

# Quiz 6 Solutions

Wed Apr 26

1. Which of the following password schemes is the more secure authentication mechanism? Explain why and provide evidence.

- (a) A 5-digit PIN (digits 0–9 only).
- (b) A 3-character password consisting of lower-case letters and digits.

The first password scheme has  $10^5$  possibilities, which is 100,000.

The second scheme is  $(26 + 10)^3 = 36^3 = 46,656$ .

So scheme (a) is better.

2. Explain how some web sites approximate *two-factor authentication* when you log in. Which categories of authentication are they using?

The categories are:

- (a) Something you **know**
- (b) Something you **have**
- (c) Biometric

Usually a web site asks for your user name and password, which is entirely category (a) – something you know. When web sites do two-factor authentication, they typically send a unique random code to your phone as a text message, and then you have a limited amount of time in which to type in that code. So it (more or less) involves something you **have** – your phone.