UNIT IV

MasterCard/Visa Secure Electronic Transaction: Introduction – Business Requirements – Concepts – Payment processing – E-mail and secure e-mail technologies for electronic commerce. Introduction – The Mean of Distribution – A model for message handling – Working of Email - MIME: Multipurpose Internet Mail Extensions – S/MIME: Secure Multipurpose Internet Mail Extensions – MOSS: Message Object Security Services.

2 MARKS

1. Write the Role of payment Systems.

Payment systems and their financial institutions will pays a significant role by establishing open specification for payment card transactions that:

- Provide for confidential transmission.
- Authenticate the parties involved.
- Ensure the integrity of payment instruction for goods and services order data. And

Authenticate the identity of the card holder and the merchant to each other.

2. Secure Electronic Transaction (SET)

Secure Electronic Transaction (SET) is a system for ensuring the security of financial transactions on the Internet. It was supported initially by Master card, Visa, Microsoft, Netscape, and others.

3. Features of SET

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication

4. Payment processor

A **payment processor** is a company (often a third party) appointed by a merchant to handle credit card transactions for merchant banks. They are usually broken down into two types: front-end and back-end.

5. List the objective of Payment Security. (Nov 2012)

The objectives of payment security are to:

- Provide authentication of cardholders, merchants and acquirers.
- Provide confidentiality of payment data.
- Preserve the integrity of payment data and

Define the algorithms and protocols necessary for these security services.

6. List the objective of Market Acceptance:

The objectives of market acceptance are to:

- Achieve global acceptance, via ease of implementation and minimal impact on merchant and cardholder end users,

- Allow for ―bolt-on‖ implementation of the payment protocol to existing client applications.
- Minimize change to the relationship between acquirers and merchant and cardholders and issuers,
- Allow for minimum impact to existing merchant, acquirer and payment system applications and infrastructure and
- Provide an efficient protocol viewed from the financial institution perspective.

7. Write the Feature of the specification.

These requirements are addressed by the following features of these specifications

- Confidentiality of information,
- Integrity of data,
- Cardholder account authentication
- Merchant authentication.
- Interoperability.

8. Write the Motivation for secure payment.

The primary motivation for the backend associations to provide specifications for secure payment is:

- To have the backend community take a leadership position in establishing secure payment specifications and in the process, avoid any cost associated with future reconciliation of implemented approaches,
- To respect and preserve the relationship between merchants and acquirers and between cardholders and issuers,
- To facilitate rapid development of the market place.
- To respond quickly to the needs of the financial services market and
- To protect the integrity of bankcard brands.
-

9. List the objectives of Interoperability.

The objectives of interoperability are to:

- Clearly define detailed information to ensure that applications developed by ont vendor will interoperate with applications developed by other vendors.
- Create and support an open payment card standard.
- Define exportable technology throughout, in order to encourage globally interoperable software,
- Build on existing standards where practical,
- Ensure compatibility with and acceptance by appropriate standards bodies, and

Allow for implementation on any combination of hardware and software platforms such as Power PC, Intel, Sparc, Unix, MS-DOS,OS/2,Windows and Macintosh

10. Describe privacy enhanced mail.

PEM describes formats and techniques for encryption and authenticating message senders. PEM allows users to send e-mail and have automatically encrypted.PEM supports confidentiality, originator authentication, message integrity, and no repudiation of origin.

11. What are all the types of PEM message?

There are three types of PEM message

- MIC(Message Integrity Code)-CLEAR, message integrity checked in clear text has a digital signature affixed to its unencrypted content
- MIC-ONLY. Message integrity checked is encoded to protect the message's content.
- ENCRYPTED messages are also integrity checked and contain cipher text.

12. Define MIME. (Apr 2012)

MIME is a standard that defines the format of textual messages exchanged on the internet. Its purpose is to standardize the format of message bodies in the way that enables them to carry many types of recognizable non-ASCII data.

13. Define Front-end processors.

Front-end processors have connections to various card associations and supply authorization and settlement services to the merchant banks' merchants.

14. Define Back-end processors.

Back-end processors accept settlements from front-end processors and, via The Federal Reserve Bank, move the money from the issuing bank to the merchant bank.

15. What is Electronic mail? (Nov 2014)(Apr 2015)

Electronic mail, commonly known as **email** or **e-mail**, is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks.

16. List Components of an E-mail?

An email message consists of three components, the message envelope, the message heade*r*, and the message body. The message header contains control information, including, minimally, an originator's email address and one or more recipient addresses.

17. What is Secure Email service?

The Secure Email service is designed for faculty and staffs that need to use email to send Prohibited, Restricted, or Confidential Data—in particular, Protected Health Information (PHI) in accordance with the HIPAA guidelines, as defined by the Information Security Office.

18. Features of secure Email services.

- Uses reliable technology to encrypt email messages sent to off-campus addresses.
  Easy to use for busy medical employees who must comply with HIPAA guideline.

19. **Define Multipurpose Internet Mail Extensions (MIME).**

Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of email to support:

- Text in character sets other than ASCII
- Non-text attachments

- Message bodies with multiple parts
- Header information in non-ASCII character sets

20. Define MIME-Version.

The presence of this header indicates the message is MIME-formatted. The value is typically "1.0" so this header appears as MIME-Version: 1.0

21. What is Content-Type of MIME?

This header indicates the Internet media type of the message content, consisting of a *type* and subtype, for example:

Content-Type: text/plain

22. Define S/MIME (Secure/Multipurpose Internet Mail Extensions).

S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity, non-repudiation of origin (using digital signatures), privacy and data security (using encryption).

23. Define MIME Object Security Services (MOSS).

MIME Object Security Services (MOSS) is a protocol that uses the multipart/signed and multipart/encrypted framework to apply digital signature and encryption services to MIME objects.

24. What exactly is MIME?

MIME is an extension to the Internet mail standard, known as Simple Mail Transfer Protocol (SMTP) that allows mail messages containing different type of multimedia information to be sent across the network this includes, but is not limited to, word-processor documents, spreadsheets, programs, graphics, audio, and motion picture files, as well as links that enable users to retrieve information from remote databases from within a mail message.

25. How MIME works?

The developers of MIME found a clever way to work around the limitation. It packages different data types into a 7-bit ASCII format. That way, all e-mail, regardless of the data it contains, appears as standard e-mail messages to the internet's SMTP servers. The beauty of the solution lies in the fact that SMTP didn't have to change to handle such data.

26. What is New MIME headers?

Required fields

- MIME - Version
- Date - Time

Optional fields

1. Content- type

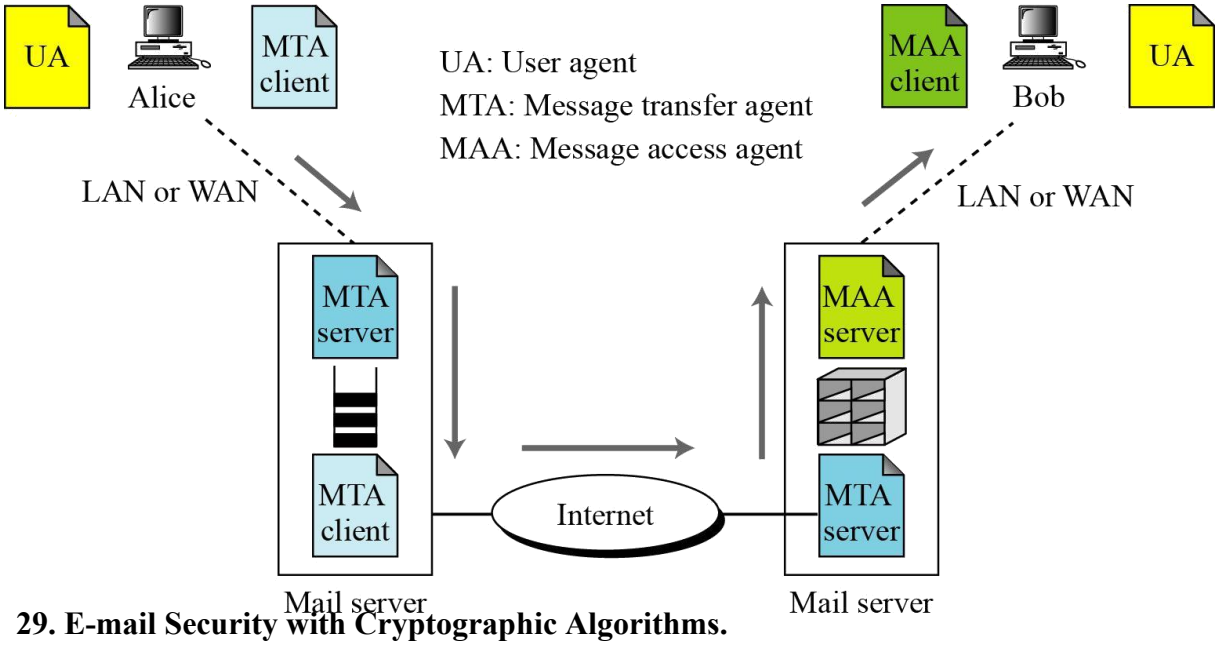
2. Content-transfer encoding
3. Content-ID
4. Content-description
5. Content-disposition

27. The Content-type Applications of MIME. (Nov 2014)(Apr 2015)

Subtypes:

- Postscript
- Octet-Stream-Unidentified binary data
- Many others will be added

28. E-mail architecture



29. E-mail Security with Cryptographic Algorithms.

In e-mail security, the sender of the message needs to include the name or identifiers of the algorithms used in the message.

30. Define E-mail Security with Cryptographic secrets.

In e-mail security, the encryption/decryption is done using a symmetric-key algorithm, but the secret key to decrypt the message is encrypted with the public key of the receiver and is sent with the message.

31. Define Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) can be used to create a secure e-mail message or to store a file securely for future retrieval.

32.Write note on uudecode((Apr 2014)

Uuencode (also called Uuencode/Uudecode) is a popular utility for encoding and decoding files exchanged between users or systems in a network

33.Writa not on cryptography?(Apr 2014)

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The term is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption).

34.What are the key pairs used in SET? (Apr 2012)

- Certificates: need for authentication
- Certificates: need for trusted third party

35.List the internet protocols related to mail specific applications. (Nov 2012)

Simple Mail Transfer Protocol(SMTP)
Post Office Protocol(POP)
Network News Transfer Protocol(NNTP)
Domain Name System(DNS)

36. Difference between master and visa card. (Apr 2013)

Visa and **MasterCard** are both payment systems, not **credit cards** in themselves. They rely on providers to issue **credit cards** using their system. Both exist to set rules and standards for the way in which card transactions are accepted, authorised, and processed.

11 MARKS

1. **Explain objectives of business cards(Master card, Visa card) April 2012**

BACKGROUND

Impact of electronic commerce

- There is no question that electronic commerce as exemplified by the popularity of the internet is going to have an enormous impact of the financial services industry. No financial institution will be left unaffected by the explosion of electronic commerce.
- The number of payment card purchases made through this medium will grow as internet based on line ordering systems are created.
- Many banks are planning to support this new form of electronic commerce by offering card authorizations directly over the Internet.
- Several trials with electronic currency and digital cash are already underway.

Projected use

- With more than 30 million user in 1998 and 90 million projected to come on board in the next two years the internet is a new way for businesses to establish computer based resources that can be accessed by consumers as well as business partners around the world.

Internet

- The internet is changing the way we access and purchase information communicate and pay for services and acquire and pay for goods Financial services such as bill payment brokerage insurance and home banking are now or soon will be available over the Internet.

World Wide Web

- The web can display text sound images and even video allowing merchants to transmit information directly to potential consumers around the world around the clock.

Consumer payment devices

- With open networks payment will increasing be made by consumer driven devices. As advanced technologies become more practical and affordable the marketplace will move from brick and mortar to more convenient locations such as the home or office. As financial services evolve consumers will consolidate their payment needs into one multi functional relationship product that enables widespread around the clock access.

Publicity

Internet and the possibilities for consumers and merchants to create a new type of shopping called electronic commerce. The publicity has focused on three areas:

- Marketing opportunities to develop new ways to browse select and pay for goods and services to on- line consumers.
- New products and services and
- Security risks associated with sending unprotected financial information across public networks.

Role of payment systems

Payment systems and their financial institutions will play a significant role by establishing open specifications for payment card transactions that:

- Provide for confidential transmission,
- Authenticate the parties involved,
- Ensure the integrity of payment instructions for goods and services order data and
- Authenticate the identity of the cardholder and the merchant to each other.

Procedures needed

- Because of the anonymous nature of communications networks procedures must be developed to substitute for existing procedures used in face to face or mail order /telephone order (MOTO0 transactions including the authentication of the cardholder by the merchant.

Use of payment card products

- Financial institutions have a strong interest in accelerating the growth of electronic commerce. Although electronic shopping and ordering does not require electronic payment a much higher percentage of these transactions use payment card products instead of cash or checks.

Purpose of secure electronic transaction

To meet these needs the secure electronic transaction (SET) protocol uses cryptography to:

- Provide confidentiality of information
- Ensue payment integrity and
- Authenticate both merchants and cardholders.

OBJECTIVES

Motivation

The primary motivations for the bankcard associations to provide specifications for secure payments are:

- To have the bankcard community take a leadership position in establishing secure payment specifications and in the process avoid any cost associated with future reconciliation of implemented approaches

- To respect and preserve the relationship between merchants and acquirers and between cardholders and Issuers,
- To facilitate rapid development of the marketplace,
- To respond quickly to the needs of the financial services a market and
- To protect the integrity of bankcard brands.

Payment security

The objectives of payment security are to

- Provide authentication of cardholders merchants and acquires,
- Provide confidentiality of payment data
- Preserve the integrity of payment data and
- Define the algorithms and protocols necessary for these security services.

Interoperability

The objectives of interoperability are to:

- Clearly define detailed information to ensure that applications developed by one vendor will interoperate with applications developed by other vendors.
- Create and support an open payment card standard,
- Define exportable technology throughout, in order to encourage globally interoperable software,
- Build on existing standards where practical
- Ensure compatibility with and acceptance by appropriate standards bodies and
- Allow for implementation on any combination of hardware and software platform such as power PC, Intel, spare, UNIX, MS-DOS, OS/2, WINDOWS and MACINTOSH.

Market acceptance

The objectives of market acceptance are to:

- Achieve global acceptance via ease of implementation and minimal impact on merchant and cardholder end users,
- Allow for ―bolt-on‖ implementation of the payment protocol to existing client applications,
- Minimize change to the relationship between acquirers and merchant cardholders and issuers,
- Allow for minimum impact to existing merchant, acquirer and payment system applications and infrastructure and
- Provide an efficient protocol viewed for the financial institution perspective.

2. Explain about business requirements and scope, features. (Nov 2012)

BUSINESS REQUIREMENTS

Introduction:

The business requirements for secure payment processing using payment processing using payment card products over both public networks (such as the Internet) and private networks.

Security issues noncompetitive

Security issues regarding electronic commerce must be viewed as noncompetitive in the interests of financial institutions, merchants and cardholders.

Seven business requirements

There are seven major business requirements addressed by SET:

- Provide confidentiality of payment information and enable confidentiality of order information that is transmitted along with the payment information.
- Ensure integrity for all transmitted data.
- Provide authentication that a cardholder is a legitimate user of a branded payment card account.
- Provide authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring financial institution.
- Ensure the use of the best security practices and system design techniques to protect all legitimate parties of an electronic commerce transaction.
- Ensure the creation of a protocol that is neither dependent on transport security mechanisms nor prevents their use.
- Facilitate and encourage interoperability across software and network providers.

FEATURES

Features of the specifications

These requirements are addressed by the following features of these specifications.

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication
- Interoperability

For the sake of clarity, each of these features has been described as a distinct component. It should be noted, however, that these elements do not function independently; all security functions must be implemented.

Confidentiality of information

- The cardholder, account and payment information must be secured as it travels across the network, preventing interception of account numbers and expiration dates by unauthorized individuals.
- ***On-line shopping***: In today's on-line shopping environment, payment instructions containing account information are often transmitted from cardholders to merchants over open network with little or no security precautions.
- ***Fraud***: while it is possible to obtain account information in other environments, there is a heightened concern about the ease of doing so with public network transactions. This concern reflects the potential for high volume fraud, automated fraud the potential
- For ―mischievous fraud‖ that appears to be characteristic of some hackers. In addition, the transmission of account information in a relatively unsecure manner has triggered a great deal of negative press.
- The specifications must guarantee that message content is not altered during the transmission between originator and recipient.
- Payment information sent form cardholders to merchants includes order information, personal data and payment instructions. If any component is altered in transit; the transaction will not be processed accurately.

Cardholder account authentication

- Merchant need a way to verify that a cardholder is a legitimate user of a valid branded payment card account number. A mechanism that uses technology to link a cardholder to a specific payment card account number will reduce the incidence of fraud and therefore the overall cost of payment processing.

- These specifications define the mechanism to verify that a cardholder is a legitimate user of a valid payment card account number.

Merchant authentication

The specifications must provide a way for cardholders to confirm that a merchant has a relationship with a financial institution allowing it to accept payment cards. Cardholders also need to be able to identify merchants with whom they can securely conduct electronic commerce.

Interoperability

The specifications must be applicable on a variety of hardware and software platforms and must include no preference for one over another. And cardholder with compliant software must be able to communicate with any merchant software that also meets the defined standard.

SCOPE

Use of payment cards

The SET specifications address a portion of the message protocols that are necessary for electronic commerce. It specifically addresses those parts of the protocols that use or impact the use of payment cards.

Electronic shopping experience

The electronic shopping experience can be divided into several distinct stages.

Stage	Description
1	The cardholder browses for items. This may be accomplished in a variety of ways, such as: Using a browser to view an on-line catalog on the merchants world wide web page; Viewing a catalog supplied by the merchant on a CD-ROM; or Looking at a paper catalog.
2	The cardholder selects items to be purchased.
3	The cardholder is presented with an order form containing the list of items, their prices, ant a total prices including shipping, handling and taxes. This order form may be delivered electronically from the merchant's server or created on the cardholder's computer by electronic shopping software.
4	The cardholder selects the means of payment.
5	This cardholder sends the merchant a completed order along with a means of payment.
6	The merchant request payment authorization from the cardholder's financial institution.
7	The merchant sends confirmation of the order.
8	The merchant ships the goods or performs the requested services from the order
9	The merchant request payment from the cardholder's financial institution.

Within the scope:

The following are within the scope of these specifications:

- Application of cryptographic algorithms
- Certificate message and object formats
- Purchase messages and object formats
- Authorization messages and object formats

- Message protocols between participants

Outside the scope:

The following are outside the scope for the set specifications:

- Message protocols for offers, shopping, delivery of goods, etc.
- Operational issues such as the criteria set by individual financial institutions for the issuance of cardholders and merchant certificates
- Screen formats including the content, presentation and layout of order entry forms as defined by each merchant
- General payments beyond the domain of payment cards
- Security of data on cardholders, merchant. And payment gateway systems including protection from viruses, Trojan horse programs, and hackers.

3. Explain about concept of payment system.

CONCEPTS

1. Payment System Participation
2. Cryptography
3. Certificate Issurance
4. Kinds of shopping

PAYMENT SYSTEM PARTICPATION

Interaction of participants

SET (Secured Electronic Transaction) changes the way the participants in the payment system interact. In a face-to-face retail transaction or a mail order transaction, the electronic processing of the transaction begins with the merchant or the acquirer. However, in an SET transaction, the electronic processing of the transaction begins with the cardholder.

Cardholder

In the electronic commerce environment, consumers and corporate purchasers interact with merchants form personal computers. A cardholders uses a payment card that has been issued by an issuer, SET ensures that the interactions the cardholders has with a merchant keep the payment card account information confidential.

Issuer

An issuer is the financial institution that establishes an account for a cardholder and issues the payment card. The issuer guarantees payment for authorizes transactions using the payment card in accordance with payment card brand regulations and local legislation.

Merchant

A merchant offers goods for sale or provides services in exchange for payment. SET allows a merchant to offer electronic interactions that cardholders can use securely.

Acquirer

An acquirer is the financial institution that establishes an account with a merchant and processes payment card authorizations and payments.

Payment gateway

A payment gateway is a device operated by an acquirer or a designated third party that processes merchant payment messages

Brand

Financial institutions have founded bankcard associations that protect and advertise the brand, establish and enforce rules for use and acceptance for their bankcards, and provide networks to interconnect the financial institutions.

Third parties

Issuers and acquirers sometimes choose to assign the processing of payment card transactions to third party processors. This document does not distinguish between the financial institution and the processor of the processor of the transactions.

CRYPTOGRAPHY(4.Explain various secure e-payment system Or Explain various secure e-payment systems and its certificate issuance. Or What are the technique used for secure e-payment system and explain.)

Protection of sensitive information

- Cryptography has been used for centuries to protect sensitive information as it is transmitted from one location to another.
- In a Cryptography graphic system, a message is encrypted using a key. The resulting cipher text is then transmitted to the recipient where it is decrypted using a key to produce the original message.
- There are two primary encryption methods in use today: secret-key encryption and public key Cryptography. SET uses both methods in its encryption process.

Secret key Cryptography

Secret key Cryptography also known as symmetric Secret key Cryptography, use the same key to encrypt and decrypt the message. Therefore, the sender and recipient of a message must share a secret, namely the key. A well known secret key Secret key Cryptography algorithm is the data encryption standard which is used by financial institutions to encrypt PINs.

Public key Cryptography

- Public key Cryptography, also known as asymmetric cryptography, uses two keys: one key to encrypt the message and the other key to decrypt the message.
- The two keys are mathematically related such that data encrypted with either key can only be decrypted using the other. Each user has two keys: a public key and private key. The user distributes the public key. Because of the relationship between the two keys, the user and anyone receiving the public key can be assured that data encrypted with the public key and sent to the user can only be decrypted by the user using the private key.

Encryption

Confidentially is ensured by the use of message encryption

- **Encryption: relationship of keys**

  When two users want to exchange messages securely, each transmits one component of their key pair, designated the private key. Because messages encrypted with the public key can only be decrypted using the private key, these messages can be transmitted over an insecure network without fear that an eavesdropper can use the key to read encrypted transmissions.

  Encryption: use of symmetric key

  SET will rely on cryptography to ensure message confidentially. In SET, message data will initially be encrypted using a randomly generated symmetric encryption key. This key, in turn, will be encrypted using the message recipient's public key. This is

referred to as digital envelope; the recipient decrypts it using his or her private key to obtain the randomly generated symmetric key and then uses the symmetric key to unlock the original message.

Digital Signatures

Integrity and authentication are ensured by the use of digital signatures.

Digital Signatures: relationship of keys

Because of the mathematical relationship between the public and private keys, data encrypted with either key can only be decrypted with the other. This allows the sender of a message to encrypt it using sender's private key. Any recipient can determine that the message came from the sender by decrypting the message using the sender's public key.

Digital Signature: using message digests

When combined with message digests, encryption using the private key allows users to digitally sign messages. A message digest is a value generated for a message that is unique to that message. A message digest is generated by passing the message through a one way cryptographic function i.e., one that cannot be reversed. When the digest of a message is encrypted using the sender's private key and is appended to the original message, the result is known as the digital signature of the message.

Digital Signature: Example

For example, Alice computes the message digest of a property description and encrypts it with her private key yielding a digital signature for the message. She transmits both the message and the digital signature to Bob. When Bob receives the message, he computes the message digest of the property description and decrypts the digital signature with Alice's public key. If the two values match, Bob knows that the message was signed using Alice's private key and that it has not changed since it was signed.

Two key pairs

SET uses a distinct public/private key pair to create the digital signature. Thus, each SET participant will possess of encryption and decryption, and a ―signature‖ pair for the creation and verification of digital signatures.

Certificates: need for authentication

Before two parties use public-key cryptography to conduct business, each wants to be sure that the other party is authentication. Before Bob accepts a message with Alice's digital signature, he wants to be sure that the public key belongs to Alice and not to someone masquerading as Alice on an open network. One way to sure that the public key belongs to Alice is to receive it over a secure channel directly from Alice. However, in most circumstances this solution is not practical.

Certificates: need for trusted third party

An alternative to secure transmission of the key is to use a trusted third party to authenticate that the public key belongs to Alice. Such a party is known as a Certificate Authority (CA). The certificate authority authenticates Alice's claims according to its published policies.

SET authentication

The means that a financial institution uses to authenticate a cardholder or merchant is not defined by these specifications. Each payment card brand and financial institution will select an appropriate method.

ENCRYPTION SUMMARY

Encryption

The encryption diagram consists of

1. Alice runs the property description through one-way algorithm to produce a unique value known as the message digest.
2. She then encrypts the message digest with her private signature key to produce the digital signature.
3. Next, she generates a random symmetric key and uses it to encrypt the property description, her signature and a copy of her certificate. Which contains her public signature key? In order to decrypt the property description, bob will require a secure copy of this random symmetric key.
4. Bob's certificate which Alice must have obtained prior to initiating secure communication with him contains a copy of his public key-exchange key. To ensure secure transmission of the symmetric key, Alice encrypts it using bob's public key-exchange key. The encrypted key referred to as the digital envelope is sent to bob along with the encrypted message itself.
5. Finally, she sends a message to bob consisting of the following: the symmetrically encrypted property description, signature and certificate as well as the asymmetrically encrypted symmetric key.

Decryption

6. Bob receives the message from Alice and decrypts the digital envelope with his private key exchange key to retrieve the symmetric key.
7. He uses the symmetric key to decrypt the property description, Alice signature and her certificate.
8. He decrypts Alice digital signature with her public signature key, which he acquires from her certificate. This recovers the original message digest of the property description.
9. He runs the property description through the same one-way algorithm used by Alice and produces a new message digest of the decrypted property description.
10. Finally he compares his message digest to the one obtained from Alice digital signature.

Introduction of dual signature

SET introduces a new application of digital signatures, namely the concept of dual signatures. To understand the need for this new concept, consider the following scenario: Bob wants to send Alice and offer to purchase a piece of property and an authorization to his bank to transfer the money if Alice accepts the offer, But bob does not want the bank to see the terms of the offer nor does he want Alice to see his account information.

Generation of a dual signature

A dual signature is generated by creating the message digest of both messages concatenating the two digests together; computing the message digest of the result and encrypting this digest with the signer's private signature key. The signer must include the message digest of the other message in order for the recipient to verify the dual signature.

Uses of dual signatures

Within set, dual signatures are used to link an order message sent to the merchant with the payment instructions containing account information sent to the acquired. When the merchant sends an authorization request to the acquirer, it includes the payment instruction sent to it by the cardholder and the message digest of the order information.

Import/export issues

A number of governments have regulations regarding the import or export of cryptography. As a
General rule these governments allow cryptography to be used when:

- The data being encrypted is of a financial nature;
- The content of the data is well defined
- The length of the data is limited ; and
- The cryptography cannot easily be used for other purposes

CERTIFICATE ISSUANCE

- Cardholder certificates function as an electronic representation of the payment card. Because they are digitally signed by a financial institution they cannot be altered by a third party and only the financial institution can generate one. A cardholder certificate does not contain the account number and expiration date.
- A certificate is only issued to the cardholder upon approval of the cardholder's issuing financial institution. By requesting a certificate a cardholder has indicated the intent to perform commerce via electronic means.

Merchant certificates

Merchant certificates function as an electronic substitute for the payment brand decal that appears in the store window. (The decal itself is a representation that the merchant has a relationship with a financial institution allowing it to accept the payment card brand)

- A merchant must have at least one pair of certificates in order to participate in the SET environment but there may be multiple certificate pairs per merchant. A merchant will have of certificates for each payment card brand that it accepts

Payment gateway certificates

- Payment gateway certificates are obtained by acquires or their processors for the systems that process authorization and capture messages. The gateway's encryption key which the cardholder gets form this certificate is used to protect the cardholder's account information
- Payment gateway certificates are issued to the acquirer by the payment brand

Acquirer certificates

- An acquirer must have certificates in order to operate a certificate Authority that can accept and process certificate requests directly from merchants over public and private networks. Those acquirers that choose to have the payment card brand process certificate requests on their behalf will not require certificate because they are not processing SET messages. Acquirers receive their certificates from the payment card brand

Issuer certificates

- An issuer must have certificates in order to operate a certificate authority that can accept and process certificate requests directly from cardholders over public and private

networks. Those issuers that choose to have the payment card brand process certificate requests on their behalf will not require certificates because they are not processing SET messages. Issuers receive their certificates from the payment card brand.

HIERARCHY OF TRUST

- SET certificates are verified through a hierarchy of trust. Each certificate is linked to the signature certificate of the entity that digitally signed it. By following the trust tree to a known trusted party one can be assured that the certificate is valid. For example a cardholder certificate is linked to the certificate of the Issuer (or the association on behalf of the issuer).

Root key validation

- Software can confirm that it has a valid root key by sending an initiate request of the certificate authority that contains the hash of the root certificate. In the event that the software does not have a valid root certificate, the certificate authority will send on in the response.

Root key replacement

- When the root key is generated a replacement key will also be generated. This replacement key is stored securely until it is needed.
- The self signed root certificate and the hash of the replacement key are distributed together.
- Software will be notified of the replacement through a message that contains a self signed certificate of the replacement root and the hash of the next replacement root key.
- Software validates the replacement root key by calculating its hash and comparing it with the hash of the replacement key contained in the root certificate.

KINDS OF SHOPPING (5.Describe about different types of shopping)

Variety of experience

- There are many ways that cardholders will shop. This section describes two ways. The SET protocol supports each of these shopping experiences and should support others as they are defined.

Online catalogues

- The growth of electronic commerce can largely be attributed to the popularity of the World Wide Web. Merchants can tap into this popularity by creating virtual storefronts on the Web that contain on line catalogues. These catalogues can be quickly promotions.
- Cardholders can visit these web pages selecting items for inclusion on an order.

Electronic catalogues

- Merchants may distribute catalogues on electronic media such as diskettes or CD-ROM. This approach allows that cardholder to browse through merchants off-line. With an on-line catalogue the merchant has to be concerned about bandwidth and may chose to include fewer graphics or reduce the resolution of the graphics. By providing an off-line catalogue such constraints are significantly reduced.

6.Explain Different type e-payment processing. Or Describe about e-payment processing with protocol description. (Nov 2014)(Apr 2015)

PAYMENT PROCESSING

OVERVIEW

Transaction described

This describes the flow of transaction as they are processed by various system.

SET defines a variety of transaction protocols that utilize the cryptographic concepts.

This action describes the following transactions:

- Cardholder registration
- Merchant registration
- Purchase request
- Payment authorization
- Payment capture

Other transactions

The following additional transactions are part of these specifications,

- Certificate query
- Purchase inquiry
- Purchase notification
- Sale transaction
- Authorization reversal
- Capture reversal
- Credit
- Credit reversal

A guide to the diagrams

Initial	participant
C	Cardholder
M	Merchant
P	Payment Gateway
GA	Certificate Authority

The following symbols are used in the detailed diagram

The teeth of the key indicate the key's owner.
Keys with ―PV‖ on the handle are private keys
Keys with ―PB‖ are public keys.
Keys with a diamond ( ) are signature keys
Keys with small key ( ) are key-exchange keys.
Dual signature, initial indicates which private key was used to create the signature
Certificates. The initial in the ―seal‖ indicates which private key was used to sign the certificate.
Symmetric key used to encrypt data.
Payment card used to indicate when the cardholder's account number is being transmitted.
Protected data used to represent account information sent in the digital envelope of registrations
Encrypted message including the digital envelope.

The data in the shaded region has been encrypted using a randomly generated symmetric key.

Protocol description

The description of the processing differ from the formal protocol definition, the formal protocol definition take precedence.

Certificate Authority functions

The primary authorities are to:

- Receive registration requests;
- Process and approve/decline requests; and
- Issue certificates.

Payment card brands and individual financial institutions will review their business needs for these functions to select a solution for implementation. The selected solution may be to implement a single server device that provides the Certificate Authority functions or multiple devices that distribute the processing. Payment card brands and financial institutions will select an appropriate solution based on their individual business needs.

Optional cardholder certificates

Payment card brands at their option may allow cardholders to process transactions without a certificate as a temporary measure to facilitate implementation of these specifications.

No digital signature

When a cardholder does not possess a signature certificate, no digital signature is generated. In place of the digital signature, the cardholder generates the message digest of the data and inserts the message digest into the digital envelope.

Assurance of integrity

The recipient of data from the cardholder uses the message digest from the digital envelope to confirm the integrity of the data.

Strength of cardholder certificates

The strength depends on the methods employed by the payment card brand and the payment card issuer to authenticate the cardholder prior to the certificate being issued.

Cardholder authentication

If a cardholder signature certificate is not present, authentication of the cardholder must be performed by other means where SET uses cardholder certificate to confirm.

CARDHOLDER REGISTRATION (7.Briefly discuss about cash holder registration)

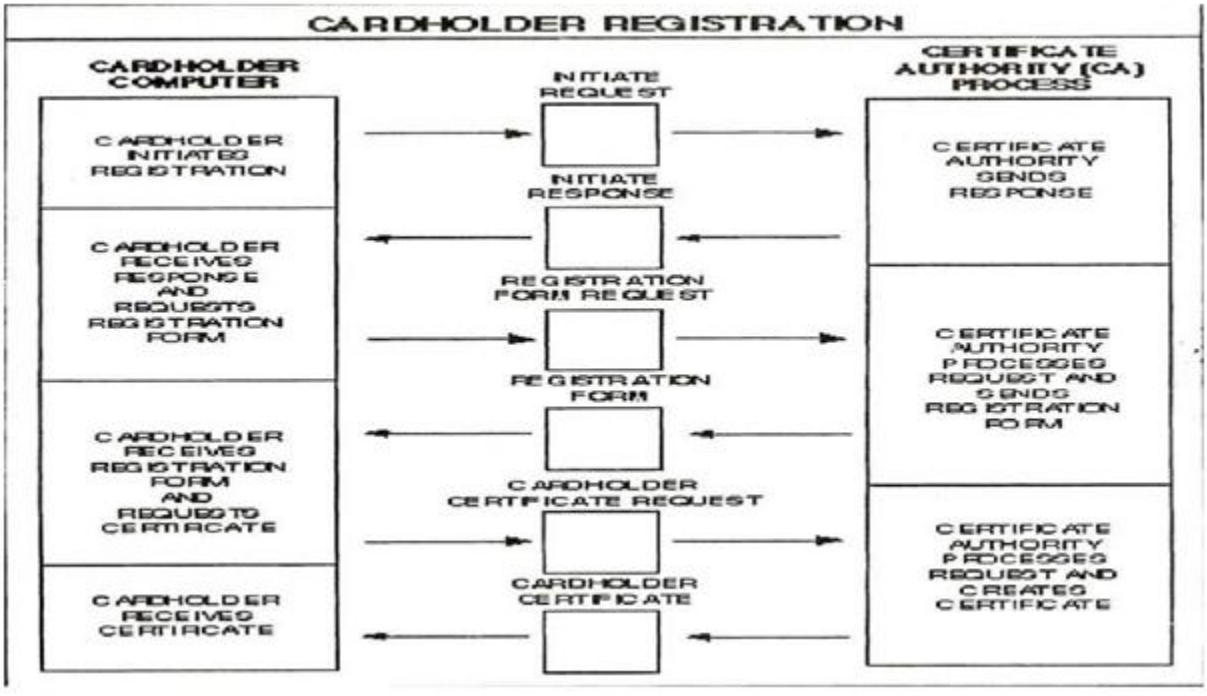
This scenario is divided into its seven fundamental steps.

Cardholder must register with a Certificate Authority (CA) before they can send SET messages to merchants.

For sending SET messages to CA the cardholder must have copy of the CA public key-exchange key, copy of the registration form from the cardholder's financial institution.

The CA provides the registration form, for this it requires two exchanges between the cardholder software and the CA.

The registration process is started when the cardholder software requests a copy of the CA's key-exchange certificate.



- **Cardholder initiates registration**

CARDHOLDER COMPUTER

INITIATE REQUEST

1. Cardholder software sends initiative

Request to CA → REQ

C INIT

C INIT REQ

C INIT REG

2. CA receives initiative request

INITIATE RESPONSE

3. CA generates response and digitally signs it by generating a msg digest of the response & encrypting it with the CA private signature key.

4. CA sends response along with the CA certificates to cardholder

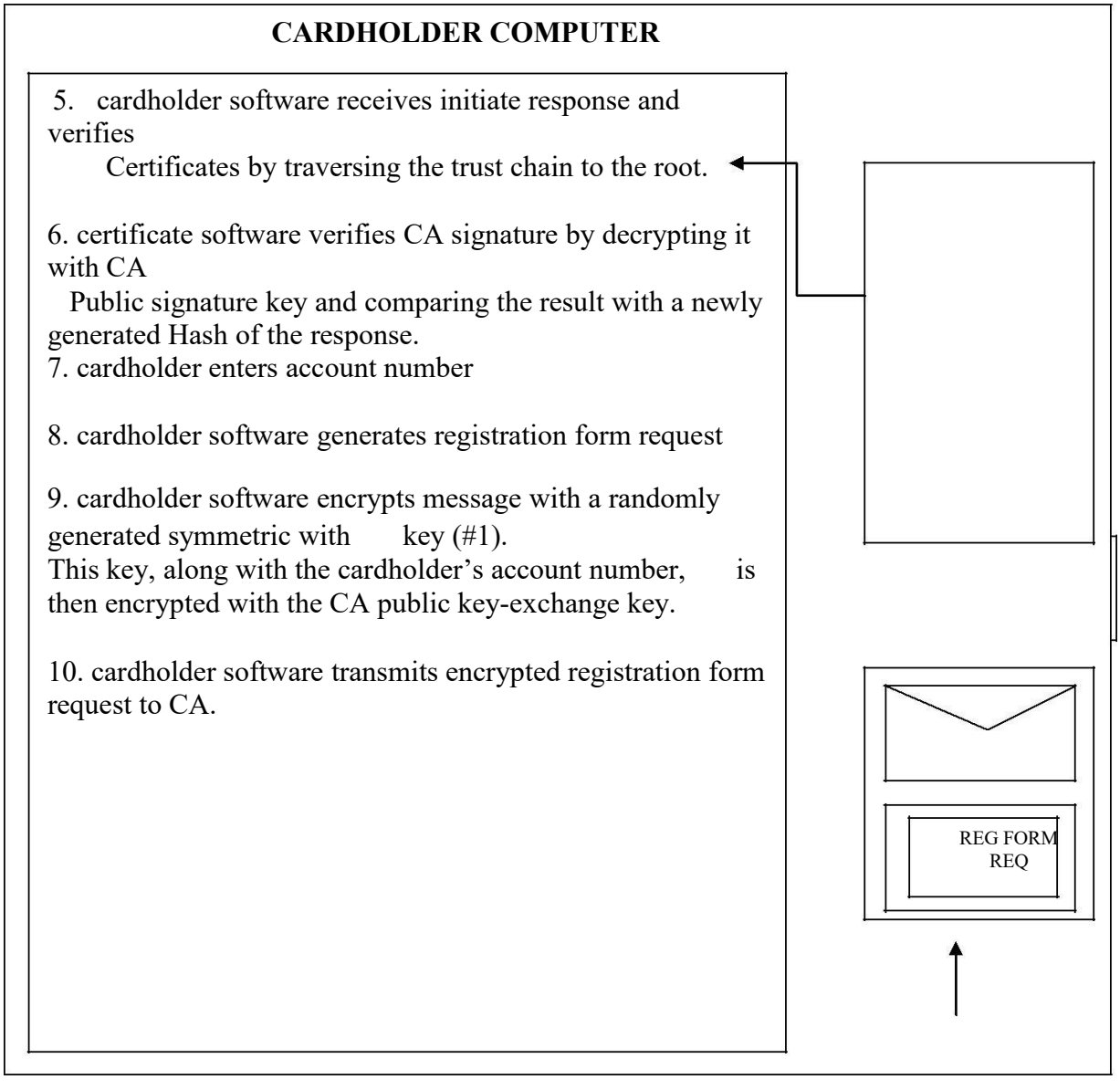
CAP RBG

Once the software has a copy of the CA key-exchange certificate, the cardholder can request a registration form. The cardholder software creates a registration form request message then it generates a random symmetric encryption key. This random key is used to encrypt the registration form request message, which is then encrypted along with the account number into the digital envelope using the CA public key-exchange key. Finally the software transmits all of these components to the CA.

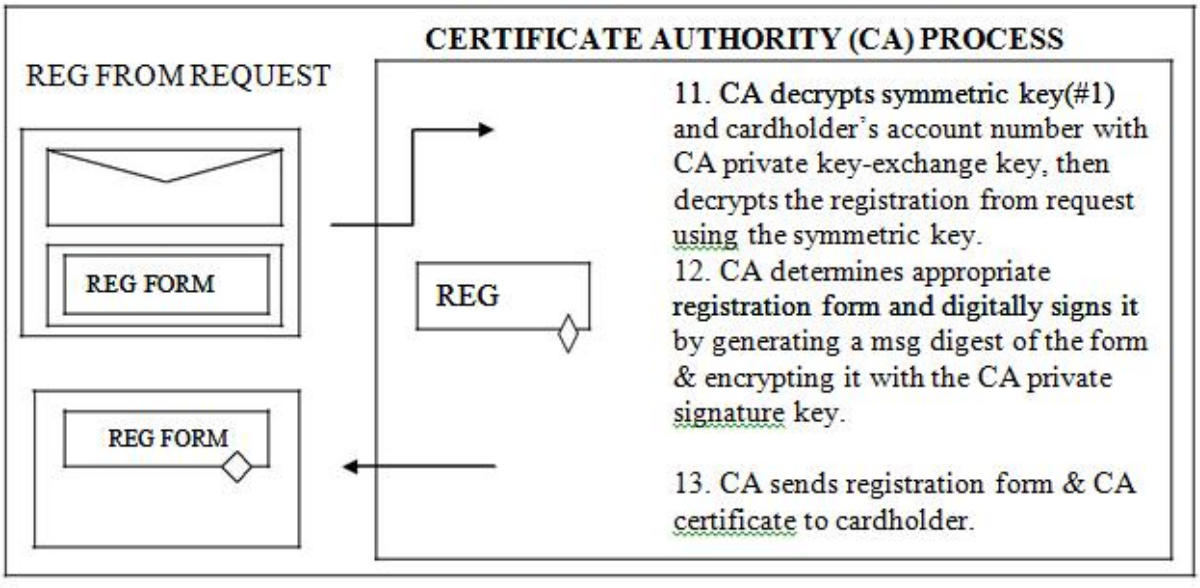
Cardholder receives response and requests registration form

The CA identifies the cardholder's financial institution and selects the appropriate registration form.

It digitally signs and then returns this registration form to the cardholder. The CA may not have a copy of the registration form but can inform the cardholder software.



The cardholder needs a signature public/private key pair for use with SET. The cardholder software generates this key pair if it does not already exist.



To register an account, the cardholder fills out the registration form that was returned by the CA with information such as the cardholder's name, expiration date, account billing address, and any additional information the issuing financial institution deems necessary to identify the certificate requester as the valid cardholder.

The cardholder software generates a random number that will be used by the CA in generating the certificate, which is combining with the public key in the registration message.

The software digitally signs the registration messages, and generates two random symmetric encryption keys. It places one random key inside the message; the CA will use this key to enc the response. It uses the other random key to encrypted the registration message. This key is then encrypted along with the acc number, expiration date, and the random number into the digital envelope using the CA public key-exchange key. Finally the software transmits all of these components to the CA.

Cardholder receives registration form and requests certificate

When the CA receives the cardholder's request, it decrypted the digital envelope to obtain the symmetric encrypted Key, the account Information And the random number generated by the cardholder Software.

- It uses the symmetric key to decrypted the registration request.
- If signature Is verified, the message processing continues; otherwise, the message is rejected and an appropriate response message is returned to the cardholder
- The CA must verify the information from the registration request using the cardholder's account Information
- If the information In the registration request is verified, a certificate will be issued. First the CA generates a random number that is combined with the random number created by the cardholder Software to generate a secret value, which is used to protect the account Information In the cardholder Certificate.

- The value are encoded using one way hashing algorithm, the result is placed into the cardholder Certificate.
- A response message containing the random number generated by the CA and the other information Is then generated and encrypted Using the symmetric key sent by the cardholder Software in the registration message the response is then transmitted to the cardholder.

Certificate authority processes request and creates certificate

When the cardholder Software receives the response from the CA, it verifies the certificate By traversing the trust chain to the root key, then cardholder Software decrypted the registration response using the symmetric encrypted Key that it sent to the CA in the registration message, combines the random number returned by the CA with the value that it sent in the registration message to determine the secrete value.

MERCHANT REGISTRATION

Merchants must register with a certificate Authority (CA) before they can receive the SET payment instructions from cardholder Or process SET transactions through a payment gateway. To send the merchant mush has a copy of the CA public key-exchange key, a copy of registration form from the merchant's financial institution. The merchant software must identify the Acquirer to the CA. The registration process Is started when the merchant software request a copy of the CA's key-exchange certificate And the appropriate registration form.

Merchant requests registration form

The CA identifies the merchant's financial institution and selects the approved egistration form. It returns third registration form alone with a copy of its own key-exchange certificate to the merchant.

Certificate authority processes request and sends registration form

- The merchant software verifies the CA certificate By traversing the trust chain to the root key, it must hold a CA certificate
- The merchant can register to accept SET payment instructions and process SET transactions. The merchant needs two public/private key pairs for use with SET key-exchange and signature the merchant Software generates these key pairs if they do not already exist.
- To register, the merchant Fills out the registration form, the merchant Software takes this registration form and combines it with the public keys in a registration message the software digitally signs the registration message. The software generates a random symmetric encryption key, which is used to encrypt the message finally the software transmits all of these components to the CA.

Merchant receives registration form and requests certificates

When the CA receives the merchant's request, it decrypts the digital envelope to obtain the symmetric encryption key, which it uses to decrypt the registration request.

If signature is verified, the message processing continues; otherwise, the message is rejected and an appropriate response message is returned to the merchant

The CA must verify the information from the registration request using known merchant Information

If the information in the registration request is verified, the CA creates and digitally signs the merchant Certificate

The certificate Are then encrypted Using a randomly generated symmetric key, which in turn is encrypted Using the merchant Public key-exchange key. the response is then transmitted to the merchant.

Certificate authority processes request and creates certificate

When the merchant software receives the response from the CA, it decrypted the digital envelope to obtain the symmetric encryption key. It uses the symmetric key to decrypted the registration response containing the merchant Certificate

After the merchant Software verifies the certificate by traversing the trust chain to the root key, it stores the certificates on the merchant's computer.

PURCHASE REQUEST

The SET protocol is invoked after the cardholder has completed browsing, selection and ordering. The cardholder will have selected a payment card as the means of payment. In order to send SET messages to merchant, the cardholder must have a copy of the merchant public key-exchange key as well as the payment gateway's key-exchange keys. When cardholder software requests a copy of the merchants and gateway's certificates. The message from the cardholder indicates which payment card brand will be used for the transaction.

Cardholder initiates request

When the merchant receives the request, it assigns a unique transaction identifier to the message. It then transmits the merchant and gateway certificates that correspond to the payment card brand indicated by the cardholder along with the transaction identifier to the cardholder.

Merchant sends certificate(s)

The cardholder software verifies the merchant and gateway certificates. It creates the order Information (OI) and Payment Instruction (PI).

It places the transaction identifier assigned by the merchant in the OI and PI, for linking the OI and PI together when the merchant requests authorization. This information is exchanges between the cardholder and merchant software during the shopping phase before the first SET message.

The cardholder Software generates a dual signature For the OI and PI by computing the msg. digests of both, concatenating the two digests, computing the msg. digest of the result and encrypting that using the cardholder private signature Key.

Then the software generates a random Symmetric encryption key & uses it to encrypt the dual signed PI. The software then encrypts the cardholder Account No. as well as the random Symmetric Key used to encrypted The PI into a digital envelope using the payment gateway's key-exchange key. Finally the software transmits a msg. consisting of the OI and the PI to the merchant.

Cardholder Receives response and sends request

When the merchant software receives the order, it verifies the cardholder signature Certificate By the traversing the trust chain to the root key. The merchant Software then processes the order including the payment authorization. After the OI has been processed, the merchant software generates & digitally signs a purchase response message. If transaction was approved, the merchant will perform the services indicated in the order.

Merchant processes request message

When the cardholder Software receives the purchase response message from the merchant, it verifies the merchant Signature Certificate and uses merchant Public signature Key to check the merchant Digital signature, and then it takes some action based on the contents of the response message. The cardholder can determine the status of the order by sending an order inquiry msg.

PAYMENT AUTHORIZATION

During the processing of an order from a cardholder, the merchant will authorize the transaction. The merchant software generates and digitally signs an authorization request, which the amount to be authorized, the transaction identifier from the OI and the other information about the transaction. The request is then encrypted using the public key-exchange key of the payment gateway. Then the authorization request and the cardholder payment instructions are transmitted to the payment gateway.

Merchant requests authorization

When the payment gateway receives the authorization request, it decrypts the digital envelope of the authorization request to obtain the symmetric encryption key.

- It uses the symmetric key to decrypt the request. It then verifies the merchant signature certificate by traversing the trust chain to the root key; it also verifies that the certificate has not expired.
- It uses the merchant public signature key to ensure the request was signed using the merchant private signature key.
- Then the payment gateway decrypts the digital envelope of the payment instructions to obtain the symmetric encryption key and the account information by using symmetric key.
- It verifies the cardholder signature certificate by traversing the trust chain to the root; it also verifies that the certificate has not expired.
- The payment gateway verifies that the transaction identifier received from the merchant matches the one in the cardholder payment instructions. Then it is formatted and sends a authorization request to the issuer via a payment system.
- After authorization, the payment gateway generates and signs a response message. It is encrypted using a new randomly generated symmetric key, which is again encrypted using the merchant public key-exchange key. Finally the response Is transmitted to the merchant.

Payment gateway processes authorization request

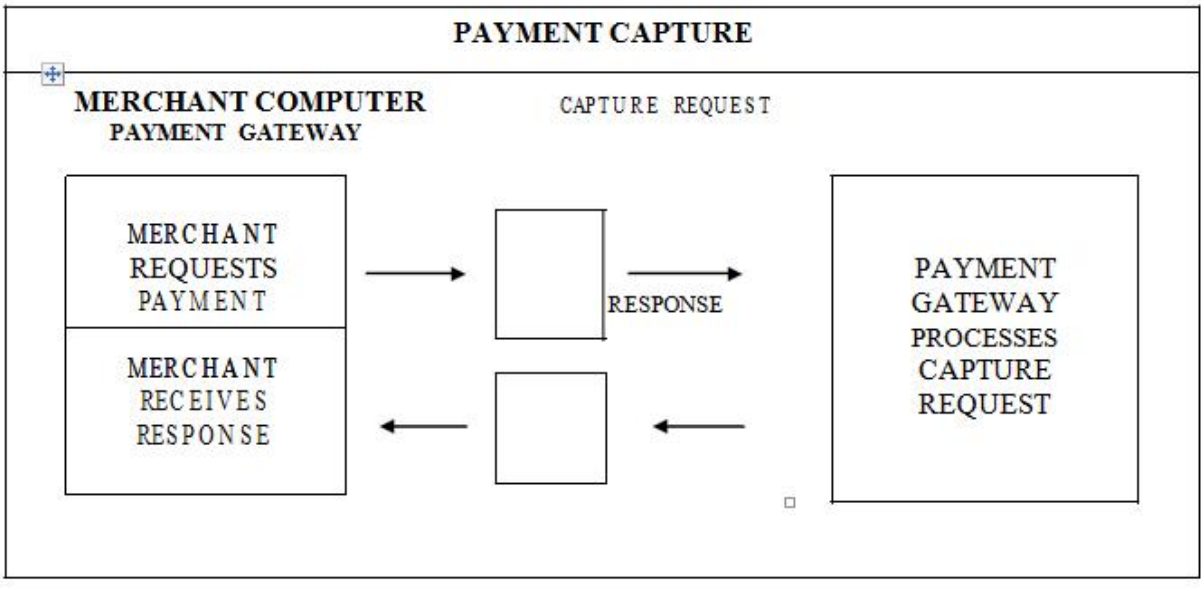
When the merchant software receives the authorization response message from the payment gateway, it decrypts the digital envelope to obtain the symmetric encryption key.

- Uses symmetric key to decrypt the response message, then verifies the payment gateway signature certificate by traversing the trust chain to the root key.
- It uses the payment gateway public signature key to check the payment gateway digital signature
- The merchant software will store the authorization response and the capture token to be used when requesting payment through a capture request.
- The merchant then completes processing of the cardholder's order by shipping the goods or performing the services indicated in the order.

PAYMENT CAPTURE

The diagram provides a high level overview of a merchant's payment capture process.

Payment capture



It is divided into its three fundamental steps.

After completing the processing of an order from a cardholder the merchant will request payment.

The merchant software generates and digitally signs a capture request, the request is then encrypted using a new randomly generated symmetric key, which in turn is encrypted using the public key-exchange key of the payment gateway.

The capture request is then transmitted to the payment gateway.

When the payment gateway receives the capture request, it decrypts the digital envelope of the capture request to obtain the symmetric encryption key.

It uses the symmetric key to decrypt the request. It then uses the merchant public signature key to ensure the request was signed using the merchant private signature key.

The payment gateway decrypts the capture token and then uses the information from the capture request and the capture token to format a clearing request, which it sends to the issuer via a payment card payment system.

This then generates and digitally signs a capture response message, which includes a copy of the payment gateway signature certificate. The response is then encrypted and transmitted to the merchant.

Payment gateway processes capture request

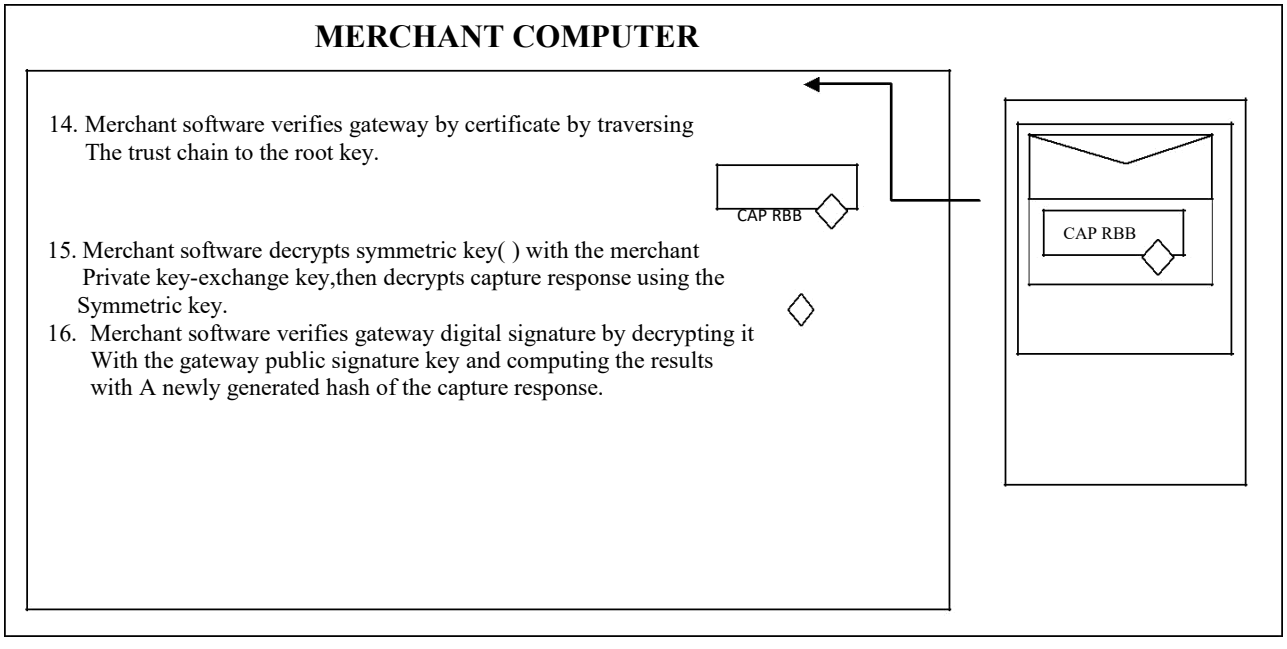
When the merchant software receives the capture response message from the payment gateway, it decrypts the digital envelope to obtain the symmetric encryption key.

It uses the symmetric key to decrypt the response message. It then verifies the payment gateway signature certificate by traversing the trust chain to the root key.

It uses the payment gateway public signature key to check the payment gateway digital signature.

The merchant software will store the capture response to be used for reconciliation with payment received from the acquirer.

Merchant receives response



Purchase inquiry

Cardholders can check the status of the processing of an order after the purchase response has been received by sending an order inquiry.

It does not include status of back ordered goods but indicate the status of authorization, capture and credit processing.

Authorization reversal

- This message allows a merchant to correct previous authorization requests.
- If part of the order will not be completed, the merchant will reverse part of the amount of the authorization.

Capture reversal

This message allows a merchant to correct errors in capture requests such as transaction amounts that were entered incorrectly by a clerk.

Credit

This message allows a merchant to issue a credit to a cardholder's account such as when goods are returned or were damaged during shipping.

Payment gateway certificate request

This message allows a merchant to query the payment gateway and receive a copy of the gateway's current key-exchange and signature certificates.

Batch Administration

This message allows a merchant to communicate information to the payment gateway regarding merchant batches.

8. Explain about email and secure e-mail technologies for E- Commerce.

THE MEANS OF DISTRIBUTION:

Electronic mail and messaging systems are an increasingly important part of an enterprise's computing and communications strategy. E-mail can be distributed over a private enterprise network, on-line networks (such as AOL), and the Internet. The growth in the subscriber population of Internet-based services for both individuals and businesses, makes Internet e-mail a pervasive tool.

- Most companies using the Internet for electronic commerce or EDI use mail communications with customers and business partners; they also use FTP for accessing public archives and for delivering software patches. As described elsewhere, the Internet provides a variety of capabilities for e-commerce/EDI use, including e-mail, file transfer, World Wide Web, and remote logins.
- TCP/IP provides the underlying transport protocol; the applications support different protocols, dependent on function. For example, a business application may need to utilize SMTP for mail, FTP for file transfer, HTTP for Worldwide Web access, and Telnet for remote logins. Each of these protocols supports different capabilities with respect to use and value-added functions
  such as security, encryption, and non repudiation.

- The Internet Engineering Task Force (IETF) meets regularly to discuss operational and technical issues impacting the Internet community. Capabilities related to security are under development or have recently been developed by the IETF.

- Working groups are set up for further investigation of important issues. Anyone can attend either of these meetings and become a member of a working group. Each working group has the responsibility of producing documentation and deciding how issues should be handled. The reports are called RFCs (Requests for Comments).

- To obtain an RFC, one can send a mail message to rfc-info@isi.edu with a message body of Retrieve: RFC
- Doc-ID: RFCxxxx
- where xxxz is the number of the RFC.
- The original RFCs that define how Internet e-mail messages are transmitted and how the format of the e-mail messages should appear are RFC-821' and RFC-822;8 these have been made obsolete by RFC-1123.
- SMTP performs the message transmission function, but only supports seven-bit American Standard Code for Information Interchange (ASCII) transmissions and limits the maximum message size.
- Modifications to SMTP were needed to address the needs of e-commerce/EDI. Some of these modifications came in the form of Multipurpose Internet Mail Extensions (MIME), as described in RFC-15219.
- MIME defines mail body part structure and content types that pro-vided an SMTP-compatible way to encapsulate documents in e-mail messages, while supporting multipart content types including text, audio, image, video, and even application data.

- MIME also provides support for several content-transfer encodings including base64, which enables incorporation of 8-bit binary data as 7-bit ASCII data.
- Further refinements were introduced in RFC-1767 to specifically address the encapsulation of EDI objects within MIME. This permitted the transmission of EDI transactions through Internet mail supporting both EDIFACT and ANSI X12 EDI standards as MIME content types and ensured that EDI objects retained their syntax and semantics during transmission'-'.

A MODEL FOR MESSAGE HANDLING:

ITU-T model:

- In 1971, the International Federation for Information Processing, a prestandards organization, developed a model for message handling. This model was eventually adopted and expanded by the International Telecommunication Union-Telecommunication (ITU-T), which developed the X.400 series recommendations, Message Handling System (MHS).

- Although Internet mail is not based on ITU-T standards, it is useful to look at this abstraction.
- E-mail messages are transported by a message transfer system (MTS), which is

  composed of one or more message transfer agents (MTAs). At the borders of the system, a user agent (UA) acts on behalf of a user and interfaces to its local message transfer agent.10-" From the perspective of the message transfer system, the e-mail message being sent is called the content, and all delivery information associated with the message is the envelope.

- In theory, the MTS is not aware of the structure of the content it transports; the UAs bilaterally agree as to what this structure is. Although there are no strict requirements as to the structure, there are usually two types of content in each e-mail message: control information (often called the headers) and data information (often called the body). A way of thinking about all these terms is as follows:
    - The envelope is meaningful to the message transfer agents.
    - The headers are meaningful to the user agents.
    - The body is meaningful to the users (people or programs).
- When an e-mail message is sent from one user to another, the following activities occur: the originating user indicates to the UA the address of the recipient; the UA places the destination address and the sender's address into the envelope and then posts the message through a posting slot to a message transfer agent, which involves a posting protocol in which the validity of those addresses and the syntax of the e-mail message are considered.
- Upon successful completion of the submission protocol, the MTA accepts the responsibility to deliver the e-mail message or, if delivery fails, to inform the originating user of the failure by generating an error report.
- After accepting responsibility to deliver the e-mail message, an MTA must decide if it can deliver the message directly to the recipient; if so, it delivers the e-mail message through a delivery slot to the recipient's UA, using a delivery protocol. If not, it contacts an adjacent MTA that is closer to the recipient and negotiates transfer of the e-mail message. This process repeats until some MTA is able to deliver the e-mail message or some MTA determines that the message is undeliverable. Given this model for e-mail, one realizes that:10, 11.
- E-mail transfer is third-party in nature: once an e-mail message passes through the posting slot, the user agent has no claims on the message. The MTS takes responsibility for the e-mail message at posting time and retains that responsibility until delivery time.

- E-mail transfer is store-and-forward in nature: the UAs for the originator and recipient need not be on-line simultaneously for mail to be submitted, transported, and delivered. In fact, only the node currently responsible for the
  e-mail message and the "next hop" taking responsibility for the 'message need be connected in'\\ order for the message to be transferred.

To summarize, there are three general protocols involved in the model:

- A messaging protocol used between two UAs
- A relaying protocol used between two MTAs
- A submission/delivery protocol used between an MTA and a UA

INTERNET APPARATUS:

We can view the Internet suite of protocols used for generic transmission as having four layers:

1. The interface layer describes physical and data-link technologies used to realize the transmission at the media (hardware) level.
2. The internet layer describes the internetworking technologies used to realize the internetworking function; this is realized with a connectionless mode network service, provided by the Internet Protocol (IP), originally defined in 1981 in RFC-791.
3. The transport layer describes the end-to-end technologies used to realize reliable communications between end systems; this is realized with a connection-oriented transport service provided by the Transmission Control Protocol (TCP), originally defined in 1981 in RFC-793.

4. The application layer describes the technologies used to provide end-user services.

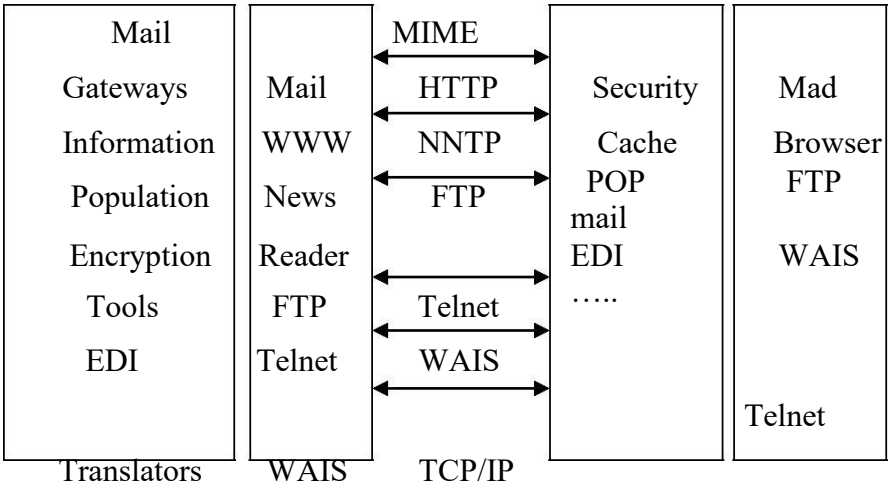
The Internet protocols related to mail-specific applications are as follows:

- The Simple Mail Transfer Protocol (SMTP), defined in RFC-821 (August 1982) and RFC-974 (January 1986), which provides store-and-forward service for textual e-mail messages, and RFC822 (August 1982), which defines the format of those messages.

- The Pbst Office Protocol (POP), defined in RFC-1225 (May 1991), which provides a simple mailbox retrieval service.
- The Network News T ansfer Protocol (NNTP), defined in RFC-977 (February 1986), which provides store-and-forward service for news messages.
- The Domain Name System (DNS), defined in RFC-1033 (November 1987) ,and RFC-1034 (November 1987), which provides map-ping between host names and network addresses.

In terms of the generic protocols described earlier, RFC-822 corresponds to the messaging protocol and SMTP corresponds to the relaying protocol. In the Internet suite, submission and delivery are local matters.

Shows how different business applications support different protocols depending on usage."



Business applications Vs Different protocols.

9. How does e-mail work? Explain. (Apr 2013)

Figure depicts how e-mail works. Basically, two architectures are involved in this diagram. The first architecture is commonly referred to as a file-based system. In this architecture, the mail client creates a file containing the message header, text, and pointers to attachments and posts it to a directory on a post office server.

Next, message-transport software, usually hosted on another PC, uses TCP/IP transport capabilities to route messages from post office to post office, as needed. The recipient's e-mail client periodically polls the local post office server's directory and notifies

the user when new mail arrives. The second example is the more popular client/server architecture.

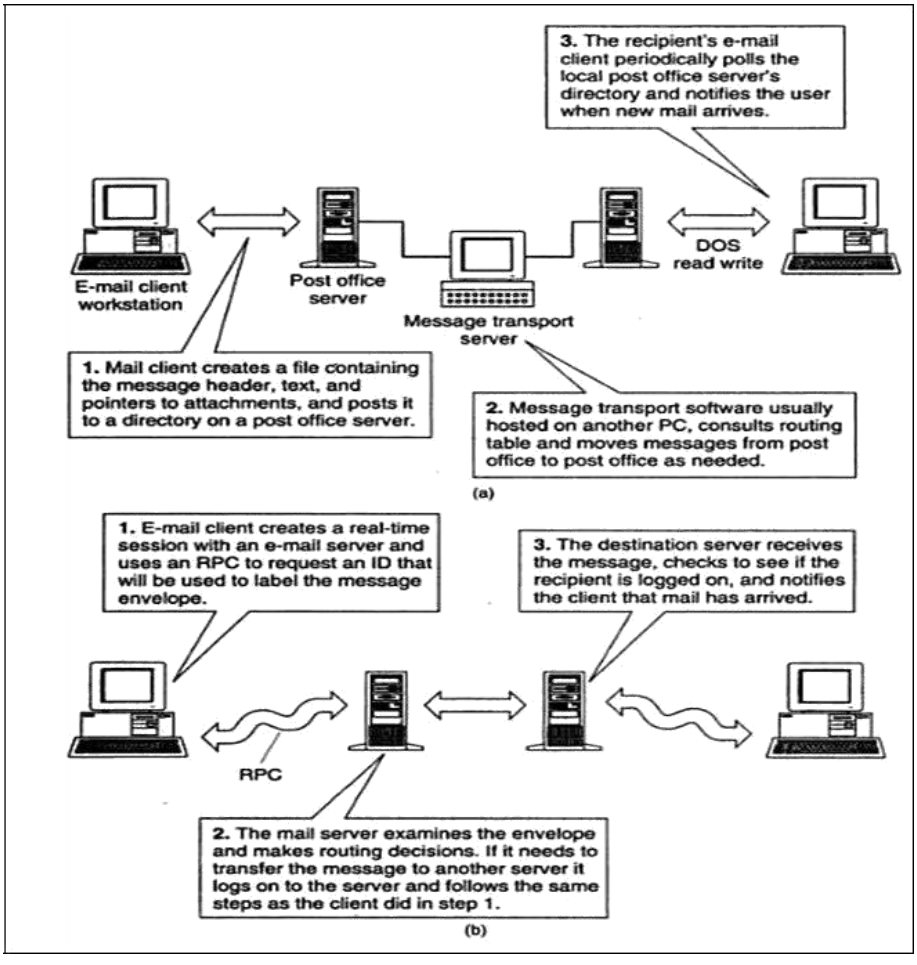
Here, the first step involves the e-mail client workstation creating a real-time session with an e-mail server and using a remote procedure call (RPC) to request an ID that will be used to label the message envelope. Next, the mail server examines the envelope and makes routing decisions. If it needs to transfer the message to another server, it does. The destination server receives the message, checks to see if the recip - ient is logged on, and notifies the client that mail has arrived. "Two basic components of an Internet e-mail message are the header and the body. The header requires the following lines:1z"

- **Delivery-Date:** This line shows the date and time the message was received in the mailbox.
- **Return-Path:** This line shows the reply address of the original sender.
- **Received:** Every entry in the header starting with Received represents a computer/gateway that has transferred the message, also referred to as a hop. If there are too many hops, the message will be bounced, or returned, to the original sender. A message will also bounce if the person is no longer found at that mail system.
- **Date:** This line shows the date and time the message left the sender. This will vary by several seconds or minutes from the delivery date line.
- **From:** This line specifies the full name and e-mail address of the original sender.
- **Message-ID:** This line serves as a unique identifier of each mail message. It includes the name of the machine sending the message, the date, time, and file name.
- **To:** Each person receiving the message will appear on this line. If there is more than one address, the addresses will be separated by a comma.
  - Some e-mail systems may add these lines at the Internet gateway and may not be transparent to the sender. Most e-mail systems will also add the following lines, even though they are not required: subject, content type, and priority status.
  - Internet e-mail addresses are made up of two parts: the user name and domain name. The user name is the account from which a message is sent. Some systems use the person's last name, while others use an alias which shields the name from the recipient. The domain name is an alphabetical mnemonic.
  - Machines use the IP number assigned by the InterNlC to every machine or network connected to the Internet. (Note: The InterNIC assigns and organizes domains and addresses, maintains directories of Internet users, and provides information for connection to the Internet.) A special (set of) computer(s), known as the Name Server, uses DNS (Domain Naming System) to convert the domain name into the proper IP address.
  - For example, an Internet address is denise_derkacs@merck.com. The user name is denise derkacs. The domain name is merck.com.

The last identifier in the domain name, .com, identifies this address as an ad-dress on a commercial organization's mail system. Other classical domain identifiers are

- .edu for educational institutions
- .gou for federal governmental offices or organizations
- .org for any other address that does not fall into the previous identifiers-usually nonprofit organizations

Figure: How E-Mail works three staps to mail delivery: (a) File-Based systems; (b) Client/Server-Based systems.



- Addresses outside the United States will append a two-letter country identifier, such as.ca (Canada).
- To send a message on a mail system, one needs to specify where the message is being sent. Let us take, for example, a message one sends to a user on the Rutgers University mail system, thatch@eden. rutgers.edu.

After the message has been written and the address is entered, the sender's MTA starts the sending process.

- The MTA first spools/queues the message to a directory on the machine that is running the transfer. This is to prevent the loss of the message, in case the machine is busy and one needs to try again. (Spooling messages is the same concept used in spooling print jobs on a busy public printer: the print job stays in the queue until the printer is ready to handle it.)

- This entire process takes place in only a few seconds. The protocol that allows these two machines to talk to one another about e-mail is SMTP. This protocol is often used on large systems, but can also be used by an MTA to connect smaller LANs to the Internet.
- SMTP gateways are typically referred to as Internet gateways. The SMTP gateway software allows users on a LAN-based mail system to send and receive Internet mail. The gateway software allows the transmission of Internet messages, transparent to the sender.
- The SMTP gateway translates the message to the acceptable RFC-822

format and then transfers the message to the TCP/IP transport system which will send the message to its final destination.12^{-2}2 The SMTP gateway also listens to the Internet for messages being sent to its LAN-based e-mail system. It translates the incoming message from the RFC-822 format to the format recognized by the local e-mail system. There are several ways in which attachments are handled. Some SMTP gateways support UUEncoded files and/or MIME attachments.

- In the early 1990s, the RFC-1425 (1993) extended the SMTP protocol to become ESMTP (Extended SMTP). The main reason for this extension was to allow the transmission of 8-bit binary files in addition to the 7-bit ASCII in e-mail messages. This allows programs, word processor files, and other application files to be transmitted over e-mail systems. SMTP will sometimes clear the eighth bit off every character to reduce it to an acceptable 7-bit format.

UUENCODE/UUDECODE:

- UUEncoding was created as a simple program to be used between a small group of users exchanging information on UNIX systems. The most common way to accomplish the transferring of 8-bit binary files to the •7-bit format was to use UNIX-to-UNIX Encoding (UUEncode).
- Some mail systems support UUEncoding and will automatically trans-late the data for the recipient. To avoid confusing and wasting the time of an e-mail recipient, one should include a statement letting the recip-ient know the attachment is UUEncoded.

10.Explain about MIME and data encoding techniques (Apr 2014)

MIME: Multipurpose Internet Mail Extensions

Multipurpose Internet Mail Extensions (MIME) (RFC-1521) provides Internet e-mail support for messages containing formatted text, sound images, video, and attachment. MIME is backward-compatible with SMTP messaging specifications and is easier to implement.

- Common way in which binary files are sent as e-mail on the internet.
- Content types are
  1. Primary type – indicates general content of the material
  2. Subtype – indicates the specific format
- Five basic primary MIME content-types are text, image, audio, video, and application.
- Composite MIME content types:
  1. Message – one can send the message inside another message, labeling it message/rfc822.
  2. Multipart – allows more than one piece of MIME to be included in a message.
     Eg: multiple objects, multipart/parallel, and multi-part/alternative.

- **MIME encoding:**
  - Uses many different encoding methods, depending on the file type it is sending.
  - MIME provides the ability to encapsulate different content types within the body of the message. With the MIME specification, RFC-1351, the internet was only able to transmit and receive ASCII type data. If one wants to send binary data, one had to convert it to ASCII-type data.

- The RFC-1521 version of MIME added the ability of Internet e-mail to handle binary and text data, as well as multiple body parts without conversion to ASCII.

An internet electronic mail message consists of two parts:

- The header
- The body

The header form a collection of field/value pairs structured is defined according to MIME.

The multipart/signed content type contains two body parts:

- The first body part is the body part over which the digital signature was created, including its MIME headers. It may contain valid MIME content type.
- The second body part contains the control information necessary to verify the digital signature.

Message Integrity Check (MIC)

The Message Integrity Check (MIC) is the name given to the quantity computed over the body part with a message digest or hash function, in support of the digital signature service.

The framework is provided in RFC-1847 by defining two new security subtypes of the MIME multipart content type: signed and encrypted.
In each of the security subtypes, there are two related body parts:

1. One for the protected data and
2. One for the control information.

The multipart/signed content type specifies how to support authentication and integrity services via digital signature. The control information is carried in the second of the two required body parts.
When creating a multipart/signed body part, the following sequence of steps describes the processing necessary:

1. The content of the body part is prepared according to a local convention. The content is then transformed into a MIME body part in canonical MIME format, including MIME headers.
2. The body part to be digitally signed is prepared for signature according to the value of the protocol parameter. The headers are included in the signature to protect the integrity of the MIME labeling of the data that is signed.
3. The body part is made available to the signature creation process, which made available to a MIME implementation two data streams:

- The control information necessary to verify the signature.
- The digitally signed body part.

When receiving a multipart/signed body part, the steps describes the processing to verify signature.

1. The first body part and the control information in the second part must be prepared for the signature verification process according to the value of the protocol parameter.
2. The prepared body parts must be made available to signature verification, then to the MIME implementation of the signature verification and the body part that was digitally signed.
3. The result is made available to the user and the MIME implementation continues processing with the verified body part.

When creating a multipart/encrypted body part, the following steps are required

1. The contents are prepared and transformed into a MIME body part in canonical MIME format, including MIME headers.
2. Then the body part is prepared for encryption according to the value of the protocol parameter.
3. The prepared body part is made available to the encryption process according to local convention, then to MIME implementation two data streams

   - The control information necessary to decrypt the body part
   - The encrypted body part.

When receiving a multipart/encrypted body part, the following steps are required.

1. The second body part and the control information in the first body part must be prepared for the decryption process according to the value of the protocol parameter.
2. The prepared body must be made available to the decryption process according to a local convention. The decryption process must make available to the MIME implementation.
3. The result is made available to the user and the MIME implementation continues processing with the decrypted body part.

MIME body parts

MIME specifications currently support seven body types:

1. Text,
2. Multipart,
3. Application,
4. Message,
5. Image,
6. Audio,
7. Video.

I) Text:

The text body part enables a message to contain simple message data such as ASCII and can be transported using the current 7-bit message content specified within MIME.

The richtext subtype is used to handle simple text format protocols that support boldfacing, italicizing, indenting, and so on. The richtext protocols are a reduced subset of the Standard Generalized Markup Language(SGML) commands. Two categories of character set are supported:

1. Charsert=US-ASCII
2. ISO-8859-1 through ISO-8859-9.

AI) Multipart:

This part consists of several body parts containing unrelated data. The contents are divided into subtypes.

The four initial subtypes are mixed, alternative, parallel, and digest. Only 7-bit, 8-bit, or binary may be used for the content type encoding.

Mixed: It ensures that a number of very different message content types, such as text, graphics, or images, can be transmitted in the same message.

Alternative: This subtype presents the same data in different formats, such as a word processing document in three representations such as ASCII, word for windows, and word perfect. **Parallel:** This subtype contains body parts that must be viewed at the same time.

Digest: This subtype is used when all the body parts are messages in their own right. It is important that an e-mail gateway interpret that the message body is a nested message as opposed to a video image or graphic.

- **Message:** It contains other messages, such as forwarded or transferred messages. It is the most basic body part in MIME and its subtypes are as follows:
- **RFC-822:** primary and most frequently used subtype, is the specification for a complete standard Internet e-mail message.
- **Partial:** It allows messages to be sent in parts through the e-mail networks. It is necessary when the message has exceeded the 64-KB.
- **External-Body:** It is for specifying larger data files, such as text, video, audio, or others that are not contained within the message.

- **Image:** It contains time varying images or images that contain movement-like motion picture and full motion video.

The current subtypes are

1. MPEG motion picture experts group – standard for digitally compressing movies.
2. GIF – compuServ's Graphic Image Format.

- **Audio:** It contains sound data such as voice or music. The basic subtype indicates 8-bit, integrated services digital network(ISDN), with a sample rate of 8000Hz.
- **Application:** It contains spreadsheets, calendar information, word processing documents, and presentation formats such a word perfect or Microsoft word. Its current subtypes are ODA-Office Document Architecture.
- **Postscript:** It defined by Adobe Systems and supports high-quality postscripts printer output. It should not be used with nonprinter interpreters.

MIME data encoding techniques:

The current SMTP network only supports 7-bit ASCII, up to 1000 characters per line of data, and a normal message length of 64KB.

ESMTP supports binary data exchange.

The RFC-821(SMTP) –compliant networks will not handle binary data contained in the MIME structure.

RFC-1521 specifies that the body of the message can be encoded in a form that will be transportable by the SMTP network. A new field called Content-Transfer-Encoding has been added to the header of the RFC-822 message. It may have one of the following six different encoding values:

Base64

It is for any series of octets and is used in Private Enhanced Messaging(PEM), specified in RFC-1113. Binary input strings are converted to a series of 65 ASCII characters which are the only ones that are represented the same in ISO 646, US ASCII, and EBCDIC.

8-bit

Eight bit means that lines are of the same form as they are in 7-bit encoding. It also means that the body has not been encoded.

Binary

Binary means that there is not a line length limit within the message. It also means that the body has not been encoded.

Quoted printable encoding

This encoding value is for data that generally uses an ASCII character set. It allows unsophisticated MTAs to convey data, the format of which may be a little off, readable by the end user.

7-bit:

Seven-bit is the default value when the Content-Transfer-Encoding header field is not present in the header. This means that the data is of the type specified in RFC-821,7-bit US ASCII code, and has not been encoded.

x-token

This value is for defining a nonstandard encoding which has been put in place by mutual agreement between the parties to the transfer.

Address directory

The SMTP architecture does not define an address directory. Users find names by enrolling in distribution lists, using a utility program called FINGER to search on their system and a query facility called WHOIS to find addresses. ITU-T X.500 directory services are also expected to become available.

11.Explain S/MIME (Apr 2013)

S/MIME was designed to add security to e-mail messages in MIME format. The security services offered are authentication (using digital signatures) and privacy (using encryption).

S/MIME joins crypto-graphic constructs with standard e-mail practices and was designed to be interoperable, so that any two packages that implement S/MIME can communicate securely.

S/MIME is a specification for secure electronic mail. S/MIME was designed to add security to e-mail messages in MIME format. The security services offered are authentication using digital signatures and privacy using encryption.

Need for S/MIME:

There is a growing demand for e-mail security. S/MIME melds proven cryptographic constructs with standard e-mail practices. More importantly, it was designed to be interoperable, so that any two packages that implement S/MIME can communicate securely.

How does SIMIME compare with PGP and PEM?

S/MIME PGP, and PEM all specify methods for securing electronic mail. All offer privacy and authentication services. Since PGP and PEM are all different, they need to be compared with S/MIME individually.

PGP can be thought of as both a specification and an application. PGP relies on users to exchange keys and establish trust in each other.

Cryptographic Algorithms In S/MIME

Hybrid approach to providing security often referred to as envelope. The bulk message encryption is done with a iq cipher, and a public-key (asymmetric encryption) algorithm key exchange.

A public-key algorithm is also used features. S/MIME recommends three symmetric encryption DES,32 Triple-DES, and RC2.

Does S/MIME use digital certificates?

S/MIME does use digital certificates. The X.509 format is used due to its wide acceptance as the standard for digital certificates.19 VeriSign has set up a hierarchy specifically to support the S/MIME effort.

Does S/MIME only work on the Internet?

S/MIME is not specific to the Internet and can be used in any electronic mail environment. This is accomplished by making the implementation guidelines flexible and scalable.

Is a public domain implementation of S/MIME available?

A free version of S/MIME was planned to be available soon. A future version of the popular public domain mailer RIPEM will implement S/MIME.

RIPEM is a program developed by Mark Riordan that enables Internet e-mail. RIPEM provides both encryption and digital signatures. RIPEM is free for noncommercial use.

12.Expalin MOSS: Message Object Security Services

- MIME Object Security Services (MOSS), defined in RFC-1848,37 is a protocol used to apply digital signature and encryption services to MIME objects.
- The services are offered through the use of end-to-end cryptography between an originator and a recipient, at the application layer. This protocol is needed since MIME itself does not provide for the application of security services.

- MOSS is a protocol that uses the multi- part/signed and multipart/encrypted framework to apply digital signature and encryption services to MIME objects2-20 MOSS can be thought of as a framework rather than a specification, and consider-able work in implementation profiling has yet to be done. MOSS is new at the time of this writing.

- MOSS uses a framework of security services defined in RFC-1847 to be applied to MIME body parts.
- In each of these subtypes, there are two related body parts: one for the protected

- data and one for the control information.
- MOSS is based in large part on the Privacy Enhanced Mail protocol. PEM is message encryption and message authentication for text based electronic mail messages. It uses a certified key management procedure Several specifications of PEM are supported by MIME.
- **For example**, the transfer encoding operation and the content- domain header
- The private key is used to digitally sign MIME objects. The recipient of the message uses the stored originator as public key to verify the digital signature. The recipient's public key is used to encrypt the data-encrypting key that is used to encrypt the MIME object; a recipient uses the corresponding private key to decrypt the data-encrypting key in order to decrypt the MIME objects.

MOSS services-overview

- The MOSS digital signature service. The MOSS digital signature service requires two components the data to be digitally signed and the private key of the originator.
- The digital signature is created by generating a hash of the data and encrypting the hash value with the private key of the message originator.
- The digital signature, some supplemental information, and the data are incorporated into a multipart/signed body part. This multipart/ signed body part may be

processed further when transferred to the recipient-it may become encrypted. To apply the digital signature service, the following sequence of events must take place.

1. The body part to be signed must be converted to a canonical form that is uniquely and unambiguously represented in both the environment in which it was created and the environment in which it will be verified.

The canonicalization transformation takes place in two steps: (1) the body part must first be converted to a form that is unambiguously representable on many different host computers; (2) the body part must have its line delimiters converted to a unique and unambiguous form. The digital signature service requires the originator and the recipient to use the same line delimiter.

2. The digital signature and other control information must be generated. Some control information that is generated by the digital signature service is a version of the MOSS protocol, originator-ID and the MIC header.

3. The control information must be incorporated in an appropriate MIME content type. The application/moss-signature content type is used on the second body part of an enclosing multipart/signed. It must include the digital signature of the data in the first body part of the enclosing multipart/signed and the other control information required to verify the signature.

4. The control information body part and the data body part must be incorporated in a multipart/signed content type. The multipart/ signed content type is created as follows:

a. the value of its required parameter protocol is set to application/moss-signature;

b. the signed body part becomes its first body part;

c. its second body part is labeled application/moss-signature and is filled with the control information generated by the digital signature service; and

d. the value of its required parameter micalg is set to the same value used in the MIC-Info: header in the control information.

The MOSS encryption service

The MOSS encryption service requires three components:

The data to be encrypted, a data encrypting key to encrypt the data, and the public key of the recipient.

The originator creates a data-encrypting key and encrypts the data.

The recipient's public key is used to encrypt the data-encrypting key.

To apply the encryption service, the following events must take place:

1. The body part to be encrypted must be in MIME-compliant form.

2. The data-encrypting key and other control information must be generated. The application of the encryption service generates control information which includes the data-encrypting key used to encrypt the data itself. The syntax of the control information is that of a set of RFC-822 headers, except that the folding of header values onto continuation lines is forbidden.

3. The control information must be incorporated into an appropriate MIME content type. The application/moss-keys content type is used on the first body part of an enclosing multipart/encrypted. Its content is comprised of the data encryption key used to encrypt the data in the second body part and other control information required to decrypt the data.

4. The control information body part and the encrypted data body part must be incorporated into a multipart/encrypted content type. The definition of the multipart/encrypted body part in RFC-1847 specifies three steps for creating the body part:

a The body part to be encrypted is created according to a local convention, for example, with a text editor or a mail user agent.

b. The body part is prepared for encryption according to the protocol parameter; in this case, the body part must be in MIME canonical form.

c. The prepared body part is encrypted according to the protocol parameter.

The multipart/encrypted content type is constructed as follows:

- The value of its required parameter protocol is set to application/moss-keys.
- The first body part is labeled application moss-keys and is filled with the control information generated by the encryption service.
- The encrypted body part becomes the content of its second body part, which is labeled application/octet-stream.

Definition of security subsystem:

Multipart/Signed – this type specifies how to support authentication and integrity services via digital signature. There are three required parameters: boundary, protocol and micalg. The content type contains two body parts: the first one contains the body over which the digital signature was created, including its MIME headers, and the second body part contains the control information necessary to verify the digital signature. The second body part is labeled according to the value of the protocol parameter.

In support of the digital signature service there is a quantity computed over the body part with a message digest or hash function. It is called MIC and is part of the definitions of RFC1421, Privacy-Enhanced Mail.29

Creating process of multipart/signed. The following sequence is descriptive of the activities involved and is an amplification of the description in the previous section.

1. The content of the body part to be protected is prepared according to a local convention (i.e., text editor or local user agent) and is then transformed into a MIME body part in canonical format, including the appropriated MIME headers. In addition, the body is constrained to 7 bits, considering the restrictions of the standard Internet SMTP infrastructure. Binary material must be encoded
using quoted-printable or base64 encoding.

2. The body part (headers and content) to be digitally signed is prepared for signature according to the value of the protocol parameter.

3. The signature is created according to a local convention, and the process must make available to a MIME implementation two data streams: the control information necessary to verify the signature, which will be placed in the second body part, and the digitally signed body part, which will be used as the first body part.

Receiving and verifying process of multipart/signed. The following sequence is descriptive of the activities involved and is an amplification of the description in the previous section.

1. The first body part and the control information in the second body part must be prepared for the signature verification process according to the value of the protocol parameter.

2. The prepared body parts must be made available to the signature verification, process according to a local convention. The signature verification process must make available to the MIME implementation the result of the signature verification and the body part that was digitally signed.

3. The result of the signature verification process is made available to the user and the MIME implementation continues processing with the verified body part, that is, the body part returned by the signature verification process.

Multipart/encrypted: This type contains two body parts.

i) The first one contains the control information necessary to decrypt the data in the second body part and is labeled according to the value of the protocol parameter.

ii) The second body part contains the data which was encrypted and is always labeled application/octet-stream.

It has two required parameters: boundary and protocol.

Creating process of multipart/encrypted. The following sequence is descriptive of the activities involved and is an amplification of the description in the previous section.

1. The contents of the body part to be protected is prepared according to a local convention. The contents are then transformed into a MIME body part in canonical MIME format, including an appropriate set of MIME headers.

2. The body part (headers and content) to be encrypted is prepared for encryption according to the value of the protocol parameter. The MIME headers of the encrypted body part are included in the encryption to protect from disclosure the MIME labeling of the data that is encrypted.

3. The prepared body part is made available to the encryption process according to a local convention. The encryption process must make available to a MIME implementation two data streams: the control information necessary to decrypt the body part, which the MIME implementation will place in the first body part and label according to the value of the protocol parameter, and the encrypted body part, which the MIME implementation will place in the second body part and label application/octet-stream.

Thus, when used in a, multipart/encrypted, the application/octet-stream data is comprised of a nested MIME body part.

Receiving and verifying process of multipart/encrypted. The following sequence is descriptive of the activities involved and is an amplification of the description in the previous section.

1. The second body part and the control information in the first body part must be prepared for the decryption process according to the value of the protocol parameter.

2. The prepared body parts must be made available to the decryption process according to a local convention. The decryption process must make available to the MIME implementation the result of the decryption and the decrypted form of the encrypted body part.
3. The result of the decryption process is made available to the user and the MIME implementation continues processing with the decrypted body part, that is, the body part returned by the decryption process.

APPLICATION (13.Discuss about Application of MIME Object Security Services.(Apr 2014))

MOSS is based in large part on the Privacy Enhanced Mail protocol as defined by RFC-1421/1422/1423, which defines message encryption and message authentication procedures for text-based electronic mail messages using a certificate-based key management mechanism.

In order to make use of the MOSS services, a user is required to have at least one public/private key pair. The public key must be made available to other users with whom secure communication is desired.

An originator's private key is used to digitally sign MIME objects; a recipient would utilize the originator's public key to verify the digital signature. A recipient's public key is used to encrypt the data encrypting key that is used to encrypt the MIME object; a recipient would utilize the corresponding private key to decrypt the data encrypting key so that the MIME object can be decrypted. The ownership of the public keys used in verifying digital signatures and encrypting messages should be verified. A stored public key should be protected from modification.

The framework defined in RFC-1847 provides an embodiment of a

MIME object and its digital signature or encryption keys. When used by MOSS, the framework provides digital signature and encryption services to single and multipart textual and non-textual MIME objects.

LDigital signature service:

The verification of the MOSS digital signature service requires the following components:

- A recipient to verify the digital signature
- A multipart/signed body part with two body parts: the signed data and the control information
- The public key of the originator

The digital signature is verified by recomputing the hash of the data decrypting the hash value in the control information with the originator's public key, and comparing the two hash values. If the two hash values are equal, the signature is valid.

The definition of the multipart/signed body part in RFC-1847 specifies three steps for receiving it:

1. The digitally signed body part and the control information body par are prepared for processing.
2. The prepared body parts are made available to the digital signature verification process.
3. The results of the digital signature verification process are made available to the user and processing continues with the digital, signed body part, as returned by the digital signature verification process.

Encryption service:

The decryption of the MOSS encryption service requires the following components:

- A recipient to decrypt the data

- A multipart/encrypted body part with two body parts: the encrypt data and the control information
- The private key of the recipient

The data-encrypting key is decrypted with the recipient's private key and used to decrypt the data. The definition of the multipart/encrypted body part in RFC-1847 specifies three steps for receiving it:

1. The encrypted body part and the control information body part prepared for processing.

2. The prepared body parts are made available to the decrypted process.

The results of the decryption process are made available and processing continues with the decrypted body part and key by the decryption process. Identifying originators, recipients, and their keys. In the PEM specifications, public keys are required to be embodied in certificates, objects that bind each public key with a distinguished name.

In MOSS, a user is not required to have a certificate. The MOSS ser-vices require that the user have at least one public/private key pair.

The MOSS protocol requires the digital signature and encryption services to transmit the Originator-ID: and Recipient-ID: headers, as appropriate.

MOSS allows other identifiers in Originator-ID: header and Recipient-ID: header. These other identifiers are comprised of two parts:

1. a name form and
2. a key selector.

Since a user may have more than one public key and may wish to use the same name form for each public key, a name form is insufficient for uniquely identifying a public key. Hence, a unique key selector must be assigned to each public key. The combination of a name form and the key selector uniquely identifies a public key. This combination is called an identifier.

With a public/private key pair for a user and software that is MOSSaware, an originating user may digitally sign arbitrary data and send it to one or more recipients.

Key management content types:

RFC-1848 defines two key management content types: one for requesting cryptographic key material and one for sending cryptographic key material.

Key management functions are based on the exchange of body parts. Two content types are used:

- application/mosskey-request Content Type:

A user would use this is content type to specify needed cryptographic key information. The application/mosskey-request content type is an independent body part because it is entirely independent of any other body part. One possible response to receiving an application/mosskey-request body part is to construct and return an application/mosskey-data body part.

- application/mosskey-data Content Type:

The principal objective of this content type is to convey cryptographic keying material from a source to a destination. This might be in response to the receipt of an application/mosskey-request content type.

Pretty Good Privacy (PGP) :

Pretty Good Privacy (PGP), is a public key encryption system in circulation. PGP uses the RSA (Rivest, Shamir, and Andleman) public-key cryptosystem. PGP supports the following functions:

- Generates public/private RSA keys
- Encrypts messages to be transmitted using the destination's public key
- Decrypts messages received using the recipient's private key
- Authenticates messages with digital signatures
- a Manages key rings that keep track of destination's public keys

All encryption systems security is based on a cryptographic key or the key to the cryptography's electronic lock. Private-key encryption systems, or conventional cryptography, use a single or private key. This private key is used for both encryption and decryption. The sender and recipient of the mail message must share the same key. Public-key systems generate two mathematically related keys. A message encrypted with one key can be decrypted only with the other.

Cryptography is the science of using mathematics to hide or code the meaning of messages. The goal behind cryptography is to make it impossible to take a ciphertext and reproduce the original plaintext without the corresponding key.

The secret key is used to decrypt messages that have been encrypted with an organization's public key. The key is called the secret or private key, since the organization must keep it a secret.

The session key is randomly generated for every message encrypted with PGP's public-key encryption system following is a simplified description of how PGP is used to send an e-mail message:

1. PGP creates a random session key for the message being sent.
2. PGP uses the IDEA (International Data Encryption Algorithm) private-key algorithm to encrypt the message with the session key. This is because encrypting in software the entire message would take extraordinary amounts of computing power. IDEA is an iterated block cipher with 64-bit input and output blocks, with a 128-bit key (DES only has a 56-bit key32).

3. PGP then uses the recipient's public RSA key to RSA-encrypt the session key (not the message itself, as noted in the previous point).
4. PGP bundles the IDEA encrypted message and the RSA-encrypted session key together.

The message is now ready to be sent.

If someone has the organization's public key, that person can send e-mail but cannot read the organization's e-mail. A key certificate is created each time a public key is stored. It contains the public key, one or more user IDs for the key's creator, the creation date, and sometimes a list of digital signatures. The digital signatures would be used to verify that a message was sent by the person who matches the digital signature. These public keys are kept in a single file called the key ring (pubring.pgp); the public key ring is like an address book.

The organization also has a secret key ring that contains the organization's secret Key.

Problem with the public key:

The availability of public keys has one problem. If someone were to replace the organization's listed public key, with his or her own public key, that person would be able to intercept and read any messages sent to the organization. The intruder could then reply to the messages and re-encrypt the messages with the organization's public key.

The only way to prevent such a problem is to use a digital signature. The digital signature encrypts a special number into the information of the file. The number is checked against the original message and the public key of the sender. If the numbers match, the message has not been modified since it was signed and transmitted. If the numbers do not match, the message has been modified and the recipient is notified.

Encrypted data is binary data, which cannot be sent by standard electronic mail. The ASCII Armor encoding actually uses four ASCII characters to represent three binary, characters.

Some of the standard file extensions are as follows:

.txt - is attached to files created by a text editor or word processor before the file is encrypted.

.Pgp - is attached to an encrypted binary file. It is also used for key rings.

.asc - is attached to an ASCII-armored encrypted file.

.bin - is crated when you use PGP's key-generate option. It is used for the randseed.bin file, which stores the seed for PGP's random number generator.

Pondicherry University Questions

2 MARKS

1. What are the key pairs used in SET? **(Apr 2012) (Ref.Qn.No.34)**
2. What is a MIME? **(Apr 2012) (Ref.Qn.No.12)**
3. Mention the objectives of payment security. **(Nov 2012) (Ref.Qn.No.5)**
4. List the internet protocols related to mail specific applications. **(Nov 2012) (Ref.Qn.No.35)**
5. Difference between master card and visa **(Apr 2013) (Ref.Qn.No.36)**
6. What is S/MIME? **(Apr 2013) (Ref.Qn.No.22)**
7. Write a short note Uudecode?**(Apr 2014) (Ref.Qn.No.32)**
8. Write a note on cryptography?(**Apr 2014) (Ref.Qn.No.33)**
9. Define Email?(**Nov 2014)(Apr 2015) (Ref.Qn.No.15)**
10. What is the use of MIME? (**Nov 2014)(Apr 2015) (Ref.Qn.No.27)**

11 MARKS

1. Discuss the objective of bank card associations. **(Apr 2012) (Ref.Qn.No.1)**
2. Explain in detail about MIME. **(Apr 2012)(Apr 2014)(Nov 2014) (Nov 2012)(Apr 2015) (Ref.Qn.No.10)**
3. Discuss about the business requirements. **(Nov 2012) (Ref.Qn.No.2)**
4. Explain about S/ MIME in detail. **(Apr 2013) (Ref.Qn.No.10)**
5. How does e-mail work? Explain in detail. **(Apr 2013) (Ref.Qn.No.9)**

6. Describe the message object security services in detail**.(Apr 2014)(Ref.Qn.No.12)**
7. Explain the basic aspects of payment processing.**(Nov 2014)(Apr 2015)(Ref.Qn.No.6)**