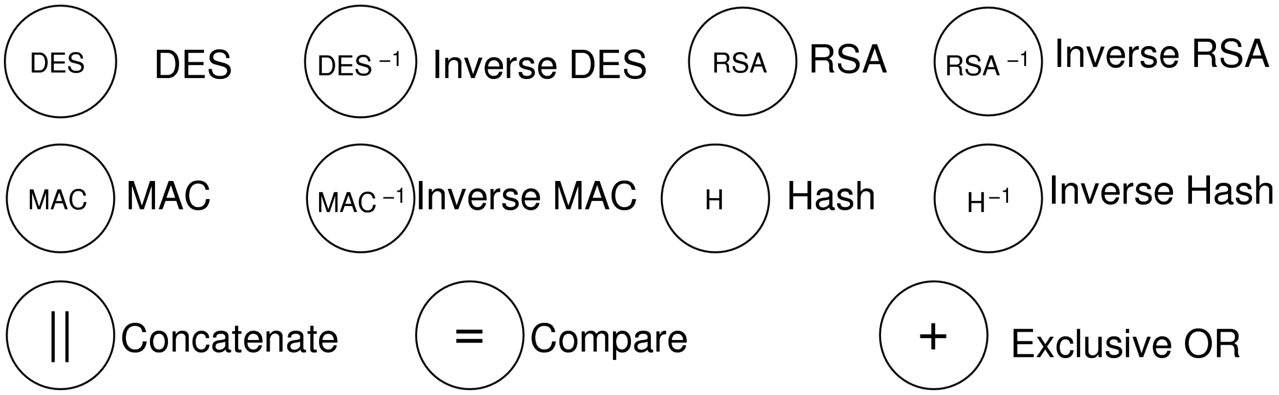
CSS322 – Quiz 5

Name: ____

ID: __________________________ Mark: _________ (out of 10)

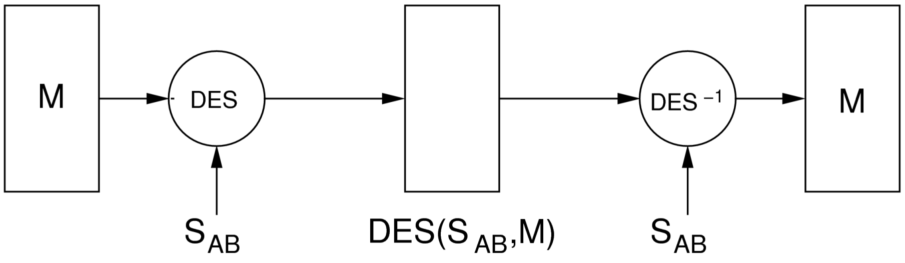
Question 1 [6 marks]

In the following questions you need to draw a diagram illustrating the mechanism used when sending information from A to B. In your answer you can use the following operations:



as well as the following keys: S_{AB}, PU_A, PR_A, PU_B, PR_B.

As an example, the following diagram illustrates DES symmetric key encryption for confidentiality.



a) Authentication only (no confidentiality), using a Message Authentication Code [3 marks]

b) Confidentiality using DES; and authentication using a Hash function and RSA [3 marks]

Question 2 [4 marks]

Three properties of hash functions for practical implementations are: Hash function can be applied on any size input message; fixed length output message is produced; Hash function is easy to calculate.

Three properties of hash functions for security are: one way property; weak collision resistance; strong collision resistance.

a) Which Hash function property is the easiest for a malicious user to attack? [1 mark]

b) Referring to the properties, explain why collisions will occur in practical Hash functions. [1 mark]

c) Explain a security benefit of using Hash functions with Public Key Cryptography to provide authentication and confidentiality (compared to using Hash functions with Symmetric Key Cryptography to provide authentication and confidentiality). [1 mark]

d) Explain (or define) the *one way property* for Hash functions. [1 mark]