Exercise 7(a)

Suppose that KU_A and KR_A are the public and private keys of a party *A* respectively, that KU_B and KR_B are those of a party *B*, and that each of *A* and *B* can use any cryptosystems.

(i) If *A* wants to send a very long message to *B*, suggest an encryption method by which only *B* can decrypt the message and the encryption/ decryption processes are the most efficient. Make clear the role of PKI in this method design.

(ii) Can *A* encrypt a message so that anyone receiving the message will be assured that the message came only from *A* (i.e. authenticity protection)? If yes, give your method; and if not, explain why not.

(iii) Suggest an *efficient* method by which both confidentiality and authenticity protections are provided.

Answers to Exercise 7(a)

(i) *A* encrypts a message *M* with a secret session *k* chosen randomly, and then *k* with *B*'s public key KU_B, i.e. $E(k, M)$ and $E(KU_B, k)$. *A* sends both $E(k, M)$ and $E(KU_B, k)$ to *B*. Should mention that the public key should be trusted; this means before using B's public key, A should perform all the checks to ensure that the key is trust-worthy. So what are these checks?

(ii) *A* encrypts the hash value of the message *M* with its own private key, i.e. $M||t||E(KR_A, H(M||t))$.

(iii) *There are three possible answers to this question:*

(1) *A* can send $E(KU_B, k)$, $E(k, M)$, t, $E(KR_A, H(t||E(k, M)||E(KU_B, k)))$ to *B*, where *t* is a time stamp, *H*() is a one-way hash function, and $E(KR_A, H(t||E(k, M)||E(KU_B, k)))$ is *A*'s signature on the other items. In this solution, the signature is signed on the ciphertext.

(2) $E(KU_B, k)$, $E(k, M||t||E(KR_A, H(M||t))$ – in this solution, the signature enjoys the confidentiality protection; the signature verification is done after the two decryptions, so this solution is more vulnerable to DoS attacks than the first solution.

(3) $E(KU_B, k)$, $E(k, M)$, t, $E(KR_A, H(t||M))$ – in this solution, the signature is on plaintext, and the signature is not confidentiality protected; the signature verification is done after two decryptions are done, so again it is more vulnerable to DoS attacks than solution (i).