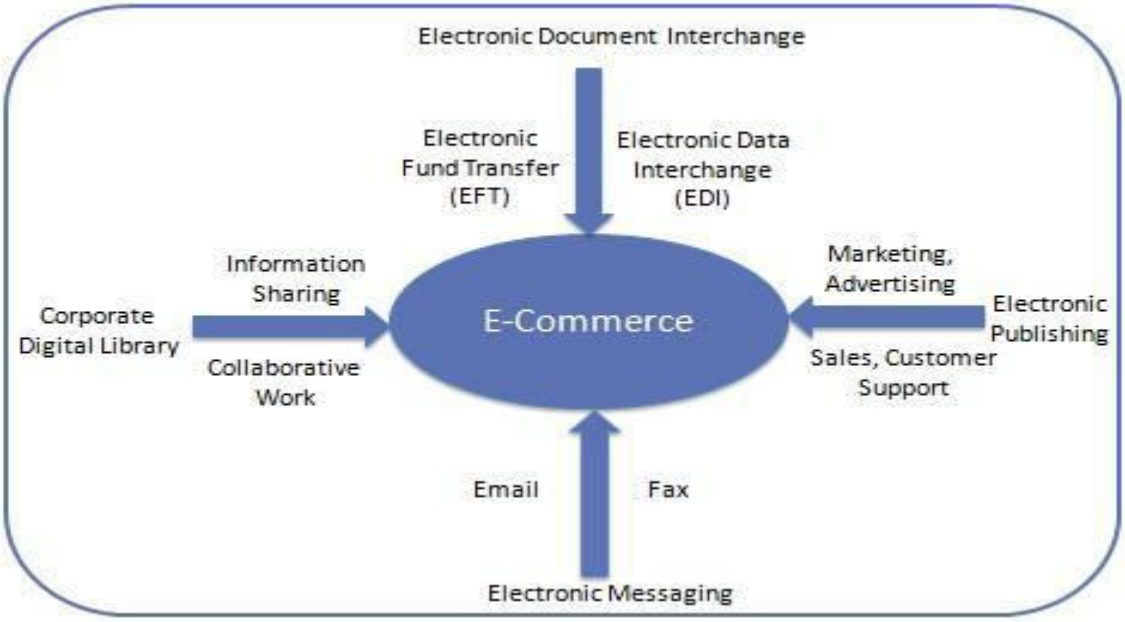
E-Commerce

E-Commerce or Electronics Commerce is a methodology of modern business which addresses the need of business organizations, vendors and customers to reduce cost and improve the quality of goods and services while increasing the speed of delivery. E-commerce refers to paperless exchange of business information using following ways.

- Electronic Data Exchange (EDI)
- Electronic Mail (e-mail)
- Electronic Bulletin Boards
- Electronic Fund Transfer (EFT)
- Other Network-based technologies



Features of E-Commerce

E-Commerce provides following features

1. **Non-Cash Payment:** E-Commerce enables use of credit cards, debit cards, smart cards, electronic fund transfer via bank's website and other modes of electronics payment.

2. **24x7 Service availability:** E-commerce automates business of enterprises and services provided by them to customers are available anytime, anywhere. Here 24x7 refers to 24 hours of each seven days of a week.

3. **Advertising / Marketing:** E-commerce increases the reach of advertising of products and services of businesses. It helps in better marketing management of products / services.

4. **Improved Sales:** Using E-Commerce, orders for the products can be generated

anytime, anywhere without any human intervention. By this way, dependencies to buy a product reduce at large and sales increases.

5. **Support:** E-Commerce provides various ways to provide pre sales and post sales assistance to provide better services to customers.

6. **Inventory Management:** Using E-Commerce, inventory management of products becomes automated. Reports get generated instantly when required. Product inventory management becomes very efficient and easy to maintain.

7. **Communication improvement:** E-Commerce provides ways for faster, efficient, reliable communication with customers and partners.

Traditional Commerce v/s E-Commerce

Sr. No.	Traditional Commerce	E-Commerce
1	Heavy dependency on information exchange from person to person.	Information sharing is made easy via electronic communication channels making little dependency on person to person information exchange.
2	Communication/ transaction are done in synchronous way. Manual intervention is required for each communication or transaction.	Communication or transaction can be done in asynchronous way. Electronics system automatically handles when to pass communication to required person or do the transactions.
3	It is difficult to establish and maintain standard practices in Traditional commerce.	A uniform strategy can be easily Established and maintain in ecommerce.
4	Communications of business depends upon individual skills.	In e-Commerce or Electronic Market, there is no human intervention.
5	Unavailability of a uniform platform as traditional commerce depends heavily on Personal communication.	E-Commerce website provides user a platform where al l information is available at one place.
6	No uniform platform for information sharing as it depends heavily on personal communication.	E-Commerce provides a universal platform to support commercial / business activities across the globe.

Advantages of E-Commerce

E-Commerce advantages can be broadly classified in three major categories:

1. Advantages to Organizations

2. Advantages to Consumers
3. Advantages to Society

1. Advantages to Organizations

- Using E-Commerce, organization can expand their market to national and international markets with minimum capital investment. An organization can easily locate more customers, best suppliers and suitable business partners across the globe.
- E-Commerce helps organization to reduce the cost to create process, distribute, retrieve and manage the paper based information by digitizing the information.
- E-commerce improves the brand image of the company.
- E-commerce helps organization to provide better customer services.
- E-Commerce helps to simplify the business processes and make them faster and efficient.
- E-Commerce reduces paper work a lot.
- E-Commerce increased the productivity of the organization. It supports "pull" type supply management. In "pull" type supply management, a business process starts when a request comes from a customer and it uses just-in-time manufacturing way.

Advantages to Customers

- 24x7 support. Customer can do transactions for the product or enquiry about any product/services provided by a company any time, any where from any location. Here 24x7 refers to 24 hours of each seven days of a week.
- E-Commerce application provides user more options and quicker delivery of products.

- E-Commerce application provides user more options to compare and select the cheaper and better option.

- A customer can put review comments about a product and can see what others are buying or see the review comments of other customers before making a final buy.

- E-Commerce provides option of virtual auctions.

- Readily available information. A customer can see the relevant detailed information within seconds rather than waiting for days or weeks.

- E-Commerce increases competition among the organizations and as result organizations provides substantial discounts to customers.

Advantages to Society

- Customers need not to travel to shop a product thus less traffic on road and

low air pollution.

- E-Commerce helps reducing cost of products so less affluent people can also afford the products.

- E-Commerce has enabled access to services and products to rural areas as well which are otherwise not available to them.

- E-Commerce helps government to deliver public services like health care, education, social services at reduced cost and in improved way.

Disadvantages of E -Commerce

E -Commerce disadvantages can be broadly classified in two major categories:

1. Technical disadvantages
2. Non-Technical disadvantages

1. Technical Disadvantages

- There can be lack of system security, reliability or standards owing to poor implementation of e-Commerce.

- Software development industry is still evolving and keeps changing rapidly.

- In many countries, network bandwidth might cause an issue as there is insufficient telecommunication bandwidth available.

- Special types of web server or other software might be required by the vendor setting the e-commerce environment apart from network servers.

- Sometimes, it becomes difficult to integrate E-Commerce software or website with the existing application or databases.

- There could be software/hardware compatibility issue as some E-Commerce software may be incompatible with some operating system or any other component.

2. Non-Technical Disadvantages

1. Initial cost: The cost of creating / building E-Commerce application in-house may be very high. There could be delay in launching the E-Commerce application due to mistakes, lack of experience.

2. User resistance: User may not trust the site being unknown faceless seller.

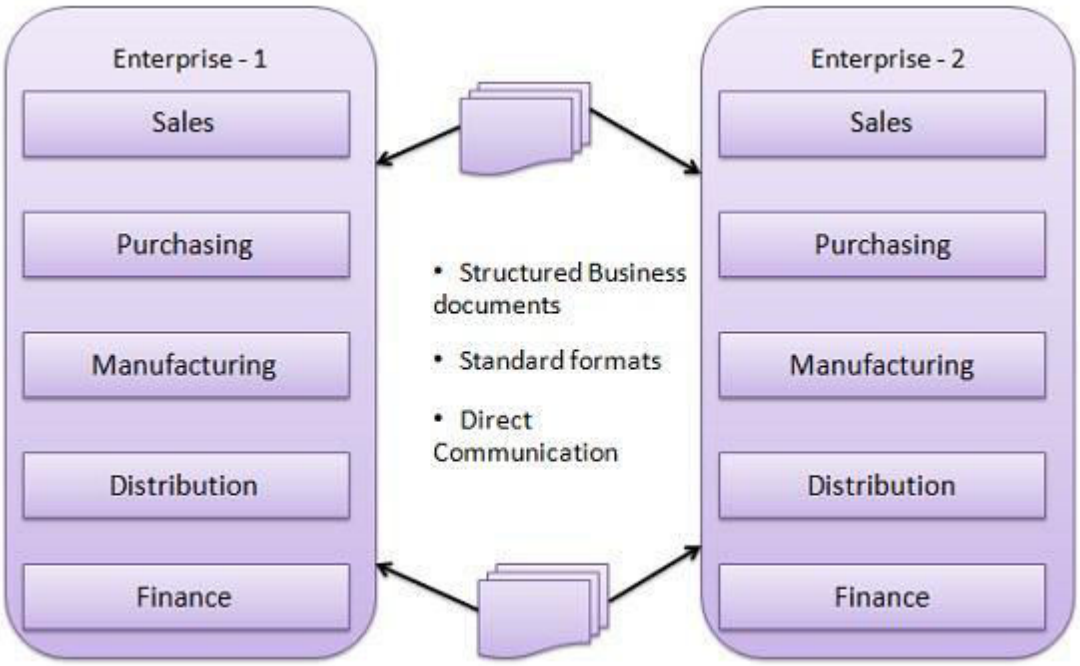
Such mistrust makes it difficult to make user switch from physical stores to online/virtual stores.

3. **Security / Privacy:** Difficult to ensure security or privacy on online transactions.

4. Lack of touch or feel of products during online shopping.
5. E-Commerce applications are still evolving and changing rapidly.
6. Internet access is still not cheaper and is inconvenient to use for many potential customers like one living in remote villages.

EDI

EDI stands for Electronic Data Exchange. EDI is an electronic way of transferring business documents in an organization internally between its various departments or externally with suppliers, customers or any subsidiaries etc. In EDI, paper documents are replaced with electronic documents like word documents, spreadsheets etc.



EDI Documents

Following are few important documents used in EDI:

- Invoices
- Purchase orders
- Shipping Requests
- Acknowledgement
- Business Correspondence letters

- Financial information letters

Steps in an EDI System

Following are the steps in an EDI System.

- A program generates the file which contains the processed document.
- The document is converted into an agreed standard format.
- The file containing the document is send electronically on network.
- The trading partner receives the file.
- An acknowledgement document is generated and sent to the originating organization.

Advantages of an EDI System

Following are the advantages of an EDI System.

- **Reduction in data entry errors.** - Chances of errors are much less being use of computer in data entry.
- **Shorter processing life cycle** - As orders can be processed as soon as they are entered into the system. This reduced the processing time of the transfer documents.
- **Electronic form of data** - It is quite easy to transfer or share data being in electronic format.
- **Reduction in paperwork** - As lot of paper documents are replaced with electronic documents there is huge reduction in paperwork.
- **Cost Effective** - As time is saved and orders are processed very effectively, EDI proves to be highly cost effective.
- **Standard Means of communication** - EDI enforces standards on the content of data and its format which leads to clearer communication.

Payment Systems

E-Commerce or Electronics Commerce sites use electronic payment where electronic payment refers to paperless monetary transactions. Electronic payment has revolutionized the business processing by reducing paper work, transaction costs, labour cost. Being user friendly and less time consuming than manual processing, helps business organization to expand its market reach / expansion. Some of the modes of electronic payments are following.

- Credit Card
- Debit Card
- Smart Card
- E-Money
- Electronic Fund Transfer (EFT)

Credit Card

Payment using credit card is one of most common mode of electronic payment. Credit card is small plastic card with a unique number attached with an account. It has also a

magnetic strip embedded in it which is used to read credit card via card readers. When a customer purchases a product via credit card, credit card issuer bank pays on behalf of the customer and customer has a certain time period after which he/she can pay the credit card bill. It is usually credit card monthly payment cycle.

Following are the actors in the credit card system.

- The card holder - Customer
- The merchant - seller of product who can accept credit card payments.
- The card issuer bank - card holder's bank
- The acquirer bank - the merchant's bank
- The card brand - for example, visa or MasterCard.

Credit card payment process

Step	Description
Step 1	Bank issues and activates a credit card to customer on his/her request.
Step 2	Customer presents credit card information to merchant site or to merchant from whom he/she want to purchase a product/service.
Step 3	Merchant validates customer's identity by asking for approval from card brand company.
Step 4	Card brand company authenticates the credit card and paid the transaction by credit. Merchant keeps the sales slip.
Step 5	Merchant submits the sales slip to acquirer banks and gets the service chargers paid to him/her.
Step 6	Acquirer bank requests the card brand company to clear the credit amount and gets the payment.
Step 7	Now card brand company asks to clear amount from the issuer bank and amount gets transferred to card brand company.

Debit Card

Debit card, like credit card is a small plastic card with a unique number mapped with the bank account number. It is required to have a bank account before getting a debit card from the bank. The major difference between debit card and credit card is that in case of payment through debit card, amount gets deducted from card's bank account immediately and there should be sufficient balance in bank account for the transaction to get completed whereas in case of credit card there is no such compulsion.
Debit cards free customer to carry cash, cheques and even merchants accepts debit card more readily. Having restriction on amount being in bank account also helps customer to keep a check on his/her spending.

Smart Card

Smart card is again similar to credit card and debit card in appearance but it has a small microprocessor chip embedded in it. It has the capacity to store customer work related/personal information. Smart card is also used to store money which is reduced as per usage.
Smart card can be accessed only using a PIN of customer. Smart cards are secure as they stores information in encrypted format and are less expensive / provide faster processing. Mondex and Visa Cash cards are examples of smart cards.

E-Money

E-Money transactions refer to situation where payment is done over the network and amount gets transferred from one financial body to another financial body without any involvement of a middleman. E-money transactions are faster, convenient and save a lot of time.
Online payments done via credit card, debit card or smart card are examples of emoney transactions. Another popular example is e-cash. In case of e-cash, both customer and merchant both have to sign up with the bank or company issuing e-cash.
Electronic Fund Transfer
It is a very popular electronic payment method to transfer money from one bank account to another bank account. Accounts can be in same bank or different bank. Fund transfer can be done using ATM (Automated Teller Machine) or using computer. Now a day, internet based EFT is getting popularity. In this case, customer uses website provided by the bank. Customer logins to the bank's website and registers another bank account. He/she then places a request to transfer certain amount to that account. Customer's bank transfers amount to other account if it is in same bank otherwise transfer request is forwarded to ACH (Automated Clearing House) to transfer amount to other account and amount is deducted from customer's account. Once amount is transferred to other account, customer is notified of the fund transfer by the bank.

Security Systems

Security is an essential part of any transaction that takes place over the internet. Customer will lose his/her faith in e-business if its security is compromised. Following are the essential requirements for safe e-payments/transactions:

1. **Confidential** - Information should not be accessible to unauthorized person. It should not be intercepted during transmission.
2. **Integrity** - Information should not be altered during its transmission over the network.
3. **Availability** - Information should be available wherever and whenever requirement within time limit specified.
4. **Authenticity** - There should be a mechanism to authenticate user before giving him/her access to required information.
5. **Non-Repudiabiity** - It is protection against denial of order or denial of

payment. Once a sender sends a message, the sender should not able to deny sending the message. Similarly the recipient of message should not be able to deny receipt.

6. **Encryption** - Information should be encrypted and decrypted only by authorized user.
7. **Auditability** - Data should be recorded in such a way that it can be audited for integrity requirements.

Measures to ensure Security

Major security measures are following:

1. **Encryption** - It is a very effective and practical way to safeguard the data being transmitted over the network. Sender of the information encrypts the data using a secret code and specified receiver only can decrypt the data using the same or different secret code.
2. **Digital Signature** -Digital signature ensures the authenticity of the information. A digital signature is a e-signature authentic authenticated through encryption and password.
3. **Security Certificates** - Security certificate is unique digital id used to verify identity of an individual website or user.

Security Protocols in Internet

Following are the popular protocols used over the internet which ensures security of transactions made over the internet.

Secure Socket Layer (SSL)

It is the most commonly used protocol and is widely used across the industry. It meets following security requirements:

- Authentication
- Encryption
- Integrity
- Non-reputability

Secure Hypertext Transfer Protocol (SHTTP)

SHTTP extends the HTTP internet protocol with public key encryption, authentication and digital signature over the internet. Secure HTTP supports multiple security mechanism providing security to end users. SHTTP works by negotiating encryption scheme types used between client and server.

Secure Electronic Transaction

It is a secure protocol developed by MasterCard and Visa in collaboration. Thereoritically, it is the best security protocol. It has following components:

1. **Card Holder's Digital Wallet Software** - Digital Wallet allows card holder to make secure purchases online via point and click interface.
2. **Merchant Software** - This software helps merchants to communicate with potential customers and financial institutions in secure manner.
3. **Payment Gateway Server Software** - Payment gateway provides automatic and standard payment process. It supports the process for merchant's certificate request.
4. **Certificate Authority Software** -This software is used by financial institutions to issue digital certificates to card holders and merchants and to enable them to register their account agreements for secure electronic commerce.

Digital Signature

- is a type of **asymmetric cryptography** used to simulate the security properties of a **signature** in digital, rather than written, form. Digital signature schemes normally give two algorithms, one for signing which involves the user's secret or **private key**, and one for verifying signatures which involves the user's **public key**. The output of the signature process is called the "digital signature."
- is an **electronic signature** that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

How it works

- The use of digital signatures usually involves two processes, one performed by the signer and the other by the receiver of the digital signature:
- **Digital signature creation** uses a hash result derived from and unique to both the signed message and a given private key. For the hash result to be secure, there must be only a negligible possibility that the same digital signature could be created by the combination of any other message or private key.
- **Digital signature verification** is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key.

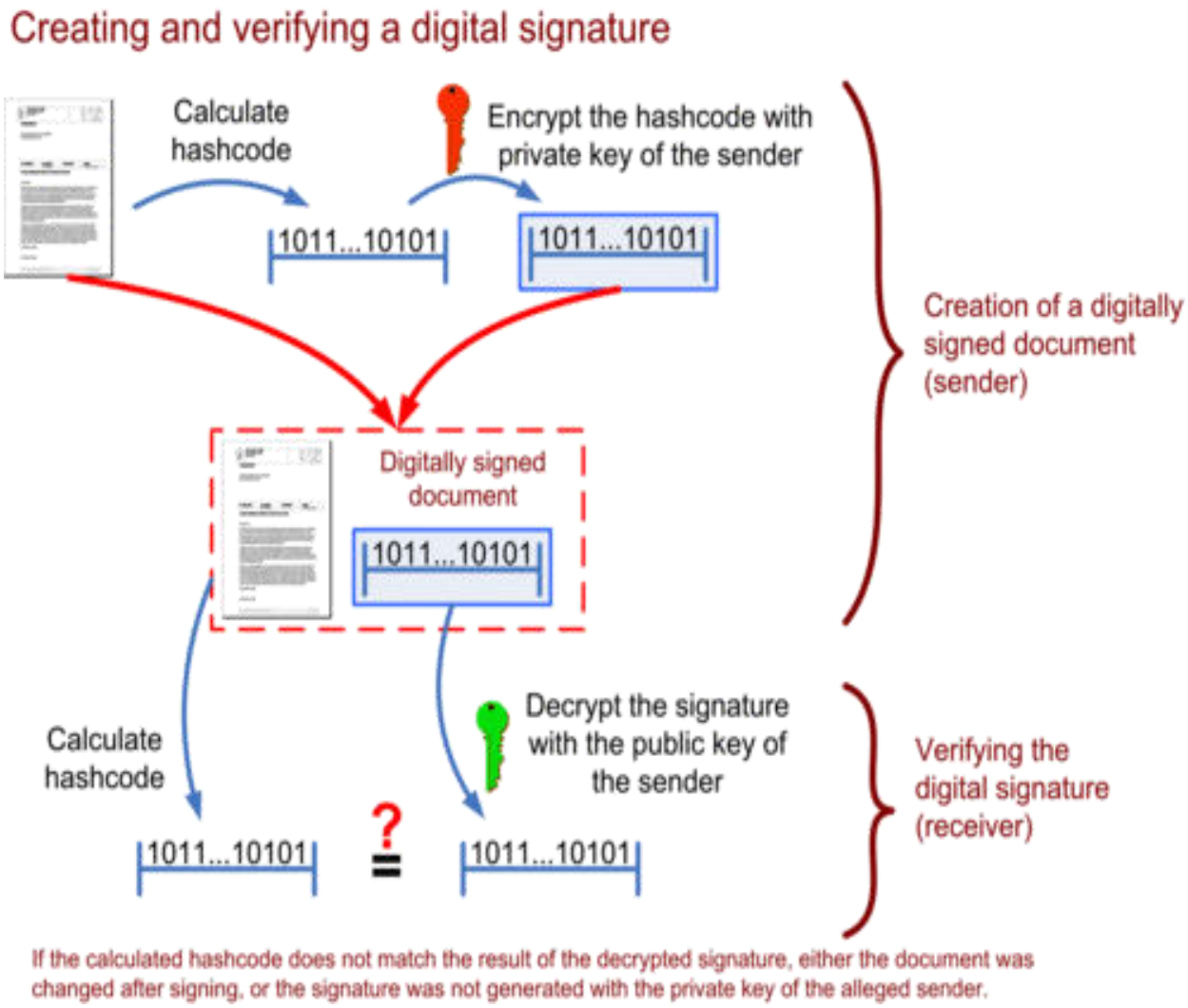
Example

- Assume you were going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you.

1. You copy-and-paste the contract (it's a short one!) into an e-mail note.
2. Using special software, you obtain a message hash (mathematical summary) of the contract.
3. You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash.
4. The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.)

- At the other end, your lawyer receives the message.

1. To make sure it's intact and from you, your lawyer makes a hash of the received message.
2. Your lawyer then uses your public key to decrypt the message hash or summary.
3. If the hashes match, the received message is valid.



Benefits of digital signatures

These are common reasons for applying a digital signature to communications:

1. **Authentication**

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

2. **Integrity**

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to *change* an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message will invalidate the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions.

Drawbacks of digital signatures

Despite their usefulness, digital signatures do not alone solve all the problems we might wish them to.

1. **Non-repudiation**

In a cryptographic context, the word *repudiation* refers to the act of disclaiming responsibility for a message. A message's recipient may insist the sender attach a signature in order to make later repudiation more difficult, since the recipient can show the signed message to a third party (eg, a court) to reinforce a claim as to its signatories and integrity. However, loss of control over a user's private key will mean that all digital signatures using that key, and so ostensibly 'from' that user, are suspect. Nonetheless, a user cannot repudiate a signed message without repudiating their signature key.

Main Questions

1. **In the digital signature who use the private key and who use the public key?**
   Private key: sender
   Public key: receiver
2. **What are the benefits of digital signatures?**
   Authentication and Integrity