Biyani's Think Tank

Concept based notes

E-Banking and Security Transaction

BCA Part-III

Pratibha Pathak
Revised By: Ms Ekta Sharma
Lecturer
Deptt. of Information Technology
Biyani Girls College, Jaipur

Published by :
Think Tanks
Biyani Group of Colleges

Sector-3, Vidhyadhar Nagar,
Jaipur-302 023 (Rajasthan)
Ph : 0141-2338371, 2338591-95 • Fax : 0141-2338007
E-mail : acad@biyanicolleges.org
Website :www.gurukpo.com; www.biyanicolleges.org

ISBN: 978-93-82801-82-5

Edition : 2011
Price:

Leaser Type Setted by :
Biyani College Printing Department

Preface

I am glad to present this book, especially designed to serve the needs of the students. The book has been written keeping in mind the general weakness in understanding the fundamental concept of the topic. The book is self-explanatory and adopts the "Teach Yourself" style. It is based on question-answer pattern. The language of book is quite easy and understandable based on scientific approach.

Any further improvement in the contents of the book by making corrections, omission and inclusion is keen to be achieved based on suggestions from the reader for which the author shall be obliged.

I acknowledge special thanks to Mr. Rajeev Biyani, *Chiarman* & Dr. Sanjay Biyani, *Director (Acad.)* Biyani Group of Colleges, who is the backbone and main concept provider and also have been constant source of motivation throughout this endeavour. We also extend our thanks to Biyani Shikshan Samiti, Jaipur, who played an active role in co-ordinating the various stages of this endeavour and spearheaded the publishing work.

I look forward to receiving valuable suggestions from professors of various educational institutions, other faculty members and the students for improvement of the quality of the book. The reader may feel free to send in their comments and suggestions to the under mentioned address.

Author

Syllabus

E-Banking and Security Transctions

Introduction : Defination, Transaction websites components, E-Banking support services, Wireless Banking.

E-Banking Risk : Transaction/Operation Risk, Credit Risk, Liquidity/Internet Risk, Price Risk, StrategicRisk, ReputationRisk.

Risk Management of E-Banking Activities : Board of Management oversignt, Managing outsourcing realtionship, Information security Program Administrative control, Legal and compliance Issue.

Laws regulation and guidelines: Electronics money, Regulating e-transactions, Role of RBI and Legal issues, Transnational transactions of E-Cash, Credit Card and Internet, Laws relating to Internet credit cards, Secure Electronic Transtions.

E-security: Introduction to New Challenges and new Threats, Secuirty, Legal consideration.

Content

S.No	Topic
1	Introduction to E- Banking
2	Wireless Banking
3	E-Banking Risk
4	Risk Management of E-Banking Activities
5	Laws regulation and guidelines
6	E-security
7	Unsolved Papers 2010 - 2006

Chapter 1

Introduction to E-Banking

Q.1 What is E-Banking?

Ans. E-banking is the combination of traditional banking and Information Technology. "E-banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels."

Q.2 What is meant by account aggregation?

Ans. Account aggregation is a service that gather information from many websites, presents that information to the customers in a consolidated format, and in some cases, may allow the customer to initiate activity in the aggregated accounts.

Account aggregation is the ability to view and manage online accounts in one central location or one web page. This includes financial information from online accounts with multiple financial institutions such as banks, credit and companies, brokerage firms, as well as non-financial information accounts such as e-mail, news and travel.

Q.3 Define screen scraping.

Ans. Aggregation services can improve customer convenience by avoiding multiple logins and providing access to tool that help customers analyze and manage their various accounts portfolios. Some aggregation use the customers – provided users IDS and passwords to sign in as the customer. Once the customer's account is accessed, the aggregator copies the personal account information from the website for representation on the aggregator's site (i.e. screen scraping). Other aggregators use direct data-feed arrangements with website operators or other firms to obtain the

customers information. Generally, direct data feeds are through to provide greater legal protection to the aggregation than does screen scraping.

Q.4 Define the website components of E-Banking.

Ans. The e-banking websites can be primarily classified into two categories:

- Informational websites
- Transactional websites

- **Informational Websites :**

Informational websites provide customers access information to general information about the financial institution and its products or services. Risk issues examiners should when reviewing informational websites include.

- **Transactional Websites :**

A transactional websites is a type of website where you can things from, for example, Amazon or eBay. This is connection between the customers and the company, therefore a transaction is being made.

Q.5 Write a short note on credit card.

Ans. Credit Card:

A **credit card** is a small plastic card issued to users as a system of payment. It allows its holder

to buy goods and services based on the holder's promise to pay for these goods and services.

The issuer of the card creates a revolving account and grants a line of credit to the consumer (or the user) from which the user can borrow money for payment to a merchant or as a cash advance to the user.

Credit cards are issued by a credit card issuer, such as a bank or credit union, after an account has been approved by the credit provider, after which cardholders can use it to make purchases at merchants accepting that card.

When a purchase is made, the credit card user agrees to pay the card issuer. The cardholder indicates consent to pay by signing a receipt with a record of the card details and indicating the amount to be paid or by entering a personal identification number (PIN). Also, many merchants now accept verbal authorizations via telephone and electronic authorization using the Internet, known as a card not present transaction (CNP).Electronic verification systems allow merchants to verify in a few seconds that the card is valid and the credit card customer has sufficient credit to cover the purchase, allowing the verification to happen at time of purchase. The verification is performed using a credit card payment terminal system with a communications link to the merchant's acquiring bank.

Multiple Choice Questions

Q1 Development financial institution in India that has got merged with a bank is

A. IDBI
B. ICICI
C. IDFC
D. UTI

Q2. Which is the current revision & year of UCPDC?

A. UCPDC 500, 1993
B. UCODC 400, 1993
C. UCPDC 300, 1973
D. All of the above

Q3. Legal risk arises because of:
A. Violation of laws
B. Non-confirmation with law
C. Legal rights non established
D. All of the above

Q4. TSP helps financial institution of:
A. Manage cost
B. Improve service quality
C. Obtain necessary expertise
D. All of the above

Q5. Which one of the following is a safety measure in banking network?
A. Router
B. Firewall
C. Modem
D. None of the above

Q6. Loss of trust due to unauthorized activity on customer account is concerned with:
A. Reputational risk
B. Liquidity risk
C. Market risk
D. None of the above

Q7. The card by which you cannot buy a product is:
A. Credit card
B. ATM card
C. Debit card
D. Smart card

Q8.Knowing someone else password by certain illegal means is…….

A. Hacking
B. Plagiarism
C. Log on script
D. Password policy

Q9. Which transaction cannot be done by ATM card:

A. Cash withdrawal of 500
B. Cash withdrawal of 350
C. Cash withdrawal of 1000
D. Cash withdrawal of 4000

Q10. PIN in ATM card id of:

A. 4 alphabets
B. 2 alphabets and 2 digits
C. 4 digits
D. None of the above

Chapter 2

Wireless Banking

Q.1 What is wireless banking?

Ans. Wireless banking delivers on the promise of any time, any place access by instantly putting your customers in touch with their accounts and the information they want. Wireless banking is a delivery channel that can extend the reach and enhance the convenience of internet banking products and services. Wireless banking occurs when customers access a financial institution's networks using cellular phones, pages, and personal digital assistants (PDA) though telecommunication companies wireless networks. Wireless banking services in the United States typically supplement a financial institutions e-banking products and services.

Wireless Internet banking, commonly called wireless banking, allows customers to access account information and perform transactions over the Internet using a mobile phone or a personal digital assistant (PDA) instead of a personal computer.

Q.2 How does wireless banking work?

Ans. Before you sign up for wireless banking, you should find out exactly how your mobile phone connects to your bank and verify that your information is secure at all times. Mobile phone service can connect to your bank in a variety of ways. In some cases, your mobile phone uses your Internet service provider to dial up and connect to a Web server located at your bank. Alternatively, you may be given a special access telephone number to dial, and your bank may act as the Internet service provider. In either case, once you are connected, you enter your request using the keypad of your mobile phone or PDA.

Q.3 What additional services may wireless banking provide?

Ans. Wireless banking provides most of the services on-line banking provides, and may also include:

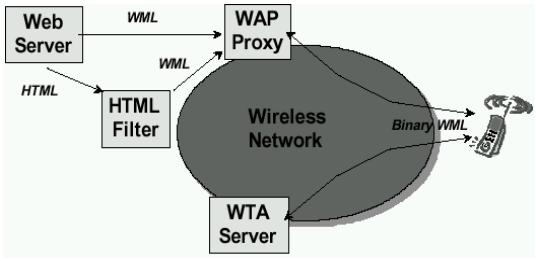
* Information notification and alerts prompting you to view balances, see whether checks have cleared, and receive e-mail messages about deposits and other changes to accounts .
* On-demand transactions allowing you to transfer money from one account to another, make electronic payments, and perform transactions just as in on-line banking, but by using a mobile phone .

Wireless banking involves the same security and privacy issues as on-line banking with a PC. Unlike PCs, however, mobile phones and PDAs are small and easily lost or stolen, making it even more important that a password be required to access account information or perform transactions. In addition, check to ensure that the information being sent to you is encrypted.

Q.4 What is Wireless Application Protocol (WAP)?

Ans. Wireless Application Protocol (WAP) is the emerging connectivity method that gives your customers secure wireless access to a wider array of information from the World Wide Web. Recognizing the need for standardization of mobile technology several leading manufactures. Wireless network operators and software providers, now known as the WAP forum, created WAP as a wireless specification for multiple phone technologies, pages, two-way radios, smart phones and communications.

WAP Architecture:-



Wireless application protocol (WAP) is an application environment and a set of communication protocols for wireless devices designed to give manufacturer, vendor,

and technology-independent access to the Internet and advanced telephony services. The wireless industry came up with the idea of WAP. The point of this standard was to show internet contents on wireless clients, like mobile phones.

WAP is an **application communication protocol.**

WAP is used to **access services and information.**

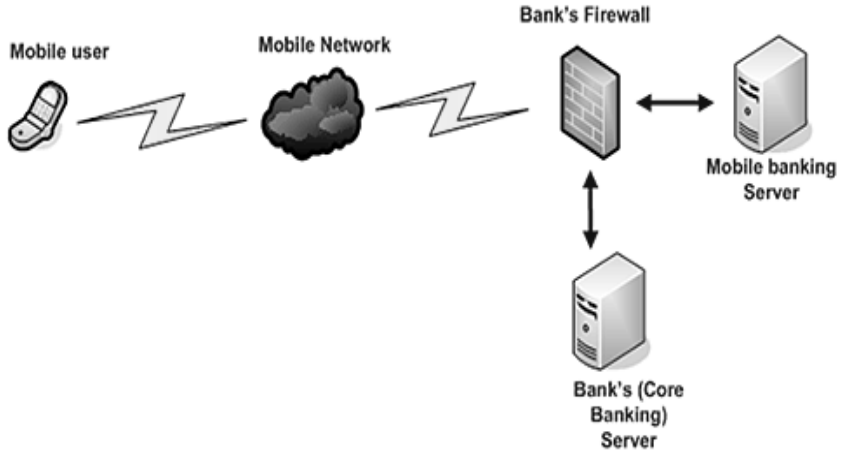
WAP is **inherited** from Internet standards.

WAP is for **handheld devices** such as **mobile phones.**

WAP is a **protocol** designed for **micro browsers**

WAP enables the creating of **web applications** for mobile devices.

WAP uses the **mark-up language WML** (not HTML).



The Wireless Application Protocol

The WAP protocol is the leading standard for information services on wireless terminals like digital mobile phones. The WAP standard is based on Internet standards (HTML, XML and TCP/IP). It consists of a WML language specification, a WMLScript specification, and a Wireless Telephony Application Interface (WTAI) specification.

Multiple Choice Questions

1. You have a credit limit of Rs.50,000 on your credit card, you have purchased readymade garments of Rs. 40,000 in the current month. How much more money can you use for purchasing from your credit card:
   (a) **Rs. 10,000**
   (b) Rs. 5,000
   (c) Rs. 50,000
   (d) None ( )

2. What is true about electronic money:
   (a) **Both bank and customers would have public key encryption keys**
   (b) Only bank has public key encryption keys
   (c) Only customers have public key encryption keys
   (d) No one has public encrypting keys ( )

3. The liability of the credit card holder on loss of the credit card is:
   (a) Unlimited
   (b) Up to credit limit
   (c) **Up to the time, matter is reported to the issuing bank**
   (d) Till two days after the matter reported to the bank ( )

4. For which card one has to made advance payment:
   (a) **Credit Card** (b) Debit Card
   (c) Smart Card (d) Gold Card ( )

5. The primary type of website used for E-banking
   (a) Information (b) **Transaction**
   (c) Both a and b (d) None of the above ( )

6. Transactional E-Banking is typically a front end system. That realises on a programming like called:
   (a) **Inter phase**
   (b) Interlink
   (c) Inter join
   (d) None of the above ( )

7. The most common payment especially for low value puchase, is made by:
   (a) **Debit card** (b) Credit card
   (c) Cash (d) ATM ( )

8. In credit card what is the grace period of payment?

(a) 10-15 days
(b) 5-20 days
(c) **15-45 days**
(d) 1-2 days ( )

9. Who can pass the law for e-banking?
(a) SBI (b) Parliament
(c) **RBI** (d) Merchant Association ( )

10. The customer access E-banking services using:
(a) PC
(b) PDA
(c) ATM
(d) **All of the above**

Chapter 3

E-Banking Risk

Q.1 Describe various e-banking Risks?

Ans. E-banking risk can be categorized as:

•Transactional or Operational Risk

•Credit Risk

•Liquidity or Interest Rate / Price Risk

•Reputation Risk

•Compliance / Legal Risk

•Strategic Risk

•**Transactional or Operational Risk** :

E-banking involves several specific operational risks. One operational risk mainly relates to the security system and transactions, including data confidentially and authentication of the parties involved. Another operational risk refers to the continuous availability of the internet as a medium for financial transactions.

• **Credit Risk** :

Credit Risk is that a counter party will not settle an obligation for full value, either when due or at any time thereafter. Banks may not be able to properly evaluate the credit worthiness of the customer while extending credit through remote banking procedures; which could enhance the credit risk.

The following aspects of online origination and approval tend to make risk management of the sending process more challenging. If not properly managed, these aspects can significantly increase credit risk.

- Verifying the customer's identity for on-line credit application and executing an enforceable contract;

- Monitoring and controlling the growth, pricing, underwriting standards, and ongoing credit quality of loans originated thorough e-banking channels;
- Monitoring and oversight of the third-parties doing business as agents or on behalf of the financial institution (for example, an Internet loan origination site or electronic payments processor);

• **Liquidity or Interest Rate / Price / Market Risk**

Liquidity risk arises out of bank's inability to meet it obligation when they become due without incurring unacceptable loses, even through the bank may ultimate be able to meet its obligations. Funding and investments-related risk could increase with an institution's e-banking initiatives depending on the ability to market their products and services globally.

The institution should modify its policies as necessary to address the following e-banking funding issues:

- Potential, increase in depending on brokered funds or other highly rate sensitive deposits;
- Potential acquisition of funds from markets where the institution is not licensed to engage in banking, particularly if the institution does not establish, disclose, and enforce geography restrictions;
- Potential impact of loan or deposit growth from an expanded internet market, including the impact of such growth on capital ratios; and
- Potential increase in volatility of funds should e-banking security problems negatively impact customer confidence or the market's perception of the institution.

• **Reputation risk** :

Reputation risk is the risk of getting significance negative public opinion, which may result in a loss of lending of customer.

An institution's decision to offer e-banking services, especially the more complex transactional services, significantly increases its level of reputation risk. Some of the ways in which e-banking can influence an institution's reputation include.

- Loss of trust due to unauthorized customer accounts.
- Disclosure or theft of confidential customer information to unauthorized parties (e.g. , hackers),
- Failure to deliver on marketing claims.

• **Compliance / Legal Risk**

This type risk arises from legal and regulatory uncertainty in e-finance transactions referring in particular to the difficulty of indentifies the headquarters of an e-finance firm. This is the risk to earnings, or capital arising from violations of, or non –conformance with, laws, regulations, and ethical standards.

Specific regulatory and legal challenges include

- Uncertainty over legal jurisdiction and which state's or country's laws govern a specific e-banking transaction,
- Delivery of credit and deposit -related disclosure/notices as required by law or regulation, retention of required compliances documentation for on-line advertising, application statements, disclosures and notices; and
- Establishment of legally binding electronic agreements.

• **Strategic risk**

This type risk is one of the most significance risks that e-banking activities present for banking organization. Strategic risk differs from others risk categories in that it is more general and broad in nature. Strategic decision to be taken by a bank's senior management has implications for all other risk categories. Give growing customers acceptance and demand for e-banking, most banks will need to develop a strategy to use the Internet delivery channel to provide informational content and/or transactional serviced to customers.

In particular, financial institutions should pay attention on the following:

- Adequate of management information system (MIS) to track e-banking usage and profitability;
- Cost involved in monitoring e-banking activities or cost involved in overseeing e-banking vendors and technology service providers;

- Design, delivery, and pricing of services adequate to generate sufficient customer demand.

Multiple Choice Questions

1. Intercepting and altering information relating to payment is:
   (a) Impersonation
   (b) **Tampering**
   (c) Authenticating
   (d) None of the above ( )

2. Loss of trust due to unauthorized activity on customer account is concerned with:
   (a) **Reputation Risk**
   (b) Liquidity Risk
   (c) Market Risk
   (d) None of the above ( )

3. Interim rules providing guidance on how the E-sing Act applies to the customer financial services is issued by:
   (a) Federal reserve board
   (b) E sign authority
   (c) The issuing bank
   (d) **RBI** ( )

4. SSL is:
   (a) Secret Sockets layers
   (b) **Securred Sockets layer**
   (c) Symmetric Sockets Layer
   (d) None of the above ( )

5. Which type of transaction are not permitted on Credit Cards;
   (a) Rail Booking
   (b) Airline Booking
   (c) **Puchase of medicines**
   (d) Gambling transactions ( )

6. Who can pass the law for E-banking?
   (a) **RBI**
   (b) Merchant Association

(c) Parliament
(d) None of the above ( )

7. For which card one has to make advance payment:
(a) Credit Card
(b) Debit Card
(c) **Smart Card**
(d) Gold Card ( )

8. What is E-sign Act?
(a) **Electronic Sign Act**
(b) Electronic signatures in Global and National Commerce Act
(c) Electronic Signatures in National And Global Act
(d) None of the above

Chapter 4

Risk Management of E-Banking Activities

Q.1 What are E-banking activities of management?

Ans. Because the Board of Directors and senior management are responsible for developing the institution's business strategic and effective management oversight over risks, they are expected to take an explicit, informed and documented strategic decision as to whether and how the bank is to provide e-banking services.

The board of directors and senior management are responsible for developing the institution's e-banking business strategy, which should include :

- The rational and strategy for offering e-banking services including informational, transactional, or e-commerce include.
- A cost-benefit analysis, risk assessment, and due diligence process for evaluating e-banking processing alternatives including third party providers.
- Goal and expectations that management can use to measure the e-banking strategy's effectiveness.
- Accountability for the development and maintenance of the risk management polices and controls to manage e-banking risks and for the audit of banking activities.

Q.2 How to manage outsourcing relationship?

Ans. The board and senior management must provide effective oversight of third party vendors providing e-banking services and support. Effective oversight requires that institutions ensure the following practices are in place:

- Effective due diligence in the selection of new service providers that considers financial condition, experience, expertise, technological compatibility and customer satisfaction:

- Written contracts with specific provisions protecting the privacy and security of an institution's data, the institution's ownership of the data, the right to audit security and controls, and the ability to monitor the quality of service, limit the institution's potential liability for acts of the services provider, and termite the contract:
- Appropriate processes to monitor vendor's ongoing performance, service quality, security controls, financial condition and contract compliance; and
- Monitoring reports and expectations including incidence response and notification.

Q.3 What is information security program?

Ans. E-banking introduces information security risk management challenges. Financial institution directors and senior management should ensure the information security program addresses these challenges and takes the appropriate actions.

- Ensure compliance with the "Guidelines Establishment standard for safeguarding customer information" (as issued pursuant to section 501 (b) of the Gramm-Leach-Bliley Act of 1999 (GLBA).
- Ensure the institution has the appropriate security expertise of its e-banking platform.
- Implement security controls sufficient to manage the unique security risks confronting the institution. Control consideration include:
    - Ongoing awareness of attack sources, scenarios, and techniques;
    - Up-to-date equipment inventories and network maps;
    - Rapid identification and mitigation of vulnerabilities;
    - Network access controls over external connections;
    - Hardened systems with unnecessary or vulnerable services or files disabled or removed.
    - Use of intrusion detection tools and intrusion response procedures;
    - Physical security of all e-banking computer equipment and media; and
    - Baseline security setting and usage policies for employees accessing the e-banking system or communicating with customers.

- Use verification procedures sufficient to adequately identify the individual asking to conduct business with the institution.

Q.4 Write a short note an Administrative control.

Ans. E-banking presents new administrative controls to requirements and potentially increases the importance of existing controls.

Management must evaluate its administrative controls to maximize the availability and integrity e-banking system. E-banking information can support identify theft for either fraud at the subject institution or for creating fraudulent accounts at other institutions. Institution should consider the adequate of the following controls:

- Segregation of e-banking duties to minimize the opportunity for employee fraud;
- Dual-control procedures especially for sensitive functions like encryption key retrieval or large on-line transfer;
- Reconcilement of e-banking transactions;
- Suspicious activity reviews and fraud detection with targeted review of unusually large transaction amount or volumes;

Q.5 What are legal and compliance issues relating to e-commerce.

Ans. Because e-banking limits face-t—face interaction and the paper-based exchange of information with customers, e-banking introduces new compliances or legal risks. Institutions should.

- Clearly identify the official name of the financial institution providing the e-banking services;
- Properly disclose their customer privacy and security policies on their websites; and
- Ensures that advertisements, notices, and disclosures are in compliances with applicable statutes and regulations, including the E-sign Act.

Multiple Choice Questions

1. Intrusion detection system helps in:
   (a) User enrolment
   (b) **Rapid intrusion detection and reaction**
   (c) Training
   (d) Independent testing ( )

2. If a customer service executive does not give proper information after proper security checks, this is:
   (a) Compliance
   (b) Six sigma
   (c) Effectiveness
   (d) **None of the above** ( )

3. What is E-sign Act?
   (a) Electronic Sign Act
   (b) Electronic signature in Global and National Commerce Act
   (c) **Electronic signature in National and Global Act**
   (d) None of the above ( )

4. A Debit Card/ATM card is a.....digit number:
   (a) 12
   (b) 13
   (c) **16**
   (d) 10 ( )

5. The potential hard for informational website E-banking is:
   (a) Viewing Account by a customer
   (b) **Spreading Virus**
   (c) Checking balance by a customer
   (d) Making online payment by a customer ( )

6. What is the full form of ATM ?
   (a) **Automated Teller Machine**
   (b) Automatic Transaction Machine
   (c) Advanced Teller Machine
   (d) Accurate teller money ( )

7. What are the reasons that institutions offer E-banking Services?
   (a) Lower Operating Cost
   (b) Greater Geographic Distribution
   (c) Maintained Competitive Portion
   (d) New revenue opportunities

(a) i, ii, iv (b) iii, iv
(c) i, iii, iv (d) **i, ii, iii, iv** ( )

8. The card by which you can not by a product is :
(a) Credit card
(b) **ATM card**
(c) Debit card
(d) Smart card ( )

9. Which one of the following is acquirer of a credit card Transaction?
(a) ICICI Bank (b) RBI
(c) **VISA** (d) Bank of Rajasthan ( )

10. A Banker's cheque is:
(a) **A local DD**
(b) an outstation DD
(c) An outdated cheque
(d) A prredata Cheque ( )

Chapter 5

Law Regulations & Guidelines

Q.1 What are types of electronic payment systems?

Ans. Electronic Payment System (EPS) is defined as "any transfer of funds initiated through as electronic terminate, telephonic instrument, or computer or magnetic taps so as to order, instruct, or authorize a financial institution to debit to credit an account."

Work of EPS can be segmented into three broad categories:

- Banking and Financial Payments
  - Large-scale or wholesale payments (e.g., bank to bank transfer)
  - Small-scalar or retail payments (e.g., automated teller machines and cash dispensers)
  - Home banking (e.g., bill payments)
- Retailing Payments
  - Credit cards (e.g., VISA or MasterCard)
  - Private label credit / debit cards (e.g., J.C. Penney card)
  - Charge cards (e.g., Americans Express).
- On-line Electronic Commerce Payments
  - Token based payment systems
    - Electronic Cash (e.g., Digicash)
    - Electronic checks (e.g., Netcheque)
    - Smart card or debit cards (e.g., Mondex Electronic currency card)

Q.2 What are types of electronic money, Explain it?

Ans. Electronic Money:

Electronic money, which is also knows electronic cash or digital money is way of making payments on the internet. Electronic money is nothing but money represented by computer files.

Types of Electronic Money

• Identified electronic money

• Anonymous electronic money

• **Identified electronic money**

Identified electronic money more or less works like a credit card. The progress of the identified electronic money from the very first time it is issued by a bank to one of its customership to its final return to the bank can be easily tracked by the bank. As a result, the bank can precisely know how and when the money was spent by the customer.

• **Anonymous electronic money**

The anonymous electronic money (also called as blinded money) works like real hard cash. There is no trace of how the money was spent. There is no trail of the transactions involved in this type of electronic money. Products like Digicash provide this kind of electronic money to internet users to spend, by typing up with blanks.

The key difference between identified electronic money and anonymous electronic money (which creates the anonymity) is the fact that whereas in case of the identified electronic money the bank creates the serial number, in case of the anonymous electronic money, it is the customer who creates the serial number.

Q.3 What is credit card? Explain its working?

Ans. Credit Cards:

A Credit Card is part of a system of payments named after the small plastic card issued to users of the system. The issuer of the card grants a line of credit to the consumer (or the user) from which the user can borrow money for payments to a merchant or as a cash advance to the user. A credit card is different from a charge card, which requires the balance to be paid in full each month. In contrast, credit

cards allow the consumer to 'revolve' their balance, at the cost of having interest charged.

How Credit Card Work:

Credit card are issued after an account has been approved by the credit proved, after which cardholders can use it to make purchase at merchant accepting that card.

When a purchase is made, the credit card user agrees to pay the card issuer. The cardholder indicates his/her consent to pay, by signing a receipt with a record of the card details and indicating the amount to be paid or by signing a receipt with a record of the card details and indicating the amount to be paid or by entering a Personal identification number (PIN). Also many merchants now accept verbal authorization via telephone and electronic authorization using the Internet, knows as a 'Card/Cardholder Not Present' (CNP) transaction.

Q.4 What is the use of SET? Explain SET process in detail?

Ans. The Secure Electronic Transactions (SET) protocol relies on two different encryption mechanisms, as well as an authentication mechanism. SET uses symmetric encryption, in the form of the aging Data Encryption Standard (DES), as well as asymmetric, or public key encryption to transmit session keys for DES transactions (IBM, 1998), Rather than offer the security and protection afforded by public-key cryptography, SET simply uses session keys (56bits) which are transmitted asymmetrically – the remainder of the transaction uses symmetric encryption in the form of DES. This has disturbing connotations for a "secure" electronic transaction protocol – because public key cryptography is only used only to encrypt DES keys and for authentication, and not for the main body of the transaction.

SET Transactions

The sequence of events required for a transaction as follows.

• The customer opens an account with a card issuer.

- *MasterCard, Visa, etc.*

• The customer receives a X.509 V3 certificate signed by a bank.

- *X.509 V3*

- A merchant who accepts a certain brand of card must possess two X.509 V3 certificates.
    - *One for signing & one for key exchange.*
- The customer places an order for a product or service with a merchant.
- The merchant sends a copy of its certificate for verification.
- The customer sends order and payment information to the merchant.
- The merchant request payment authorization from the payment gateway prior to shipment.
- The merchant confirms order to the customer.
- The merchant provides the goods or service to the customer.
- The merchant requests payments from the payments gateway.

Q.5 Write Importance of SET

Ans. Importance of secure transactions

Secure electronic transactions will be an important part of electronic commerce in the future. Without such security, the interests of the merchant, the consumer, and the credit or economic institution cannot be served, Privacy of transactions and authentication of all parties, is important for achieving the level of trust that will allow such transactions to flourish. However, it is important that the encryption algorithm and key-sizes used, will be robust enough to prevent observation by hostile entities (either criminal or foreign powers). The ideal of the secure electronic transaction protocol (set) is important for the success of the electronic commerce. However it remains to be seen whether the protocol will be widely used because of the weakness of the encryption that it uses.

Q.6 Explain RBI Guidelines for Internet Banking

Ans. Reserve Bank of India (RBI) had set up a "Working Group on Internet Banking" to examine different aspects of Internet Banking (I-Banking) The group had focused on three major areas of I-Banking i.e.

a) Technology and security issues.

b) Legal issues and

c) Regulatory and supervisory issues.

RBI has accepted the recommendations of the Group to be implemented in a phased manner. Accordingly guidelines are issued for implementation by banks.

1. Technology and Security Standards:

a) Banks should designate a network and database administrator with clearly defined roles as indicated in the Group's report.

b) Banks should have a security policy duly approved by the Board of Directors. There should be a segregation of duty Security/Officer/Group dealing exclusively with information system security and Information Technology Division which actually implements the computer systems. Information System security and information Technology Division which actually implements the computer systems. Further, information system auditor will audit the information systems (para 6.3.10, 6.4.1)

2. Legal Issues

a) Considering the legal position prevalent, there is an obligation on the part of banks not only to establish the identity but also to make enquiries about integrity and reputation of the prospective customer. Therefore, even though request for opening account can be accepted over internet, accounts should be opened only after proper introduction and physical verification of the identity of the customer.

b) From a legal perspective, security procedure adopted by bank for authenticating users needs to be recognized by law as a substitute for signature. In India, the information Technology Act, 2000, in section 3(2) provides for a particular technology (viz., the asymmetric crypto system and hash function) as a means of authenticating electronic record. Any other method used by banks for authentication should be recognized as a source of legal risk.

3. Regulatory and Supervisory Issues

As recommended by the group, the existing regulatory framework over banks will be extended to internet banking also. In this regard, it is advised that:

a) Only such banks which are licensed and supervised in India and have a physical presence in India will be permitted to offer internet banking products to residents of India. Thus, both banks and virtual banks incorporated outside the country and having no physical presence in India will not, for the present, be permitted to offer internet banking services to Indian residents.

b) The products should be restricted to account holders only and should not be offered in other jurisdictions.

c) The service should only include local currency products.

Q.7 Explain RBI Guidelines for Mobile Banking in India

Ans. The reserve bank of India issued a new set of guidelines for mobile Banking in India, highlights below,

- Mobile Banking can now be offered to customer without any debit or credit cards too.
- In order to register for Mobile Banking, the customer should be physically present. But there could be relaxation applied later.
- Banks will have to offer the mobile banking service with all mobile operations, before 6 months of the staff of Mobile Banking.
- Mobile banking customers are allowed to transfer funds of a maximum of Rupees 5000 daily, and purchase goods or services worth Rupees 2500 (total Rupees 7500 per day)
- Banks may put in place end-to-end encryption of the mobile PIN number (mPIN) for better security.
- Internet login IDs and Passwords can be used for mobile banking also.

Electronic Fund Transfers and RBI

After Technology Act has paved the path for digital signatures and digital contracts, Reserve Bank of India with the National Payment Council, is finalizing the draft of the Payment System Regulations Act. The Act will bring in all electronic fund transfers/entire-c-commerce payment system in the country be it money orders or settlements at payment gateways, stock and commodity exchanges or clearing houses under the jurisdiction of the RBI. Even the payment gateways and commodity exchanges will come under the RBI jurisdiction.

Law: Regulations and Guidelines for e-banking

Payment system legislation may include three Acts,

1. Payment System Regulation Act,
2. Payment System Netting Act and
3. Electronic Fund Transfer Act,

Together these Acts will cover all electronic fund transfers including inter-bank payments, pay order, remittances and transactions done through ATMs credit and debit cards besides money orders and other settlements in clearing houses and stock exchanges.

Legal Framework for Electronic Banking

Legal issues relating to electronic transaction processing at banks are very many and the need to address them by amending some of the existing Acts and by promoting legislation in a few hitherto unexpected areas has assumed critical urgency. Necessary legislative support is essential to protect-the interests as much of the customers as of the banks/branches in several areas relating to electronic banking and payment systems. This is specially required to establish the credibility of ECS and EFT schemes based on the electronic message transfer. Since the Reserve Bank is embarking on large electronic schemes such as the nationwide RTGS, it is time that efforts are made to bring about necessary legislative framework synchronizes and synthesizes with the initiatives taken by the Government of India, Department of

Electronics for promotion of the information Technology Bill, 1999 and/or the electronic commerce Bill, 1999.

Electronic Funds Transfer Act

In 1995, the Reserve Bank has set up the committee for proposing legislation on Electronic Funds Transfer and other Electronic Payment. The Share Committee had recommended set off EFT regulations by the Reserve Bank under the Reserve Bank of India Act, 1934 and amendment to the Bankers Books Evidence, Act, 1881 as short term measures and promotion of a few acts like the Electronic Funds Transfer Act, the Computer Misuse and Data Protection Act Etc. as long term measures. The reserve bank has already initiated steps for framing of EFT regulations.

Multiple Choice Questions

1. Which type of transaction are not permitted on credit card?
   (a) Rail Booking
   (b) Airline Booking
   (c) Purchase of medicines
   (d) **Gambling transaction** ( )

2. Securer electronic transaction is a :
   (a) **Protocol**
   (b) Transaction type
   (c) Security agency
   (d) JSP ( )

3. True about debit cards and ATM cards:
   (a) Offline E-money
   (b) **Online E-money**
   (c) Cash Money

4. IDS is:
   (a) **Intrusion Detection System**
   (b) Integrated Development System
   (c) Integrated Detection Service
   (d) Intrusion Development Service ( )

5. SET stands for:
   (a) Selective Electronic Transfer
   (b) **Secure Electronic Transaction**
   (c) Safe Electronic Transaction
   (d) None of the above ( )

6. Intrusion detection system helps in:
   (a) User enrollment
   (b) **Rapid Intrusion detection and reaction**
   (c) Training
   (d) Independent testing ( )

7. Smart cards are based on.....standards:
   (a) SET
   (b) MIME
   (c) HTTP
   (d) **TULIP** ( )

8. If a customer service executive does not give proper information after proper secruity checks, this is:
   (a) **Compliance**
   (b) Six Sigma
   (c) Effectiveness
   (d) None of the above ( )

9. Asymmetric key cryptography is also knows as:
   (a) **Public key technique**
   (b) Private key technique
   (c) Solo key technique
   (d) None of the above ( )

Chapter – 6

E-Security

Q.1 What is a E-Security?

Ans. E-Security can be defined as the use of adequate precautions to protect you data and systems, Risks posed to your security include : loss of or damage to computer equipment : loss of power : loss of network connectivity : unauthorized access : movement / alteration/ deletion of files : Theft of data : denial of service : and virus attack.

Ensuring security in cyberspace is a major issue in the uptake of electronic commerce and the development of the internet for both business and individuals, E-security is concerned with three main areas:

- Confidentiality – Information should only available to those who rightfully have access to it.
- Integrity – Information should be modified only by those who authorized to do so.
- Availability – Information should be accessible to those who are authorized to do so.

Top 9 it Security Threats and Solutions

Threat: 1 malicious insider (Rising Threat) Employees with malicious intent have always been the biggest threat to their organization.

Resolution: Conduct employee Security Awareness Training: Raising the awareness level of employees through mandatory, monthly online courses is a terrific way to remind them that security is everyone's responsibility. Choose a training program that offers up-to-date courses, ensures users understand policies and procedures, and provides reporting to management.

Threat: 2

Malware (Steady Threat): Malicious software can include viruses, worms, Trojan horse programs etc. but most importantly websites that host malware, which has become the most prolific distribution method.

Resolution: URL Filtering, patch management and other protections. Proactively manage the site where employees are allowed to surf by limiting them to safe, approved site from reputable web publishers. Employ patch management and system AV & Spyware protection to combat the malware threat.

Threat: 3

Exploited Vulnerabilities (Weakening Threat) Hackers find a weakness in a commonly used system or software product and exploit it for their gain.

Resolution: Implement comprehensive patch management: often some of the most sensitive data are on non-Microsoft system such as Linus, UNIX or Macintosh. Invest in a patch management solution offering full visibility into your network and covering all operating systems and vendors, not just Microsoft. Consider host based intrusion prevention (HIPS) which can monitor your system looking for anomalous behavior, application attempting to be installed, user escalation, and other non-standard events.

Threat: 4

Social Engineering (Rising Threat): With hacking you are compromising a computer, but with social engineering you compromise a human by tricking him/her into supplying personal information and passwords. Any method of communication will be used to perpetrate this fraud.

Resolution Social Engineering Testing: In addition to employee training to raise awareness you can hire a firm to come in and test your employees for their

resilience to social engineering. A 3rd party can use mock scenarios to assess your vulnerability to a real attack.

Threat: 5

Careless Employees (Rising Threat) Mistakes made by careless or untrained employees can lead to a significant security compromise. A poor economic climate puts strains on employees causing them to cut comers or important duties. It can also lead to less formal employee training.

Threat: 6

Reduced Budgets (Rising Threat):

A weak economy leads companies to tighten their budgets. Which results in less headcount and less money for upgrades and new systems.

Resolution: Consider option for a software-service (SaaS) solution to cut costs. A company that has traditionally kept their security management and monitoring in house may use this as an opportunity to look at the cost benefits of outsourcing it to a leading security firm. Choose a provider that offers a broad range of services, is financially, viable and is audited by multiple independent 3rd parties.

Threat:7

Remote workers & Road warriors (Steady Threat) telecommuting and mobile workers are on the upswing.

Resolution: Use the same system for telecommuters as for on-site employees. Don's forget to stall security on your remote VPNs make sure that remote users use company issued system with updated security patches and web content filtering. Provide easily accessible on-call tech support so that employees don's resort to fixing things themselves and possibly disabling necessary security measures. Isolate work computers at home from the kids who can download threats along with their games.

Threat:8

Unstable 3rd Party providers (Rising Threat) : While there is an increase in IT security expenses required to keep up with the growing threatscape and regulatory and regulatory environment, there is a decrease in revenues in the market. This may lead many providers to go out of business or cut comers that could lead to a security compromise.

Resolution:

Consider streamlining you 3rd party providers. Ensure that you are using providers that have been in business for a long time, have seen hard times before and have been regulatory focused for years. Ask for audited financial and ensure you provider is profitable choose a firm that can offer you multiple solutions via one integrated portal to gain the benefits of economics of scale and reduce the burden on existing IT staff resources.

Threat:9

Downloaded software Including open source and P2P files (Steady threat): It Administrators may download and install opens source software or freeware in an attempt to save money, which can lead to a huge waste of time in software configuration in and fine tuning to a data breach.

Resolution:

Limit download and system update administration to a trained IT professional. Don's allow users to download and install software on their desktops. Regularly update system AV and spyware protection. Consider host-based intrusion prevention (HIPS) which can monitor you system looking for anomalous behavior, applications attempting to be installed, user escalation, and other non- standard events but make sure that only IT managers have access to this.

There are so many other common threats for security.

Hacker:

Hacker is a person intensely interested in the hidden and complete working of any computer operation system.

Cracker:

A cracker is one who breaks into or otherwise violates and system integrity of remote machines with malicious intent.

Virus:

Virus is a piece of programming code usually disgnised as something else that causes same unexpected and usually undesirable event.

Worm: A warm is a self replicating virus that does not after files but resides in active memory and duplicates itself.

Backup:

Backup is the activity of copying files or databases so that they will be preserved in case of equipment failure or other catastrophe.

Spam:

Spam is unsolicited email an the internet. From the sender's is point of view, it's a form of bulk mail.

Phishing:

It is a scam to steal valuable information such as credit, social security numbers user IDs and passwords.

Multiple Choice Questions

1. A computer which converts data transmission protocol between network is:
   (a) Gateway (b) **Switch**
   (c) Hub (d) None of the above ( )

2. VAN stands for:
   (a) Varied Area Network
   (b) Virtual Area Network
   (c) **Value Added Network**
   (d) None of the above ( )

3. Payment gateways are used for:
   (a) **Interbank** (b) Delivery process

(c) Purchase (d) None of the above ( )

4. Digital signature certificated are issued by:
(a) Central Government (b) State Government
(c) **Certifying Authority** (d) None of the above ( )

5. Smart Cards are based in.....standards:
(a) SET (b) MIME
(c) HTTP (d) **TULIP** ( )

6. For which card one has to made advance payment?
(a) **Smart card**
(b) Gold Card
(c) Debit Card
(d) Credit Card ( )

7. Key used to create digital signature is:
(a) **Public key**
(b) Private key
(c) Linear key
(d) None of the above ( )

8. License to issue digital signature certificates are issued by:
(a) Finance Minister (b) Banks
(c) **Controller** (d) None of the above ( )

9. Poor e-banking planning is connected with:
(a) **Strategic Risk**
(b) Legal Risk
(c) Market Risk
(d) None of the above ( )

10. Board and management oversight does not include:
(a) Cost benefit and risk assessment
(b) Customers expectation ignores
(c) **Customers expectation ignores**
(d) Monitoring and accountability ( )

11. If you have an ATM Card of SBI and a balance of Rs. 1200 you want to get money from the ATM of HDFC, you can get moncy:
(a) Equal to your balance
(b) **Less than you balance**
(c) You cannot get money
(d) None of the above ( )

Keywords

1. Pc-Personal Computer
2. PDA- Personal Digital Assistant
3. ATM-Automated teller Machine
4. PKI- Public key infrastructure
5. PINS-Personal identification number
6. Client-A workstation or personal computer in a client/server environment
7. Domain Name-The term may refer to any type of domain within the computer field, since there are several types of domains. However, today, it often refers to the address of an Internet site.
8. EDI -Electronic data interchange (EDI) is the exchange of documents in a structured form between computers via telephone lines
9. EFT- Electronic Funds Transfer
10. Encryption -To encode data for security purposes
11. Firewall -A method for keeping a network secure
12. Proxy Server -Serves as a relay between two networks
13. Ftp-File Transfer Protocol:A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.).
14. GIF -A popular bitmapped graphics file format developed by CompuServe.
15. Home Page (also called Web Page) -The first page retrieved when accessing a Web site. It serves as a table of contents to the rest of the pages on the site or to other Web sites
16. Host -A computer that acts as a source of information or signals.
17. HTML-Hypertext Markup Language.
18. Hypertext -A linkage between related text.
19. Image Map -A picture that is logically separated into areas.
20. IP Address -internet Protocol address the address of a computer attached to a TCP/IP network.
21. ISDN –(Integrated Services Digital Network) An international telecommunications standard for transmitting voice, video and data over digital lines running at 64 Kbps.
22. ISP/Internet Service Provider -An organization that provides access to the Internet.

23. Meta Tags -An HTML tag that identifies the contents of a Web page
24. Navigation -"Surfing the Web." To move from page to page on the Web.
25. Router -A device that forwards data packets from one local area network (LAN) or wide area network (WAN) to another.
26. Search Engine -Software that searches for data based on some criteria
27. Server -A computer in a network shared by multiple users
28. XML -(EXtensible Markup Language)
29. Denial of Service Attack (DoS) - a simple form of DoS attack is by sending large volumes of data to a single server thereby making it unstable or even crashing it.
30. Cookie - information which a website places on your harddrive so that it can remember something about you at a later date.
31. Hacker - a person who uses a computer to break into other computer systems in order to steal, change or destroy information. To protect yourself from hackers you should install firewall software on your computer and keep it up to date.
32. Malware - an abbreviation of 'malicious software', malware refers to viruses, trojans, spyware, keyloggers, dialers and browser hijackers.
33. Spam - unwanted and unsolicited email. The electronic equivalent of paper junk mail.
34. URL- Uniform Resource Locator is the specifying of the location of something on the Internet,
35. WML- Wireless markup language.
36. WAP-Wireless application protocol
37. CDMA-Code division multiple access
38. TDMA- Time division multiple access
39. VPN-Virtual private network
40. 3G-Third generation.

BACHELOR OF COMPUTER APPLICATIONS

(Part III) EXAMINATION

(Faculty of Science)

(Three – Year Scheme of 10+2+3 Pattern)

PAPER 317

E-Banking and Security Transaction

OBJECTIVE PART- I

Year - 2010

Time allowed : One Hour *Maximum Marks : 20*

The question paper contains 40 multiple choice questions with four choices and students will have to pick the correct one. (Each carrying ½ marks.).

1. Which represents an offline e-money?
   (a) Debit Card (b) ATM Card
   (c) Credit Card (d) All of the above ( )

2. Authentication methodologies are based on:
   (a) Password (b) Smart card
   (c) Fingerprint Pattern (d) All of the above ( )

3. Which of the following is not a type of web hosting services?
   (a) Virtual Web Hosting
   (b) Cluster Web Hosting
   (c) Screen Web Hosting
   (d) Reseller Web Hosting ( )

4. CDMA stands for:
   (a) Code Division Modular Access
   (b) Code Davison Multiple Access
   (c) Coded Division Module Access
   (d) None of the above ( )

5. Which of the not a retail services among the following?
   (a) Loan approval (b) Account management
   (c) New Account opening (d) None of the above ( )

6. What can be done with wireless banking?
   (a) View your account wireless banking
   (b) Enquire about cheque status
   (c) Transfer funds between accounts
   (d) All of the above ( )

7. Which of the following is an example of electronic money?
   (a) Credit Card
   (b) Debit Card
   (c) Smart Card
   (d) All of the above ( )

8. Which transaction can not be done by ATM card?
   (a) Cash Withdrawal of 500
   (b) Cash Withdrawal of 750
   (c) Cash Withdrawal of 1000
   (d) Cash withdrawal of 2000 ( )

9. What is true about electronic money?
   (a) Both Bank and Customer would have public key encryptions keys
   (b) Only Bank Has Public Encryption Keys
   (c) Only customer has public key encryption keys
   (d) No one has public encryption keys ( )

10. GPRS stands for:
   (a) General Packet Radio Service
   (b) General Purpose Radio Service
   (c) General Purpose Recording Service
   (d) General Packet Record Service ( )

11. E-banking planning is concerned with:
   (a) Strategic Risk
   (b) Legal Risk
   (c) Market Risk
   (d) None of the above ( )

12. Knowing someone else password by certain illegal means is:
   (a) Hacking (b) Plagiarism
   (c) Sniffing (d) None of the above ( )

13. Which risk arises from and violation of non-conformance, with laws, rules and regulations?
    (a) Legal Risk
    (b) Strategic Risk
    (c) Operational Risk
    (d) Credit Risk ( )

14. Which risk is associated with the financial institution's future business plan and strategies?
    (a) Operational Risk
    (b) Strategic Risk
    (c) Credit Risk
    (d) Legal Risk ( )

15. EFT stands for:
    (a) Electronic Fund Transfer (b) Ensuring Fund Transfer
    (c) External Fund Transfer (d) None of the above ( )

16. The third level of e-banking Services is offered by:
    (a) Simple Transactional Website
    (b) Fully Transactional Website
    (c) Basic Level Website
    (d) All of the above ( )

17. ISAC stands for
    (a) Information System and Analysis
    (b) Information Sharing and Analysis Centre
    (c) Information System Authorized Centre
    (d) All of the above ( )

18. The full form of IRDA is:
    (a) Information Regulatory and Development Authority
    (b) Insurance Regulatory and Development Authority
    (c) Indians Resources of Development Authority
    (d) None of the above ( )

19. Payment gateways are used for:
    (a) Purchase Process
    (b) Inter Bank Transaction
    (c) Delivery Process
    (d) None of the above ( )

20. Web management is concerned with:
    (a) Commercial (b) Quick link
    (c) Effective use of space (d) All of the above ( )

21. The RBI regulates:
(a) Commercial (b) Urban Co-operative
(c) Both a and b (d) None of the above ( )

22. The private mutual funds are allowed to operate in market by:
(a) SBEI
(b) SEBI
(c) SBI
(d) None of the above ( )

23. IDS stands for:
(a) Intrusion Detection System
(b) Integrated Detection System
(c) Integrated Detection Service
(d) Intrusion Development Service ( )

24. All Parties Need Digital Certificates in:
(a) URL (b) SSL
(c) SET (d) All of the above ( )

25. SSL stands for:
(a) Secret Socket Layer (b) Secured Socket Layer
(c) Symmetric Socket Layer (d) None of the above ( )

26. The full form of WAP is:
(a) Wireless Application Protocol
(b) Wireless Application Program
(c) Wide Area Program
(d) Wireless Access Protocol ( )

27. Which committee on Banking Supervision has elaborated risk management principles for e-banking at the international level?
(a) Ranganathan Committee
(b) Basel Committee
(c) Loknathan Committee
(d) Rasel Committee ( )

28. IAB stand for:
(a) Internet Architecture Board
(b) Internet Advisory Board
(c) Internet Authorization Board
(d) None of the above ( )

29. Encrypted message is:

(a) Plain text
(b) Cipher text
(c) Language
(d) Phrase ( )

30. MAC stands for:
(a) Machine Authentication Code
(b) Message Authentication Code
(c) Message Advisory Council
(d) None of the above ( )

31. A trick to steal valuable information such as credit, user ids and passwords is knwon as:
(a) Phishing
(b) Alternation
(c) Eavesdropping
(d) None of the above ( )

32. DES stands for:
(a) Double Encryption standard
(b) Data Encryption standard
(c) Digest Encryption Standard
(d) Dual Encryption Standard ( )

33. Who violates the system integrity of remote machine with malicious inten?
(a) Hacker (b) Cracker
(c) Both a and b (d) None of the above ( )

34. The RBI has set up a.....to examine different aspects of internet banking:
(a) Working Group on Internet Banking
(b) Non-Working Group on Internet Banking
(c) Banking Group of India
(d) All of the above ( )

35. The bank should ensure that it has access to relevant audit trails maintained by the:
(a) Services Provider
(b) User
(c) Government
(d) None of the above ( )

36. The PIN in ATM card is of:
(a) 4 alphabets
(b) 4 digit
(c) 2 alphabets, 2 digits
(d) Any of the above ( )

37. Which is used to view and manage the online in one central locations?
    (a) Account Aggregation
    (b) Screen Scrapping
    (c) Authentication
    (d) Hosting ( )

38. The time when website is not available is referred as:
    (a) Uploading time (b) Downloading time
    (c) Non-availability (d) Non-Website time ( )

39. Which is not a method to establish authentication?
    (a) PINs
    (b) Passwords
    (c) Smart Card
    (d) Fund Transfer ( )

40. Value at Risk (VAR) is a :
    (a) Strategic Risk
    (b) Technical Risk
    (c) Statistical Risk
    (d) All of the above ( )

Answer Key

1. (d)	2. (d)	3. (c)	4. (b)	5. (d)	6. (d)	7. (d)	8. (b)	9. (a)	10. (a)
11. (c)	12. (b)	13. (a)	14. (b)	15. (a)	16. (b)	17. (a)	18. (b)	19. (a)	20. (d)
21. (c)	22. (b)	23. (a)	24. (b)	25. (b)	26. (a)	27. (b)	28. (a)	29. (b)	30. (b)
31. (a)	32. (b)	33. (a)	34. (a)	35. (c)	36. (b)	37. (a)	38. (c)	39. (d)	40. (d)

DESCRIPTIVE PART-II

Year- 2010

Time allowed : 2 Hours ***Maximum Marks : 30***

Attempt any four descriptive types of questions out of the six. All questions carry 7½ marks each.

Q.1 Define the concept of E-banking and its various types. Explain how Third Party providers E-banking?

Q.2 What are the main concepts of wireless system? Explain each of them in detial.

Q.3 Define risk. What do you mean by transaction or operational risk?

Q.4 What do you mean by Audit Trial? What are the different audit trail practices of E-banking systems?

Q.5 Why E-security is important and what are its legal considerations ?

Q.6 Write short notes on any three of the following?

(a) Secured Electronic Transaction

(b) Legal Risk

(c) E-banking Support Services

(d) Credit Cards

OBJECTIVE PART- I

Year - 2009

Time allowed : One Hour *Maximum Marks : 20*

The question paper contains 40 multiple choice questions with four choices and student will have to pick the correct one. (Each carrying ½ marks.).

1. The customer access E-banking services using:
   (a) PC
   (b) PDA
   (c) ATM
   (d) All of the above ( )

2. Which of the used to view and manage the online account in one central location?
   (a) Account aggregation
   (b) Authentication
   (c) Hosting
   (d) Screen Scraping ( )

3. E-Banking risk can be categorized as:
   (a) Operational Risk
   (b) Credit risk
   (c) Reputational risk
   (d) All of the above ( )

4. Legal risk arises because of:
   (a) Violation lf law
   (b) Non-confirmation with law
   (c) Legal right not established
   (d) All of the above ( )

5. TSP helps financial institution of:
   (a) Manage cost (b) Improve services quality
   (c) Obtain necessary expertise (d) All of the above ( )

6. Key used to verify a digital signature is:
   (a) Code key
   (b) Primary key
   (c) Public key
   (d) None of the above ( )

7. Full form of FINCEN is:
   (a) Financial Crimes Enforcement network
   (b) Financial Customer Enforcement network
   (c) Foreign Customer Entry Network
   (d) Financial Crimes Entry Notes ( )

8. SET is heavily influenced by:
   (a) HTTP
   (b) TCP
   (c) IKP
   (d) IP ( )

9. After encryption message is converted into:
   (a) Message Receiver
   (b) Message digest
   (c) Hash
   (d) None of the above ( )

10. Digital Signature Certificates are issued by:
   (a) Central Government
   (b) State Government
   (c) Certifying Authority
   (d) None of the above ( )

11. Which of the following is a safety measure in Banking netowrk?
   (a) Router
   (b) Fire well
   (c) Modem
   (d) None of the above ( )

12. Intercepting and altering information relating to payment it?
   (a) Impersonation
   (b) Tempering
   (c) Authenticating
   (d) None of the above ( )

13. DES stands for:
   (a) Data Encryption Standard
   (b) Double Encryption Standard
   (c) Dual Encryption Standard
   (d) None of the above ( )

14. Asymmetric key cryptography is also known as:
   (a) Public Key technique
   (b) Private Key technique

(c) Solo key technique
(d) None of the above ( )

15. Loss of trust due to unauthorized activity on customer account is concerned with:
(a) Reputation risk
(b) Liquidity risk
(c) Market risk
(d) None of the above ( )

16. URL stand for:
(a) Uniform Resources Locator
(b) Unified Research Lab
(c) Universal Research Lab
(d) None of the above ( )

17. Smart cards are based on.....standards:
(a) HTTP
(b) MIME
(c) TULIP
(d) SET ( )

18. Generally .....SSL encryption is used in internet banking:
(a) 16-bit
(b) 32 - bit
(c) 64- bit
(d) 128-bit ( )

19. SWIFT stands for:
(a) Society for worldwide information financial telecommunication
(b) Security for worldwide interbank financial telecommunication
(c) Society for worldwide interbank financial telecommunication
(d) None of the above ( )

20. PKI stands for:
(a) Public key Infrastructure
(b) Public key Input
(c) Personal Key Input
(d) Personal Key Identification ( )

21. For which card one has to made advance payment:
(a) Credit Card (b) Debit Card
(c) Smart Card (d) Gold Card ( )

22. The primary type of website used for E-banking

(a) Information (b) Transaction
(c) Both a and b (d) None of the above ( )

23. Transactional E-Banking is typically a front end system. That realises on a programming like called:
(a) Inter phase
(b) Interlink
(c) Inter join
(d) None of the above

( )

24. The most common payment especially for low value puchase, is made by:
(a) Debit card (b) Credit card
(c) Cash (d) ATM ( )

25. In credit card what is the grace period of payment?
(a) 10-15 days
(b) 5-20 days
(c) 15-45 days
(d) 1-2 days ( )

26. Who can pass the law for e-banking?
(a) SBI (b) Parliament
(c) RBI (d) Merchant Association ( )

27. Intrusion detection system helps in:
(a) User enrolment
(b) Rapid intrusion detection and reaction
(c) Training
(d) Independent testing ( )

28. If a customer service executive does not give proper information after proper security checks, this is:
(a) Compliance
(b) Six sigma
(c) Effectiveness
(d) None of the above ( )

29. What is E-sign Act?
(a) Electronic Sign Act
(b) Electronic signature in Global and National Commerce Act
(c) Electronic signature in National and Global Act
(d) None of the above ( )

30. A Debit Card/ATM card is a.....digit number:
(a) 12
(b) 13
(c) 16
(d) 10 ( )

31. The potential hard for informational website E-banking is:
(a) Viewing Account by a customer
(b) Spreading Virus
(c) Checking balance by a customer
(d) Making online payment by a customer ( )

32. What is the full form of ATM ?
(a) Automated Teller Machine
(b) Automatic Transaction Machine
(c) Advanced Teller Machine
(d) Accurate teller money ( )

33. What are the reasons that institutions offer E-banking Services?
(a) Lower Operating Cost
(b) Greater Geographic Distribution
(c) Maintained Competitive Portion
(d) New revenue opportunities
(a) i,ii,iv (b) iii,iv
(c) i,iii,iv (d) i,ii,iii,iv ( )

34. The card by which you can not by a product is :
(a) Credit card
(b) ATM card
(c) Debit card
(d) Smart card ( )

35. Which one of the following is acquirer of a credit card Transaction?
(a) ICICI Bank (b) RBI
(c) VISA (d) Bank of Rajasthan ( )

36. A Banker's cheque is:
(a) A local DD
(b) an outstation DD
(c) An outdated cheque
(d) A prredata Cheque ( )

37. Which type of transaction are not permitted on credit card?
(a) Rail Booking
(b) Airline Booking

(c) Purchase of medicines
(d) Gambling transaction ( )

38. Securer electronic transaction is a :
(a) Protocol
(b) Transaction type
(c) Security agency
(d) JSP ( )

39. True about debit cards and ATM cards:
(a) Offline E-money
(b) Online E-money
(c) Cash Money
(d) Both a and b ( )

40. Board and management oversight does not include :
(a) Audit
(b) Cost benefit analysis and risk assessment
(c) Customer expectation ignores
(d) Monitoring and accountability ( )

DESCRIPTIVE PART - II

Year 2009

Time allowed : 2 Hours ***Maximum Marks : 30***

Attempt any four questions out of the six. All questions carry 7½ marks each.

Q.1 What is electronic authentication? Explain various authentication methods.

Q.2 What are the legal issues associated with the secure electronic transaction?

Q.3 Write notes on these:

(i) Managing Outsourcing

(ii) Digital Signature

Q.4 What are the aspects that can significantly increase the credit risk if not properly managed?

Q.5 What are information security controls? Explain the need of training and independent testing.

Q.6 Write short notes on any two:

(a) Electronic Money

(b) Credit card

(c) Secure electronic transaction

OBJECTIVE PART- I

Year - 2008

Time allowed : One Hour *Maximum Marks : 20*

The question paper contains 40 multiple choice questions with four choices and student will have to pick the correct one. (Each carrying ½ marks.).

1. Intercepting and altering information relating to payment is:
   (a) Impersonation
   (b) Tampering
   (c) Authenticating
   (d) None of the above ( )

2. Knowing someone else password by certain illegal means is.....
   (a) Hacking
   (b) Plagiarism
   (c) Log on Scripts
   (d) Password Policy ( )

3. Which one of the following is a safety measure in E-banking network:
   (a) Firewall
   (b) Telephone Line
   (c) Coaxial Cable
   (d) OFC ( )

4. Loss of trust due to unauthorized activity on customer account is concerned with:
   (a) Reputation Risk
   (b) Liquidity Risk
   (c) Market Risk
   (d) None of the above ( )

5. Interim rules providing guidance on how the E-sing Act applies to the customer financial services is issued by:
   (a) Federal reserve board
   (b) E sign authority
   (c) The issuing bank
   (d) RBI ( )

6. SSL is:
   (a) Secret Sockets layers
   (b) Securred Sockets layer

(c) Symmetric Sockets Layer
(d) None of the above ( )

7. Which type of transaction are not permitted on Credit Cards;
(a) Rail Booking
(b) Airline Booking
(c) Puchase of medicines
(d) Gambling transactions ( )

8. Who can pass the law for E-banking?
(a) RBI
(b) Merchant Association
(c) Parliament
(d) None of the above ( )

9. For which card one has to make advance payment:
(a) Credit Card
(b) Debit Card
(c) Smart Card
(d) Gold Card ( )

10. What is E-sign Act?
(a) Electronic Sign Act
(b) Electronic signatures in Global and National Commerce Act
(c) Electronic Signatures in National And Global Act
(d) None of the above ( )

11. IDS is:
(a) Intrusion Detection System
(b) Integrated Development System
(c) Integrated Detection Service
(d) Intrusion Development Service ( )

12. SET stands for:
(a) Selective Electronic Transfer
(b) Secure Electronic Transaction
(c) Safe Electronic Transaction
(d) None of the above ( )

13. Intrusion detection system helps in:
(a) User enrollment
(b) Rapid Intrusion detection and reaction
(c) Training
(d) Independent testing ( )

14. WML stands for:
    (a) Wide Area Markup Language
    (b) Wired Markup Language
    (c) Wireless Markup Language
    (d) None of the above ( )

15. Smart cards are based on.....standards:
    (a) SET
    (b) MIME
    (c) HTTP
    (d) TULIP ( )

16. If a customer service executive does not give proper information after proper secruity checks, this is:
    (a) Compliance
    (b) Six Sigma
    (c) Effectiveness
    (d) None of the above ( )

17. Asymmetric key cryptography is also knows as:
    (a) Public key technique
    (b) Private key technique
    (c) Solo key technique
    (d) None of the above ( )

19. Board and management oversight does not include:
    (a) Cost benefit and risk assessment
    (b) Customers expectation ignores
    (c) Customers expectation ignores
    (d) Monitoring and accountability ( )

20. If you have an ATM Card of SBI and a balance of Rs. 1200 you want to get money from the ATM of HDFC, you can get moncy:
    (a) Equal to your balance
    (b) Less than you balance
    (c) You cannot get money
    (d) None of the above ( )

21. EFT stands for:
    (a) Electronic fund transfer (b) Ensuring fund transfer
    (c) External fund transfer (d) None of the above ( )

22. Which amount you can not deposit in ATM at one go:
    (a) 40 Notes of Rs. 100 (b) 5 Notes of Rs.100
    (c) 10 Notes of Rs. 500 (d) 7 Notes of Rs. 50 ( )

23. The card by which you can not buy a product:
(a) Credit Card
(b) ATM Card
(c) Debit Card
(d) Smart Card ( )

24. PIN in ATM card is of:
(a) 4 alphabets (b) 4 digit
(c) Any of the above (d) 2 alphabets and 2 digits ( )

25. Poor E-Banking planning and investment decision can increase a financial institutions:
(a) Legal Risk
(b) Reputation Risk
(c) Market Risk
(d) Strategic Risk ( )

26. A banker's cheque is:
(a) A local DD (b) An outstation DD
(c) An outdated cheque (d) None of the above ( )

27. Which represents an offline e-money:
(a) Debit Card
(b) ATM Card
(c) Credit Card
(d) All of the above ( )

28. DTD stands for:
(a) Data Term Definition
(b) Data Transaction Definition
(c) Document Type Definition
(d) All of the above ( )

29. Key used to create digital signature is:
(a) Public key
(b) Private key
(c) Linear key
(d) None of the above ( )

30. PIN is encrypted by using:
(a) DLL (b) DES
(c) TCP (d) None of the above ( )

31. Which is used to view and manage the online account in one central location:
    (a) Account aggregation (b) Authentication
    (c) Hosting (d) Screen scraping ( )

32. SET is achieved by:
    (a) Cryptography
    (b) Encryption
    (c) Both a and b
    (d) Decryption ( )

33. When somebody intercepts you credit and information while in transit, it is known is:
    (a) Eares dropping (b) Tempering
    (c) Spooling (d) None of the above ( )

34. Generally.....SSL encryption is used in internet banking:
    (a) 16 bit
    (b) 32 bit
    (c) 64 bit
    (d) 128 bit ( )

35. The primary types of website used for E-banking
    (a) Information Website
    (b) Transaction website
    (c) Both a and b
    (d) None of the above ( )

36. DEs Stands for:
    (a) Data Encryption Standard
    (b) Double Encryption Standard
    (c) Dual Encryption Standard
    (d) None of the above ( )

37. System.....is teh process of removing/disabling unnecessary or insecure service and files:
    (a) Fragmentation
    (b) Coding
    (c) Hardening
    (d) Malicious ( )

38. You have a credit limit of Rs.50,000 on your credit card, you have purchased readymade garments of Rs. 40,000 in the current month. How much more money can you use for purchasing from your credit card:
    (a) **Rs. 10,000**
    (b) Rs. 5,000

(c) Rs. 50,000
(d) None ( )

39. What is true about electronic money:
(a) **Both bank and customers would have public key encryption keys**
(b) Only bank has public key encryption keys
(c) Only customers have public key encryption keys
(d) No one has public encrypting keys ( )

40. The liability of the credit card holder on loss of the credit card is:
(a) Unlimited
(b) Up to credit limit
(c) **Up to the time, matter is reported to the issuing bank**
(d) Till two days after the matter reported to the bank ( )

Answer Key

1. (b)	2. (a)	3. (a)	4. (a)	5. (d)	6. (b)	7. (c)	8. (a)	9. (c)	10. (a)
11. (a)	12. (b)	13. (b)	14. (c)	15. (d)	16. (a)	17. (a)	18. (b)	19. (c)	20. (b)
21. (a)	22. (d)	23. (b)	24. (b)	25. (d)	26. (a)	27. (c)	28. (c)	29. (a)	30. (b)
31. (a)	32. (c)	33. (a)	34. (d)	35. (c)	36. (a)	37. (a)	38. (a)	39. (a)	40. (c)

DESCRIPTIVE PART - II

Year 2008

Time allowed : 2 Hours ***Maximum Marks : 30***

Attempt any four questions out of the six. All questions carry 7½ marks each.

Q.1 What do you understand by authentication and encryption in context of secured E-banking?

Q.2 Describe various e-banking risks?

Q.3 Write short notes on:

(a) Smart cards

(b) Digital Signatures

Q.4 What internal controls can help to assure the integrity and availability of E-banking systems?

Q.5 Why E-security is important and what are the legal considerations?

Q.6 Describe new challenges and threat to E-Security.

OBJECTIVE PART- I

Year - 2007

Time allowed : One Hour *Maximum Marks : 20*

The question paper contains 40 multiple choice questions with four choices and student will have to pick the correct one. (Each carrying ½ marks.).

1. The customers access e-banking services using:
   (a) PC (b) PDA
   (c) ATM (d) All of the above ( )

2. Pin in ATM Card is of:
   (a) 4 Alphabet
   (b) 4 Digit
   (c) 2 A;phabet and 2 Digit
   (d) Any of the above ( )

3. The existing customers can access the e-banking services by:
   (a) Internet viewing
   (b) Typing the customer name
   (c) User name and password authentication
   (d) None of the above ( )

4. Wireless banking can be done using:
   (a) Cellular phone
   (b) Pager
   (c) PDA
   (d) All of the above ( )

5. Which is used to view and manage the online account in one central location?
   (a) Account aggregation
   (b) Authentication
   (c) Hosting
   (d) Screen Scraping ( )

6. A webling is a:
   (a) Word (b) Phrase
   (c) Image (d) All of the above ( )

7. WML stands for:

(a) Wide Area Markup Language
(b) Wired Markup Language
(c) Wireless Markup Language
(d) None of the above ( )

8. Which is the process of changing data form one format to another?
(a) Transition (b) Transco ding
(c) Transmission (d) Translation ( )

9. DTD stands for:
(a) Data Term Definition
(b) Data Transaction definition
(c) Document type definition
(d) All of the above ( )

10. E-banking risk can be categorized as:
(a) Operational bank (b) Credit risk
(c) Reputation risk (d) All of the above ( )

11. Legal risk arises because of:
(a) Violation of law
(b) Non conformance with laws
(c) Legal right no established
(d) All of the above ( )

12. The third level of e-banking services is offered by:
(a) Basic level website
(b) Simple transactional website
(c) Fully transactional website
(d) All of the above ( )

13. TSP help financial institutions to:
(a) Mange cost (b) Improve service quality
(c) Obtain necessary expertise (d) All of the above ( )

14. What is the full form of form?
(a) Automated Teller Machine
(b) Automated Transaction Machine
(c) Advanced Teller Machine
(d) Accurate Teller Money ( )

15. Intrusion detection system helps in:
(a) User enrolment
(b) Training
(c) Independent testing

(d) Rapid intrusion detection and reaction ( )

16. Key used to verify a digital signature is :
(a) Code Key (b) Private key
(c) Public key (d) None of the above ( )

17. PKI stands for:
(a) Public key infrastructure
(b) Financial Customer enforcement network
(c) foreign customer entry network
(d) Financial Crimes Entry Note ( )

18. Full form of FINCEN is:
(a) Financial Crimes Enforcement
(b) Financial Customer Enforcement Network
(c) Foreign Customer Entry Network
(d) Financial Crimes Entry Note ( )

19. The Private mutual funds are allowed to cerate in the market by:
(a) SEBI (b) RBI
(c) SBI (d) None of the above ( )

20. Which has been enacted for E-Commerce?
(a) IT ACT, 2000 (b) IT ACT< 2001
(c) IT ACT< 2002 (d) IT ACT, 2003 ( )

21. SET stands for:
(a) System Environment Transactions
(b) Secure Electronic Transaction
(c) Secure External Transaction
(d) None of the above ( )

22. SET is heavily influenced by:
(a) Electronic Bill Personal Program
(b) Electronic Bill presentation and Payment
(c) Electronic Business Process and Program
(d) None of the above ( )

23. EBPP stands for:
(a) Electronic bill personal program
(b) Electronic bill presentation and program
(c) Electronic Business process and program
(d) None of the above ( )

24. WAP stands for:
    (a) Wireless application protocol (b) Wireless application program
    (c) Wide area program (d) Wireless access protocol ( )

25. Which of the following is encryption technique?
    (a) Symmetric key
    (b) Modulation
    (c) Demodulation
    (d) All of the above ( )

26. Intercepting and altering information relating to payment is:
    (a) Impersonation (b) Tampering
    (c) Authenticating (d) None of the above ( )

27. Digital signature are based in:
    (a) Symmetric key
    (b) Asymmetric key
    (c) Duplicate key
    (d) None of the above ( )

28. After encryption message is converted into:
    (a) Message Reserve
    (b) Message digest
    (c) Hash
    (d) None of the above ( )

29. PIN in encrypted by using:
    (a) DLL (b) DES
    (c) Hash (d) None of the above ( )

30. Loss of trust due to unauthorized activity on customer account is covered with:
    (a) Liquidity Risk
    (b) Market Risk
    (c) Reputation Risk
    (d) None of the above ( )

31. A computer which converts data transmission protocol between network is:
    (a) Gateway (b) **Switch**
    (c) Hub (d) None of the above ( )

32. VAN stands for:
    (a) Varied Area Network
    (b) Virtual Area Network
    (c) **Value Added Network**
    (d) None of the above ( )

33. Payment gateways are used for:
(a) **Interbank** (b) Delivery process
(c) Purchase (d) None of the above ( )

34. Digital signature certificated are issued by:
(a) Central Government (b) State Government
(c) **Certifying Authority** (d) None of the above
( )

35. Smart Cards are based in.....standards:
(a) SET (b) MIME
(c) HTTP (d) **TULIP**
( )

36. For which card one has to made advance payment?
(a) **Smart card**
(b) Gold Card
(c) Debit Card
(d) Credit Card ( )

37. Key used to create digital signature is:
(a) **Public key**
(b) Private key
(c) Linear key
(d) None of the above ( )

38. Who can pass the law for e-banking?
(a) Parliament (b) **RBI**
(c) SBI (d) None of the above ( )

39. License to issue digital signature certificates are issued by:
(a) Finance Minister (b) Banks
(c) **Controller** (d) None of the above ( )

40. Poor e-banking planning is connected with:
(a) **Strategic Risk**
(b) Legal Risk
(c) Market Risk
(d) None of the above ( )

Answer Key

1. (d)	2. (b)	3. (c)	4. (d)	5. (a)	6. (d)	7. (c)	8. (b)	9. (c)	10. (d)
11. (d)	12. (c)	13. (b)	14. (a)	15. (d)	16. (b)	17. (a)	18. (a)	19. (a)	20. (a)
21. (b)	22. (c)	23. (b)	24. (a)	25. (a)	26. (b)	27. (b)	28. (d)	29. (b)	30. (c)
31. (b)	32. (c)	33. (a)	34. (c)	35. (d)	36. (a)	37. (a)	38. (b)	39. (c)	40. (a)

DESCRIPTIVE PART - II

Year 2007

Time allowed : 2 Hours ***Maximum Marks : 30***

Attempt any four questions out of the six. All questions carry 7½ marks each.

Q.1 (i) Explain transactional Website with its categories.
(ii) Explain E-banking services.

Q.2 What is electronic authentication? Explain various authentication methods.

Q.3 What are legal requirement and regulatory guidance that frequently apply to E-banking products and services?

Q.4 What are different procedures to authenticate E-banking customers?

Q.5 What are the legal issues associated with the secure electronic transaction?

Q.6 What are different sound practices for the management and supervision of operational risk?

OBJECTIVE PART- I

Year - 2006

Time allowed : One Hour *Maximum Marks : 20*

The question paper contains 40 multiple choice questions with four choices and student will have to pick the correct one. (Each carrying ½ marks.).

1. When somebody intercepts your credit and information while in transit it is known is:

   (a) Eares dropping (b) Tampering
   (c) Spooling (d) None of the above ( )

2. Which of the following is a safety measure in e-banking network:
   (a) Router (b) Fire well
   (c) Modem (d) None of the above ( )

3. .....facilitates payments by authenticating the parties:
   (a) Payment gateway
   (b) Virus
   (c) Firewall
   (d) None of the above ( )

4. Intercepting and altering information relating to payment is:
   (a) Impersonation (b) Tampering
   (c) Authenticating (d) None of the above ( )

5. Modes of electronic payment includes:
   (a) Smart cards (b) Bills
   (c) Both (a) and (b) (d) Observation ( )

6. SET stands for:
   (a) Selective Electronic Transfer
   (b) Secure electronic Transaction
   (c) Safe electronic Transaction
   (d) None of the above ( )

7. Which of the following is encryption technique?
   (a) Symmetric key
   (b) Modulation
   (c) Demodulation
   (d) All of the above ( )

8. In symmetric key cryptography .....is used:
   (a) Key pair (b) Single key
   (c) Both (a) and (b) (d) None of the above ( )

9. DES stands for:
   (a) Data encryption (b) Key pair
   (c) Both a and b (D) None of the above ( )

10. Asymmetric key system uses:
   (a) Single key
   (b) Key pair
   (c) Both a and b
   (d) None of the above ( )

11. Digital signatures are based on:
   (a) symmetric key
   (b) asymmetric key
   (c) duplicate key
   (d) none of the above ( )

12. Asymmetric key cryptography is also knows is:
   (a) Public key technique (b) Private Key Technique
   (c) Solo key technique (d) None of the above ( )

13. After encryption message is converted into:
   (a) Message reserve
   (b) Message digest
   (c) Hash
   (d) None of the above ( )

14. PIN is encrypted by using:
   (a) DES (b) TCP
   (c) DLL (d) None of the above ( )

15. Full form of ATM is:
   (a) Advanced teller machine (b) automated Teller Machine
   (c) Accurate transfer machine (d) None of the above ( )

16. Credit card payment are made:
   (a) Monthly (b) Yearly
   (c) Weekly (d) Daily ( )

17. Loss of trust due to unauthorized activity on customer account is concerned with:
   (a) Reputation risk (b) Liquidity Risk

(c) Weekly (d) None of the above ( )

18. Poor-e banking planning is concerned with:
    (a) Strategic Risk
    (b) Liquidity Risk
    (c) Market Risk
    (d) None of the above ( )

19. By.....plain text is converted into cipher text:
    (a) Decryption
    (b) Encryption
    (c) Protocol
    (d) None of the above ( )

20. URL stands for:
    (a) Uniform Resources locator (b) Unified Research Lab
    (c) Universal Research Lab (d) None of the above ( )

21. A computer whihc converts data transaction protocol between network is:
    (a) Hub
    (b) Gateway
    (c) Switch
    (d) None of the above ( )

22. SSL is:
    (a) Secret Sockets layer
    (b) Secured sockets layer
    (c) Symmetric sockets layer
    (d) None of the above ( )

23. VAN stands for:
    (a) Varied area network (b) Value added network
    (c) Symmetric sockets layer (d) None of the above ( )

24. Payment gateways are used for:
    (a) Purchase process
    (b) Inter bank transaction
    (c) Delivery process
    (d) None of the above ( )

25. .....is a plastic card with embedded chip:
    (a) Debit Card
    (b) Credit Card
    (c) Both a and b
    (d) None of the above ( )

26. .....provides no line of credit.
    (a) Debit Card
    (b) Credit Card
    (c) both a and b
    (d) None of the above ( )

27. EFT stands for:
    (a) Electronic fund transfer
    (b) Ensuring fund transfer
    (c) External fund transfer
    (d) None of the above ( )

28. Token based payment system include:
    (a) Electronic cash
    (b) Electronic checks
    (c) Both a and b
    (d) None of the above ( )

29. Digital signature certificates are issued by:
    (a) Central Government (b) State Government
    (c) Certifying Authority (d) None of the above ( )

30. License to issue digital signature certificates are issued by:
    (a) Banks (b) Finance Minister
    (c) Controller (d) None of the above ( )

31. Smart cards are based on.....standards:
    (a) HTTP
    (b) MIME
    (c) TULIP
    (d) SET ( )

32. Web management is concerned with:
    (a) Cost factor
    (b) Quick link
    (c) Effective use of space
    (d) All of the above ( )

33. Schemes that transmit number from one computer to another for payment are:
    (a) Digital Cash
    (b) Electronic cash
    (c) E-cash
    (d) All of the above ( )

34. .....is a set of rules defining the way computer system interact with each other.
(a) Layer (b) Bridge
(c) Router (d) Protocol ( )

35. Generally.....SSL encryption is used in internet banking.
(a) 16-bit (b) 32-bit
(c) 64-bit (d) 128-bit ( )

36. All parties need digital certificates in:
(a) URL (b) SSL
(c) SET (d) All of the above ( )

37. Key used to create digital signature risk:
(a) Linear key (b) Public key
(c) Private key (d) None of the above ( )

38. Key used to verify a digital signature is:
(a) Code key
(b) Private key
(c) Public key
(d) None of the above ( )

39. Who can pass the law for e-banking?
(a) RBI
(b) Merchant Association
(c) Parliament
(d) None of the above ( )

40. 'SWIFT' stands for:
(a) Society for world wide inter government financial telecommunication
(b) Security for world interbank financial Telecommunication
(c) Society for World Wide Interbank Financial Telecommunication
(d) None of the above ( )

Answer Key

1. (a)	2. (b)	3. (a)	4. (b)	5. (a)	6. (b)	7. (a)	8. (b)	9. (a)	10. (b)
11. (b)	12. (a)	13. (d)	14. (a)	15. (b)	16. (a)	17. (a)	18. (a)	19. (b)	20. (a)
21. (c)	22. (b)	23. (b)	24. (b)	25. (b)	26. (a)	27. (a)	28. (c)	29. (c)	30. (c)
31. (c)	32. (d)	33. (d)	34. (d)	35. (d)	36. (c)	37. (b)	38. (b)	39. (a)	40. (c)

DESCRIPTIVE PART - II

Year 2006

Time allowed : 2 Hours ***Maximum Marks : 30***

Attempt any four questions out of the six. All questions carry 7½ marks each.

Q.1 Describe various E-banking risks.

Q.2 Write notes on the following:
(a) Secure Electronic Transaction
(b) E-Banking Support Services

Q.3 What are information security controls? Discuss the administration controls needed to maintain the data security.

Q.4 Write a note an new challenges and threats to e-security.

Q.5 Write notes on:
(a) Cost benefit analysis
(b) Credit cards

Q.6 Write notes on:
(a) Managing outsourcing
(b) Digital signature