Electronic Commerce

3. Secure Messaging

V Rajaraman

V Rajaraman is with the Jawaharlal Nehru Centre for Advanced Scientific Research and the Indian Institute of Science, Bangalore. Several generations of scientists and engineers in India have learnt computer science using his lucidly written textbooks on programming and computer fundamentals.

Part 1. What is E-Commerce?, *Resonance*, Vol.5, No.10, 13-23, 2000.
Part 2. E-Commerce System Architecture, *Resonance*, Vol.5, No.11, 26-36

In this part we will describe some of the security issues which arise in e-commerce. In particular we will describe firewalls, encryption techniques and digital signature.

Electronic commerce usually uses a public switched telephone network (PSTN) and is often between entities which are not known to one another. Ensuring security of communication between the entities participating in e-commerce is hence an important requirement. Apart from ensuring the security of messages on the PSTN network, an organization should protect data stored in computers which are connected to a local area network (LAN) from malicious damage. It is also necessary to be able to authenticate messages received via the internet. In this article we will describe filters which protect an organization's network from intruders, encryption methods to ensure secrecy of message contents and stored data and digital signature to authenticate messages received from customers or business associates.

Filters

A filter is a computer program or a piece of hardware (with associated software) used to monitor message packets which enter or leave an organization's network (*Figure* 1). One may decide to allow a message packet to enter or leave the network based either on the information contained in the header of the packet or the contents of the packet. Header has the internet source and destination addresses (IP addresses) and port number which identifies the internet service, namely, telnet, ftp, http, etc .

A commonly used filter is called a firewall. The simplest firewall

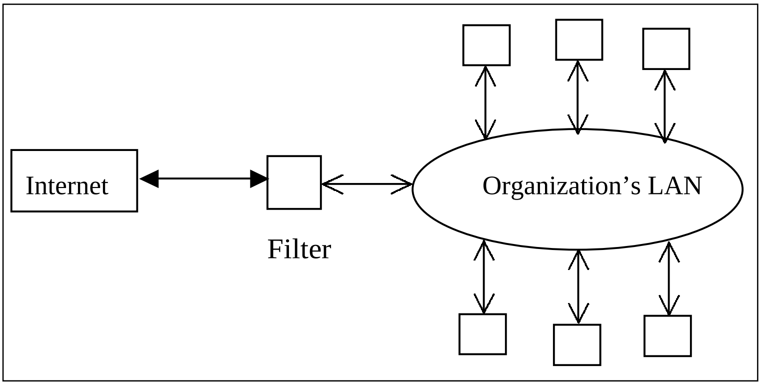


Figure 1. Filter to protect organization’s computers.

allows access to an organization's network only to a specified set of IP addresses. Another screening rule may be to allow outsiders to access only one IP address in the organization which may be hosting its web page. The other two filters which are used commonly are to filter out junk e-mail (called spam) entering a system and a web filter which is used to prevent specified material from entering a system while users are browsing the web. Junk e-mail filters scan the ‘From’, ‘X-Sender’ and ‘Sender’ fields in the header of a message. If these are in a list of unsolicited known junk mailers the messages are deleted. Automatic deletion may sometimes delete legitimate e-mail and careful monitoring is needed.

Data Encryption with Private Key

As a message sent using PSTN may be snooped by unauthorized persons it is necessary to scramble it before sending it on a public network so that even if an outsider is able to read it he will not be able to understand it and use it. One should also take precautions to prevent unauthorized persons from accessing a database. If, by some means, he is able to access it, the data stored should be in an encoded form, i.e., scrambled form so that he cannot read and use it to harm the organization. For example, sensitive databases are those containing credit card numbers, passwords, financial data, etc. Encoding or scrambling data to make it difficult to decode is called encryption. Encryption is a transformation of a data in any form (text, audio, video,

Encoding or scrambling data to make it difficult to decode is called encryption.

graphics) into another form which cannot be understood. In order to understand the data one needs a key which is used to decrypt the message. Messages to be encrypted are also known as plain text and encrypted messages are known as cryptograms or ciphertext.

There are two methods of encryption. One of them is called a symmetric or private key encryption and the other a public key encryption.

There are two methods of encryption. One of them is called a symmetric or private key encryption and the other a public key encryption. In symmetric key encryption a message sent on a PSTN is encrypted using a key (i.e. it is transformed using a transformation). The receiver applies the inverse transformation (as he knows the key) and recovers the message (see *Figure* 2). A common method uses a combination of permutuation and substitution on the plain text to obtain the ciphertext. Consider the plain text:

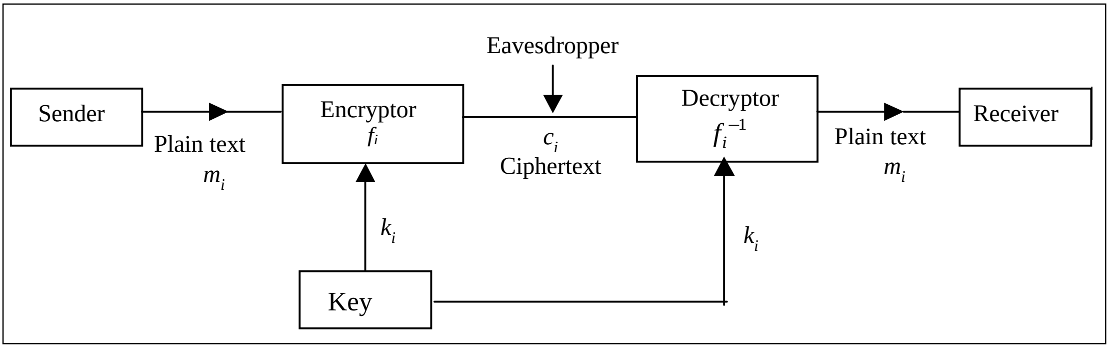
Plain text: QUICKFOXJUMPS

It is first transformed using transposition. Transposition is applied on blocks of characters. A transposition key (41253) is interpreted as a procedure to first block the message as 5 character blocks and then permute the characters using the rule: replace 1st character by the 4th character, 2nd by the 1st, 3rd by the 2nd, 4th by the 5th and 5th by the 3rd character. A block at the tail which has less than 5 characters is left unchanged. Applying this procedure the plain text becomes.

Permuted plain text: CQUKIJFOUXMPS

The next transformation is substitution. A substitution rule

Figure 2. Use of private key for encyption.



with key 4 will replace every letter by a letter which is 4 letters away from it in the collating sequence. For example, A will be replaced by E, B by F and Z by D. After applying this transformation we obtain the following ciphertext:

Ciphertext: GUYOMNJSYQTW

DES applies transformations on blocks of 64 bits corresponding to binary encoding (may be ASCII).

The algorithm on how the encryption is done can be publicized without compromising the encrypted message as a person not knowing the transposition and transformation keys will not be able to easily decode the message. If the transposition and substitution keys are changed every time a message is sent it will be impossible for a snooper to break the code even if he obtains a large sample of transmitted text.

Data Encryption Standard (DES)

This general idea is used in a very popular encryption method called the data encryption standard (DES) introduced by IBM in 1975 and standardized by US Government in 1977. It is reasonably secure, i.e. trying out all possible keys exhaustively to break the code will take too long even using a very fast computer. We will briefly describe it. DES applies transformations on blocks of 64 bits corresponding to binary encoding (may be ASCII) of message text. The plain text is exclusive ORed with the key to obtain the ciphertext ($A \oplus B = A.\overline{B} + \overline{A}.B$ where $\oplus$ is exclusive OR operator). If the key is exclusive ORed with the ciphertext we get back the original plain text as shown below:

M = Plain text	01101100	11011000	11011010
K = Key	10101111	00101100	01011011
$E = M \oplus K =$	11000011	11110100	10000001
			(Encryption)
$E \oplus K =$	01101100	11011000	11011010
			(Decryption)

This general idea is used in DES. DES encrypts 64 bit blocks. First the 64 bits are permuted with a secret key. The resulting block is divided into two 32 bit blocks (L_i, R_i) which are the left and right half of each block. The following complex procedure is applied 16 times.

$$L_{i+1} = R_i,\ R_{i+1} = L_i \oplus f(R_i, K_i),$$

where K_i is the secret key used in the i th round and f a complex function which uses both permutation and substitution operations and depends on the key. The resulting block is again permuted using the secret key to obtain the final encrypted block. DES was designed to be implemented in hardware. Integrated circuit chips implementing DES have been marketed. However, with increasing speed of computers it is possible to break the code as it uses only a 56 bit key (plus 8 parity bits) to encrypt. A new standard is being developed called advanced encryption standard (AES) which uses 128 bit blocks and 128 bit keys [2]. AES is not yet standardized and DES is still used widely. (See *Box* 1)

The encryption method we have discussed so far are called

Box 1. Advanced Encryption Standard (AES)

Exports of products using DES encryption was banned by United States Government till 1998. In 1998, DES encrypted text was cracked by a special purpose computer in 56 hours, which led to relaxation of US export controls. It was also agreed that stronger encryption is needed. National Institute of Standards and Technology (NIST) of USA initiated a process to select a new secret key encryption standard to replace DES. A competition to bid for this standard called Advanced Encryption Standard (AES) was announced by NIST. Non U.S. participation was allowed. The requirements were specified as:

1. Plain text is to be split into 128 bit blocks on which the algorithm is to be applied.
2. Three key sizes: 128, 192 and 256 bits to be used.
3. The system should effectively work with a variety of systems such as 8 bit processors, smartcards, digital video, voice, ATM networks, etc.

It was also said that the winning standard should be available world wide on a royalty free, non-exclusive basis and that the evaluation criteria would be on implementation flexibility, strength of security and cost. Of the 21 entries submitted five have been picked as finalists in August 1999. The winner(s) will be announced soon. For details of AES and current status, readers are referred to the website aes.nist.gov.

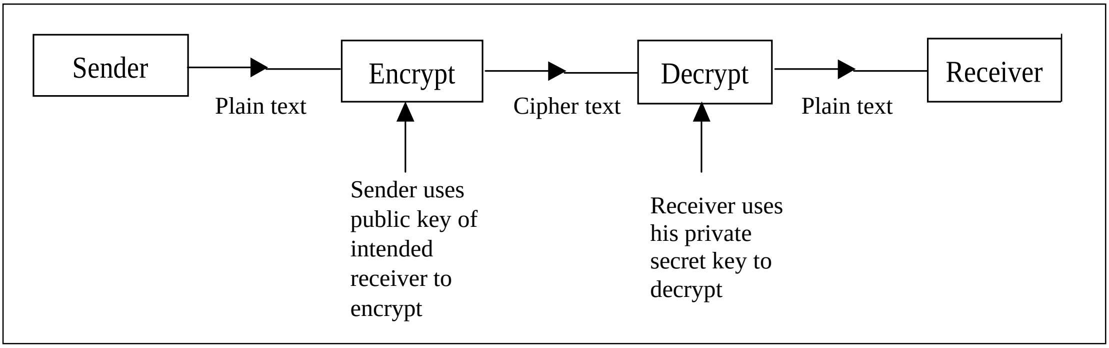
symmetric key or private key encryption as the encryption and decryption use the same key known to the two parties exchanging messages. The main problems with this method are the need to have a private key for each of the organizations with which an organization transacts business and the requirement to securely distribute the keys to all of them. Key distribution must use a different channel to avoid it being stolen.

The public key cryptography allocates two keys to each organization wanting to communicate with one another.

Data Encryption with Public Key

The public key cryptography allocates two keys to each organization wanting to communicate with one another. One of the keys is called a public key of the organization as it is available to any one wanting to send a ciphertext to that organization. The organization has another key which it uses to decrypt the ciphertext it receives to recover the plain text. This is shown in *Figure* 3. A popular public key system is known as RSA system named after its three inventors Rivest, Shamir and Adleman. The procedure has been described in detail in the article by Sarkar, which appeared in *Resonance* [3]. There are two important points to note regarding RSA. First, if a message is encrypted by a sender S with his private key it can be decrypted by a receiver R using S's public key. Second, RSA derives its strength from the fact that, given a number n which is a product of two large prime numbers, it is difficult to factor n and get the two prime components. Compared to DES the RSA encryption technique is computationally complex. Thus for large plain texts RSA is not applied in practice. The plain text is encrypted

Figure 3. Public Key Encryption System.


Sender
Plain text
Encrypt
Cipher text
Decrypt
Plain text
Receiver
Sender uses public key of intended receiver to encrypt
Receiver uses his private secret key to decrypt

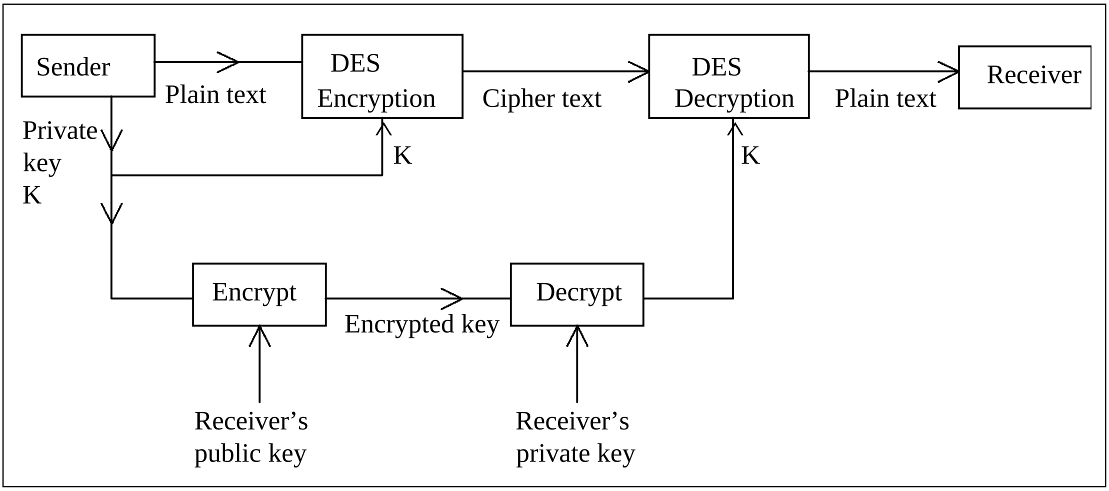


Figure 4. Combining private and public key encryption.

using DES and the secret private key necessary to decrypt the ciphertext is sent using RSA (See *Figure* 4). There are two advantages in following this procedure. First, encrypting using DES is faster as it is normally done using hardware. Second, the private key used in DES can be unique for each message as it is sent along with the message in encrypted from. Thus even if a snooper gets a large number of messages exchanged between the sender and the receiver he cannot decode them as the key is changed for each message transmitted.

Digital Signature

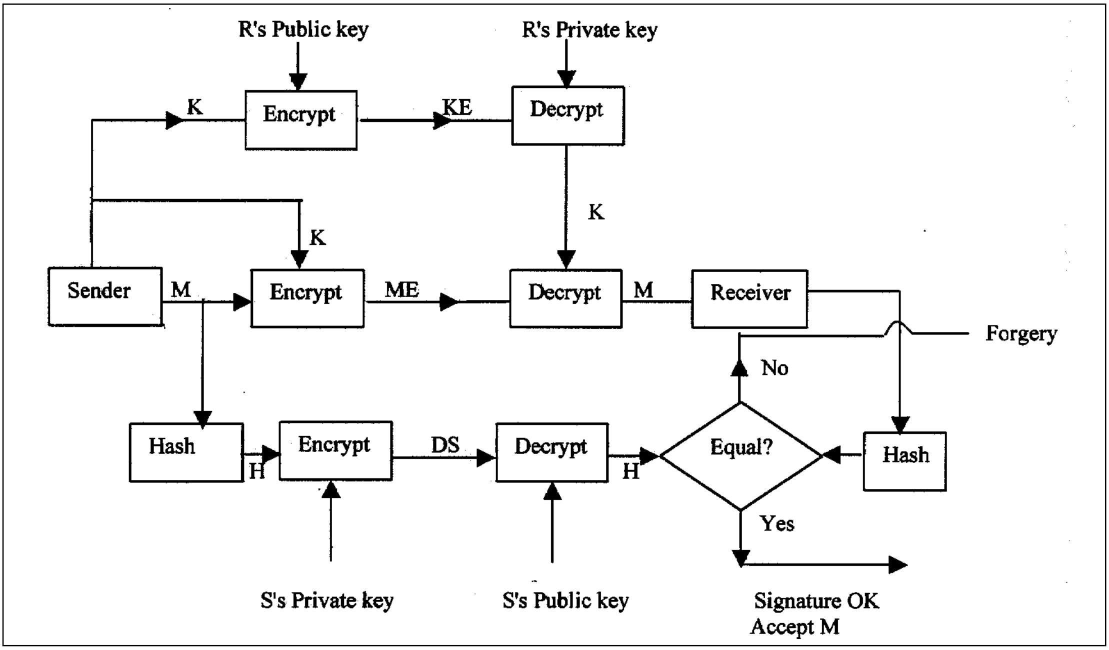
There are two important aspects of a signed paper document, which has to be imitated by an electronic signed document. First, the letterhead and signature convinces a receiver about the authenticity of the sender. Second, the signature physically appears following the text and this ties the signature to the matter typed. In legal documents every page is signed and every correction is also signed.

The RSA system is used primarily to protect messages being sent on a public network from illegal snoopers.

The RSA system is used primarily to protect messages being sent on a public network from illegal snoopers. There are two problems which may occur. First, if a senders S sends a message to R, unless it is signed by S, R cannot be sure of its authencity. Physical signatures are unique and can be verified. We need a similar method of signing an e-mail message so that *S* cannot later on say that he never sent the message. In other words, *S* should not repudiate after sending say, a purchase order to *R*. Secondly, a person say, *W*, should not be able to act as though he is *R* and receive messages intended for *R*. The public keys of all potential participants in e-commerce are known. If W somehow is able to convince *S* that *R*'s public key is his, *S* will be sending messages intended for *R* to *W* and *W* can read it using his private key. There is thus a need for a third party to authenticate public keys of all the participants. We will first explain how a digital signature system works (See *Figure* 5). Assume that a sender *S* wants to send a message to a receiver *R* and sign it. The following steps are carried out by *S*.

1. *S* picks a random key K, encrypts the plain text message (M) to be sent to *R* using K, and sends the ciphertext ME to *R*. The encryption normally uses a private key system such as DES.
2. *S* encrypts the random key K using *R*'s public key and sends it to *R*. We will call the encrypted key KE. Observe that K is encrypted using RSA system.

Figure 5. Signing a message using digital signature.



RSA algorithm is symmetric, i.e., if encryption is done with a private key, decryption can be done with the corresponding public key.

3. *R* will be able to decrypt KE using his private key and get K.
4. Having obtained K, *R* can decrypt the ciphertext ME sent by *S* and gets M.
5. Now *R* has to be convinced that *S* sent the plain text. This can be done only if *S* signs the message. Signing of the message is done as follows:
6. The message M is hashed using a hashing function, which compresses M to H. The hashing function should try to avoid collisions. In other words, two messages M1 and M2 when hashed should give unique hashed values H1 and H2. H should also be much shorter compared to M. Hashing is done primarily to reduce the size of the signature. (A hashing method called MD5 (Message Digest 5) is popular). Also hashing the message M ties H to M. In other words the signature will use H, which is tied to the document being sent.
7. H is encrypted by *S* using his private key and transmitted to *R*. This is his digital signature DS.
8. As *R* already has M he can hash it using the known hash function to obtain H.
9. When *R* receives DS, he decrypts it using the public key of the sender S.
10. The decrypted value must be H. If it is not then it is a fake message. If it is H then *R* is convinced that it is signed by *S*. *S* cannot repudiate (i.e. say that he did not send the message) as he has encrypted H using his private key which is known only to him.

The procedure works because RSA algorithm is symmetric, i.e., if encryption is done with a private key, decryption can be done with the corresponding public key.

Security systems will continue to improve to counter the threats of malicious intruders.

The second question we raised at the beginning of this section was about the authenticity of public keys. This is done by some organizations which issue public key certificates after verifying the credentials of an organization or individual. Thus if an organization A wants to do business with another organization B electronically, B can send an e-mail to the certification author-

Box 2. Information Technology Act

Parliament passed the information technology bill in the monsoon session this year and it has now become an Act. The Act was passed to promote e-commerce in India. Among other aspects this act gives legal status to digitally signed soft copies of documents. The Act describes public key encryption, digital signature, certifying authority among many other terms. In October 2000, Government of India has appointed a certifying authority in the Ministry of Information Technology. Our lawyers have to become more mathematically savvy to argue cases under this Act!

ity requesting certification of A's public key, e-mail identity, etc. Once the certifying authority certifies the public key, transaction can proceed. The certification authority takes on legal responsibility in case of disputes on identity (see *Box* 2).

In this part we saw how transactions in e-commerce are protected and authenticated. Such a protection is essential to establish mutual trust between customers and businesses. Even though the procedures seem complex, in practice, the operations such as encryption, signing, etc . are carried out by a touch of the mouse button pointing icons on a video terminal as the requisite software is stored in the computer's memory. Security systems will continue to improve to counter the threats of malicious intruders. A designer must thus pick a system appropriate to the perceived threat.

Suggested Reading

[1] **William R Cheswick and Steven M Bellevoin, *Firewalls and Internet Security*, Addison-Wesley, 1994.**

[2] **S Landau, Designing Cryptography for the New Century, *Communications of ACM*, 43(5), pp.115-120, May 2000.**

[3] **Palash Sarkar, A Sketch of Modern Cryptology, *Resonance*, 5(9), pp.22-40, September 2000.**

[4] **William Stallings, *Cryptography and Network Security - Principles and Practice*, Second Edition, Prentice Hall, NJ, USA, 1999.**

Address for Correspondence
V Rajaraman
IBM Professor of Information Technology
JNCASR
Bangalore 560 064, India.
Email:rajaram@serc.iisc.ernet.in