

A22650
se

No calculator permitted in this examination



School of Computer Science

Undergraduate Occasional
Computer Science/Software Engineering

Degree of MSc

Advanced Computer Science
Computer Security
Intelligent Systems Engineering
Internet Software Systems

06 20009

Network Security

Summer Examinations 2007

Time allowed: 1 ½ hours

[Answer THREE Questions]

**[Marks indicated on this paper add up to 102%.
The final mark will be capped at 100%.]**

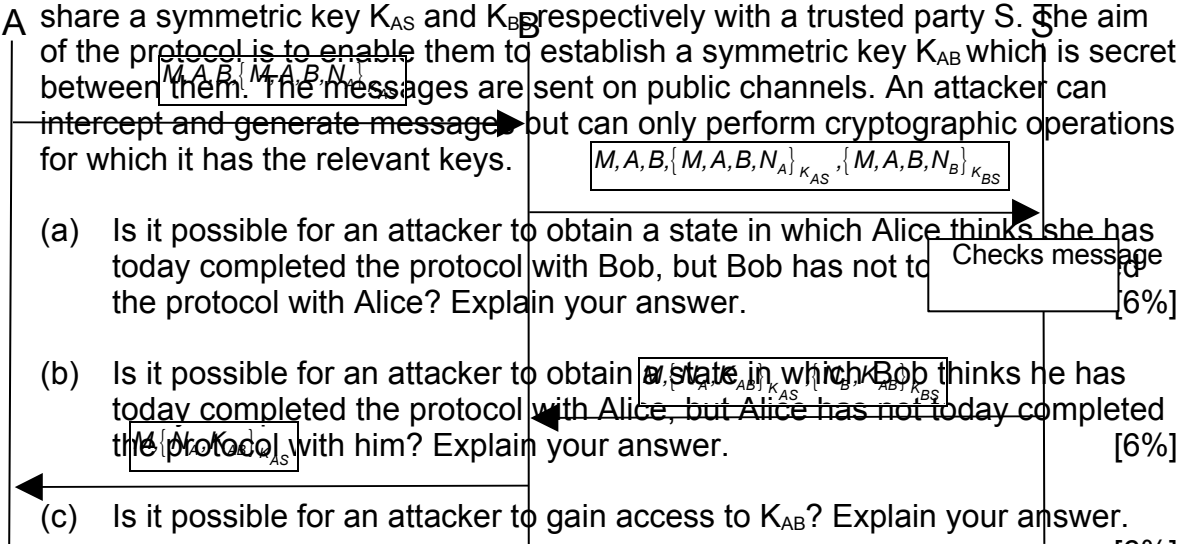
[Answer THREE Questions]



Authentication protocols



In the Otway-Rees authentication protocol (illustrated), Alice and Bob each share a symmetric key K_{AS} and K_{BS} respectively with a trusted party S. The aim of the protocol is to enable them to establish a symmetric key K_{AB} which is secret between them. The messages are sent on public channels. An attacker can intercept and generate message but can only perform cryptographic operations for which it has the relevant keys.



- (a) Is it possible for an attacker to obtain a state in which Alice thinks she has today completed the protocol with Bob, but Bob has not to the protocol with Alice? Explain your answer. [6%]
- (b) Is it possible for an attacker to obtain a state in which Bob thinks he has today completed the protocol with Alice, but Alice has not today completed the protocol with him? Explain your answer. [6%]
- (c) Is it possible for an attacker to gain access to K_{AB} ? Explain your answer. [6%]
- (d) Is it possible for an attacker to obtain a state in which Alice and Bob have received different versions of K_{AB} ? Explain your answer. [6%]
- (e) Using a similar illustration to the one shown, write a protocol which achieves the desired effect, i.e. for which the answer is “no” to each of the questions (a)-(d). [10%]

2. Digital cash

It is the year 2012. Birmingham City Council wishes to implement a Bullring Congestion Charge on shoppers at weekends. The charge is a fixed amount. Shoppers will carry a wireless smart card which they will present at a turnstile when they enter the Bullring. The smart cards can be re-charged with credit by using debit or credit cards at a hole-in-the-wall cash point. These days, awareness of privacy issues is much greater than it used to be, and the city council would like a solution which guarantees that the system *cannot* record the identity of an individual shopper.

Three companies are approached to provide a design, and they produce the following solutions.

- (a) Company A. The card serves only to identify the customer to the cash-point and to the turnstile; all the live data is held on a database. At recharge time, the customer's credit value held on the database is increased and a corresponding debit is made to their bank account. On entry to the shopping centre, the fixed charge is debited from the customer's credit value on the database.
- (b) Company B. The card contains the credit value; there is no database. At recharge time, the customer selects the number of credits, say n , that it she wishes to put on the card. The card invents a set of n nonces, blinds them using the bank's public key, and transmits them to the bank. The bank signs each one with a key which is used to indicate the value of an entrance to the centre, and sends the signed, blinded nonces back to the card. The card unblinds the nonces. When the customer enters the shopping centre, the card sends a nonce, still signed by the bank, to the turnstile. The turnstile checks that this signed nonce has not been used before.
- (c) Company C. The card contains the credit value, and again there is no database. At recharge time, the cash machine transmits a message updating the card with an appropriate number of credits. When the customer enters the shopping centre, the turnstile sends a message to check that the stored value of credits is at least one, and to decrement the stored value.

By completing the table shown below, comment on the relative merits of each solution, making any assumptions which you think are reasonable. For each scheme, state the additional assumptions you chose to make, if any. Explain whether the basic security requirement is satisfied (namely, that customers pay the correct amount to enter the shopping centre). Explain whether the privacy requirement is satisfied (namely, that the system cannot determine whether an individual entered the shopping centre). Please present your answer as a table (shown below).

Scheme	Additional assumptions	Basic security	Privacy requirement
--------	------------------------	----------------	---------------------

	made [10%]	requirement satisfied? [12%]	satisfied? [12%]
A			
B			
C			

3. Wifi

- (a) State as precisely as you can the properties of the cryptography algorithm RC4 that are exploited by the Stubblefield, Ioannidis and Rubin attack on WEP (*wired-equivalent privacy*). [10%]
- (b) Consider the following changes to WEP that one might consider to address the attack. For each one, state whether the proposed change would block the attack or not. Give reasons for your answers.
 - (i) The first 10 bytes of the RC4 output stream are thrown away. [8%]
 - (ii) A WEP plaintext packet is defined to be $h(M) \cdot M$ (instead of $M \cdot c(M)$ as is actually done in WEP), where M is the plaintext, c is a non-cryptographic checksum function and h is a cryptographic hash function, and \cdot is concatenation. [8%]
 - (iii) The RC4 key is defined as $k \cdot IV$ (instead of $IV \cdot k$ as is currently done in WEP), where IV is the per-packet initial vector and k is the WEP shared key. [8%]

4. Network layers

Network security can be provided at the network layer (e.g., IPSec) and at the transport layer (e.g., TLS).

- (a) State an advantage that network layer security has over transport layer; and then an advantage that transport layer security has over network layer. [10%]
- (b) In order to prevent spam, an organisation wants to implement access restrictions on its SMTP server from outside. However, it also wants to provide a facility for authorised users to connect to the server from home. It considers the following solutions:
- (i) Only allow IP addresses within the organisation to connect. Provide ssh tunnelling for home users.
 - (ii) Deploy IPSec authentication headers to allow only authorised computers (whether at home or at work) to connect.
 - (iii) Deploy TLS to allow only authorised computers (whether at home or at work) to connect.

Copy and complete the following table, writing one advantage and one disadvantage of each approach.

	Advantage [4%,4%,4%]	Disadvantage [4%,4%,4%]
i		
ii		
iii		

5. Self-study topics. [34%]

Pick **one** of the following topics, and write brief notes (max 300 words) about it.

- (a) SMS vs email sender authentication
- (b) Describe the protocols used in online multiplayer games, and their security properties.
- (c) How do the network file systems NSF and SMB compare from a security point of view?
- (d) How could biometric authentication be used for online banking?
- (e) What network attacks on home computers are made via broadband connections?
- (f) What is “computational proof” in the context of spam fighting, and how can it help?
- (g) What practical difficulties are there in WEP key cracking?
- (h) What approaches to anonymity can one find in the literature on digital cash?
- (i) Why is GNU/Linux used on consumer boxes such as routers, network-attached storage devices, and ethernet/USB switches, and how can one extend them with more services?
- (j) Could electronic voting protocols such as the one by Fujioka, Okamoto and Ohta [1992] be used for UK national political elections?
- (k) Given a laptop with a TPM inside it, how would you write programs which demonstrate the TPM’s capabilities?