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

Assignment 1, Semester 2 2020

Due Date: September 2, 23:59

Objectives

This assignment is designed to improve your understanding of the Euclid's algorithm, classical ciphers and basics of probability. It's also aimed at improving your problem-solving and written communication skills.

Questions

1. Classical Ciphers [20 marks]

   Consider the following version of a classical cipher where plaintext and ciphertext elements are the integers from 0 to 35. Note that this alphabet may be used when plaintexts are 26 English characters and 10 numeric characters. The encryption function, which maps any plaintext p to a ciphertext c, is given by

   $$c = E_{(a,b)}(p) = (ap + b) \bmod 36,$$

   where a and b are integers less than 36.

   (a) What is the decryption function for the scheme?

   (b) A key is called trivial if $c = p$ for all input p. How many non-trivial keys are possible for this scheme?

   (c) Would this cipher be considered as mono-alphabetic cipher or poly-alphabetic cipher? Why?

   (d) You are given a large amount of ciphertext characters encrypted using this scheme. Assuming its plaintext was written in English, show how an attacker can retrieve the key.

   steps:
   agenda where to break it
   method

   which steps help break.

   (e) An oracle is available to you which can output the encrypted ciphertext for arbitrary plaintext you give. Briefly describe an efficient way to retrieve the key using the oracle.

   how minimum number

   keys when , what issues, encription,
   what is module,

   don't know the keys,
   choose plaintext attack,
   oracle give cyphertext,
   explain the st

2. General Security [8 marks]

   Which of the following factors might be the most concern by the public in regards to using the COVIDSafe app[1]? Justify your answer in a few sentences.

[1] https://www.health.gov.au/resources/apps-and-tools/covidsafe-app

which part is more important?

(a) Confidentiality (b) Integrity (c) Availability

3. Euclid's algorithm [15 marks]

Perform the following implementation tasks in a language of your choice. You are at free to employ any underlying integer arithmetic library. In order to get full marks, your algorithm has to be able to work in realistic cryptographic environments (consider 10^{1000} as input).

(a) Implement the extended GCD algorithm as discussed in lectures and print the code here.

(b) Implement a function which takes two positive integers a, n as inputs, and returns the inverse of $(a \mod n)$ based on your extended GCD algorithm (that you just implemented above). Print the code for this function.

(c) Use the above function to find the inverse of $(X \mod 16777259)$, where X is your student number. You don't need to show steps for the calculation.

4. Poly-alphabetic Cipher [21 marks]

For this question, we consider the Hill cipher given in the textbook on an alphabet $\mathcal{A}$ consisting of 26 English characters (A-Z), 10 numeric characters (0-9) and space, which corresponds to integers 0 to 36. Here the plaintext is processed successively in blocks of size m. 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, which is given by:

$$\begin{aligned} c_1 &= (k_{1,1}p_1 + k_{1,2}p_2 + \cdots + k_{1,m}p_m) \bmod 37 \\ c_2 &= (k_{2,1}p_1 + k_{2,2}p_2 + \cdots + k_{2,m}p_m) \bmod 37 \\ &\cdots \\ c_m &= (k_{m,1}p_1 + k_{m,2}p_2 + \cdots + k_{m,m}p_m) \bmod 37 \end{aligned}$$

Note: For this question, correspondence between plaintext and number modulo 37 are as follows "A" ↔ 0, "B" ↔ 1, "C" ↔ 2, ..., "Z" ↔ 25, "0" ↔ 26, "1" ↔ 27, "2" ↔ 28, ..., "9" ↔ 35 and " " (space) ↔ 36

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

✓ (b) This cipher is easily broken with a known plaintext attack. An adversary discovers the following ciphertext is encrypted using this cipher with $m = 5$ (55 characters in total, no spaces):

```
A8VS3XRDEON6JEVXGJID13C07L4C1R4Q965XWRA5DQGYWTNHYO4ND8Z
```

If the following combination of plaintext and ciphertext is given (please replace both "?????" by the last five digits of your student number), decrypt the cipher by giving the plaintext as well as both encryption and decryption keys.

Plaintext	X9B6T6JAW3UEY7FHIW?????5Z
Ciphertext	2Q59ZZ1Z?????UMDNY2JHINTS

You need to show step-by-step details of your working. Make sure to include the details of any package, functions used, and/or programs developed. Simply showing the final result and/or a program would not receive marks.

5. Probability [11 marks]

   Let x be the fourth digit of your student ID (without leading zero), y be the sixth digit of your student ID. The value N used in this task is given by $5x + 6y + 15$.

   For the below tasks, you need to show your working by providing formula used, and/or **short** explanation. Also give the numerical final answer (e.g. 1024 instead of 2^{10}).

   ~~(a)~~ What is your value of N based on your student ID? You may simply show N, but please make sure that your calculation of N is correct, as you will need this value for the rest of tasks.

   ~~(b)~~ Assuming that we have 230 students enrolled in this subject, and all student numbers are randomly generated. What's the probability that at least one of your classmate shares the same N with you? Your result should be rounded to three digits after the decimal point.

   ~~(c)~~ How many ways to place N different balls into five different bins?

   ~~(d)~~ How many ways to place N identical balls into five different bins, so that all bins are non-empty?

   ~~(e)~~ How many ways to place N identical balls into five different bins?

   ~~(f)~~ How many ways to place N identical balls into five identical bins, so that at most two bins are non-empty?

Submission and Evaluation

- You must submit a PDF document via the COMP90043 Assignment 1 submission entry on the 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). Requests for extensions on medical grounds will need to be supported by a medical certificate. Any request received less than 48 hours before the assessment date (or after the date) will generally not be accepted except in the most extreme circumstances.

- This assignment will be marked out of 75 marks, and will contribute to 7.5% of your total marks in this subject. Marks are primarily allocated for correctness of your thinking and clarity of your communication, rather than (only) the correct result without justification.

- 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.