1. Please read the following news story carefully before answering questions. (35%)

A little-known legal skirmish in the case of the computer hacker Kevin Mitnick was a preview of similar fights to come as more people use encryption software to protect their files, lawyers who were involved in the case say.

Mitnick left federal prison last week after serving nearly five years for a series of crimes involving computer fraud and wire fraud. But his lawyers say they are still troubled by the judge's answer to a legal question raised early in the case: When federal agents seize encrypted files from a defendant, can they refuse to return them unless the defendant turns over the secret "key" to decode the files?

That digital-age puzzle, which the judge regarded as a novel legal question, arose in Mitnick's case in a circuitous manner, as sometimes happens in criminal trials.

In the course of the government's investigation, federal agents in 1994 and 1995 seized two laptop computers owned by Mitnick, according to Gregory L. Vinson, a lawyer who worked on the Mitnick defense team that was headed by Donald C. Randolph, a veteran criminal defense specialist in Los Angeles.

On the computers' hard drives were approximately nine gigabytes of electronic evidence, Vinson said in an interview. He estimated that of that total, perhaps one gigabyte consisted of encrypted files -- documents that were unintelligible to anyone who did not have a key to decrypt them. Mitnick, of course, had the key.

During the pre-trial discovery phase of the case, the government lawyer, Christopher Painter, an assistant United States attorney in Los Angeles, indicated that as required by the rules governing evidence, he would hand all of the seized files over to the defense -- except the encrypted ones.

That set the stage for a hearing on May 20, 1998, before federal judge Mariana R. Phaelzer in Los Angeles. Speaking for the defense, Randolph argued that Mitnick was entitled to copies of the seized encrypted files under two legal theories, according to a transcript of the hearing.

First, he contended, under Rule 16 of the Federal Rules of Criminal Procedure, which establish the ground rules for the government's disclosure of evidence to the defendant, the government must allow a defendant to inspect or copy documents that "were obtained from or belong to the defendant." Since the encrypted files belonged to Mitnick, he deserved to get a copy of them, Randolph said.

The defense also argued that the encrypted files might include information that could help Mitnick defend himself. Under the Constitution, the prosecution is obligated to hand over such material to the defense.

Painter replied that because the government could not understand what was in the files, it could not use the files as evidence at trial. He also said that Rule 16 did not apply because the encrypted files in a sense were not "really in our possession," because "we don't know what's there."

But the heart of the government lawyer's argument was that it would be wrong to hand over the files because they could contain the spoils of Mitnick's crimes -- secret information that he
illegally acquired from the companies whose computers he hacked into -- or something even more dangerous.

"For all we know, it could be plans to take down a computer system," Painter said at the hearing. "We don't know. And we think it's dangerous to release that, and that's why we don't want to release it. We're not going to use it, certainly, but we think that there's reasons not to release that information."

In considering the matter, Judge Phaelzer said that it was "clever" of Mitnick to have encrypted the files in such a way that the government could not use them in its own case but Mitnick could access them if given a copy. She asked: "Now, you know, what's the court supposed to do with that position?"

Painter said the situation was akin to Mitnick asking for his coat back and the government not knowing if there was a pistol in the pocket. Judge Phaelzer agreed, ruling that "this court is not going to order the encryptive material to be given" to Mitnick.

The judge added that if Mitnick would "tell the government how to read" the files, then the government would turn over the files in decrypted form.

Mitnick's lawyers immediately objected to this condition on the grounds that it would force him to waive his Fifth Amendment right against self-incrimination to obtain evidence he needed and that he had a legal right to see. The judge rejected this point and repeated her ruling.

Vinson, the defense lawyer, said in an interview this week that he still thought Judge Phaelzer's ruling from the bench did not give enough weight to the defense's arguments. He said he was worried that the case might create the impression that the government has no obligation to give back encrypted files that it has been unable to decrypt.

"In ten years, when encryption becomes commonplace for people to use in order to protect their files, whether their files contain financial records, conversations with their spouse or a local drug dealer, the government is going to seize the files in a criminal case, and [government lawyers] will be faced with the same situation as they were in the Mitnick case," Vinson said.

Painter, reached by telephone earlier this week, said both sides in the pre-trial legal battle over Mitnick's encrypted files had strong arguments.

He said he agreed with Vinson that similar disputes may arise in the future as more people encrypt files. But he maintained that no precedent had been set, and that the government's responses would be on a case-by-case basis.

"It could be that in future cases, depending on the circumstances, it would be more appropriate to return [encrypted files] under special procedures," Painter said.

Gerald Lynch, a law professor at Columbia University who is an expert in criminal law and a former federal prosecutor, said in an interview that it was a "panic response" on the part of the court and the government to deny Mitnick access to his files.

"If you think about this reasonably, the answer is that if the government does not have a reasonable basis to contend that something really dangerous [is in the encrypted files], and merely does not know what is in the files and can't decode them, then they should hand them over," he said.
Alan B. Davidson, a staff lawyer who follows encryption developments for the Center for Democracy and Technology, a civil liberties group, said he believed the Mitnick encryption dispute is a precursor to a coming battle in Congress.

As part of a compromise announced this fall by the Clinton administration that loosened export restrictions on strong encryption software, the administration has committed to sending a bill to Congress laying out rules for when the government can get access to encryption keys, Davidson said.

"We are anxiously awaiting the administration's new bill, which will open up a huge debate," he said.

Questions:
(Attention: Answer for question 6 must be in Chinese. Questions 1 to 5 are single-choice, and a 1-point penalty will be assessed to each wrong answer.)

1. Which of the following is not a point of contention between the parties in this case? (4%)
   A) Whether the government should return the encrypted files to the defendant
   B) Whether the Federal Rules of Criminal Procedure gives Mitnick a right to ask for the encrypted files
   C) Whether Mitnick should give the government keys to decrypt those files before he could get them back
   D) Whether disputes over encrypted files will increase in the future
   E) Whether the judge's ruling in this case would serve as a chilling precedent

2. Which of the following is not an established "fact" according to the story? (4%)
   A) Federal agents seized two laptop computers owned by Mitnick in 1994 and 1995 during its investigation.
   B) It was a "panic response" on the part of the court and the government to deny Mitnick access to his files.
   C) The government could not decode Mitnick's encrypted files.
   D) The Clinton administration promised to send a bill to Congress that would lay out rules for when the government can get access to encryption keys.

3. Which of the following was not a federal employee at that time? (3%)
   A) Donald C. Randolph
   B) Mariana R. Phaelzer
   C) Christopher Painter
   D) William Jefferson Clinton

4. Which of the following statements is true according to the story? (4%)
   A) In ten years encryption would becomes commonplace for people to use in order to protect their files.
   B) The government could not decrypted Mitnick's files because they did not know the encryption algorithm used by Mitnick.
   C) The Clinton administration submitted a bill to the Congress regarding when the government should get access to encryption keys.
D) Gerald Lynch was critical of the Court’s ruling on this matter.
E) Mitnick did not get adequate defense because he could not get access to those encrypted files.

5.) Which of the following statements about the ruling is true? (4%)
A) The Center for Democracy and Technology did not welcome the ruling.
B) Before the ruling, the defendant’s lawyer rejected Judge Vinson’s offer to surrender decryption keys in exchange for access to decrypted files.
C) The ruling touched on an issued unimaginable to the framers of the Constitution.
D) Ruling? What ruling? There was no ruling!

6.) What are the legal theories used by the defense team to get those encrypted files back, and what are the prosecuting team’s responses? (16%)

2. Please translate the following paragraph sentence by sentence into Chinese. (35%)

(1) Why is blackmail illegal? The crime is defined as an "unlawful demand of money or property under threat to do bodily harm, to injure property, to accuse of crime, or to expose disgraceful defects." (2) It is easy to understand that the demand of money is unlawful when the accompanying threats are of bodily harm of property damage. After all, these threats themselves are illegal on other grounds. (3) It is also possible to explain why you cannot demand money as the price of refraining from accusing someone of a crime. (4) But what about the case where a private individual asks another private individual for money as the price of not revealing legally obtained information about activities perfectly legal in themselves: (5) "If you do not pay me $100, I will reveal to your boyfriend the fact that I saw you coming out of another man's house at two o'clock in the morning." (6) After all, in this case it would be perfectly legal to carry through with the threat. (7) Clearly, the person being blackmailed does not wish to pay, but then many of us do not wish to pay when others ask money from us, telling us that if we do not comply with their demands they will carry out some legal and unpleasant course of action. (8) How is blackmail different from a baseball team "demanding" concessions from a city and local residents (in the form of tax reductions and parking spaces, for example) under threat of moving the team to another city? (9) It begs the question to say that the baseball team has a right to do so, whereas the blackmailer does not.
3. The following paragraphs are abridged from a brief amicus curiae in the Napster case. Please translate them into Chinese. (30%)

Copyright law has never given copyright owners control over all uses of their works. Rather, it gives copyright owners exclusive rights and expressly subjects those rights to a host of exceptions. See 17 U.S.C. §§ 106-122, 1008. Of particular relevance here, the law allows unauthorized copies, downloads, uploads, transmissions or distributions that might be fair use under § 107, lawful noncommercial consumer copies under § 1008, or private performances and transmissions over which the statute gives the copyright owner no control. In Sony Corp. of America v. Universal City Studios, 464 U.S. 417 (1984), the court makes plain that facilitation of such unauthorized but lawful uses is sufficient as a matter of law to constitute the capability for substantial noninfringing use.

The district court rejected Napster’s arguments that some or all of its users’ file trading activity might be permitted under 17 U.S.C. §1008 or the fair use doctrine codified in 17 U.S.C. §107. Yet the issue whether and when individual consumers may be liable under the copyright act for making noncommercial copies of recorded music for their personal use is a difficult one, requiring careful and thoughtful analysis. It seems evident that if individuals may legally engage in massive free copying of recorded music, a potential source of copyright owners’ revenue may be undermined. It seems equally clear, however, that the exercise of a statutory privilege does not become illegal merely because many people engage in it.

The District Court Applied an Inappropriately Narrow View of Fair Use

The district court’s analysis of fair use gave the doctrine unduly limited scope in the online context. Individual users who use Napster to share MP3 files for their personal use are engaging in consumptive rather than transformative use, but are also engaging in noncommercial personal use, which has traditionally been within the core of uses considered to be fair. The district court was unwilling to consider Napster users’ activities to be personal or private use, both because files were transmitted over the Internet and because of the “vast scale of Napster use.” The court’s reluctance is understandable, but problematic.

Most Internet-related activity involves the transfer of files over the Internet. The use of the Internet is growing at an extraordinary pace. There is a very real possibility that within our lifetimes, the Internet will be become a dominant if not the dominant medium for both personal and commercial communication in the U.S. Because individual consumers’ activities over digital networks can be tracked and recorded, a whole realm of personal uses that were essentially undetectable in the offline world become a matter of record when conducted online. Moreover, the nature of digital technology means that many activities analogous to non-infringing acts in the offline world become at least technical infringements when conducted over the Internet. Traditionally, loaning or giving a book or record to a friend infringed no rights under copyright; the distribution came within the first sale doctrine. On the Internet, however, the analysis is different. Under current technology, one cannot share material over the Internet without both reproducing it multiple times and transmitting it. The need for a balanced fair use privilege in the online world is at least as crucial as it is in the offline world.