Computer not many encryption procedures out for

Computer Fraud and CrimesIn the world of computers, computer fraud and computer crime are very prevalentissues facing every computer user. This ranges from system administrators topersonal computer users who do work in the office or at home. Computers withoutany means of security are vulnerable to attacks from viruses, worms, and illegalcomputer hackers. If the proper steps are not taken, safe computing may becomea thing of the past.

Many security measures are being implemented to protectagainst illegalities. Companies are becoming more aware and threatened by the fact that theircomputers are prone to attack. Virus scanners are becoming necessities on allmachines. Installing and monitoring these virus scanners takes many man hoursand a lot of money for site licenses. Many server programs are coming equippedwith a program called " netlog.

" This is a program that monitors the computer useof the employees in a company on the network. The program monitors memory andfile usage. A qualified system administrator should be able to tell by theamounts of memory being used and the file usage if something is going on thatshould not be. If a virus is found, system administrators can pinpoint the userwho put the virus into the network and investigate whether or not there was anymalice intended. One computer application that is becoming more widely used and, therefore, morewidely abused, is the use of electronic mail or email. In the present day, illegal hackers can read email going through a server fairly easily. Emailconsists of not only personal transactions, but business and financialtransactions. There are not many encryption procedures out for email yet.

AsGates describes, soon email encryption will become a regular addition to emailjust as a hard disk drive has become a regular addition to a computer (Gatesp. 97-98). Encrypting email can be done with two prime numbers used as keys. The publickey will be listed on the Internet or in an email message.

The second key willbe private, which only the user will have. The sender will encrypt the messagewith the public key, send it to the recipient, who will then decipher it againwith his or her private key. This method is not foolproof, but it is not easy tounlock either. The numbers being used will probably be over 60 digits in length(Gates p. 98-99). The Internet also poses more problems to users. This problem faces the homeuser more than the business user.

When a person logs onto the Internet, he orshe may download a file corrupted with a virus. When he or she executes thatprogram, the virus is released into the system. When a person uses the WorldWide Web(WWW), he or she is downloading files into his or her Internet browserwithout even knowing it.

Whenever a web page is visited, an image of that pageis downloaded and stored in the cache of the browser. This image is used forfaster retrieval of that specific web page. Instead of having to constantlydownload a page, the browser automatically reverts to the cache to open theimage of that page. Most people do not know about this, but this is an exampleof how to get a virus in a machine without even knowing it. Every time a person accesses the Internet, he or she is not only accessing thehost computer, but the many computers that connect the host and the user. Whena person transmits credit card information, it goes over many computers beforeit reaches its destination.

An illegal hacker can set up one of the connectingcomputers to copy the credit card information as it passes through the computer. This is how credit card fraud is committed with the help of the Internet. Whatcompanies such as Maxis and Sierra are doing are making secure sites.

Thesesites have the capabilities to receive credit card information securely. Thismeans the consumer can purchase goods by credit card over the Internet withoutworrying that the credit card number will be seen by unauthorized people. System administrators have three major weapons against computer crime. Thefirst defense against computer crime is system security. This is the manylayers systems have against attacks. When data comes into a system, it isscanned for viruses and safety. Whenever it passes one of these security layers, it is scanned again.

The second resistance against viruses and corruption iscomputer law. This defines what is illegal in the computer world. In