The ITB Journal

Volume 2 | Issue 1 Article 3

2001

# The Role of Cryptography in Security for Electronic Commerce

Ann Murphy

David Murphy

# The Role of Cryptography in Security for Electronic Commerce

***Ann Murphy. Dublin Institute of Technology***
***David Murphy. Institute of Technology Blanchardstown***

## Abstract

*Many businesses and consumers are wary of conducting business over the Internet due to a perceived lack of security. Electronic business is subject to a variety of threats such as unauthorised access, misappropriation, alteration and destruction of both data and systems. This paper explores the major security concerns of businesses and users and describes the cryptographic techniques used to reduce such risks.*

## Keywords

Internet, Web Security, cryptography, hackers, public and private keys, PKI, CAs, Client Security, Server Security, DES, RSA, digital signature, SSL, SET

## Introduction

Most organisations either utilise the Internet for business purposes already or intend doing so in the very near future (Ernst & Young, 1998). As the importance of information systems for society and the global economy intensifies, systems and data are increasingly exposed to a variety of threats, such as unauthorised access and use, misappropriation, alteration and destruction (OECD, 1999). The main concern cited by most decision- makers when it comes to e-commerce is the threat of computer security, or rather the lack thereof (Foresight, 1998; Hawkins *et al.*, 2000). The Internet has frequently been viewed as an unregulated, unsafe place to do business (Cross, 1999) and for all practical purposes comes with a 'use at your own risk' label (Labuchagne & Eloff, 2000). Things are not getting safer, now that more networks and PCs are linked via high-speed, always-on connections, hackers now enjoy a 24 hour window of opportunity to break into Internet-based systems, and it is difficult for companies to keep up with the latest security options (Dysart, 2000). Recent virus outbreaks such as Melissa and ILOVEYOU and web-site attacks against Yahoo,

Amazon and eBay indicate that security issues must become a primary concern for everyone doing business on the Internet (McGuire & Roser, 2000).

When networked information systems perform badly or don't work at all, lives, liberty and property can be put at risk. Interrupting service can threaten lives, while the disclosure or destruction of information or it's improper modification can disrupt the work of governments, corporations and individuals (Schneider, 1998).

Web security means different things to different users. For researchers it is the ability to browse the Web without interference. For businesses and consumers, it is the capability to conduct financial and commercial transactions safely, with confidence that neither the information, connections or sites have been interfered with. Many users need to operate with the conviction that the credentials of all parties can be verified and validated. In the Electronic Commerce Report (2000), Adams and Bond summarised the facilities required from an Internet based infrastructure as:

1. *Confidentiality* – the ability to keep things secret from prying eyes
2. *Integrity* – the ability to protect information from authorised changes or to be able to detect if such changes have occurred
3. *Authentication* – that the identities of all parties are assured
4. *Non-Repudiation* – that neither the sender nor receiver can deny communication
5. *Copy Protection* – from unauthorised copying of intellectual property
6. *Availability* – ensuring that access to information or services are available as and when required
7. *Legal Admissibility* – the capability of providing irrefutable evidence that a particular transaction has occurred.
8. *Standards Based* – maximum use of industry-accepted standards

The quality of security for information and communication systems and the data that is stored and transmitted on them depends not only on the technical measures, including the use of both hardware and software tools, but also on good managerial, organisational and operational procedures (OECD, 1997; 1999)

This paper examines the major security concerns of businesses and consumers engaging in electronic commerce and focuses principally on the role of cryptography in reducing the risk of conducting business on the Internet. The techniques and terminology used by cryptologists, including private and public key encryption and their use and advantages in securing both information and systems are described in detail. The issues involved in authentication using digital signatures and Certification Authorities are discussed, as are the issues involved in key management.

## The Internet

### *Brief History*

The web has emerged as the most dynamic force in the Information Technology (IT) industry during the past decade. This growth has been facilitated by the confluence of increasingly powerful and inexpensive technologies that permitted large-scale usage and the provision of scalable systems and applications, allied with the growing availability of telecommunications due to declining costs and increasing bandwidth thereby allowing the spread of digital information (Salnoske, 1998).

### *Benefits to Business*

Greenstein and Feinman (2000) identify potential benefits to business which include :

1. Internet and web-based electronic commerce is more affordable and hence allows more business partners to be reached than with traditional electronic data interchange (EDI).
2. A geographically dispersed customer base is available
3. Procurement processing and purchasing costs can be lowered
4. Reduction in inventories with lower cycle times and
5. Better customer services with lower marketing and sales costs

### *Benefits to Consumers*

Consumers benefit in a number of ways such as :

1. Increased choice of vendors and products
2. Convenience coupled with competitive prices and increased price comparison capabilities

3. Greater amounts of information that can be accessed on demand
4. Customisation in the delivery of services

   (US Department of Commerce, 1998).

## Web Security

While technology can deliver innumerable benefits, it introduces new vulnerabilities that can be exploited by persons with the necessary technical skills. Hackers represent a well-known threat, but increasingly other criminal elements must be taken into consideration (Furnell, 1999). An international survey carried out in 1998 reported that 73% of all companies reported some security breach or corporate espionage during the previous 12 months. Companies carrying out their business electronically were significantly more likely to be victims of security loss that affected their revenues and corporate data than traditional businesses (Information Week, 1998). The joint annual study between the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) has shown that verifiable losses in 1999 soared to $265.6 million, more than double the total reported for the three years 1996 to 1998 inclusive (Gold, 2000). Over 90% of respondents had detected some form of security attack on their computer systems during the year– denial of service (32%), sabotage of data or networks (19%), financial fraud (14%), insider abuse of Internet access privileges (97%), virus contamination (90%), (CSI Press Release, 1999).

While outside intruders are perceived by the world to be the largest threat to security, FBI studies have revealed that 80% of intrusions and attacks come from within organisations (Price, 1999). An insider is someone who has been (explicitly or implicitly) granted privileges that authorise them to use a particular system of facility. Insider misuse involves misuse of authorised privileges. Insiders may have better knowledge of system vulnerabilities and the whereabouts of sensitive information (Neuman, 2000).

Nonetheless, to understand the security threats involved in using the Internet for communications, it is essential to understand that there are threats evident at different parts of the infrastructure used for electronic commerce.

Web system infrastructures are composed of three parts :

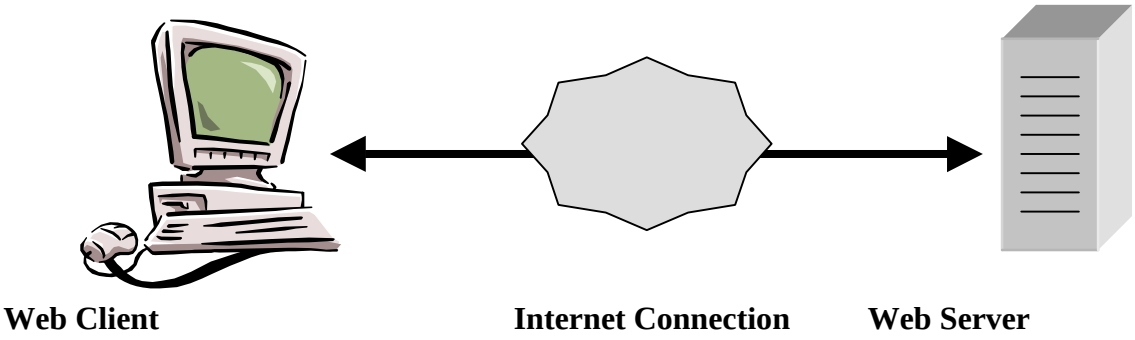



***Figure 1: Web Infrastructure (Stein, 1998)***

1. The Web Client[1]
2. The Web Server
3. The Connection between the two

Regarding security, the entire system is only as strong as the weakest link in the chain (Budge, 1998). Stein (1998) proposes that the integrity of the system relies on the following assumptions:

**From the User's (Client's) Viewpoint**

1. The Web Server is owned and operated by the organisation that claims to own it.
2. The documents returned in response to the user's request are free from viruses.
3. The remote server will not use any information either knowingly or unknowingly provided by the user for any purpose other than that required by the transaction. Examples of this type of information would include credit card details or browsing habits.

**From the Web Servers Viewpoint**

[1] In Business to Business Transactions, the Web Client also acts as a Server

1. The user will not attempt to alter the contents of the Web site.
2. The user will not attempt to break into the Servers Computer system.
3. The user will not try to gain access to unauthorised areas of the site.
4. The user will not try to crash the server thereby making it unavailable to other users
5. That the user is who they claim to be.

**From Both Parties Viewpoint**

1. That the connection is free from third parties listening in on the communications line.
2. That the information sent between browser and server is delivered intact and free from tampering.

Section 4 describes the role of cryptography in addressing some of these issues, in particular those of information integrity and user and server authentication.

## Cryptography

The ability to conduct all kinds of transactions across open information and communication networks has led to increasing concern about the security of the information itself (DTI, 1997).

### *Background*

The word cryptography comes from the Greek word *kruptós logos* meaning *hidden word* and has been used for "secret writing" for many years. Encryption is defined as the transformation of data (plaintext), via a cryptographic mathematical process, into a form (ciphertext) that is as close as possible to unreadable by anyone who does not possess the appropriate knowledge. Decryption is the reverse of encryption, the transformation of encrypted information back into its original form. Encryption and decryption require the use of some secret information – *key*. There are two main types of encryption systems, code and cipher systems. The distinction between a code and a cipher system is that using a cipher system, anything can be encrypted while using a code system the context of the type of information that will be encrypted is needed

before the codes can be devised (Beckett, 1988). The disadvantages of a code system are that usually only a few terms of the message will be encrypted, making it easier to decrypt the message especially if a number of samples of encrypted data are available (Held, 1993).

In ancient cryptography, messages were encrypted by hand with a method (algorithm) usually based on the alphabetic letters of the message. The two main types were ***substitution ciphers*** where every occurrence of a given letter is replaced by a different letter and ***transposition ciphers*** where the ordering of the letters is shifted (Deitel *et al.*, 2000). For example, if every other letter starting with 's' in the word security creates the first word of the ciphertext and the remaining letters create the second word, the word security would encrypt to *scrt euiy*. Combining substitution and transposition ciphers created more complicated ciphers.

Some famous examples of encryption include:

1. From ancient Greece where the Spartan Generals wrote messages on narrow ribbons of parchment that were wound around a cylindrical staff known as a scytale, when the ribbon was unwound, it could only be read by a person who had an exact matching cylinder (Garfinkel & Spafford, 1996).
2. A Caesar Cipher (named after Julius Caesar) is a simple encryption system that replaces individual letters by those three positions further down the alphabet (PGP, 2001).
3. The development of Morse Code in 1832 allowed the transfer of communications over wire and used a series of dots and dashes for letters in the alphabet (Morse, 1840).

Historically, cryptography has been associated with spies, governments and the military and has been used in warfare for thousands of years, the most famous case being the Enigma Cipher, used by the Germans in World War II to code the Third Reich's most secret messages (Treese & Stewart, 1998).

The problem with many historical ciphers is that their security relied on the sender and receiver to remember the encryption algorithm and keep it secret.

### *Cryptographic Systems*

Today, cryptographic methods are more sophisticated and are used to support more than the confidentiality of the message, they also include integrity protection, authentication, non-repudiation and detection of unauthorised copying (Adams & Bond, 2000).

All cryptographic systems, no matter how complex have four basic parts :

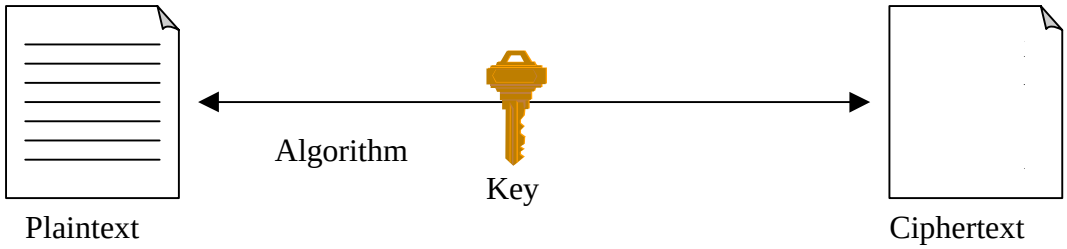



***Figure 2 : Basic Cryptographic System***

| | |
|---|---|
| *Plaintext* | A message before anything has been done to it |
| *Ciphertext* | Unreadable Plaintext message after it has been modified in some way |
| *Algorithm* | Mathematical operation used to convert plaintext into ciphertext and vice versa |
| *Key* | Secret key used to encrypt and/or decrypt the message. A key is a word, phrase, numeric or alphanumeric string which when used in conjunction with the algorithm allows the plaintext to be encrypted and decrypted. |

The advantage of cryptography is that the ciphertext can be transmitted across insecure, public communications channels. Even if the ciphertext is intercepted, it is useless to anyone who does not possess the decryption key (Stein, 1998). The key contains the binary code used to mathematically transform a message (Greenstein & Feinman, 2000). An important feature of cryptographic systems is that since the

security depends completely on the secrecy of the decryption key, it is not necessary to keep the workings of the algorithm secret. This allows the same algorithm to be reused by many people and avoids any need to protect cryptographic software (Stein, 1998). The principle is the same as that of a combination lock, where many people may use locks of the same design, but each one uses a different combination (Treese & Stewart, 1997). When creating a new algorithm, a cryptographer has no way of knowing for sure that it is airtight against thieves, the only way to achieve confidence is through trial and error as the number of people who try and fail to break it increases (Greenstein & Feinman, 2000).

### Key Length

Modern cryptosystems are digital, their algorithms are based on individual bits of the message rather than letters of the alphabet. Encryption and decryption keys are binary strings with a given key length (Deitel *et al.*, 2001). Keys in a cipher system are described by the number of bits used to hold them, for a key with n bits, there are $2^n$ possible keys (Treese & Stewart, 1997). For example, 56 bit encryption systems have 72,057,594,037,927,936 possible key combinations. Longer keys have stronger encryption, so that it takes more time to 'break the code'. Current key length recommendations are using a 75 Bit Key for present day security and encrypting using a 90 Bit Key for information that must be kept secure for 20 years

## *Cryptanalysis*

Even if keys are kept secret, it may be possible to compromise the security of a system. Trying to decrypt ciphertext without knowledge of the secret key is known as Cryptanalysis. Commercial encryption systems are constantly being researched by cryptologists to ensure that the systems are not vulnerable to attack. The most common form of attack is that in which the encryption algorithm is analysed to find relations between bits of the encryption key and bits of the ciphertext (Deitel *et al.*, 2001). The only perfect cryptosystem is called the *One Time Pad* in which the sheets of paper in a pad are filled with completely random characters. An exact copy of the pad is made and hand delivered to the correspondent, the ciphertext is created by writing the message by adding the letters pair wise where A=1$^{st}$ letter, B=2$^{nd}$ and Z wraps back to A. The process is reversed by the recipient revealing the plaintext. Once

a sheet of the pad is used, it is destroyed, if the pad contains truly random letters the code is absolutely secure (Treese & Stewart, 1997). An obvious disadvantage of this method of encryption would be the logistics of distributing the pads as each pair of correspondents would require a unique pad.

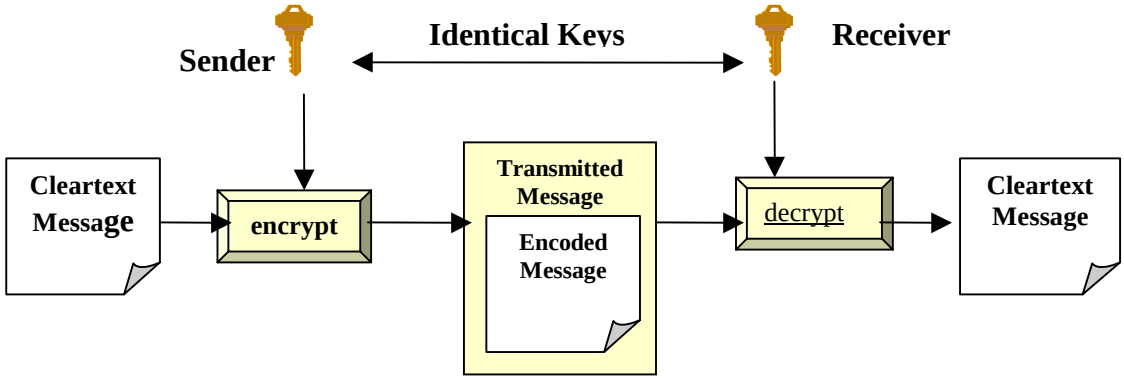
### *Public and Private Key Encryption*

There are two basic types of cryptographic mechanisms to provide encryption capability, private or symmetric cryptography where entities share a common secret key, and public or asymmetric cryptography where each communicating entity has a unique key pair.

#### Private/Symmetric Key Encryption

Private key cryptography, the traditional form of cryptography, uses a single key to encrypt and decrypt a message. The main advantage of symmetric cryptography is its speed.

***Figure 3 : Private Key Encryption*** (Greenstein & Feinman, 2000)




A **Block** cipher is a type of symmetric-key encryption that transforms a fixed-length of plaintext into a block of ciphertext data of the same length. Because each block of a cipher is independent, an eavesdropper may notice that certain blocks are repeated indicating that the plaintext blocks also repeat. A **Stream** cipher typically operates on smaller units of plain text and is designed to be exceptionally fast by using the key to produce a pseudorandom key stream which is then used to produce the ciphertext (Treese & Stewart, 1998).

Since both parties must know the same key, **authentication** is assured as when the message arrives, there is there is only one person that it could be from.

Message **integrity** can be verified by the use of a **Message Digest**, which generates a short fixed length value known as a hash. A **Hash** function is a transformation that reduces a large data message to one of a more comprehensible size – any message can be reduced to a fixed length, say 128 bits, using a hash function (Stein, 1998). There is no way to decrypt a hash, nor any known way to create two different messages that generate the same hash (Deitel *et al.*, 2001). The hash function ensures that if the information is changed in any way a different output value is produced.

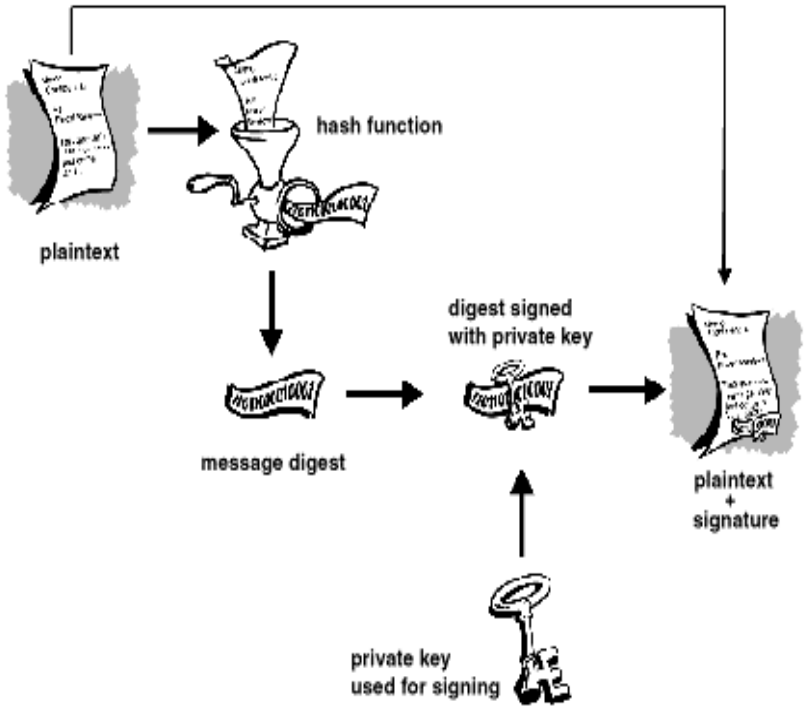



***Figure 4 : Hash Function*** (PGP,2001)

One of the most commonly used symmetric encryption algorithms is the **Data Encryption Standard (DES)**, developed by IBM and US Government. DES is a block cipher, which uses a 56-bit key to encrypt a 64-bit plaintext block into a 64 bit ciphertext. DES became a recognised standard - Federal Information Processing Standards Publication in July 1977. DES consists of 16 blocks of operations that mix the data and the key together where the encryption of each block depends on the

contents of the previous one (Cipherblock Chaining). The message is first rewritten in binary format, then encrypted using the DES algorithm. (FIPS 46-2, 1993).
The main criticism of DES is that the key is not long enough and could be solved by a Brute Force Attack, which tries all possible key combinations in turn until the code is cracked. DES was broken in 1997 in five months by a group known as DESCHALL, which divided the list of possible keys into small segments and using the Internet, gave each segment to volunteers, along with a key-testing program (Stein, 1998). In July, 1998, the supercomputer DES Cracker, designed by Electronic Frontier Foundation, assisted by 100,000 distributed PCs on the Internet was able to crack DES in only 22 hours. This DES challenge can be seen at http://www.eff.org/descracker.html (RSA, 2000).

DES in Triple Encryption Mode (**Triple DES**) is a variant that decreases the risk of brute force attack, by using longer keys. The message is first encrypted using one secret key, decrypted with the second key (the decryption operation does not yield the plain text, since a different key is used) and then encrypted again using a third key as shown in Figure 5.

Other common symmetric encryption algorithms include the European International Data block cipher Encryption Algorithm (**IDEA**), developed by James Massey and Xeujia Lai in 1990. IDEA uses 128-bit key for encryption, which is considered significantly more secure than DES. RC2 and RC4 stream ciphers, designed by RSA are widely used for bulk encryption and use keys of varying length as high as 2048 bits. Crippled versions, (versions which have been deliberately disabled to operate at only a limited key length), that use 40 bit keys have been licensed for export beyond the USA (which prohibited the export of encryption techniques until mid 2000) and are frequently used by web browsers and servers (Stein, 1998).

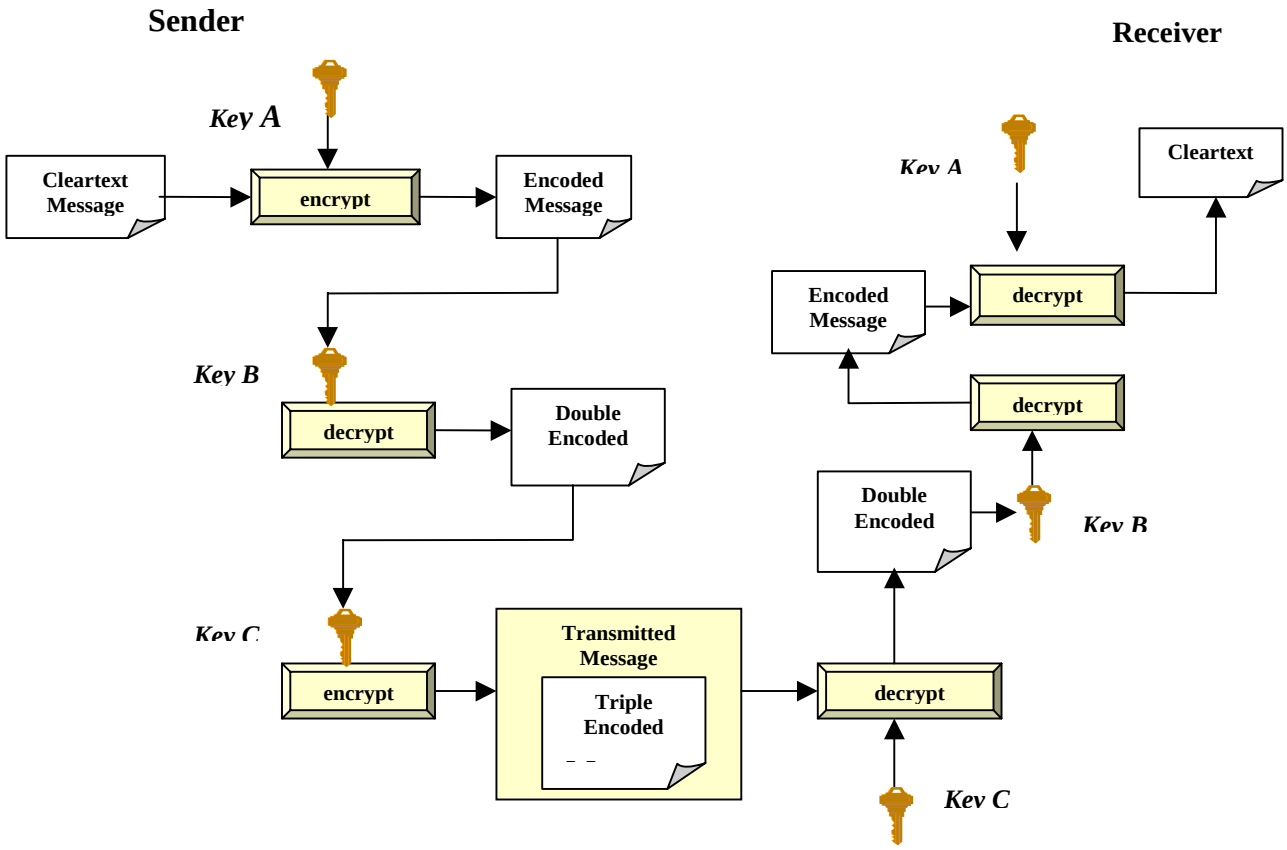



***Figure 5 : Triple DES*** (Greenstein & Feinman, 2000)

**Blowfish** is a freely available, variable length block cipher designed by Bruce Schneier of Counterpane Systems, (http://www.counterpane.com/blowfish). It is nearly three times faster than DES and is being widely used in PC file encryption and secure tunnelling applications (Treese & Stewart, 1998).

The general consensus of the U.S. National Institute of Standards and Technology is that DES is no longer strong enough for today's encryption needs and is currently working on the Advanced Encryption Standard (**AES**) which is expected to remain a standard well into the 21st century (RSA, 2000).

### Private Key Distribution

Distribution of private keys is a major issue in the security of symmetric cryptography. There are several methods for key sharing:

1. Meet in Person – simplest method but doesn't scale well
2. Courier – Can the courier be trusted, this can be overcome by splitting the key and using alternative routes to send key parts
3. Telephone, email or letter

The problem with key distribution, is that anyone who intercepts the key in transit can later modify and forge all information that is encrypted or authenticated with that key.

**Public/Asymmetric Key Encryption**

One of the main challenges for private key encryption is enabling the sender and receiver to agree on the secret key without anyone else finding out. Another important problem occurs on the Internet, where parties often need to communicate without having previously met. Even if it were possible to securely distribute the servers secret key to the thousands of users, it would be impossible to keep the key secret for long (Stein, 1998).

Public key cryptography, developed by Diffie & Hellman (1976), allows a sender and receiver to generate a shared secret key using an algorithm based on the senders and receivers public and private information.

Figure 6 illustrates the steps:

1. The sender determines a secret value a
2. A related value A, derived from a is made public
3. The receiver determines a secret value b
4. A related value B, derived from b is made public

5. The Diffie-Hellman algorithm is used to calculate a secret key corresponding to the key pairs (a,B) and (b,A),

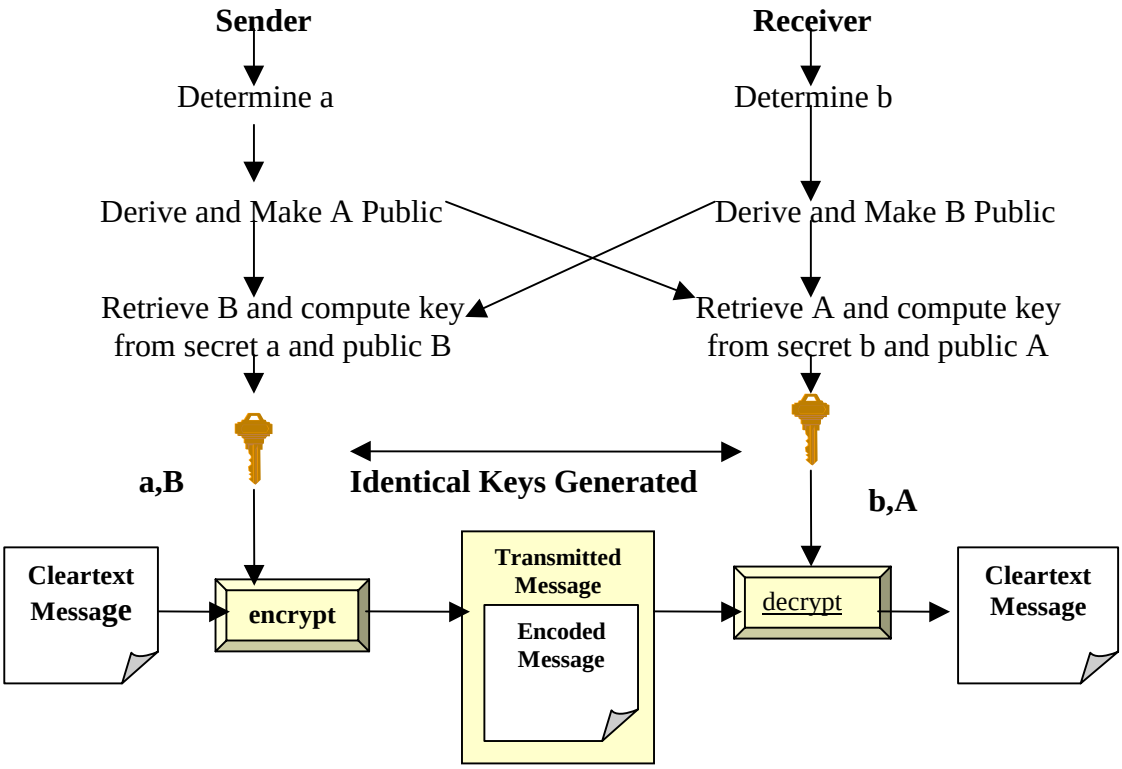



***Figure 6 : Diffie-Hellman Public Key Cryptography***(Greenstein & Feinman, 2000)

Two way public key communication using Diffie-Hellman cryptography is vulnerable to a man-in-the-middle attack where a hacker intercepts both the senders and receivers public keys and replaces them with his own value, then either renders the communication indecipherable or generates a matching key in order to alter the message. Neither sender nor receiver realise their message has been intercepted or altered (Greenstein & Feinmann, 2000).

RSA is an asymmetric encryption scheme, which was developed by **R**ivest, **S**hamir and **A**dleman in 1977. It uses a pair of keys for encryption, a **public** key which encrypts data, and a corresponding **private** key for decryption. The public key method allows a sender and receiver to generate a shared secret key over an insecure telecommunications line, where each participant creates his own key pair, the private key is kept secret and never revealed or shared, while the public key is distributed

freely (Treese & Stewart, 1998). The need for the sender and receiver to share secret information is eliminated, as all communications involve only public keys. Anyone can send a confidential message using the public key but the message can only be decrypted using the private key, which is in the sole possession of the intended recipient (RSA, 2000). An illustration of a public key system is a safe with a slot at the top, anyone can put items into the safe, but only the person who knows the combination can get the items out (Treese & Stewart, 1998).

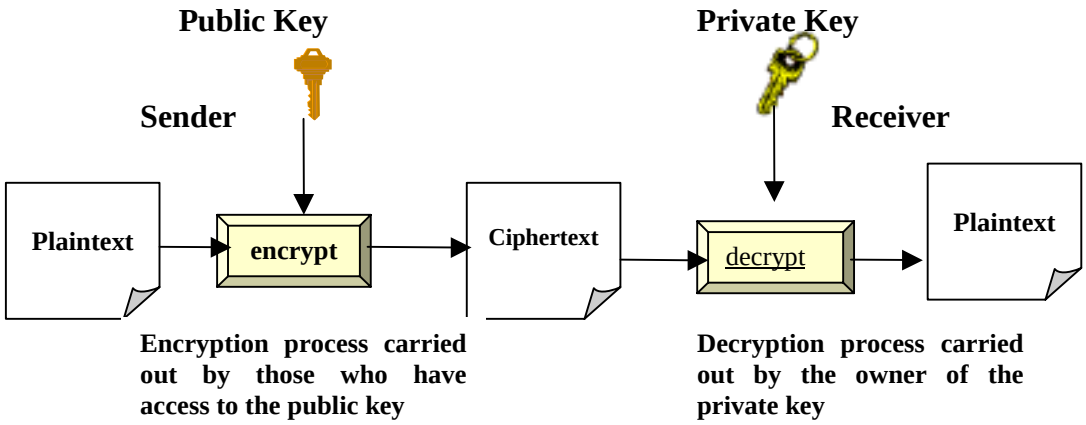



***Figure 7 : Public Key/Asymmetric Encryption***

The RSA encryption algorithm is based on prime numbers and uses variable key lengths ranging from 512 to greater than 1024 bits.

In some applications, a critical document may be divided into pieces and allocated to different locations over the Internet for security access concern, to access the document, the divided pieces must then be reconstructed from these locations (Lee *et al.*, 2000).

## Digital Signatures

One problem with public key encryption is that anyone could have sent the message. Digital signatures are a reversal of the public key encryption /decryption scheme. Instead of encryption taking place using the receiver's public key, the message is encrypted (signed) using the sender's private key. This receiver of the message

decodes the signature using the sender's public key thereby verifying the message sender's identity.

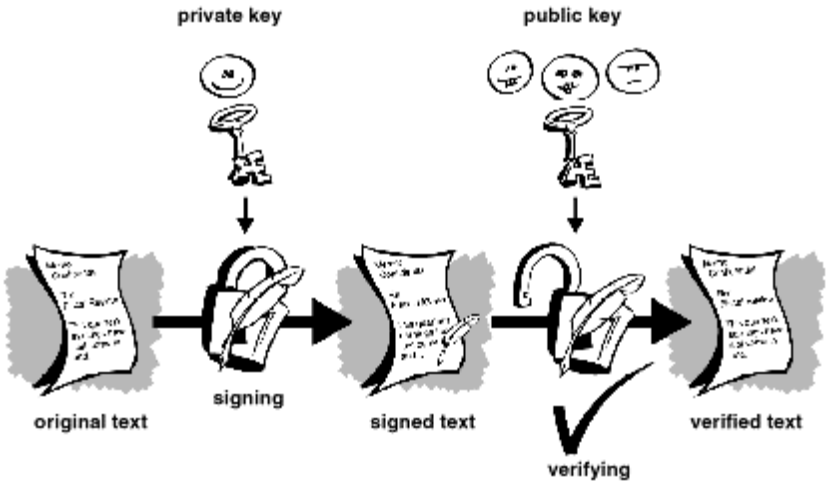



***Figure 8 : Digital Signature*** (PGP, 2001)

Rather than creating a digital signature by encrypting the entire message using the sender's private key, a hash of the message can be encrypted instead. This creates a small fixed size signature, regardless of the length of the message. However, a digital signature does not prove that the authenticated sender actually sent the message, only that the computer did! If the computer were inappropriately infected, malicious code could use the key to sign documents without the user's knowledge or permission. The legal acceptance of digital signatures shifts the burden of proof to the negative, that the signature in dispute was not signed rather than was signed (Ellison & Schneier, 2000)

**Digital Envelopes and Session Keys**

One of the main disadvantages of public key encryption is speed since public key encryption is noticeably slower than private key encryption (Garfinkel, 1996 ; RSA, 2000). Since encryption using public key cryptography is much slower to carry out than symmetric key cryptography, the use of public key cryptography would reduce business exchanges to a crawling pace. Consequently, a symmetric key is used to encrypt bulk documents and then public key cryptography is used to deliver the key to the recipient. Under this regime, session symmetric keys are randomly generated for

each exchange (Adams & Bond, 2000). This combination of private and public is carried out as follows:

1. A secret (session) key is generated at random
2. The message is encrypted using the session key and the symmetric algorithm
3. The session key is then encrypted with the receiver's public key – this is known as the Digital Envelope
4. Both the encrypted message and the digital envelope are sent to the receiver
5. The receiver uses their private key to decrypt the digital envelope recovering the session key which is used to decrypt the message (Stein, 1998).

### Notarisation and Time Stamping

Digital Certificates can be used to irrefutably sign a document. If an electronic notary receives the signatures of two or more parties, he can formally record an agreement between the parties. Using a reliable and verifiable independent clock to time stamp the receipt of the digital signatures, the exact time of a commercial event can be recorded (Cross, 1999).

## *Key Management*

While secure communication over the Internet has become an essential requirement for any value-added Internet application, the use of cryptography for secure communication brings out the need for cryptographic key management (Zhou, 2000). The main challenge for symmetric cryptography is getting the sender and receiver to agree on the secret key without anyone else finding out and then storing the key safely. The generation, distribution and storage of keys is known as key management (RSA, 2000). In addition, encrypted messages must remain secret for the useful life of the information. There is usually a need to update keys, if, for example, a key can be broken in two years and the lifetime of the information is 6 months then the key should be changed every 18 months.

### Key Storage

Proper short and long-term storage of cryptographic keys is essential for good security. When a key is used on a computer, it must be stored in memory, which makes it available to other software on the same system, an online key is only as

secure as access to the machine and the password protection mechanisms. Cryptographic keys are usually stored in disk files as they may be randomly generated and are too long to be used manually. At present private keys are generally stored on the owner's PC and protected by a password. If the PC is hacked or stolen, the private key could be fraudulently used, hence the keys themselves are usually stored in an encrypted format.

**Smart Cards**

A smart card contains a microprocessor and storage unit. Features such as card size, contact layout and electrical characteristics have been standardised (ISO 7816). Smart cards have physical tamper-resistant properties, plus secure storage and processing capabilities. The mechanism employed to ensure that the card is being used by its authorised user is achieved by off-line entry of a PIN ('something you know') known only to the card and its rightful holder ('something you have') (Trask & Meyerstein, 1999). This 'two-factor' authentication is currently being extended to incorporate biometric properties 'something you are'. An example of this is currently being piloted by the Bank of America using fingerprint recognition to give individuals access to their on-line services (Internet News, 1999). Biometrics are unique identifiers but they are not secrets. Anyone can steal a copy of your fingerprint or your iris patterns. If someone steals an element of your biometrics, it remains stolen for life, there's no getting back to a secure situation (Schneier, 1999).

The use of a smart card for private key storage both allows more security and enables the key to be used on any PC. The owner can store a number of digital certificates containing different private keys on the same smart card (Cross, 1999). For greater security, the smart card can by synchronised with the host computer to generate a new password at pre-specified intervals after which time the password is unusable (Greenstein & Feinman, 2000).

**Secret Sharing**

Truly valuable keys may be used only on isolated computer systems and stored safely when not in use, for example in a bank vault. If the safety of a single copy could be compromised, the key may be split, thereby allowing the trust of a secret to be

distributed among a designated set of people whose cumulative information suffices to determine the secret.

**Key Recovery**

This term refers to the useful technology that allows a key to be revealed if a user accidentally loses or deletes the key, or if a law enforcement agency wants to eavesdrop on a suspected criminal without the suspect's knowledge.

**Key Destruction**

Keys should be destroyed after use, as they remain valuable after they have been replaced. If the attacker retains the ciphertext and the key becomes available, then it can be easily decrypted.

## *Public Key Infrastructure (PKI)*

A well-designed and implemented PKI is essential to establish maintain trust in digital certificates. Many studies have shown that the full potential of electronic commerce will not be realised until public key infrastructures emerge which generate sufficient trust for businesses and individuals to commit their information and transactions to the emerging public networks (OECD, 1997).

**Trusted Third Parties**

In order for public key systems to work in the public domain, not only must the public key be freely accessible, but also senders and receivers must have a reliable way of determining that public keys are truly the keys of those parties with whom they wish to interact (OECD, 1997).

In a world where more and more transactions are taking place on open electronic networks, there has been a growing demand for strong encryption services to help protect the integrity and confidentiality of information while safeguarding law enforcement which encryption can prevent (Taylor, 1997). A critical issue presented by cryptography is the possible conflict between privacy and law enforcement, since cryptography can also be put to improper use such as hiding the illegal activities of criminals and terrorists. Many governments consider it essential that the ability of security, intelligence and law enforcement agencies to conduct effective legal

interception of communications under the Interception of Communications Act 1985 is preserved (DTI Proposals, 1997; usdoj, 2001). The need to maintain a balance between commercial requirements, together with the need to protect users and the need to safeguard law enforcement and national security requirements has been met by the introduction of licensed Trusted Third Parties (TTPs) for the provision of encryption services.

Legal access can be achieved by making use of a key escrow/recovery system which allows authorised persons, under certain conditions to decrypt messages with the help of cryptographic key information, held in escrow, and supplied by one or more trusted parties (DTI Proposals, 1997).

**Certification Authorities**

A digital certificate is an electronic credit card that establishes the credentials for doing business or other transactions on the Web. A Certification Authority (CA) issues the certificate which contains the user's name, a serial number, expiration dates, a copy of the certificate holder's public key and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real (DeVeau, 1999).

A CA acts like the passport office, which checks the credentials of individuals and entities and issues them with electronic certificates that are trusted throughout the community. Trust models are emerging, within diverse online business partnerships, through the mutual recognition of their respective CAs (Wilson, 1997).

The two of the main components of PKI are:

1. Certification Authority (CA) run by a Trusted Third Party (TTP) which issues and revokes certificates according to a published Certification Practice Statement and,
2. A Registration Authority which authenticates the identities of individuals and authorities who apply for digital certificates (Cross, 1999)

### *Secure Sockets Layer (SSL)*

SSL is a non-proprietary protocol, developed by Netscape, used to secure communication on the Internet. SSL uses public-key technology and digital certificates to authenticate the server in a transaction and protects private information as it passes from one party to another. SSL transactions do not require client authentication (Deitel *et al.*, 2001).

The steps in the process are shown in Figure 9.

1. Client opens a connection to the Server port and sends a 'Client Hello' Message, letting the server know the version of SSL used, the cipher suites and data compression it supports
2. Server responds with the chosen cipher suite and data compression methods, along with a session identifier. If there is no match between the cipher suites supported by the client and server, the server sends a 'handshake failure' message and hangs up.
3. Server sends its signed CA certificate, if the CA is not a root certifing authority, the server sends the chain of signed certs that lead to the primary CA.
4. The client generates a session key which the browser encrypts using the Servers Public key to create a digital envelope which is forwarded to the server, this session key is decrypted using the servers private key
5. Both client and server confirm that they are ready to start communicating using the agreed cipher and session key
6. Client and Server send *Finished* messages which confirm that their messages were received intact and not tampered with en-route.

At this point, both client and server switch to encrypted mode, using the session key to symmetricaly encrypt subsequent transmissions in both directions (Stein, 1998)

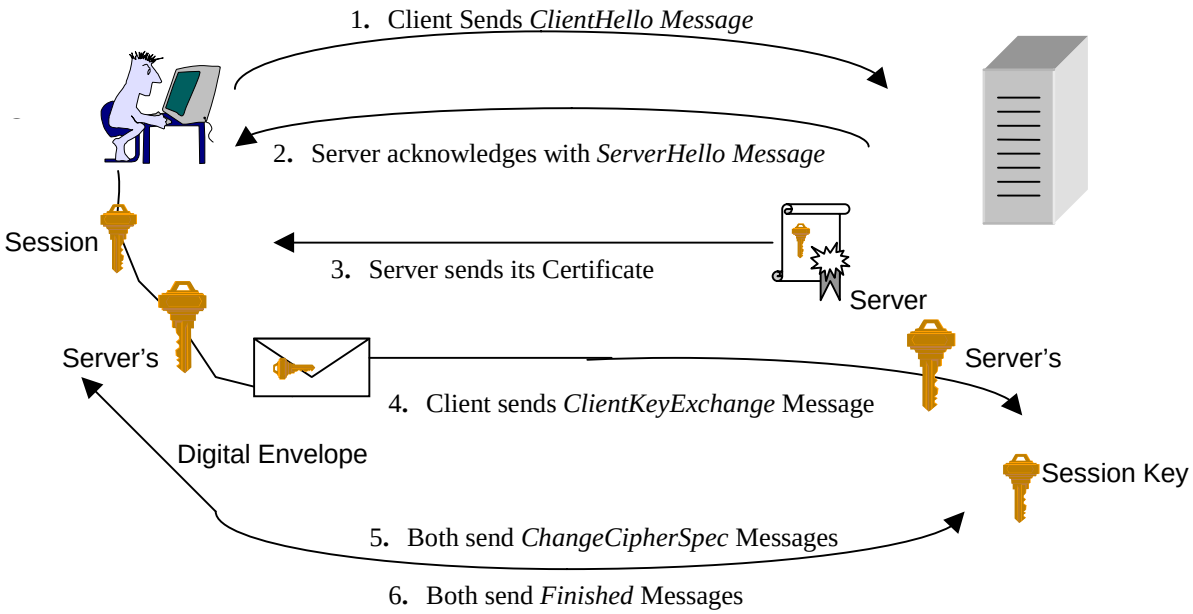



***Figure 9 : SSL Handshake*** (Stein, 1998)

If Client authentication is required, in addition to the steps outlined above, the server can request a Client Certificate. If the client has no certificate, the server may choose to abort the transmission with a 'handshake failure' message or continue on. If client authentidation is in place, the client sends a digital signature to prove its identity.

While SSL is the dominant protocol for encrypting general communications between client and server, *it does not encrypt data at the server site* (Larsen, 1999). This means that if private information, for example, credit card numbers, are stored on the merchant's server they are vulnerable to both outside and insider attack (Deitel *et al.*, 2001).

### *Secure Electronic Transactions (SET)*

SET is a specialised protocol, developed by Visa, Mastercard, Netscape and Microsoft, for safeguarding credit-card-based transactions between customers and merchants (Stein, 1998) and uses cryptography to:

1. Provide confidentiality of information through encryption
2. Ensure payment integrity through digital signatures and message digests
3. Authenticate both merchants and cardholders through the use of digital signatures and certificates
4. Interoperate with other protocols (Greenstein & Feinman, 2000).

The SET protocol involves the cardholder, the merchant, the card-issuing bank and the merchant's bank using public/private key pairs and signed certificates to establish each player's identity. Figure 10 shows how SET works.

1. **The Customer initiates a purchase**

   Customer browses Web Site, fills out order form and Presses Pay Button, Server sends customers computer a message initiating SET software
2. **The Client's Software sends the order and payment information**

   Clients SET software creates two messages, one containing order information, which is encrypted using a random session key and packaged into a digital envelope using the Merchant's public key. The other message contains payment information encrypted using the Merchant Banks public key. The software computes a hash of the order and payment information and signs it with the customer's private key.
3. **The Merchant passes payment information to the bank**

   SET software on the Merchants server generates an authorisation request, forwarding the customers encrypted information to the Bank, signing the message with its private key to prove its identity to the Bank. This request is encrypted with a new random session key and incorporated into a digital envelope using the Banks public key
4. **The Banks checks the validity of the card**

   The Bank decrypts and verifies the Merchant's message, then decrypts and verifies the customer's identity. It then generates an encrypted and digitally signed authorisation request to the Customer's bank
5. **The Customers Bank authorises payment**

The customer's bank confirms the merchant's bank identity, decrypts the information, checks the customer account and approves/rejects the request by digitally signing and encrypting it and returning it to the merchant's bank

6. **The Merchants Bank authorises the transaction**

   The Bank authorises, signs and returns the transaction to the Merchant

7. **The Merchant's Web Server completes the transaction**

   Merchant acknowledges the confirmation to the customer, via a confirmation page, and proceeds to transact the order

8. **The Merchant confirms the transaction to the Bank**

   The Merchant confirms the purchase to its bank, causing the customer's credit card to be debited and the merchant's account to be credited.

9. **The Customer's Bank sends credit card bill to customer**

   The charge appears on the customer's monthly statement

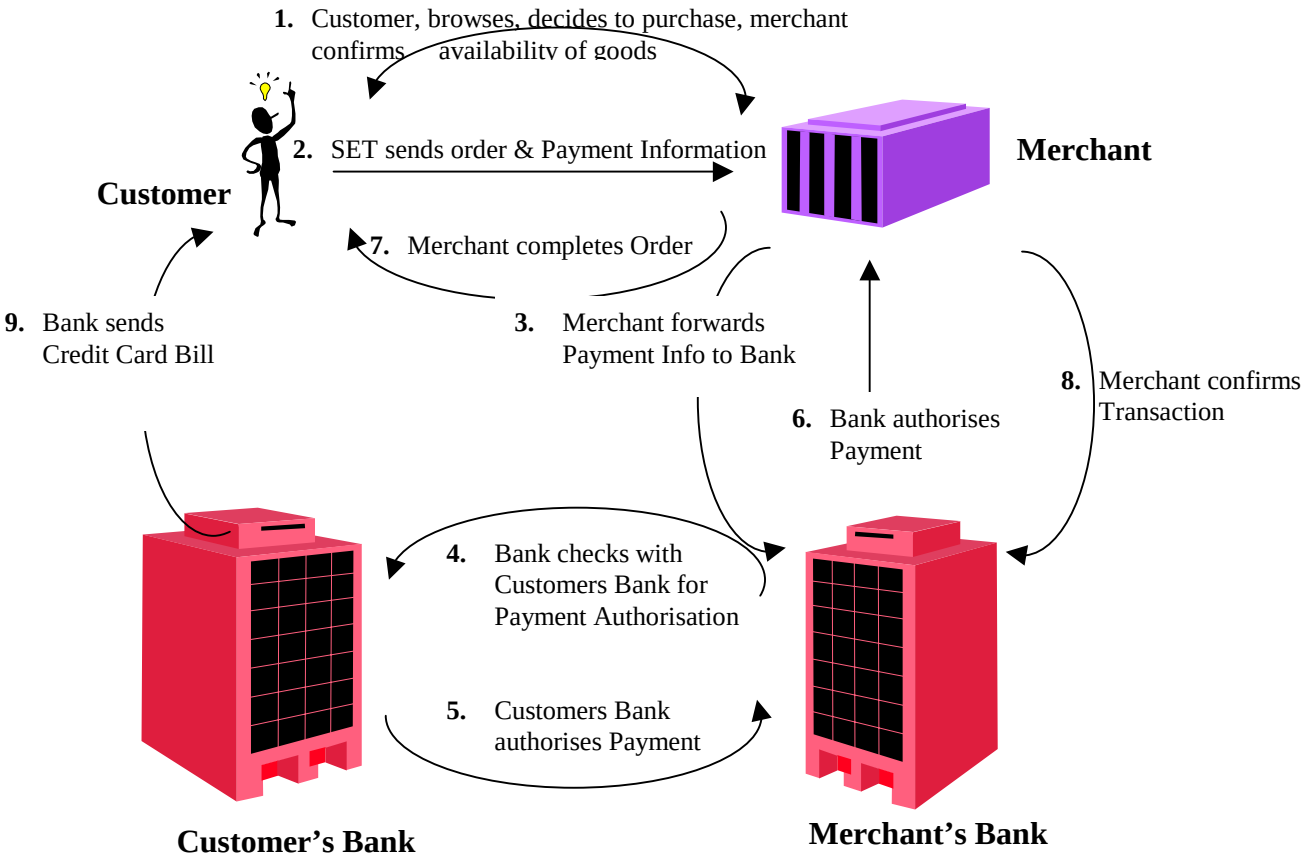



***Figure 10 : SET Protocol*** (Stein, 1998)

In the SET protocol, the merchant never sees the client's proprietary information, considerably reducing the risk of fraud (Deitel *et al.*, 2001). SET focuses on confidentiality and authentication and ensures that not only can thieves not steal a credit card number but prevents merchants from seeing the number while still providing assurances that the card is valid (Hawkins *et al.*, 2000).

While SET provides a high level of security, business have been slow to embrace this technology because of the increased transaction time and the specialised software requirement on both the client and server sides which increases transaction costs (Deitel *et al.*, 2001).

## Summary and Conclusions

### *Summary of techniques*

The applications of cryptography that meet the facilities required from an Internet based infrastructure are summarised in Table 1.

| Facilities Required | Method | Unique Features | Limitations |
|---|---|---|---|
| **Confidentiality** | • Encryption | • Scrambles the data before transmission | • Speed of transmission |
| **Integrity** | • Encryption /Decryption | • Electronic Key required to open encrypted data | • User may loose key<br>• Key may fall into wrong hands |
| **Authentication** | • Digital Certificate confirmed by a CA | • Verifies the authenticity of sender<br>• Alerts recipient if message has been altered | • Only useful if companies use a trusted third party Certificate Authority<br>• Only verifies that the message was sent from the users computer or private key |
| **Non-Repudiation** | • Digital Certificate<br>• Time Stamp from a CA | • Neither sender nor receiver can deny communication | |
| **Copy Protection** | • Encryption<br>• Digital Time Stamp | • Prevents the data from being reproduced<br>• Proves authorship | |

***Table 1 : Internet Security Components Addressed by Cryptography***

Security, message integrity and authentication can be achieved by using SSL, which ensures secure communication between client and server by using public key technology to encrypt the data and authenticate the server. Although more complex and expensive to implement, SET enhances SSL by providing mechanisms to ensure Client Authentication and the security of financial transactions through the separation of merchant and payment information.

### *Conclusion*

This paper has considered the history and techniques of cryptography used for securing communications over the Internet. The use of public and private key encryption infrastructures, digital signatures and time stamping, to ensure authentication and non-repudiation have been described. The significance of key management systems and the importance of establishing a Public Key Infrastructure using Trusted Third Parties and Certification Authorities to establish and maintain trust in digital certificates have been discussed. Methods of ensuring secure electronic communication using SSL and safeguarding financial transactions using SET have been described.

*In order for companies to be confident that their electronic transactions can be carried out securely, Internet security will always be a never-ending challenge. As improvements in protocols, authentication, integrity, access control and confidentiality occur hacking techniques will also improve. The future of Internet Security will remain in human hands to continually monitor network infrastructures and to assess and implement hardware and software solutions.*

## Bibliography

Adams D. & Bond R. (2000) Secure E-Commerce – A Competitive Weapon, Electronic Commerce Report, UNICOM Seminars Ltd.

Beckett B. (1988) Introduction to Cryptography, Blackwell Scientific Publications, UK.

Budge P. (1998) How Safe is the Net ?. Business Week, June 22.

Cross B. (1999) BT Trustwise – Enabling eCommerce Through Trust. BT Technol J. Vol 17(3), 44-49.

CSI Press Release – March 5th 1999, Cyber Attacks Rise From Outside and Inside Corporations –

Dramatic Increase in Reports to Law Enforcementhttp://gocsi.com/prelea990301.htm accessed 15th March 2001

Deitel H., Deitel P. & Nieto T. (2001) e-Business & e-Commerce : How to Program. Prentice Hall NJ.

DeVeau P. (1999) VPN = Very Private News. America's Network, Vol. 103(21) May 21, p16.

Diffie W. & Hellman M. (1976) New Directions in Cryptography. IEEE Transaction on Information Theory, Nov. 644-654

DTI, (1997) Department of Trade and Industry Proposals for the Licensing of Trusted Third Parties for the Provision of Encryption Services, Public Consultation Paper on Detailed Proposals for Legislation.http://www.dti.gov.uk/pubs accessed March 15th 2001

Dysart J. (2000) Internet Security : Safeguard Your Network, Electrical World Vol. 214(3) 41-42.

Ellison C. & Schneier B. (2000) Risks of PKI, 116. Communications of the ACM, (42),12. Also available from the Collection of Inside Risks Columns on Peter Neumans Site at http://www.csl.sri.com/users/neumann/insiderisks.html. Accessed 14/03/01

Ernst & Young. (1998) Internet Shopping : An Ernst & Young Special Report, Section 2, January

Everett J. (1998) Internet Security. Employee Benefits Journal, Vol 23(3), 14-18.

FIPS 46-2, (1993) Data Encryption Standard. http://www.itl.nist.gov/fibpubs/fip46-2.htm Accessed 05/02/01

Foresight (1998) E-Commerce Sets New Rules. Systems Relationships Marketing, on behalf of Datatec Ltd. Vol. 1 No. 3, November

Furnell S. & Warren M. (1999) Computer Hacking and Cypher Terrorism : The Real Threats in the New Millennium. Computers & Security 18 (1) 28-34

Garfinkel S. & Spafford G. (1996) Practical UNIX and Internet Security, O'Reilly and Associates, NY.

Gold S. (2000), Costs of Online Breaches Soaring Says CSI/FBI Report, Newsbytes 22 March http://www.newsbytes.com/pubNews/00146090.html accessed March 15th 2001

Greenstein M. & Feinman T., (2000) Electronic Commerce : Security, Risk Management and Control, Irwin, McGrawHill, Boston.

Hawkins S., Yen D. & Chou D. (2000) Awareness And Challenges Of Internet Security. Information Management and Computer Security, 8(3), 131-143.

Held G. (1993) Top Secret Data Encrypting Techniques, SAMS Publishing, USA.

InformationWeek (1998), Global Information Security Survey Reflects IT Professionals Views Worldwide, Press Release, September 9.

Internet News (1999) Bank of America Offers Fingerprint Access to Online Banking http://www.internetnews.com/ec-news/article/0,,4_33221,00.html Accessed 18/04/01

ISO 7816 Identification Cards – Integrated Circuit(s) Cards With Contacts http://iso.ch/cate/d29257.html

Labuschagne L. & Eloff J. (2000) Electronic Commerce : The Information Security Challenge. Information Management and Computer Security, 8(3), 154-157

Larsen A. (1999) Global Security Survey : Virus Attack. Information Week, July, 42-46

Lee C., Yeh Y., Chen D. & Ku K. (2000) A Share Assignment Method to Maximise the Probability of Secret Sharing Reconstruction under the Internet. IEICE Transactions on Information Systems E83D (2) 190-199.

McGuire B. & Roser S. (2000) What Your Business Should Know About Internet Security. Strategic Finance, Vol. 82(5), 50-5

Morse S. (1840) US Patent for Morse Code, United States Patent and Trademark Office (USPTO), http://www.patentmuseum.com/listing.html Accessed 15/03/01

Neumann P. (2000) Risks of Insiders, 114. Communications of the ACM, (43),2. Also available from the Collection of Inside Risks Columns on Peter Neumans Site at http://www.csl.sri.com/users/neumann/insiderisks.html. Accessed 14/03/01

OECD (1997) Cryptography Policy : The Guidelines and the Issues
Available at http://www.oecd.org/dsti/sti/it/secur/prod/e-crypto.html
Accessed 02/04/01

OECD (1999) Joint OECD-Private Sector Workshop on Electronic Authentication. Available at http://www.oecd.org//dsti/sti/it/secur/act/wksp-auth.htm
Accessed 02/04/01

PGP (2001) How PGP Works http://www.pgpi.org/doc/pgintro/

Price K. (1999) Intrusion Detection Pages. http://www.cerial.purdue.edu/coast/intrusion-detection/welcome.html Accessed 18/04/01.

RSA (2000) Frequently Asked Questions About Today's Cryptography. RSA Laboratories

Salnoske K. (1998) Testimony before the Subcommittee on Telecommunications Trade and Consumer Protection Committee on Commerce. May 21 in Greenstein & Feinman (2000)

Schneider F. (1998) Towards Trustworthy Networked Information Systems, Inside Risks. 101. Communications of the ACM, (41),11. Also available from the Collection of Inside Risks Columns on Peter Neumans Site at http://www.csl.sri.com/users/neumann/insiderisks.html. Accessed 14/03/01

Schneier B. (1999) Biometrics : Uses and Abuses, Inside Risks. 110. Communications of the ACM, (42),8. Also available from the Collection of Inside Risks Columns on Peter Neumans Site at http://www.csl.sri.com/users/neumann/insiderisks.html. Accessed 14/03/01

Schneier B. (1999) Risks of Relying on Cryptography, Inside Risks. 112. Communications of the ACM, (42),10. Also available from the Collection of Inside Risks Columns on Peter Neumans Site at http://www.csl.sri.com/users/neumann/insiderisks.html. Accessed 14/03/01

Schneier B. (1999) The Trojan Horse Race, Inside Risks. 111. Communications of the ACM, (42),9. Also available from the Collection of Inside Risks Columns on Peter Neumans Site at http://www.csl.sri.com/users/neumann/insiderisks.html. Accessed 14/03/01

Stein L., (1998) Web Security : A Step-by-Step Reference Guide, Addison Wesley, MA.

Taylor I (1997) Forward to 'Licensing of Trusted Third Parties for the Provision of Encryption Services, Public Consultation Paper on Detailed Proposals for Legislation.'
http://www.fipr.org/polarch/ttp.html accessed March 15th 2001

The Computer Law & Security Report (1997) Binding Cryptography : A Fraud Detectable Alternative to

Key-Escrow Proposals. Available at http://cwis.kub.nl/~frw/people/koops/bind-art.htm Accessed 29/03/01

Trask N. & Meyerstein M. (1999) Smart Cards in Electronic Commerce. BT Technol J. Vol.17(3), 57-66

Treese G. & Stewart L. (1998) Designing Systems for Internet Commerce. Addison-Wesley, MA.

U.S. Department of Commerce (1998) The Digital Economy, April http://www.ecommerce.gov/danc1.html

usdoj (2001) United States Department of Justice. http://www.usdoj.gov/criminal/cybercrime/compcrime.html Accessed 10/04/01

Wilson S. (1997) Certificates and Trust in Electronic Commerce. Information Management and Computer Security, Vol.5(5) 175-181

Zhou J. (2000) Further analysis of the Internet Key Exchange Protocol. Computer Communications 23(17) 1606-1612