a. Users often mix up user-ID and password at login prompts. How should the designer of a login function take this into consideration?

b. The log file of your HTTP server shows odd requests such as
   GET /scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+C:
   GET /scripts/..%u002f..%u002fwinnt/system32/cmd.exe?/c+dir+C:
   GET /scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+dir+C:

c. (2004 P3 Q9) Consider the standard POSIX file-system access control mechanism:
   • Under which conditions can files and subdirectories be removed from a parent directory?
   • Many Unix variants implement an extension known as the sticky bit. What is its function?
   • On a POSIX system that lacks support for the sticky bit, how could you achieve an equivalent effect?

d. Which of the Unix commands that you know or use are setuid root, and why?

e. Which Unix command finds all installed setuid root programs?

f. Briefly describe three common software vulnerabilities. Explain stack buffer overflow attack. Name four ways to make it more difficult to exploit. What counter-measures are there to mitigate stack overflow vulnerabilities?

g. (2002 P8 Q6) Explain the concept of a Trusted Computing Base and outline its meaning in the context of the access control provided by a typical Unix workstation.

h. Explain briefly mechanisms that software on desktop can use to securely generate secret keys for use in crypto protocols

i. Give two different ways of implementing residual information protection in an operating system and explain the threat addressed by each.
j. VerySafe Ltd offers two vaults with electronic locks. They open only after the correct decimal code has been entered. The VS100, a low-cost civilian model, expects a 6-digit code. After all six digits have been entered, it will either open or it will signal that the code was wrong and ask for another try. The VS110, a far more expensive government version, expects a 40-digit code. Users of a beta-test version of the VS110 complained about the difficulty of entering such a long code correctly. The manufacturer therefore made a last minute modification. After every five digits, the VS110 now either confirms that the code has been entered correctly so far, or it asks for the previous five digits again. Compare the security of the VS100 and VS110.

k. A and B play a simple game. A chooses a number $R_A \in \mathbb{Z}_3$ and B chooses a number $R_B \in \mathbb{Z}_3$. Then A and B communicate their respective choice to each other simultaneously, meaning that the players cannot change their choice after having seen that of the opponent. These rules decide who wins the game:

\[
\begin{cases} 
R_A = R_B + 1 \pmod{3} & \text{then A wins} \\
R_B = R_A + 1 \pmod{3} & \text{then B wins}
\end{cases}
\]

(1)

In any other case, the result of the game is a draw.

(a) What complication arises when this game is played at a distance, for example via email?

(b) Suggest a cryptographic protocol that prevents cheating when this game is played via email. Your solution should not rely on a trusted third party.

(c) What assumptions do you make about the cryptographic functions used in your solution of [kb]?

(d) What assumptions do you make about the amount of computing power available to the opponent in your solution of [kb]?

l. Alice wants to attack Bob’s computer via the Internet, by sending IP packets to it, directly from her own computer. She does not want Bob to find out the IP address of her computer.

(a) Is this easier to achieve for Alice with TCP- or UDP-based application protocols? Explain why.

(b) For the more difficult protocol, explain one technique that Alice could try to overcome this obstacle and one countermeasure that Bob could implement in his computer.

(c) Name three things that Alice’s Internet service provider might do to make it more difficult for Alice to achieve her goal.

m. How can we construct a MAC (Message Authentication Code) from a secure hash function?

n. How can we construct a MAC from a block cipher (use Supervision 2 to fall back to question [m]).
o. A source of secure, unpredictable random numbers is needed to choose cryptographic keys and nonces.

- Name six sources of entropy that can be found in typical desktop computer hardware to seed secure random-number generators.
- What sources of entropy can a smartcard chip, like the one in your University Card, access for this purpose?

p. A C program uses the line:

```c
buf = (char *) malloc((n+7) >> 3);
```

in order to allocate an $\lceil n/8 \rceil$ bytes long memory buffer, large enough to receive $n$ bits of data, where $n$ is an unsigned integer type.

- How could this line represent a security vulnerability?
- Modify the expression that forms the argument of the `malloc()` call to avoid this vulnerability without changing its normal behaviour.

q. Outline briefly the purpose of an organization’s security policy and what steps should be considered in its development