Cryptography and network security

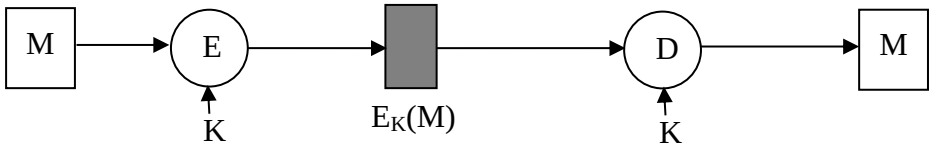
- Final, Jan. 8, 2013 -

1. (20%) How does SHA-512 need to set an initial value? Why? How many constants does it use? What are these constants used for?

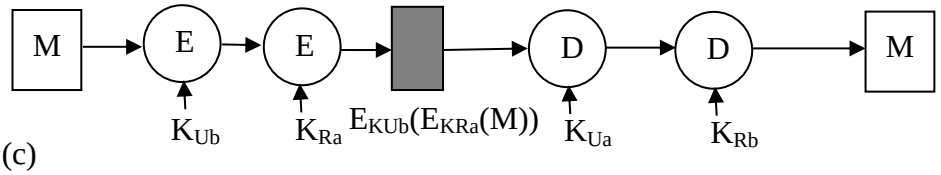
2. (15%) If both authentication and digital signature are the major concern, design a protocol to send an email by using a public-key encryption approach.

3. (15%) Compare/contrast the following message encryption protocols, where K is a secret key, U_a and U_b are public keys, R_a and R_b are private keys, and M is a message.

(a)



(b)



(c)