26 januari 2012	08:45-12:15	201100072	Introduction to Information Security

Answer 6 out of 8 questions. Each question is worth 10p.

Illegible answers or excessively long answers will not be marked.

1. The protocol below aims at key distribution of K_{ab}. Here N_a is a nonce, pk(X) is the public key of agent X, and {M}pk(X) is message M encrypted with the public key of X using a suitable public-key algorithm (messages 1, 2 and 3). Message 4 uses symmetric encryption with key K_{ab}.

   1. A→S: $\{N_a, B\}pk(S)$
   2. S→A: $\{N_a, K_{ab}\}pk(A)$
   3. S→B: $\{K_{ab}\}pk(B)$
   4. B→A: $\{B\}K_{ab}$

To ensure the delivery of the key to the correct agents, authentication is required. Explain for each of the six options below whether the protocol aims at:

(a) Mutual authentication without the use of a server
(b) Mutual authentication using a trusted third party (TTP)
(c) Provide authentication of A to S
(d) Provide authentication of S to A
(e) Provide authentication of B to A
(f) Provide authentication of B to S

2. Compare the static and dynamic data authentication in the EMV banking standard.

3. Consider the following 2 users, which have specific privacy problems. What solutions (PETs) you can propose to them? Motivate your choice.
   (g) Bob is an engineer and is running a blog, which is in contravention with his company's rules. How can he avoid getting caught and fired?
   (h) Alice is a financial analyst for an investment bank. She has to advise on a company merge. How can she investigate the takeover target without revealing which company is the target and even that anybody is interested in it?

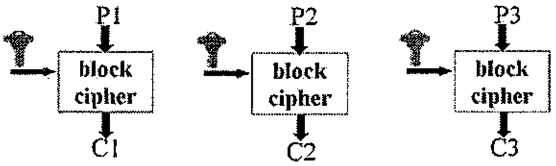
4. Define the FAR, FRR, and EER in a biometric system. Explain why the EER of a biometric system cannot be 0.

5. (a) RFID tags are a potential threat to people's privacy, especially when attached to items purchased in shops. It is relatively easy to disable an RFID tag permanently during checkout. However, an operational RFID tag could provide some useful services to the customer. List three uses of RFID tags after the purchase of expensive, RFID tagged goods.

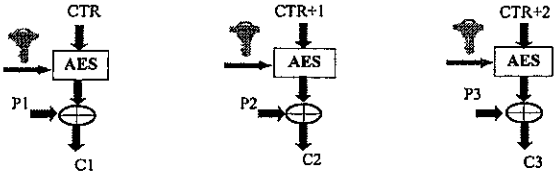
(b) List methods than can be used to disable an RFID tag, either temporarily or selectively.

6. (a) Which of the three block cipher modes depicted below should be used and which should not be used in secure cryptosystems and why?

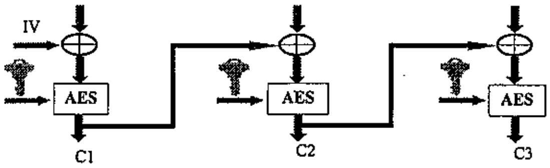
(1)



(2)



(3)



(a) Give the three most important properties that a cryptographic hash function should satisfy.

7. There are mainly three types of access control systems, namely Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Role-Based Access Control (RBAC). Which of them should be used in the following scenarios, and why?

(a) In a company, where there are many employees and many resources and access control decisions are based on job functionalities.
(b) You have some files and want to share them with a couple of your friends.
(c) In a military department, where there are strict hierarchies among resources and employees.

8. Adding security in Inter-Vehicle Communication creates computational and communication overheads. Cite three techniques to reduce these overheads. Explain briefly how they work.