College English Model Test ThreeBand FourPart   Writing(30 minutes) Directions: For this part, you are allowed thirty minutes to write a letter to your American friend Lawrence, to introduce Spring Festival in China and invite him to join you to spend this Spring Festival. Suppose you are Yuan Chao. You should write at least 120 words following the suggestions given below in Chinese: 1.   Lawrence   2.   3.   Lawrence   :   1   A Letter to LawrenceSeptember 23, 2005Dear Lawrence, Yours,Yuan Chao Part   Reading Comprehension (Skimming and Scanning) (15 minutes) Directions:In this part,you will have 15 minutes to go over the passage quickly and answer the questions on Answer Sheet 1. For questions 1-7,markY (for YES) if the statement agrees with the information given in the passage.N (for NO) if the statement contradicts the information given in the passage.NG (for NOT GIVEN) if the information is not given in the passage.For questions 8-10,complete the sentences with information given in the passage. Computer CrimeA computer crime is generally defined as one that involves the use of computers and software for illegal purposes. This doesn't mean that all the crimes are new types of crime. On the contrary, many of these crimes, such as embezzlement of funds, the alteration of records, theft, vandalism, sabotage, and terrorism, can

be committed without a computer. But with a computer, these offenses can be carried out more quickly and with less chance that the person responsible for the crime will be discovered. Computer crimes are on the rise and have been for the last twelve years. Just how much these computer crimes cost the American public is in dispute, but estimates range from 3 billion to 5 billion annually. Even the FBI, which attempts to keep track of the growth or decline of all kinds of crimes, is unable to say precisely how large a loss is involved. however, it estimates that the average take from a company hit by computer crime is 600,000. A number of reasons are given for the increase in computer crime: (A) more computers in use and, thus, more people who are familiar with basic computer operation. (B) more computers tied together in satellite and other datatransmission networks. and (C) the easy access of microcomputers to huge mainframe data bases. The CriminalMovies and newspaper stories might lead us to believe that most computer crimes are committed by teenage " hackers" brilliant and basically good children who let their imagination and technical genius get them into trouble. But a realistic look at the crimes reveals that the offender is likely to be an employee of the firm against which the crime has been committed, i.e., an " insider" .Difficulty of Detection and PreventionGiven the kind of person who commits a computer crime and the environment in which the crime occurs, it is often difficult to detect who the criminal is. First of all, the crime may be so complex that months or years go by before anyone discovers it. Second, once the crime has been revealed, it is not easy to find a clear

trail of evidence that leads back to the guilty party. After all, looking for " weapons" or fingerprints does not occur as it might in the investigation of more conventional crimes. Third, there are usually no witnesses to the computer crime, even though it may be taking place in a room filled with people. Who is to say if the person at the next terminal, calmly keying in data, is doing the company' s work or committing a criminal act?Fourth, not enough people in management and law enforcement know enough about computer technology to prevent the crimes. Authorities have to be familiar with the computer' s capabilities within a given situation to guard against its misuses. In some large cities, such as Los Angeles, police departments have set up specially trained computer crime units.But even when an offender is caught, the investigators, attorneys (   ), judges, or juries may find the alleged crime too complicated and perplexing to handle. More attorneys are specializing in computer law and studying the computer' s potential for misuse. After a computer crime has been discovered, many companies do not report it or prosecute   the person responsible. A company may not announce the crime out of fear that the pubic will find out the weaknesses of its computer system and lose confidence in its organization. Banks, credit card companies, and investment firms are especially sensitive about revealing their vulnerabilities (because they rely heavily on customer trust.To avoid public attention, cautious companies will often settle cases of computer tampering out of court. And if cases do go to trial and the offenders are convicted, they may be punished only by a fine or light sentence

because the judge or jury isn't fully trained to understand the nature and seriousness of the crime. 100Test