The University of Melbourne
School of Computing and Information Systems
COMP90043 Cryptography and Security

Assignment 1, Semester 2 2018

Due Date: August 24, 23:59

Objectives

To improve your understanding of the Euclid's algorithm, divisibility properties and classical ciphers. To develop problem-solving and design skills. To improve written communication skills.

Questions

1. Euclid's algorithm and Divisibility properties [3 marks]

   (a) Let a, b, c, d be integers and $GCD(a, b) = 1$. If $c|a$ and $d|b$, prove that $GCD(c, d) = 1$.

   (b) You should perform the following implementation tasks in a language of your choice. You are at free to employ any underlying integer arithmetic library.

      i. Implement the extended Euclid's algorithm and only submit the code here.

      ii. Implement a function in that takes two positive numbers a, n, $a < n$ and output the inverse of $a \mod n$ based on your extended Euclid's algorithm. Only submit the code for the function.

   Note: Your working code framework may involve many auxiliary library functions and display routines. However you are only required to submit the required code or functions in the above questions. A typical example output based on generic magma functions is provided as an illustration.

   (c) Now choose n as a product of two primes p_1 and p_2 ($p_1, p_2 > 10^{25}$), use your implementation in (b) and output the results of your inverse $a \mod n$ function for the following cases:

      i. a is a random positive integer less than n

      ii. a is a multiple of p_1

      iii. a is $n - 1$

2. General Security and Classical Ciphers [2 marks]

   (a) Explain with an example how security risks and attacks are different. Name a security attack that has happened on computer systems in recent years. Describe how the attack took place in no more than half a page.

(b) Consider the following version of a classical cipher where plaintext and ciphertext elements are from integers 0 to 27. Note that this alphabet may be used when the plaintexts are 26 English characters and two punctuation symbols, viz: “,” “.”. The encryption function, which takes any plaintext p to a ciphertext c, is given by

$$c = E_{(a,b)}(p) = (ap + b) \bmod 28$$

where a and b are integers less than 28.

i. What is the decryption function for the scheme?

ii. How many different non-trivial keys are possible for the scheme?

iii. What are the complexities of Ciphertext only Attack and Chosen Plaintext Attack on the scheme?

3. Poly-alphabetic Cipher [2.5 marks]

For this question, we consider the Hill cipher given in the textbook on an alphabet $\mathcal{A}$ consisting of 26 English characters and the three punctuation symbols, viz: “,” “.” and “ ” (space), which corresponds to integers 0 to 28. Here the plaintext (mod 29 characters)is processed successively in blocks of size m, $m > 1$ digits at a time. The encryption algorithm takes a block with m plaintext digits and transforms into a cipher block of size m using a key matrix of size $m \times m$ by the linear transformation is given by:

$$\begin{aligned} c_1 &= (k_{1,1}p_1 + k_{1,2}p_2 + \cdots + k_{1,m}p_m) \bmod 29 \\ c_2 &= (k_{2,1}p_1 + k_{2,2}p_2 + \cdots + k_{2,m}p_m) \bmod 29 \\ &\cdots \\ c_m &= (k_{m,1}p_1 + k_{m,2}p_2 + \cdots + k_{m,m}p_m) \bmod 29 \end{aligned}$$

Note: For this question, correspondence between plaintext and number modulo 29 are as follows $A \leftrightarrow 0, B \leftrightarrow 1, C \leftrightarrow 2, \ldots Z \leftrightarrow 25$, “,” $\leftrightarrow$ 26, “.” $\leftrightarrow$ 27 and “ ” (space) $\leftrightarrow$ 28

(a) How many different keys are possible in the system?

(b) The “ciphertext only attack” on the system ’s hard to mount for the cipher. However, the cipher is easily broken with a known plaintext attack. Illustrate the steps for the attack.

(c) An adversary discovers the following ciphertext encrypted using the Hill cipher with $m = 4$: (92 characters, no spaces)

BGB.D,LYIQJNBGSQLXWRIIBKESOWGEWSXCCAC.ZCPPW.YIAFPDNB
UDOBPSFIKBSTRIQQFDOUHBZSRXVULMI,JVSGFUUG

If the following plaintext and ciphertext blocks are given, decrypt the cipher by giving the plaintext and the key used in the encipherment. Show your workings, and if you have used a package or a program you need to include the details of the package, functions used, and any programs developed.

Plaintext	Ciphertext
CTRL	JYZP
CAPS	QEPQ
HOME	CHZS
PGUP	GLXF

Submission and Evaluation

- You must submit a PDF document via the COMP90043 Assignment 1 Turnitin submission form on LMS by the due date. Handwritten, scanned images, and/or Microsoft Word submissions are not acceptable — if you use Word, create a PDF version for submission.

- Late submission will be possible, but a late submission will attract a penalty of 10% per day (or part thereof).

- This assignment contributes 7.5% of the total marks in this subject. Marks are primarily allocated for correctness, but how clearly you communicate your thinking will also be taken into account.

- We expect your work to be neat — parts of your submission that are difficult to read or decipher will be deemed incorrect. Make sure that you have enough time towards the end of the assignment to present your solutions carefully. Time you put in early will usually turn out to be more productive than a last-minute effort.

- You are reminded that your submission for this assignment is to be your own individual work. For many students, discussions with friends will form a natural part of the undertaking of the assignment work. However, it is still an individual task. You are welcome to discuss strategies to answer the questions, but not to share the work (even draft solutions) on social media or discussion board. It is University policy that cheating by students in any form is not permitted, and that work submitted for assessment purposes must be the independent work of the student concerned.

  Please see `https://academicintegrity.unimelb.edu.au`

If you have any questions, you are welcome to post them on the LMS discussion board *so long as you do not reveal details about your own solutions.* You can also email the Head Tutor, Lianglu Pan (`lianglu.pan@unimelb.edu.au`) or the Lecturer, Udaya Parampalli (`udaya@unimelb.edu.au`). In your message, make sure you include COMP90043 in the subject header. In the body of your message, include a precise description of the problem.