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

Assignment 1, Semester 2 2022

Due Date: August 21, 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. Security Properties [10 marks]

   Describe one security threat in each of the following security properties, with regard to the use of the COVIDSafe app[1].

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

2. Classical Ciphers [20 marks]

   Consider the following version of a classical cipher where plaintext and ciphertext elements are the integers from 0 to 27. The encryption function, which maps 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.

   (a) Derive the decryption function for the scheme. Show your working.

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

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

   (d) An oracle is available to you which can output the corresponding ciphertext for arbitrary plaintext you supply. Describe an efficient way to retrieve the key using this oracle.

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

3. Poly-alphabetic Cipher [25 marks]

For this question, we consider a cipher working on an alphabet $\mathcal{A}$ consisting of 26 English characters (A-Z), plus underscore (_), comma (,) and full stop (.), which corresponds to integers 0 to 28. The encryption is done by:

$$\text{ciphertext} = C_2(C_1(\text{plaintext}))$$

Here C_1 is the encryption function used in Hill cipher. The plaintext is processed successively in blocks of size m. The encryption algorithm takes a block with m plaintext digits $(p_1, p_2, \cdots, p_m)$ and transforms into a cipher block of size m $(c_1, c_2, \cdots, c_m)$ using a key matrix of size $m \times m$ by the linear transformation, which is given by:

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

C_2 is the encryption function used in Vernam cipher. It processes a block of plaintext at a time, and produces a same length ciphertext. In this task, our Vernam cipher uses the same block size m as used in Hill cipher. The encryption is performed by:

$$\begin{aligned} c_1 &= p_1 + K_1 \bmod 29 \\ c_2 &= p_2 + K_2 \bmod 29 \\ &\cdots \\ c_m &= p_m + K_m \bmod 29 \end{aligned}$$

Note: For this question, correspondence between plaintext and number modulo 27 are as follows “A” ↔ 0, “B” ↔ 1, “C” ↔ 2, . . . , “Z” ↔ 25, “_” ↔ 26, “,” ↔ 27 and “.” ↔ 28. All following tasks use block size $m = 6$.

(a) This cipher is easily broken with a known plaintext attack. Given the following combination of plaintext and ciphertext, your task here is to recover the encryption keys (for both Hill cipher and Vernam cipher). Please map the last five digits of your student number using the above correspondence, and use it as the “?????” in plaintext and ciphertext. For example, if your student number is 1234567, you should take the last five digits 34567 and use DEFGH to replace both “?????” below.

Plaintext	PMZRTZYFQFTPIRBRXXKECAHRPMZRTZYZHHK?????HKVYNGQX
Ciphertext	XRDREZLE?????XOHHKVUPYONXRDREZHZHPRBJVGLHMSPNJBU

Make sure to show details of your working, including any tool/package/library used, and/or programs developed. Only showing the final result and/or a program may attract penalties.

(b) An adversary discovers the following ciphertext, which is encrypted using keys found in (a). There are 54 characters in total.

```
VQWBUQIDKILMWT_WJBBUDVKJWTOUTFOMVZZ,OFJRDMNK,.TZBZWUXU
```

Discuss how to recover the plaintext. Show the decryption key(s) used and the decrypted plaintext.

(c) How many different keys are possible in this system? Briefly justify your answer.

4. Probability [20 marks]

Consider the following two experiments:

- Experiment 1: Alice flips a fair coin (0.5 probability of getting HEADS and 0.5 for TAILS), and shares the result with Bob.
- Experiment 2: Alice flips a fair coin, and always sends HEADS to Bob.

After each experiment, Bob needs to guess which experiment they were in. We can quantify the quality of Bob's guess using the following formula:

$$Q = |P(W_1) - P(W_2)|$$

Here W_i refers to the event that Alice performed experiment i ($i \in \{1, 2\}$), while Bob guessed they were in experiment 1. We can see that $Q = 0$ indicates Bob cannot distinguish the two experiments, while $Q = 1$ suggests Bob can always correctly identify which experiment they were in.

For the below tasks, apart from giving a numerical answer, please also show your working by providing formula used, and/or a **short** explanation.

(a) For each of the following strategies used by Bob, calculate the quality of Bob's guess, Q.

i. Always guess experiment 2.

ii. Ignore the result reported by Alice, and randomly guess experiment 1 and experiment 2 with equal probability.

iii. Guessing experiment 1 if TAILS was shared from Alice, otherwise guess experiment 2.

iv. Guessing experiment 1 if HEADS was shared from Alice, otherwise guess experiment 2.

v. Guessing experiment 1 if TAILS was shared from Alice, otherwise randomly guess experiment 1 or 2 with equal probability.

(b) What is the highest quality of Bob's guess, Q? Briefly elaborate the strategy and justify your answer.

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 Ed discussion board *so long as you do not reveal details about your own solutions.* We encourage you to make your questions public, as your classmates could have similar concerns.