1.

(A) Is it possible for a job to have a shorter turnaround time under a multiprogramming operating system than under a single-job system for the same machine? (10%)

(B) How might the operating system detect that a deadlock has occurred? (10%)

2.

(A)Describe the two parameter passing techniques :
Call-by-Reference (Address) and Call-by-Value. (5%)

(B)For the following program:

```
int i , b [2];
main( )
{
b [1]=1;
b [2]=1;
i =1;
sub (b [1] );
}

void sub (x)
int x;
{
i =1;
x=x+2;
b (i )=10;
i =2;
x=x+2;
return;
}
```

(1) If Call-by-Reference is used, show the values of i , b [1], b [2] at the end of program execution. (5%)

(2) Repeat (1) if Call-by-Value is used. (5%)

3. Describe the following three Medium Access Control (MAC) protocols :

(A) Carrier Sense Multiple Access (CSMA) (5%)

(B) Carrier Sense Multiple Access with Collision Detection (CSMA/CD) (5%)

(C) Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) (5%)

國立交通大學八十六學年度碩士班入學考試試題

科目：403系統程式（資訊管理研究所甲組）　　第 2 頁，共 3 頁

※作答前，請先核對試題、答案卷(試卷)與准考證上之所組別與考試科目是否相符!!

4.

請閱讀所附的短文"Risks of Anonymity"後，回答下列的問題。

限以中文作答

(1) 解釋名詞（每小題 4 分，計 20 分）

1. true anonymity
2. pseudo-anonymity
3. pseudonymity
4. authentication of users
5. confidentiality and integrity of contents

(2) 這篇短文的作者所想表達的觀點是什麼？（15 分）

(3) 請申論密碼學（Cryptography）在資訊社會中，特別是電子商業（electronic commerce）的環境中，所提供的技術性與社會性功能。（15分）

Risks of Anonymity

Anonymity is a sticky wicket in the online world, especially in digital commerce and email. Profound social and technological risks arise from anonymity and from the loss of anonymity—somewhat similar to privacy problems familiar to regular readers of this column. An important challenge confronts us to improve our understanding of these risks and to anticipate the effects of their future manifestations.

There is a spectrum of identity masking, with respect to individuals and computerized agents. *True anonymity* means *no one* knows who you really are. (On the Internet, no one knows that you're a dog.) It is very difficult to achieve, as noted in our October 1996 column on Disinformation Theory. *Pseudo-anonymity* means your identity is not generally known, but can be obtained—perhaps only under prescribed (and carefully controlled) circumstances. For example, your identity could be known to a pseudo-anonymizing email service or an identity-masking escrow agent. It could be compromised by someone penetrating the database of associations between real and pseudo identities. *Pseudonymity* means alternative identities may be used, either anonymously or pseudo-anonymously. (For example, America Online allows any customer to have up to six identities, all of which may be aliases.)

Some form of anonymity is clearly desirable for people who are seriously threatened in one way or another—whistle-blowers, victims of violence and hate crimes, and so on. However, anonymity can easily be abused—for example, by false accusers and perpetrators of hate crimes, frauds, and pranks—perhaps seeking to evade responsibility and accountability. As usual, the presence of electronic media can considerably escalate the risks—geographically, chronologically, and consequentially.

Pseudo-anonymous remailing services typify one way in which anonymity can be attempted with email. Perhaps the most popular was Johan Helsingius's anon.penet.fi remailer in Finland, which provided each sender with a unique aliased email address through which mail could be sent, and at which replies could be received—without revealing the actual address or identity. Helsinglus has closed down his free remailer, after having experienced a variety of problems—threats from law enforcement, pressures from The Church of Scientology to identify a source, and false accusations of having transmitted pornographic images. (The remailer was designed to reject graphical images.)

Anonymity in electronic commerce represents another huge conflict. Although it may seem desirable to have anonymous electronic cash and anonymous financial transactions, some significant measure of accountability is absolutely essential to prevent misuse. For example, the Internal Revenue Service seeks to prevent unaccountable large transactions, and law enforcement seeks to prevent money laundering. Similarly, anonymous contributors presumably want assurances that their contributions are actually going to the proper charity. Indeed, anyone sending virtual money would like to ensure that payments are not being diverted to some untraceable recipient. However, the mere existence of accountability logs is always a potential source of risks—as illustrated by the ability to track an individual's activities through credit-card purchases, telephone charges, and other records. In general, the absence of accountability and the presence of anonymity suggest the need for mutual suspicion rather than blind trust.

Cryptology provides some interesting protocols that can enhance both pseudo-anonymity and accountability, by providing authentication of users and systems, as well as confidentiality and integrity of content. However, we must be very skeptical if those protocols are embedded in an infrastructure that is not as well conceived—for example, implemented on a seriously vulnerable operating system, or on a smartcard whose keys can be compromised by one trick or another, or on network sites whose identities can be forged. There are many real misuses that can compromise identities, including opportunities for insider collusion, deceptive aliases, tampering with the controls, malicious alterations of audit trails and accountability information, and surreptitious tracking of individuals through inferences drawn from logs, databases, and unencrypted headers. From a realistic electronic-system point of view, true anonymity is both riskful and unachievable.

Technology for pseudo-anonymity must not be easily subvertible and should support both good accountability and good anonymity. In addition, the laws and social conventions must meaningfully discourage misuse. This requirement transforms the problem back into security problems of operating systems and networks, seamless incorporation of sound cryptography, and trustworthiness of operational procedures and people (including those in any key-recovery or key-escrow processes). Unfortunately, that is the classic technique of "reduction to a previously unsolved problem." As usual, the risks abound. ◻

Read the online Risks Forum at comp.risks or subscribe at risks-request@CSL.sri.com; its moderator, Peter G. Neumann, chairs the ACM Committee on Computers and and Public Policy.