SIT281 2013 TRIMESTER 2
ASSIGNMENT 1

Due: Friday August 23, 2013 at 12 noon (Australian Eastern Standard Time)
Value: 20% of your final mark in the unit.

NO EXTENSIONS allowed without medical or other certification.

LATE ASSIGNMENTS will automatically lose 10% per day up to a maximum of three days, including weekends and holidays. Assignments submitted 4 or more days late will not be marked and are given zero.

METHOD OF SUBMISSION:
Off-campus students, e-mail to Lynn Batten at lmbatten@deakin.edu.au by the due date and time. The Subject should contain the unit code, your surname and ID.

Geelong and Burwood students submit hard copies to their respective instructors through assignment drop-off boxes (Building Ka, level 3 at G, building L at B).

All assignments are required to have the assignment cover sheet attached, which is available at http://www.deakin.edu.au/scitech/current/ under the Assignment heading.

Read the following Notes before proceeding:

1. **It is important that you show your working out and explain your steps. Marks are given for this.**
2. **Do not include extraneous Maple code in your submission.**
3. **Do not copy or plagiarise. Read the University position on plagiarism – it is a serious matter. People who do this are given 0 for the question.**
4. **One file (a single zip file containing several files does not count as one file); Number all pages of your assignment.**
5. **For off-campus students who email assignments in: put your name on each page; send one file (including the cover sheet) with a maximum of 750kb.**

---

1. Simon works in a government office where encrypted messages are regularly received. He knows that an affine cipher is the standard method of encryption used by the office, and has access to the machine which encrypts.

One day, when there is not much work to do, Simon decides to work out the affine function used in the machine. He inputs 1 and the machine outputs 5. He inputs 2 and the machine outputs 19. Show how he uses this to obtain the function.

(4 marks)

2. Patrick and Jacquie both use the same Hill cipher based on the matrix
M = |2 13|
|23 1| to send each other encrypted messages.

(a) ***Without using Maple***, show how Patrick uses M to encrypt the message:
` The room for the PASS session has changed.'

(b) In order to decrypt Patrick's message, Jacquie must invert M. What matrix does she obtain? Do not use Maple.

(3+2= 5 marks)

3. The name L011 stores the first terms of an LFSR output. (a) Using Maple, determine the recurrence formula used to generate it. (b) Use the recurrence formula to find the next term in the sequence. (4+2 =6 marks)

4. Using the Euclidean Algorithm, find the inverse of 2563 modulo 3127. Show all your work and ***do not use Maple***.

(5 marks)

TOTAL MARKS: 20

THIS ASSIGNMENT IS WORTH 20% OF YOUR FINAL MARK.