

## Tutorial Week 9

### Questions

1. When constructing a digital signature, why is the hash of the message, rather than the message itself, encrypted?
2. Use the one-time-pad 1010011000 to encrypt and decrypt the message 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?
  - b. Which key will Bob use to sign the message?
  - c. Which key will Alice use to decrypt the message?
  - d. Which key will Alice use to validate the digital signature?
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.)

| Row / Column | 0  | 1  | 2  | 3 | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 | 12 | 13 | 14 | 15 |
|--------------|----|----|----|---|----|----|----|----|----|----|----|----|----|----|----|----|
| 0            | 14 | 4  | 13 | 1 | 2  | 15 | 11 | 8  | 3  | 10 | 6  | 12 | 5  | 9  | 0  | 7  |
| 1            | 0  | 15 | 7  | 4 | 14 | 2  | 13 | 1  | 10 | 6  | 12 | 11 | 9  | 5  | 3  | 8  |
| 2            | 4  | 1  | 14 | 8 | 13 | 6  | 2  | 11 | 15 | 12 | 9  | 7  | 3  | 10 | 5  | 0  |
| 3            | 15 | 12 | 8  | 2 | 4  | 9  | 1  | 7  | 5  | 11 | 3  | 14 | 10 | 0  | 6  | 13 |