Cryptography III **Assignment 1**

hand in on MyUni by 5pm 15 August 2025

Note: When answering any mathematical questions, you always need to show your working out

1. a) Suppose you use the affine cipher with the encryption rule

$$e(x) = 5x + 11 \pmod{26}$$

i. Encrypt the plaintext ALMOND

ii. Compute the decryption rule.
You need to write this in the form $d(x) = cx + d$ for some $c, d \in \mathbb{Z}_{26}$.
(Remember to show your working out.)

iii. Decrypt the ciphertext VSLJF

b) Show that you cannot use the affine cipher with the encryption rule

$$e(x) = 6x + 11 \pmod{26}$$

by finding two plaintext letters which encrypt to the same ciphertext letter.

2. Suppose we use the Vigenère cipher using

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

a) Suppose we encrypt the word CHERRY.

i. What is the ciphertext if the keyword is BROLGA?
ii. What is the ciphertext if the keyword is MARTIN?

b) Suppose we receive the ciphertext URWZZZMXZZV.

i. What is the keyword if the plaintext is INFORMATION?
ii. What is the keyword if the plaintext is APPROPRIATE?
iii. How many possible plaintexts are there for this ciphertext?
What percentage of these are a single English word?

3. Suppose you have access to two encryption algorithms, called DUV-56 and DUV-69

- DUV-56 has a 56 bit key,
- DUV-69 has an 69 bit key.

Suppose you have sufficient computing power to use an exhaustive key search to find the key of DUV-56 in 24 hours.

a) Assuming the two algorithms have a similar computational complexity, approximately how many days would you expect to take to find the key of DUV-69 using an exhaustive key search?

b) Suppose that DUV-69 has been designed so that it can be run in two separate stages, so that it is possible to conduct an exhaustive key search for the first 56 bits of a DUV-69 key, followed by a separate exhaustive key search for the last 13 bits. Approximately how many days would you now expect to take to find the key of DUV-69 using an exhaustive key search?

4. a) Compute the following, and show your working out.

   i. Exactly how many decimal digits are needed to write the number 10^{20}?

   ii. Approximately how many binary digits (bits) are needed to write the number 10^{20}?

   iii. Exactly how many binary digits (bits) are needed to write the number 2^{20}?

   iv. Approximately how many decimal digits are needed to write the number 2^{20}?

   v. Summarise your answer using a table formatted like this:

	10^{20}	2^{20}
number of decimal digits		
number of binary digits		

b) For each of the following, find the approximate number. Work out the approximate number of decimal and binary digits needed to represent the number.

A the population of the world 15 November 2022
B the number of stars in our galaxy
C the number of stars in the universe
D the number of species of insects on Earth
E the number of atoms in the known universe
F the number of seconds in a year
G the number of possible 64 bit keys
H the number of possible 128 bit keys
I the number of possible 256 bit keys

Handin your answer using a table formatted like this: (I have completed part A for you):

part	number	decimal digits	binary digits
A	8,000,000,000	10	33
B			
C			
D			
E			
F			
G			
H			
I			

5. Suppose we have a symmetric key algorithm with encryption rule $E_k(x)$, and we want to increase the security. An obvious approach is to try a 'double encryption'. That is, to apply the same cipher twice, using different keys k_1, k_2 each time, and so use the encryption rule

$$E(x) = E_{k_2}(E_{k_1}(x)).$$

We consider this for the affine cipher, and show that a double encryption with the affine cipher is only as secure as single encryption. (As is often the case in cryptography, the result is different from the expected and/or desired one.)

Consider the affine cipher and two different keys $k_1 = (a_1, b_1)$, $k_2 = (a_2, b_2)$. So we have the two encryption rules

$$\begin{aligned} E_{k_1}(x) &= a_1 x + b_1 \pmod{26} \\ E_{k_2}(x) &= a_2 x + b_2 \pmod{26}. \end{aligned}$$

a) Suppose we encrypt a plaintext by first using the encryption rule E_{k_1}, then using E_{k_2} on the result, that is, use the encryption rule

$$E(x) = E_{k_2}(E_{k_1}(x)).$$

Show that there is a single encryption rule

$$E_{k_3}(x) = a_3 x + b_3 \pmod{26}$$

which performs exactly the same encryption, that is, $E_{k_3}(x) = E_{k_2}(E_{k_1}(x))$.

b) Find the values for $a_3, b_3 \in \mathbb{Z}_{26}$ when

$$\begin{aligned} E_{k_1}(x) &= 11x + 3 \pmod{26} \\ E_{k_2}(x) &= 5x + 15 \pmod{26}. \end{aligned}$$

c) Check your solution to part 1 by:

   i. encrypt the plaintext OK first using E_{k_1} and then encrypt the result using E_{k_2}

   ii. encrypt the plaintext OK using E_{k_3}.

d) Suppose an exhaustive key-search attack is applied to a double-encrypted affine ciphertext, is the effective key space increased? (Explain your answer.)