2910326 Computer Security
Coursework 2010-11

Important Notes - Please read before you start to work on these assignments.

1. The two coursework questions below are to be done in conjunction with the study guide for 2910326, recommended books and any other source that you can obtain.
2. You must acknowledge any use of the published or unpublished works of other people (including material obtained from websites). Note that few if any marks are given for reproducing material from other sources. If your teacher gives you guidelines, please acknowledge the extent of this in your report.
3. Plagiarism detection software may be used on the submitted coursework. Last year, there were again instances where plagiarism was detected and the offenders were penalised. Please be warned that the markers are vigilant in attempting to detect plagiarism. Plagiarism includes, but is not limited to, students handing in coursework which in parts are essentially identical. Plagiarism also includes copying from the Internet without acknowledgement, copying from theses, copying from books and the subject guide, etc. Remember, if you can find it on the Internet so can the markers.
4. The two coursework questions carry equal weight.
5. Programs, if used, may be written in any programming language.
6. Note the hard copy that you have been asked to submit. The floppy disk/CD is only required for plagiarism detection software. You should not assume that markers will inspect the disk in the normal process of marking.
This assignment is about password security and how passwords can be recovered or reset if they are lost. Password log-in systems are covered in the subject guide (chapter 2). Rainbow tables, which can be used to recover lost passwords, are mentioned on pages 19 and 65. Retrieval of lost passwords is not directly covered in the subject guide, but thinking about how a user is given a new or replacement password is an important security issue. There is not much point in having a sophisticated username/password log-in system if you are lax in sending out passwords so that it is easy for anyone to log-on without the proper authorisation.

Question 1

Consider the following scenario.

Mr Smith has forgotten his password for the NotSoSafe website. He clicks on the “Forgotten Your Password” button and is asked to enter his email address, which he does.

When he logs into his email account, Mr Smith finds the following email waiting for him:

**Subject:**
New Password

**Body:**
Dear Mr Smith,
It appears that you have lost your password for NotSoSafe. Don’t worry. To regain access to your account with us, please go to [www.NotSoSafe.com](http://www.NotSoSafe.com) and enter the following information:

Username: smith
Password:smith

Best wishes,
I.N.Secure, NotSoSafe Limited

The scenario given above, is an example of a bad (meaning insecure) way to reset a lost password. Find as many things wrong with this method of resetting a password as you can, for each explaining clearly what the problem is, why it is insecure, and if possible giving a more secure alternative. [25]
**Question Two**

Find **two different methods** for resetting a lost password. For example, what happens if you forget a password for an application or website that you have registered on? You should attempt to research one high security (e.g. banking application) and one low security (e.g. a free online game) application. For each application, explain how a forgotten password is reset and compare and contrast the two different methods discussing the security, ease of use, and other relevant features of each. [40]

**Question Three**

Rainbow tables can be used to retrieve forgotten passwords. They are mentioned briefly in the subject guide. Do some further research on rainbow tables and write approximately 500 words describing how rainbow tables work, what their purpose is, how they can be abused and any other relevant information that you have found. Please write in your own words and do not forget to properly reference any material that you use. [35]
UNIVERSITY OF LONDON

DIPLOMA AND BSc IN COMPUTING AND RELATED SUBJECTS
FOR INTERNATIONAL PROGRAMMES STUDENTS

COURSEWORK SUBMISSION FORM

IMPORTANT, PLEASE NOTE:

You must complete this form in full and attach it to the coursework that is to be submitted to the University.

Full name: ........................................................................................................................................................................
(as it appears on your Registration Form)

Student number: ...................................................................................................................................................................

Unit title: ...........................................................................................................................................................................

Unit number: ...................................................................................................................................................................

Assignment number: ........................................................................................................................................................

DECLARATION

I declare that:

• I understand what is meant by plagiarism.
• I understand the implications of plagiarism.
• This assignment is all my own work and I have acknowledged any use of the published or unpublished works of other people.

Signature ................................................................. Date ............................................
Before you submit your coursework to the University, have you:

- completed the title, unit number and assignment number on the submission form?
- signed and dated the Declaration?
- put your name and student number on every page?
- put the unit number, unit name and assignment number on every page?
- used more than one page? If so, have you securely stapled or tied the pages together?
- used a disk? If so, have you used a separate disk for each assignment? (Note: you should only use a disk if it is explicitly asked for in the assignment).
- labelled clearly and securely attached any disks?
- attached all parts of the coursework required (including the submission form)?

If you fail to do these things your coursework may not be accepted.

Please send all coursework to:
The Registration and Learning Resources Office
Room STG13
Stewart House
University of London
32 Russell Square
London WC1B 5DN
United Kingdom
Tel: +44 (0)20 7862 8326
Fax: +44 (0)20 7862 8329
In the novel *Cryptonomicon* by Neal Stephenson, a cryptosystem called Pontifex is described. This is actually a cryptosystem called Solitaire – the name is changed to Pontifex in the book to disguise the fact that the scheme is based upon a pack of playing cards. The Solitaire cryptosystem was devised by Bruce Schneier.

You can find a description of Solitaire and accompanying notes at [http://www.schneier.com/solitaire.html](http://www.schneier.com/solitaire.html). Read the description of Solitaire and the accompanying notes and any other material on Solitaire or stream ciphers that is relevant (including chapter 5 of the subject guide) and then answer the following questions.

1. Solitaire is an 'output feedback stream cipher'. Explain what this means. [2]

2. Why is a pack of cards a good tool to use to produce a cryptosystem? [4]

3. a) Schneier says that “keying the deck is the most important part of the whole operation.” Why is that? [4]

   b) He suggests three methods of keying the deck:
   - using a randomly shuffled pack;
   - using notes from a bridge game;
   - using a passphrase and the Solitaire algorithm.

   Which of these three methods do you think is the best and why? [6]

4. Can you suggest a forth alternative method for keying the deck? What are the advantages and disadvantages of your suggested method? [10]

5. Why should you always use a new key for each new message? [6]

6. Put the following combinations of key and message length into order, starting with the most secure. Give a justification for your answer:
   - Short key, short message
   - Short key, long message
   - Long key, short message
   - Long key, long message

   [8]

7. Explain what is meant by error propagation with regards to encryption? Is Solitaire good or bad where error propagation is concerned? [5]

8. In your own words, describe Solitaire for an audience that knows very little about cryptography, for example, as if you were writing a newspaper article on Solitaire. Your answer should be approximately 300-400 words long. [15]

9. Starting with a pack of cards in order (ace of clubs to king of clubs, ace of diamonds to king of diamonds, ace of hearts to king of hearts, ace of spades
to king of spades, joker A, joker B) use the passphrase UNIVERSITY OF LONDON to generate five characters of "keystream". Use these keystream characters to decrypt the ciphertext message JQXPZ. You should work by hand and show your working.

As an example, the first character of the keystream is worked out below:

<table>
<thead>
<tr>
<th>Unkeyed deck</th>
<th>(top) 1 2 3 … 51 52 A B (bottom)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1, move the A joker</td>
<td>1 2 3 … 51 52 B A</td>
</tr>
<tr>
<td>Step 2, move the B joker</td>
<td>1 B 2 …50 51 52 A</td>
</tr>
<tr>
<td>Step 3, triple cut</td>
<td>B 2 3 …51 52 A 1</td>
</tr>
<tr>
<td>Step 4, count cut</td>
<td>2 3 4 … 52 A B 1</td>
</tr>
<tr>
<td>Step 5, count cut using first character of passphrase (U=21)</td>
<td>23 24 25…20 21 22 1</td>
</tr>
<tr>
<td>Step 6, output first keystream letter</td>
<td>Top card = 23</td>
</tr>
</tbody>
</table>

Starting with the pack in the order it is in now (23 24 25 ... 20 21 22 1) repeat steps 1 to 6 until you have five keystream characters. Hence decrypt the ciphertext message JQXPZ.

[Note that in question 9 we are not using Solitaire properly. In order to make the cryptosystem secure, the two correspondents must start off with the same shuffled deck before starting to generate any keystream characters. The purpose of this question is to give you some practice in carrying out the Solitaire algorithm – if you have done it right you should have a fruity answer.]

10. Imagine that you are using the Solitaire cryptosystem to encrypt a secret message of real importance (i.e., you want to make the encryption secure). Encrypt the first five letters of your own name. Tell me everything that I need to know in order to decrypt the message. You may assume that I know how Solitaire works but you will need to tell me how you've keyed the deck, and any other assumptions that you've made.
UNIVERSITY OF LONDON

DIPLOMA AND BSc IN COMPUTING AND RELATED SUBJECTS
FOR INTERNATIONAL PROGRAMMES STUDENTS

COURSEWORK SUBMISSION FORM

IMPORTANT, PLEASE NOTE:
You must complete this form in full and attach it to the coursework that is to be submitted to the University.

Full name: ........................................................................................................................................................................
(as it appears on your Registration Form)

Student number: ...................................................................................................................................................................

Unit title: ........................................................................................................................................................................

Unit number: ..................................................................................................................................................................

Assignment number: ..........................................................................................................................................................

DECLARATION

I declare that:

• I understand what is meant by plagiarism.
• I understand the implications of plagiarism.
• This assignment is all my own work and I have acknowledged any use of the published or unpublished works of other people.

Signature ………………………………………………… Date …………………….
UNIVERSITY OF LONDON

DIPLOMA AND BSc IN COMPUTING AND RELATED SUBJECTS
FOR INTERNATIONAL PROGRAMMES STUDENTS

COURSEWORK SUBMISSION CHECKLIST

Before you submit your coursework to the University, have you:

☐ completed the title, unit number and assignment number on the submission form?

☐ signed and dated the Declaration?

☐ put your name and student number on every page?

☐ put the unit number, unit name and assignment number on every page?

☐ used more than one page? If so, have you securely stapled or tied the pages together?

☐ used a disk? If so, have you used a separate disk for each assignment? (Note: you should only use a disk if it is explicitly asked for in the assignment).

☐ labelled clearly and securely attached any disks?

☐ attached all parts of the coursework required (including the submission form)?

If you fail to do these things your coursework may not be accepted.

Please send all coursework to:
The Registration and Learning Resources Office
Room STG13
Stewart House
University of London
32 Russell Square
London WC1B 5DN
United Kingdom
Tel: +44 (0)20 7862 8326
Fax: +44 (0)20 7862 8329