a long way toward ensuring that a trusted environment is created for e-business.

Digital certificates

One issue with public key cryptosystems is that users must be constantly vigilant to ensure that they are encrypting to the correct person's key. In an environment where it is safe to freely exchange keys via public servers, man-in-the-middle attacks are a potential threat. In this type of attack, someone posts a phony key with the name and ID of the user's intended recipient. Data encrypted to—and intercepted by—the true owner of this bogus key is now in the wrong hands.

In a public key environment, it is vital that you are assured that the public key to which you are encrypting data is in fact the public key of the intended recipient and not a forgery. You could simply encrypt only to those keys that have been physically handed to you. But if you need to exchange information with people you have never met, how can you tell that you have the correct key?

Digital certificates, or certs, simplify the task of establishing whether a public key truly belongs to the purported owner.

A certificate is a form of credential. Examples might be your driver's licence, your social security card or your birth certificate. Each of these has some information on it identifying you and some authorisation stating that someone else has confirmed your identity. Some certificates, such as your passport, are important enough confirmation of your identity that you would not want to lose them.

A digital certificate functions much like a physical certificate. Put simply, it is the information included with a person's public key that helps others verify that a key is genuine or valid. Digital certificates are used to thwart attempts to substitute one person's key for another.

A digital certificate consists of three things:

1. A public key

2. Certificate information ('identity' information about the user, such as name, user ID and so on)

3. One or more digital signatures

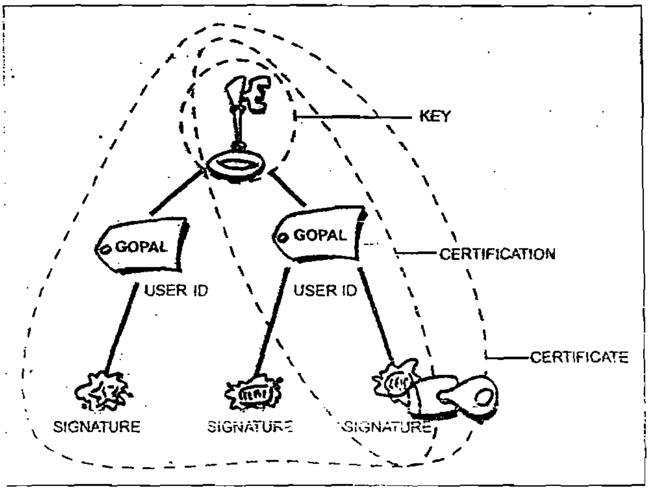

Fig. 8: Anatomy of a PGP certificate

The purpose of the digital signature on a certificate is to state that some other person or entity has attested to the certificate information. The digital signature does not attest to the authenticity of the certificate as a whole: It vouches only that the signed identity information goes along with, or is bound to, the public key.

Thus, a certificate is basically a public key with one or two forms of ID attached, plus a hearty stamp of approval from some other trusted individual.

Use of digital certificates

We know that to verify a digital signature, the recipient must have access to the signer's public key and have assurance that it corresponds to the signer's private key. Then only he will be able to decrypt the encrypted hash and authenticate the signature. However, a public and private key pair has no intrinsic association with any person; it is simply a pair of numbers. Some convincing strategy is necessary to reliably associate a particular person or entity to the key pair.

If there are only two parties to a transaction, they can communicate this information through a reliable and secure means like a telephone or courier company. This itself is no small task, especially if the parties are located far from each other. Another point to note is that parties that normally use the Internet to habitually conduct business communication are not individual persons, but rather corporations or similar artificial entities.

As electronic commerce increasingly moves from a bilateral setting to the many-on-many architecture of the world wide web on the Internet, and significant transactions occur among strangers who have no prior contractual relationship and will never deal with each other again, the problem of authentication becomes severe. A need is felt for a secure channel for communication on the Internet itself, where one can authenticate oneself or others.

A prospective signer might issue a public statement wherein he can identify his public key. However, this again leads to the same problem of authentication. The question remains as to whether the person making such an assurance is actually who he claims to be, leading to a catch-22 situation. Besides, the legality of such a claim would be in doubt since there is no precedent available for benchmarking in case this claim turns out to be false. Also the signer in such a case can later repudiate his claim if the transaction turns out to be disadvantageous to him. He can deny ever having made a statement identifying him with any key and no one would be able to disprove him because of the open nature of a medium like the Internet.

The solution then lies in the use of one or more trusted third parties to associate an identified signer with a specific public key. That trusted third party is referred to as the certification authority.

Certificate distribution

Certificates are utilised when it's necessary to exchange public keys with someone else. For small groups of people who wish to communicate securely, it is easy to manually exchange diskettes or e-mails containing each owner's public key. This is manual public key distribution.

Manual public key distribution is practical only to a certain point. Beyond that point, it is necessary to put systems into place that can provide the necessary security, storage and exchange mechanisms so coworkers, business partners or strangers could communicate if need be. These can come in the form of storage-only repositories called 'certificate servers,' or more structured systems that provide additional key management features and are called public key infrastructure.

Certificate servers

A certificate server, also called a cert server or a key server, is a database that allows users to submit and retrieve digital certificates. It usually provides some administrative features that enable a company to maintain its security policies—for example, allowing only those keys that meet certain requirements to be stored.

To be concluded next month...

G.R. Kulkarni and A.C. Suthar are professors in Electronics & Communication Department, C.U. Shah College of Engineering & Technology, Wadhwan, Distt Surendranagar (Gujarat), and Ashish N. Jani, an M.Sc in IT, is a consultant