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

Assignment 1

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. General Security [8 marks]

   Which of the following factors might be the most concern by the public in regards to the COVID passport?
   (`https://tinyurl.com/y2nxykaw`)
   Justify your ans

   (a) Confiden

2. Classical Ciphers [20 marks]

   Consider the following version of a classical cipher where plaintext elements are the integers from 0 to 27. Note that this alphabet the characters of plaintexts are elements the language $\mathcal{A}$ consisting of the 26 English characters (A – Z) along with space. The encryption function, which maps any plaintext p to a ciphertext c, is given by

   $$c = E_{(a,b)}(p) = (ap + b) \bmod 27,$$

   where a and b are integers less than 27.

   (a) For what values of a and b does a decryption function of $E_{(a,b)}$ exist? Write down the decryption function.

   (b) How many keys are possible for this scheme? Explain your reasoning.

   (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.

(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.

3. Euclid's algorithm [15 marks]

Perform the following implementation tasks in a language of your choice. You are 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 $X (\mod 16811891)$, 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 $\mathcal{A}$ consisting of 26 E e following special characte

$$: \quad ; \quad < \tag{1}$$

which corresponds to integers 0 to 40. Here the plaintext is p blocks of size m. The encryption algorithm takes a bl laintext 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:

$$\begin{aligned} c_1 &= (k_{1,1}p_1 + k_{1,2}p_2 + \cdots + k_{1,m}p_m) \bmod 41 \\ c_2 &= (k_{2,1}p_1 + k_{2,2}p_2 + \cdots + k_{2,m}p_m) \bmod 41 \\ &\cdots \\ c_m &= (k_{m,1}p_1 + k_{m,2}p_2 + \cdots + k_{m,m}p_m) \bmod 41 \end{aligned}$$

Note: For this question, correspondence between plaintext and number modulo 41 are as follows "A" $\leftrightarrow$ 0, "B" $\leftrightarrow$ 1, "C" $\leftrightarrow$ 2, ..., "Z" $\leftrightarrow$ 25, "0" $\leftrightarrow$ 26, "1" $\leftrightarrow$ 27, "2" $\leftrightarrow$ 28, ..., "9" $\leftrightarrow$ 35, " : " $\leftrightarrow$ 36, ";" $\leftrightarrow$ 37, " < " $\leftrightarrow$ 38, " = " $\leftrightarrow$ 39, "[" $\leftrightarrow$ 40

(a) The following is ciphertext where the encryption method described above has been employed:

```
OANJASCDOP7A4R82YQR[N11Z;AXCJNV9<ROAZX
UO[06;;2U4;ZXWKW:V2BMV:9264:DGOPJSB=9L9:EF
```

where the key matrix is:

$$\begin{pmatrix} 29 & 1 & 5 & 0 & 26 \\ 28 & 17 & 38 & 25 & 8 \\ 37 & 40 & 1 & 26 & 14 \\ 40 & 33 & 31 & 34 & 14 \\ 31 & 23 & 29 & 12 & 23 \end{pmatrix} \tag{2}$$

Find the corresponding plaintext.

(b) How many different keys are possible in this system described by the Question? What if we disallowed the symbols "[", " = ", " < " so as to only consider an alphabet with 38 characters? In other words, now considering a Hill cipher working mod38, how many possible keys are there?

(c) We return now to the full alphabet $\mathcal{A}$. 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):

```
A8VS3XRDEON6JEVXGJID13CQ7L4C1R4Q965XWRA5DQGYWTNHYO4ND8Z
```


If the following combination of plaintext and ciphertext is given (please replace both "????" her
by giving th

	SBJ
Ciphertext	[WQ:9B

You need to show step-by-step details of your worki
the details of any package, functions used, and/or p y
showing the final result and/or a program would not receive marks.

5. Polynomials [11 marks]

For this question, we work in the ring of polynomials with rational coefficients, $\mathbb{Q}[x] := \{a_0 + a_1 x + \ldots + a_n x^n \mid n \in \mathbb{N}, n \geq 0, a_i \in \mathbb{Q}\}$.

Definition 1. The **greatest common divisor** of two polynomials $p, q \in \mathbb{Q}[x]$ is a polynomial f (unique up to multiplication by an invertible element of $\mathbb{Q}[x]$) such that f divides both p and q, and any common divisor of p and q also divides f.

(a) Find the greatest common divisor of the following polynomials:

$$f(x) := x^4 - 3x^3 + 5x^2 - 17x + 6 \qquad \text{and} \qquad g(x) := x^3 - 4x^2 + 4x + 6 \tag{3}$$

Justify your answer.

(b) Describe (using pseudocode) an analogue of the Euclidean algorithm which finds the greatest common divisor of two arbitrary polynomials.

(c) Perform your algorithm on the pair (3). You must show *all steps* of your algorithm.

(d) Find polynomials $p, q \in \mathbb{Q}[x]$ such that

$$f(x)p(x) + g(x)q(x) = \gcd(f(x), g(x)) \tag{4}$$

(e) What is the multiplicative inverse of $g(x)$ mod $x^4 - 3x^3 - 5x^2 - 17x + 6$?

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 o

- You are reminde dividual work. For many students, discussions with friends will for undertaking of the assignment work. However, it is still an indi are welcome to discuss strategies to answer the questions (even draft solutions) on social media or discussion board. It is U 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. Answers which are not original may not receive full marks even if they are correct.

  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, Will Troiani (`william.a.troiani@gmail.com`) 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.