HET317 Tutorial Sheet 9

Questions

1. When constructing a digital signature, why is the hash of the message, rather than the message itself, signed?

   Three reasons:

   - Encrypted documents are similar in size to their plaintext form. We would like signatures to be a consistent, small size
   - Public key cryptography is very slow. While this might not matter for small documents, for large documents (including digital videos and software which can be very large) it is significant.
   - By introducing a hash-function into the process, the possibility of cryptanalysis attacks is greatly reduced.

2. Use the one-time-pad 1010011000 to encrypt and decrypt the message 1111011001

Plain text	1111011001
One time pad	1010011000
Cipher text	0101000001

Cipher text	0101000001
One time pad	1010011000
Plain text	1111011001

3. Bob wishes to send a message to Alice. He wants to encrypt it and digitally sign it using public key encryption.
   a. Which key will Bob use to encrypt the message?

      Alice's public key

   b. Which key will Bob use to sign the message?

      Bob's (his own) private key

   c. Which key will Alice use to decrypt the message?

      Alice's (her own) private key

   d. Which key will Alice use to validate the digital signature?

      Bob's public key

HET317 Tutorial Sheet 9

4. The following S-Box (S_1 from the DES standard) maps a six bit input to a four bit output. What will be the output of this box when presented with an input of 7. (All values are base 10.)

   Convert input to binary. 7 = 111.

   Input into an S-Box is six bits so input is 000111.

   Use two outer bits to index the row. Outer 2 bits are 01 = 1 so the row is 1

   Use inner four bits to index the column. Inner 4 bits are 0011 = 3 so the column is 3.

   Value is then 4.