Exam Format

The exam is three hours in a PC lab. You answer 4 questions from 6, each question is worth 25 marks. General comment:

1. I am expecting good grammar and spelling in your exam.
2. Unless explicitly stated to the contrary, if I say ‘solve’ then you are free to use brute force.
3. Keep your sentences short, clear, and devoid of ambiguity. If it helps use lists.

Moodle Resources

6 slides follow - one for each question Some terminology: if

1. ✓- this question covers ‘core’ material, as such my slides are detailed and Java code solutions are online
2. ✗- this question is on a more peripheral area, my slides are less detailed and Java code solutions are not complete.

A revision strategy would be to concentrate on the ✓questions.

Q1 ✗

1. What do prime, *composite, pseudoprime* to the base, *Carmichael number* mean?
2. Determine if a given n is a Carmichael number
3. What is a Miller-Rabin witness?
4. Determine all the witnesses for a given n.

Q2 ✓

1. Explain in general terms how a secure connection can be established over an insecure channel
2. What do the terms *greatest common denominator* and *relatively prime* mean
3. Implement (Java or pen and paper) Euclid's algorithm to determine the gcd of two numbers.

Q3 ✗

1. Explain the terms *block cipher* , *stream cipher*.
2. Describe the permutation group S_3
3. ECB, CCM and CFB are cryptographic terms; compare and contrast
4. Discuss why AES is deemed an improvement on DES.

Q4 ✓

This question is on the Diffie-Hellman

1. Describe the Diffie-Hellman protocol.
2. Evaluate the keys for some particular numbers.
3. Discuss why Eve has difficulty finding the shared secret.

Q5 ✗

1. Know the meaning of *prime number*, *cyclic group*, be able to perform simple calculations on $\mathbb{Z}_p^*$, $p =$prime,.
2. Solve $2^x = a \mod b$
3. Describe qualitatively (no code required) attack strategies to the discrete log problem
4. Describe $\mathbb{F}_{3^2}$.

Q6 ✓

Open question - it relates to employability skills - you are in a job interview and the interviewer asks two questions:

1. What do the following terms mean *cryptocurrency*, *bitcoin*, *blockchain*, *mining* and explain briefly how they work?
2. Do you think bitcoin will be about in ten years?

I am looking for one page of well-reasoned argument. Lynda has tutorials and lectures covering most of the above.