Comp5631/CSIT5710: Cryptography and Security
2019 Fall – Written Assignment Number 3
Handed out: on November 26, 2019
Due: on December 5 for COMP5631 between 10:00am and 17:00pm
COMP5631 students should submit their solutions as a single PDF file to the email address:
wxiaoae@gmail.com
Due: on December 6 for CSIT5710 between 10:00am and 21:00pm
CSIT5710 students should submit their solutions as a single PDF file to the email address:
dingvisitor@ust.hk
Please put "COMP5631 assignment 3" or "CSIT5710 assignment 3" as your email subject title
Please write your name and student ID on your solution paper

Q1. You are given a one-key cipher with encryption and decryption transformations E_k and D_k such that

$$E_{k_1}[E_{k_2}(m)] = E_{k_2}[E_{k_1}(m)]$$

for any pair of keys k_1 and k_2 and any message m. You are also told that the cipher is so designed that it is computationally infeasible to determine the key k given any message m and its ciphertext $E_k(m)$, and it is computationally infeasible to determine m given $E_k(m)$.

You task is to design a key distribution protocol meeting the following requirements:

1. The protocol involves only two parties Alice and Bob who do not share any secret key for the one-key cipher.
2. The protocol should allow Alice to send a session key to Bob with confidentiality using the one-key cipher.
3. The protocol should be secure with respect to passive attacks so that no third party is able to read the session key sent through a public communication channel.

It is assumed that the communication channel is well designed so that no active attacks are possible. You need to argue that your protocol meets the requirements above. 20 marks

Q2. Consider the DSS covered in Lecture 14. Does the intercepted $m||s||r$ contain all information about the the singer's private key? Please justify your answer carefully. 20 marks

Q3. What are the purposes of having the IKE SAs in IKEv2? 14 marks

Q4. Explain why SSL needs an alert protocol, while IPSec does not need such a protocol? 14 marks

Q5. Consider the Kerberos Authentication Protocol described on in Lecture 17 and answer the following questions:

1. How does the Client C authenticate the sender after the Client receives the message in Step 2 from the AS? 8 marks
2. How does the Client C check the integrity of the received message in Step 2 from the AS? 8 marks
3. How does the TGS check if the Ticket$_{tgs}$ was indeed issued by the AS or not? 8 marks
4. In addition to the TGS and the AS, who else can verify the validity of the ticket Ticket$_{tgs}$? Justify your answer briefly. 8 marks