Roll No. | | | | | | | | | | |

SHAMBHUNATH INSTITUTE OF ENGINEERING AND TECHNOLOGY

Subject Code: RUC-601 **Subject: CYBER SECURITY**

B.Tech. **SEMESTER-6TH**

FIRST SESSIONAL EXAMINATION, EVEN SEMESTER, (2019-2020)

Branch: ELECTRONICS & COMMUNICATION ENGINEERING

Time –1hr 30 min **Maximum Marks – 30**

SOLUTION

SECTION – A

1. Attempt all questions in brief. **(1*5 = 5)**

Q N	QUESTION	Marks	CO	BL
a.	**What is Email?** **Ans- Electronic mail** (**email** or **e-mail**) is a method of exchanging messages ("mail") between people using electronic devices. Invented by Ray Tomlinson, email first entered limited use in the 1960s and by the mid-1970s had taken the form now recognized as email. Email operates across computer networks, which today is primarily the Internet. Some early email systems required the author and the recipient to both be online at the same time, in common with instant messaging. Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver, and store messages.	**1**	**2**	**1**
b.	**What is Security Risk Analysis?** **Ans-** Risk analysis refers to the review of risks associated with the particular action or event. The risk analysis is applied to information technology, projects, security issues and any other event where risks may be analysed based on a quantitative and qualitative basis. Risks are part of every IT project and business organizations. The analysis of risk should be occurred on a regular basis and be updated to identify new potential threats. The strategic risk analysis helps to minimize the future risk probability and damage. **Enterprise and organization used risk analysis:** o To anticipates and reduce the effect of harmful results occurred from adverse events. o To plan for technology or equipment failure or loss from adverse events, both natural and human-caused. o To evaluate whether the potential risks of a project are balanced in the decision process when evaluating to move forward with the project.	**1**	**1**	**1**

	○ To identify the impact of and prepare for changes in the enterprise environment.			
c.	**What do you mean by Denial of service Attack?** **Ans-** In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source. A DoS or DDoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, thus disrupting trade.	**1**	**2**	**2**
d.	**What is cyber Security?** **Ans-** Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security. Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information.	**1**	**1**	**1**
e.	**What is backup of data?** **Ans-** A data backup is the result of copying or archiving files and folders for the purpose of being able to restore them in case of data loss.	**1**	**2**	**1**

	Data loss can be caused by many things ranging from computer viruses to hardware failures to file corruption to fire, flood, or theft (etc). If you are responsible for business data, a loss may involve critical financial, customer, and company data. If the data is on a personal computer, you could lose financial data and other key files, pictures, music, etc that would be hard to replace. As part of a data backup plan, you should consider the following: What data (files and folders) to backup What compression method to use How often to run your backups What type of backups to run* What kind of media on which to store the backups Where to store the backup data for safekeeping			

SECTION – B

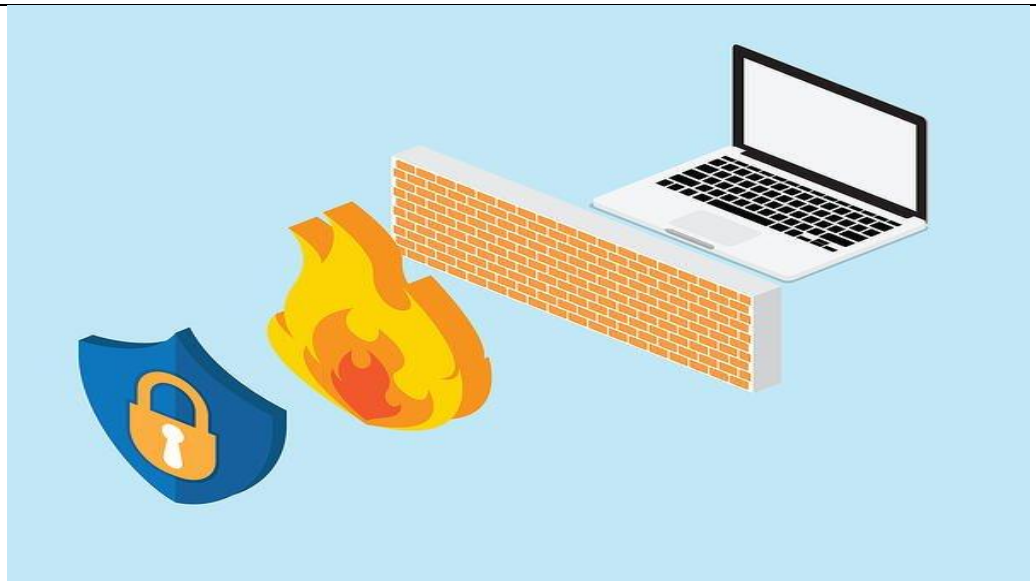
2. Attempt any <u>TWO</u> of the following. (2*5 = 10)

Q N	QUESTION	Marks	CO	BL
a.	**What do you understand by Information Assurance?** **Ans-** Information assurance (IA) is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data.[1] It uses physical, technical, and administrative controls to accomplish these tasks. While focused predominantly on information in digital form, the full range of IA encompasses not only digital, but also analog or physical form. These protections apply to data in transit, both physical and electronic forms, as well as data at rest in various types of physical and electronic storage facilities. IA is best thought of as a superset of information security (i.e. umbrella term), and as the business outcome of information risk management. The information assurance process typically begins with the enumeration and classification of the information assets to be protected. Next, the IA practitioner will perform a risk assessment for those assets. Vulnerabilities in the information assets are determined in order to enumerate the threats capable of exploiting the assets. The assessment then considers both the probability and impact of a threat exploiting a vulnerability in an asset, with impact usually measured in terms of cost to the asset's stakeholders. The sum of the products of the threats' impact and the probability of their occurring is the total risk to the information asset. With the risk assessment complete, the IA practitioner then develops a risk management plan. This plan proposes countermeasures that involve mitigating, eliminating, accepting, or transferring the risks, and considers prevention, detection, and response to threats. A framework published by a standards organization, such as NIST RMF, Risk IT, CobiT, PCI DSS or ISO/IEC 27002, may guide development. Countermeasures may include technical tools such	**5**	**1**	**2**

	as firewalls and anti-virus software, policies and procedures requiring such controls as regular backups and configuration hardening, employee training in security awareness, or organizing personnel into dedicated computer emergency response team (CERT) or computer security incident response team (CSIRT). The cost and benefit of each countermeasure is carefully considered. Thus, the IA practitioner does not seek to eliminate all risks, were that possible, but to manage them in the most cost-effective way.			
b.	**Discuss Term Virus & its types in detail?** **Ans-** A computer virus is a malicious program that self-replicates by copying itself to another program. In other words, the computer virus spreads by itself into other executable code or documents. The purpose of creating a computer virus is to infect vulnerable systems, gain admin control and steal user sensitive data. Hackers design computer viruses with malicious intent and prey on online users by tricking them. One of the ideal methods by which viruses spread is through emails – opening the attachment in the email, visiting an infected website, clicking on an executable file, or viewing an infected advertisement can cause the virus to spread to your system. Besides that, infections also spread while connecting with already infected removable storage devices, such as USB drives. Types of Computer Viruses A computer virus is one type of malware that inserts its virus code to multiply itself by altering the programs and applications. The computer gets infected through the replication of malicious code. Computer viruses come in different forms to infect the system in different ways. Some of the most common viruses are, Boot Sector Virus Direct Action Virus Resident Virus Multipartite Virus Polymorphic Virus Overwrite Virus Spacefiller Virus **Boot Sector Virus** – This type of virus infects the master boot record and it is challenging and a complex task to remove this virus and often requires the system to be formatted. Mostly it spreads through removable media. **Direct Action Virus** – This is also called non-resident virus, it gets installed or stays hidden in the computer memory. It stays attached to the specific type of files that it infect. It does not affect the user experience and system's performance. **Resident Virus** – Unlike direct action viruses, resident viruses get installed on the computer. It is difficult to identify the virus and it is even difficult to remove a resident virus. **Multipartite Virus** – This type of virus spreads through multiple ways. It infects both the boot sector and executable files at the same time. **Polymorphic Virus** – These type of viruses are difficult to identify with a traditional anti-virus program. This is because the polymorphic viruses alters its signature pattern whenever it replicates. **Overwrite Virus** – This type of virus deletes all the files that it infects. The only	**5**	**2**	**3**

	possible mechanism to remove is to delete the infected files and the end-user has to lose all the contents in it. Identifying the overwrite virus is difficult as it spreads through emails. **Spacefiller Virus** – This is also called "Cavity Viruses". This is called so as they fill up the empty spaces between the code and hence does not cause any damage to the file. **#File infectors:** Few file infector viruses come attached with program files, such as .com or .exe files. Some file infector viruses infect any program for which execution is requested, including .sys, .ovl, .prg, and .mnu files. Consequently, when the particular program is loaded, the virus is also loaded. Besides these, the other file infector viruses come as a completely included program or script sent in email attachments. **#Macro viruses:** As the name suggests, the macro viruses particularly target macro language commands in applications like Microsoft Word. The same is implied on other programs too.			
c.	**What are threats of Information System?** **Ans-** Threats to Information Security In Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest. Software attacks means attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behave differently. Malware is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or a anything that is designed to perform malicious operations on system. Malware can be divided in 2 categories: 1. Infection Methods 2. Malware Actions Malware on the basis of Infection Method are following: 1. Virus – They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. Ther Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc. 2. Worms – Worms are also self replicating in nature but they don't hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will for example consume hard disk space thus slowing down the computer. 3. Trojan – The Concept of Trojan is completely different from the viruses and	**5**	**1**	**1**

	worms. The name Trojan derived from the 'Trojan Horse' tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside. 4. **Bots –**: can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need of human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called **Botnet.**			
d.	**What do you understand Term Firewall. Discuss types of firewall?** **Ans-** A firewall is a type of cybersecurity tool that is used to filter traffic on a network. Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with each type of firewall having its own unique pros and cons. The primary goal of a firewall is to block malicious traffic requests and data packets while allowing legitimate traffic through. Types of Firewalls irewall types can be divided into several different categories based on their general structure and method of operation. Here are eight types of firewalls: • Packet-filtering firewalls • Circuit-level gateways • Stateful inspection firewalls • Application-level gateways (a.k.a. proxy firewalls) • Next-gen firewalls • Software firewalls • Hardware firewalls • Cloud firewalls	**5**	**2**	**2**

SECTION – C

3. Attempt any ONE part of the following: (1*5 = 5)

Q N	QUESTION	Marks	CO	BL
a.	**What is Information System? Explain various types of Information system?** **Ans-** A computer information system is a system composed of people and computers that processes or interprets information. The term is also sometimes used in more restricted senses to refer to only the software used to run a computerized database or to refer to only a computer system. Information Systems is an academic study of systems with a specific reference to information and the complementary networks of hardware and software that people and organizations use to collect, filter, process, create and also distribute data. An emphasis is placed on an information system having a definitive boundary, users, processors, storage, inputs, outputs and the aforementioned communication networks. Information Systems are classified by organisational levels, mode of data, processing, system objectives and type of support provided. Following are the TYPE of information system: 1. Transaction Processing System (TPS): • Transaction Processing System are information system that processes data resulting from the occurrences of business transactions • Their objectives are to provide transaction in order to update records and generate reports i.e to perform store keeping function • The transaction is performed in two ways: Batching processing and Online transaction processing. • Example: Bill system, payroll system, Stock control system. 2. Management Information System (MIS): • Management Information System is designed to take relatively raw data available through a Transaction Processing System and convert them into a	**5**	**1**	**1**

summarized and aggregated form for the manager, usually in a report format. It reports tending to be used by middle management and operational supervisors.

- Many different types of report are produced in MIS. Some of the reports are a summary report, on-demand report, ad-hoc reports and an exception report.
- Example: Sales management systems, Human resource management system.

3. Decision Support System (DSS):

- Decision Support System is an interactive information system that provides information, models and data manipulation tools to help in making the decision in a semi-structured and unstructured situation.
- Decision Support System comprises tools and techniques to help in gathering relevant information and analyze the options and alternatives, the end user is more involved in creating DSS than an MIS.
- Example: Financial planning systems, Bank loan management systems.

4. Experts System:

- Experts systems include expertise in order to aid managers in diagnosing problems or in problem-solving. These systems are based on the principles of artificial intelligence research.
- Experts Systems is a knowledge-based information system. It uses its knowledge about a specify are to act as an expert consultant to users.
- Knowledgebase and software modules are the components of an expert system. These modules perform inference on the knowledge and offer answers to a user's question

b.

Write a short note on Private Key Encryption & Public Key Encryption?

Ans- Private Key:
In Private key, the same key (secret key) is used for encryption and decryption. In this key is symmetric because the only key is copy or share by another party to decrypt the cipher text. It is faster than the public key cryptography.
Public Key:
In Public key, two keys are used one key is used for encryption and another key is used for decryption. One key (public key) is used for encrypt the plain text to convert it into cipher text and another key (private key) is used by receiver to decrypt the cipher text to read the message.
difference between them:

S.NO	PRIVATE KEY	PUBLIC KEY
1.	Private key is faster than public key.	It is slower than private key.
2.	In this, the same key (secret key) and algorithm is used to	In public key cryptography, two keys are used, one key is used for

5 **2** **1**

		encrypt and decrypt the message.	encryption and while the other is used for decryption.		
	3.	In private key cryptography, the key is kept as a secret.	In public key cryptography, one of the two keys is kept as a secret.		
	4.	Private key is **Symmetrical** because there is only one key that is called secret key.	Public key is **Asymmetrical** because there are two types of key: private and public key.		
	5.	In this cryptography, sender and receiver need to share the same key.	In this cryptography, sender and receiver does not need to share the same key.		
	6.	In this cryptography, the key is private.	In this cryptography, public key can be public and private key is private.		

4. Attempt any ONE part of the following: **(1*5 = 5)**

Q N	QUESTION	Marks	CO	BL
a.	**Explain Waterfall Model of IS?** **Ans- Definition:** The waterfall model is a classical model used in system development life cycle to create a system with a linear and sequential approach. It is termed as waterfall because the model develops systematically from one phase to another in a downward fashion. This model is divided into different phases and the output of one phase is used as the input of the next phase. Every phase has to be completed before the next phase starts and there is no overlapping of the phases. **Description:** The sequential phases described in the Waterfall model are:	**5**	**1**	**3**

1. Requirement Gathering- All possible requirements are captured in product requirement documents.

2. Analysis Read - the requirement and based on analysis define the schemas, models and business rules.

3. System Design -- Based on analysis design the software architecture.

4. Implementation Development of the software in the small units with functional testing.

5. Integration and Testing Integrating of each unit developed in previous phase and post integration test the entire system for any faults.

6. Deployment of system - Make the product live on production environment after all functional and nonfunctional testing completed.

7. Maintenance Fixing issues and release new version with the issue patches as required.

Advantages: 1. Easy to use, simple and understandable, 2. Easy to manage as each phase has specific outputs and review process, 3. Clearly-defined stages, 4. Works well for smaller projects where requirements are very clear, 5. Process and output of each phase are clearly mentioned in the document.

Disadvantages: 1. It doesn't allow much reflection or revision. When the product is in testing phase, it is very difficult to go back and change something which is left during the requirement analysis phase.

2. Risk and uncertainty are high.

3. Not advisable for complex and object-oriented projects.

4. Changing requirements can't be accommodated in any phase.

	5. As testing is done at a later phase. So, there is a chance that challenges and risks at earlier phases are not identified.			
b.	**How digital Signature is use for message authentication? Discuss the component of digital Signature?** **Ans-** Digital Signatures and Certificates **Encryption** – Process of converting electronic data into another form, called cipher text, which cannot be easily understood by anyone except the authorized parties.This assures data security. **Decryption**– Process of translating code to data. • Message is encrypted at the sender's side using various encryption algorithms and decrypted at the receiver's end with the help of the decryption algorithms. • When some message is to be kept secure like username, password, etc., encryption and decryption techniques are used to assure data security. **Types of Encryption** 1. **Symmetric Encryption**– Data is encrypted using a key and the decryption is also done using the same key. 2. **Asymmetric Encryption**-Asymmetric Cryptography is also known as public key cryptography. It uses public and private keys to encrypt and decrypt data. One key in the pair which can be shared with everyone is called the public key. The other key in the pair which is kept secret and is only known by the owner is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption. **Public key**– Key which is known to everyone. Ex-public key of A is 7, this information is known to everyone. **Private key**– Key which is only known to the person who's private key it is. **Authentication**-Authentication is any process by which a system verifies the identity of a user who wishes to access it. **Non- repudiation**– Non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. **Integrity**– to ensure that the message was not altered during the transmission. **Message digest** -The representation of text in the form of a single string of digits, created using a formula called a one way hash function. Encrypting a message digest with a private key creates a digital signature which is an electronic means of authentication Digital Signature A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. 1. Key Generation Algorithms : Digital signature are electronic signatures, which assures that the message was sent by a particular sender. While performing digital transactions authenticity and integrity should be assured, otherwise the data can be altered or someone can also act as if he was the sender and expect a reply.	**5**	**2**	**3**

	2. Signing Algorithms: To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed. The signing algorithm then encrypts the hash value using the private key (signature key). This encrypted hash along with other information like the hashing algorithm is the digital signature. This digital signature is appended with the data and sent to the verifier. The reason for encrypting the hash instead of the entire message or document is that a hash function converts any arbitrary input into a much shorter fixed length value. This saves time as now instead of signing a long message a shorter hash value has to be signed and moreover hashing is much faster than signing. 3. Signature Verification Algorithms : Verifier receives Digital Signature along with the data. It then uses Verification algorithm to process on the digital signature and the public key (verification key) and generates some value. It also applies the same hash function on the received data and generates a hash value. Then the hash value and the output of the verification algorithm are compared. If they both are equal, then the digital signature is valid else it is invalid. The steps followed in creating digital signature are : 1. Message digest is computed by applying hash function on the message and then message digest is encrypted using private key of sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm(message)). 2. Digital signature is then transmitted with the message.(message + digital signature is transmitted) 3. Receiver decrypts the digital signature using the public key of sender.(This assures authenticity,as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender's public key). 4. The receiver now has the message digest. 5. The receiver can compute the message digest from the message (actual message is sent with the digital signature). 6. The message digest computed by receiver and the message digest (got by decryption on digital signature) need to be same for ensuring integrity. Message digest is computed using one-way hash function, i.e. a hash fucntion in which computation of hash value of a message is easy but computation of the message from hash value of the message is very difficult.			

5. Attempt any ONE part of the following: (1*5 = 5)

Q N	QUESTION	Marks	CO	BL
a.	**What is Virtual Private Network (VPN)? Discuss VPN types?** **Ans- VPN (virtual private network)** A virtual private network (VPN) is programming that creates a safe, encrypted connection over a less secure network, such as the public internet. A VPN uses tunneling protocols to encrypt data at the sending end and decrypt it at the	**5**	**2**	**1**

receiving end. To provide additional security, the originating and receiving network addresses are also encrypted.

VPNs are used to provide remote corporate employees, gig economy freelance workers and business travelers with access to software applications hosted on proprietary networks. To gain access to a restricted resource through a VPN, the user must be authorized to use the VPN app and provide one or more authentication factors, such as a password, security token or biometric data.

VPN apps are often used by individuals who want to protect data transmissions on their mobile devices or visit web sites that are geographically restricted. Secure access to an isolated network or website through a mobile VPN should not be confused with private browsing, however. Private browsing does not involve encryption; it is simply an optional browser setting that prevents identifiable user data, such as cookies, from being collected and forwarded to a third-party server.

Types of VPNs

Network administrators have several options when it comes to deploying a VPN. They include:

Remote access VPN

Remote access VPN clients connect to a VPN gateway server on the organization's network. The gateway requires the device to authenticate its identity before granting access to internal network resources such as file servers, printers and intranets. This type of VPN usually relies on either IP Security (IPsec) or Secure Sockets Layer (SSL) to secure the connection.

Site-to-site VPN

In contrast, a site-to-site VPN uses a gateway device to connect an entire network in one location to a network in another location. End-node devices in the remote location do not need VPN clients because the gateway handles the connection. Most site-to-site VPNs connecting over the internet use IPsec. It is also common for them to use carrier MPLS clouds rather than the public internet as the transport for site-to-site VPNs. Here, too, it is possible to have either Layer 3 connectivity

	(MPLS IP VPN) or Layer 2 (virtual private LAN service) running across the base transport. **Mobile VPN** In a mobile VPN, a VPN server still sits at the edge of the company network, enabling secure tunneled access by authenticated, authorized VPN clients. Mobile VPN tunnels are not tied to physical IP addresses, however. Instead, each tunnel is bound to a logical IP address. That logical IP address sticks to the mobile device no matter where it may roam. An effective mobile VPN provides continuous service to users and can seamlessly switch across access technologies and multiple public and private networks. **Hardware VPN** Hardware VPNs offer a number of advantages over the software-based VPN. In addition to enhanced security, hardware VPNs can provide load balancing to handle large client loads. Administration is managed through a Web browser interface. A hardware VPN is more expensive than a software VPN. Because of the cost, hardware VPNs are a more realistic option for large businesses than for small businesses or branch offices. Several vendors, including Irish vendor InvizBox, offer devices that can function as hardware VPNs. **VPN appliance** A VPN appliance, also known as a VPN gateway appliance, is a network device equipped with enhanced security features. Also known as an SSL (Secure Sockets Layer) VPN appliance, it is in effect a router that provides protection, authorization, authentication and encryption for VPNs.			
b.	**What is Smart Card? Differentiate between Credit & Debit Card?** **Ans- Smart Card**: A **smart card** is a device with **the** dimensions of a **credit card** that uses a small microchip to store and process data. **Debit Card**:A **debit**	**5**	**2**	**1**

card is a payment card that deducts money directly from a consumer's checking account to pay for a purchase. Smart cards offer more security than debit cards.

Difference between Credit card, Debit Card and Smart Card

Credit Card	Debit Card	Smart Card
1. A Credit card is basically an electronic card with magnetic data strip or a chip, issued to customers by banks and other credit agencies.	1. Debit cards are magnetic strip and chip enabled cards, issued to customers by their respective banks.	1. A smart card contains a special embedded microprocessor, which is a computer processor or a microchip.
2. credit cards are lines of credit when you use a credit card, the issuer puts money toward the transaction.This is a loan you are expected to pay back in full unless you won't to be charged interest.	2. Any time you use a debit card to buy something, money is deducted from your account with a debit card you can really only spend the money you have available to you.	2. Smart cards applications benefit consumers where their life and business habits intersect with payment processing technologies.
3. credit cards in the U.S are not very secure and of themselves many still deted card technology.However consumers are not held liable for this poor security.	3. A PIN makes them secure so long as no one steals the card number and PIN as long as you don't lose the card itself.If the card is stolen, debit cards are very insecure .	3. Smart cards offer more security and confidentially than any other financial or transaction storage card the market.They are a safe place to store sensitive or personal information .
4.Credit Card Not required to be connected to a checking account.	4. Checking or saving accounts .	4. Smart cards links directly to the Internet .
5. Credit cards are mostly used in online payments, to sell things or the web.	5. Debit cards can be used with a PIN almost everywhere retail stores, gasoline, resturants and pay phones.	5. Smart cards widely used in telecommunications industry.
6. For the merchant credit card transactions result in	6. Debit cards are more readily accepted	6. The retail industry widely uses applications

	immediate credit to the merchants bank account.	by merchants than are checks.especially in countries where check cashing and check processing are not widely used.	of the smart card more specially to identify and reward customers.			