

## IY2760/CS3760: Coursework 2

Coursework 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. It would greatly help me if you could name the attachment <lastname>\_<initial>\_2.pdf (e.g. Mitchell\_C\_2.pdf).

Take care to ensure that you include your full name on the first page of your submission, and also the course name and coursework number (i.e. 2).

1. Explain how, if a CBC-MAC is computed without the Optional process, two one-block messages and MACs can be combined to give a 'bogus' two-block message with a valid MAC. Describe how this approach can be extended to combine two messages of arbitrary length. How does the optional process protect against this attack?
2. State, with an explanation, whether or not the following active attacks can be detected by the use of a MAC:
  - Alteration or replacement of a message;
  - Deletion of a message;
  - Insertion of a false message;
  - Replay of an old message;
  - Changing the order of two or more messages;
  - Falsifying the origin of a message.
3. **Encryption does not provide message integrity protection.** Describe, with the aid of simple examples, why this is true when a stream cipher is used for encryption. That is, show how an interceptor of a ciphertext message can manipulate the contents of a message without detection and with known effects on the message. Describe, again using a simple example, how much more serious such an attack can be if the attacker knows part of the plaintext for the intercepted ciphertext.
4. What is the main difference between a conventional encryption system and a public key encryption scheme?
5. Suppose that RSA is used to encrypt a 2-bit message without any randomisation of the plaintext, and suppose also that an interceptor of the ciphertext knows the plaintext message only contains two bits of data (i.e. it is one of '00' '01', '10' and '11'). Can the cryptanalyst discover the plaintext (suppose that the cryptanalyst knows the public encryption key used to encipher the message), and, if so, how?
6. Distinguish between digital signatures giving message recovery and digital signatures without message recovery.

7. How can RSA be used as the basis of a signature scheme without message recovery? What extra cryptographic functions do you need, and what properties should they have?

**DEADLINE:** 23:59, Friday 28th October 2011