

# IY5512: Coursework 5

---

If feedback is required, coursework solutions must be submitted electronically, as an email attachment, to the following email address: [me@chrismitchell.net](mailto:me@chrismitchell.net).

Coursework submissions should normally be in the form of a single pdf file. If you use Word, a free add-on to enable you to save a document in pdf format can be obtained from the Microsoft web site.

Take care to ensure that you include your full name on the first page of your submission, the course number (IY5512), and the coursework number.

These questions are designed to test and extend your understanding of Part 5 of the course material.

1. What precautions should be taken when choosing passwords?
2. What is wrong with the following 'challenge-response' user identification system?

Every user has a calculator capable of displaying 11 digits, and every also has a secret 10-decimal digit password. When a user wishes to authenticate him/herself to the system, the system generates a random 10-digit number and sends it to the user. The user (using the calculator) computes the sum of his/her secret password and the random number and returns it to the system, which then performs the same calculation (and hence verifies the user's identity).
3. How can the S/KEY system be attacked if a malicious party succeeds in impersonating the host?
4. Distinguish between user *identification* and identity *verification* schemes. List the five component modules of an architecture for a typical biometric system for personal identification, and briefly describe the purpose of each module.
5. Think of a human characteristic (not mentioned in the course notes) that might be used for identity verification for computer users. What sort of parameters would you measure?
6. What are meant by Type I and Type II errors in a human authentication system? Describe how this relates to threshold setting.
7. Describe how an identity management system based on the use of HTTP redirects can be attacked. How can the damaging effects of such an attack be reduced?