MANCHESTER
1824

The University of Manchester

COMP38411 – Cryptography and System Security

Coursework – An E-payment Protocol

Maximum marks available in this coursework	30
Weighting of this coursework towards the unit overall mark (%)	30%
Learning outcomes being Assessed	Stated in the course unit specification
The coursework setter	Dr Ning Zhang
Handout date	4th Oct 2020
Handin date	5:00pm, 16th Dec 2020 (Please submit your work via the Blackboard facility)

The Problem

The following gives a credit card based e-payment protocol:

Initiation	$C \xrightarrow{\textit{Purchase request}} M$
Invoice	$C \xleftarrow{\textit{Purchase details including prices}} M$
Payment	$C \xrightarrow{E(KU_A,\ Slip),} M$
Authorisation request	$M \xrightarrow{\textit{Purchase details},\ E(KU_A,\ Slip)} A$
Authorisation response	$M \xleftarrow{Signed(PR_A,\ C\|\|M\|\|Decision)} A$
Confirmation	$C \xleftarrow{Signed(PR_A,\ C\|\|M\|\|Decision)} M$

where, *C*, *M* and *A* represent a customer, a merchant and an acquirer (i.e. the merchant's bank), respectively. KU_A and PR_A are, respectively, *A*'s public and private keys, $E(K, x)$ denotes the encryption of *x* with key *K*, $Signed(PR, x)$ denotes *x* signed with key *PR* (i.e. $Signed(PR,x)=x\|E(PR,H(x)))$, $H(x)$ is cryptographic hash function, $x\|y$ is the concatenation of data items, *x* and *y*, and *Slip* = {the description of goods, prices to pay, *C*'s credit card number}, *Decision* = *yes* or *no*.

The Questions

Answer the following questions:

(a) Identify in general terms three security threats to credit card based electronic payment.

(b) Discuss whether or not the above protocol can prevent each of the three security threats identified in (a).

(c) Customer *C* wants to purchase electronic goods from merchant *M*, and wishes to have a fair trade in the sense that either *C* receives the goods and *M* receives the payment, or neither of them gets anything from the other. Extend the above protocol to achieve this fair trade, stating any assumptions you make, and justify how the extended protocol can achieve the fairness.

What you should hand in

Answers to the questions specified in the above section "The Questions", in which all texts and diagrams must be word-processed.

Guidelines/ Length

This is an **individual** coursework, so it must be completed **independently**.

This coursework should be carried out with reference to relevant textbooks or published articles. The length of your submission should not exceed TWO A4 sides (i.e. approximately no more than 1000 words).

Assessment

Tasks	**Assessment Criteria**	**Raw marks for each component**
	Clear statement of assumptions made	1
(a)	Clear explanation and convincing justifications	6
(b)	Clear explanation and convincing justifications	9
(c)	Correct protocol design, clear explanation and convincing justifications	12
	Quality and additional design considerations (e.g. protocol efficiency considerations, conciseness and accuracy, evidence of research)	2

Additional notes:
Submissions: All the submissions should be done via the Blackboard submission facility.
Late Submissions:
Extensions will only be granted as a result of formally processed Mitigating Circumstances (http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=427).
Marks for late submissions will be reduced in line with the following university policy (http://documents.manchester.ac.uk/display.aspx?DocID=24561).
Support: Support is available in the Synchronous Sessions. Additionally, questions can be posted on the Blackboard forum.

End