1) Discuss and explain the various types of malicious code and how they work. Include the different types of viruses.
Answer: Malicious code includes a variety of threats such as viruses, worms, Trojan horses, ransomware, and bot programs. A virus is a computer program that can replicate or make copies of itself and spread to other files. Viruses can range in severity from simple programs that display a message or graphic as a "joke" to more malevolent code that will destroy files or reformat the hard drive of a computer, causing programs to run incorrectly. Worms are designed to spread not only from file to file but from computer to computer and do not necessarily need to be activated in order to replicate. A Trojan horse is not itself a virus because it does not replicate but it is a method by which viruses or other malicious code can be introduced into a computer system. It appears benign and then suddenly does something harmful. For example, it may appear to be only a game and then it will steal passwords and mail them to another person. A backdoor is a feature of worms, viruses, and Trojans that allow attackers to remotely access compromised computers. Ransomware (or also known as scareware) is a type of malware (often a worm) that locks your computer or files to stop you from accessing them. Bot programs are a type of malicious code that can be covertly installed on a computer when it is attached to the Internet. Once installed, the bot responds to external commands sent by the attacker, and many bots can be coordinated by a hacker into a botnet.

2) Explain the difference between symmetric key encryption and public key encryption. Which dimensions of e-commerce security does encryption address?
Answer: Symmetric key encryption involves the use of a secret cipher that transforms plain text into cipher text. Both the sender and the receiver use the same key to encrypt and decrypt the message. The possibilities for simple substitution and transposition ciphers are endless, but there are several flaws in these types of systems that make them inadequate for use today. First, in order for the sender and the receiver to have the same key, it must be sent over a communication medium that is insecure or they must meet in person to exchange the key. If the secret key is lost or stolen, the encryption system fails. This method can be used effectively for data storage protection, but is less convenient for e-mail since the correspondents have to pass the secret key to one another over another secure medium prior to commencing the communication. Second, in the digital age, computers are so fast and powerful that these ancient encryption techniques can be quickly and easily broken. Modern digital encryption systems must use keys with between 56 and 512 binary digits in order to ensure that decryption would be unlikely. Third, for commercial use on an e-commerce site each of the parties in a transaction would need a secret key. In a population of millions of Internet users, thousands of millions of keys would be needed to accommodate all e-commerce customers.

Public key encryption solves the problem of exchanging keys. In this method every user has a pair of numeric keys: private and public. The public key is not secret; on the contrary, it is supposed to be disseminated widely. Public keys may be published in company catalogs or on the World Wide Web. The public key is used by outside parties to encrypt the messages addressed to you. The private or secret key is used by the recipient to decipher incoming messages. The main advantage of a public key cryptographic system is its ability to begin secure correspondence over the Internet without prior exchanging of the keys and, therefore, without the need for a meeting in person or using conventional carriers for key exchange.

Encryption can provide four of the six key dimensions of e-commerce security. It can provide assurance that the message has not been altered (integrity), prevent the user from denying that he/she has sent the message (nonrepudiation), provide verification of the identity of the message (authentication), and give assurance that the message has not been read by others (confidentiality).

3) What dimensions do digital signatures and hash digests add to public key encryption and how do they work?
Answer: Digital signatures and hash digests can add authentication, nonrepudiation, and integrity when used with public key encryption. Encryption technology also allows for digital signatures and authentication. The sender encrypts the message yet again using their private key to produce a digital signature.

To check the confidentiality of a message and ensure it has not been altered in transit, a hash function is used first to create a digest of the message. A hash function is an algorithm that produces a fixed-length number called a hash or message digest. To ensure the authenticity of the message and to ensure nonrepudiation, the sender encrypts the entire block of cipher text one more time using the sender's private key. This produces a digital signature or "signed" cipher text. The result of this double encryption is sent over the Internet to the recipient. Then, the recipient first uses the sender's public key to authenticate the message. Once authenticated, the recipient uses his or her private key to obtain the hash result and original message. As a final step, the recipient applies the same hash function to the original text and compares the result with the result sent by the sender. If the results are the same, the recipient now knows the message has not been changed during transmission. The message has integrity.

4) Discuss the security of communications channels. Include definitions and explanations for the terms *Secure Sockets Layer/Transport Layer Security (SSL/TLS)*, *secure negotiated session*, *session key*, and *VPN*.
Answer: The Secure Sockets Layer of the Transmission Control Protocol/Internet Protocol (TCP/IP) communications protocol is the main method for securing communications channels on the Web. When you receive a message from a Web server that you will be communicating through a secure channel, this means that SSL/TLS will be used to establish a secure negotiated session. A secure negotiated session is a client-server session in which the URL of the requested document, its contents, and the contents of the forms filled out by the user on the page, as well as the cookies that are exchanged, are all encrypted. The browser and the server exchange digital certificates with one another, determine the strongest shared form of encryption, and begin communicating using a unique symmetric encryption key, agreed upon for just this encounter. This is called a session key. SSL/TLS provides data encryption, server authentication, optional client authentication (as yet still rare for individual users), and message integrity for the TCP/IP connections between two computers.

SSL/TLS addresses the threat of authenticity by allowing users to verify another user's identity or the identity of a server. It also protects the integrity of the messages exchanged. However, once the merchant receives the encrypted credit and order information, that information is

typically stored in unencrypted format on the merchant's servers. While SSL/TLS provides secure transactions between merchant and consumer, it only guarantees server-side authentication. Client authentication is optional. In addition, SSL/TLS cannot provide irrefutability—consumers can order goods or download information products and then claim the transaction never occurred.

Virtual private networks (VPNs) enable remote users to access an internal network from the Internet. They use protocols to create a private connection between a user on a local ISP and a private network. This process is called tunneling because it creates a private connection by adding an encrypted wrapper around the message to hide its content. It is called virtual because it appears to be a dedicated secure line when in fact it is a temporary secure line. VPNs are used primarily for transactions between business partners because dedicated connections can be very expensive. The Internet and VPNs can be used to significantly reduce the costs of secure communications.

5) Explain how an online credit card transaction works, identifying the parties involved and describing how SSL/TLS is involved. What are the limitations of online credit card payment systems?
Answer: The five parties involved in a credit card transaction are the consumer, the merchant, the clearinghouse, the merchant bank (acquiring bank), and the consumer's card issuing bank. The basic payment transaction process works like this: The consumer first makes an online payment by sending his or her credit card information via an online form at the merchant's Web site. Once this information is received by the merchant, the merchant software contacts a clearinghouse (a financial intermediary that authenticates credit cards and verifies account balances). The clearinghouse contacts the card issuing bank to verify the account information. Once verified, the issuing bank credits the account of the merchant at the merchant's bank. The debit to the consumer account is transmitted to the consumer in a monthly statement. SSL is involved in sending the consumer's credit card information safe at the merchant's Web site. When the consumer checks out using the merchant's shopping cart software, a secure tunnel through the Internet is created using SSL/TLS. Using encryption, SSL/TSL secures the session during which credit card information will be sent to the merchant and protects the information from interlopers on the Internet.

There are a number of limitations to the existing credit card payment system, most importantly involving security, merchant risk, cost, and social equity. The security of the transaction is considered to be very poor because neither the merchant nor the consumer can be fully authenticated. The risk merchants face is high. Banks think of Internet credit card orders as the same type of transactions as mail orders or telephone orders. In these transactions, the credit card is not present. There is no way for the merchant to verify the legitimacy of the customer's card or identity before confirming the order. In these transactions, the merchant carries all the risk for fraudulent credit card use. Consumers can disclaim charges even though the items have already been shipped. Merchants also must pay significant charges. These high costs make it unprofitable to sell small items such as individual articles or music tracks over the Internet. Furthermore, credit cards are not very democratic. Millions of young adults and almost 100 million other adult Americans who cannot afford credit cards or who have low incomes and are,

therefore, considered poor credit risks cannot participate in e-commerce as it is presently structured in the United States.

6) Define and explain how EBPP systems work. Describe each of the main EBPP business models.
Answer: EBPP refers to electronic billing presentment and payment systems, which are forms of online payment systems for monthly bills. Analysts expect electronic bill presentment and payment to become one of the fastest growing e-commerce businesses in the United States over the next several years because everyone involved stands to benefit from the process. Billers will cut costs by eliminating printing, paper, envelopes, postage, and the processing of paper checks and payments. Furthermore, EBPP will offer billers an opportunity to enhance customer service and target market. Customers will save time and eliminate checks and postage. Companies can use EBPP to present bills to individual customers electronically or they can contract with a service to handle all billing and payment collection for them. There are two main types of EBPP business models: biller-direct and consolidator. In biller-direct systems, a biller delivers the bill to customers via its own Web site or via a third-party's site. A service bureau is often used to provide the necessary infrastructure. The second major type of EBPP business model is the consolidator model. In this model, a third party, such as a financial institution or portal, aggregates all bills for consumers and ideally permits one-stop bill payment (pay anyone).