Exercise 1

- Let us consider the following (simple) cryptosystem
- $P = \{a, b\}$;
- $Pr(a) = p$; $Pr(b) = 1-p$, with $0 \le p \le 1$

P=Plaintext
C=Ciphertext
K=Key

- $K = \{k1, k2\}$;
- $Pr(k1) = Pr(k2) = 1/2$;

Encryption Matrix

	a	b
k1	1	2
k2	2	1

- $C = \{1, 2\}$;
- $e_{k1}(a) = 1$; $e_{k1}(b) = 2$;
- $e_{k2}(a) = 2$; $e_{k2}(b) = 1$

Exercise 1

- Compute the probability distribution of the **ciphertext**
- Compute the *Conditional probability* distribution on the **Plaintext**, given that a certain ciphertext has been observed (using Bayes)

$$\Pr[x \mid y] = \frac{\Pr[y \mid x]\Pr[x]}{\Pr[y]}$$

DOES THIS CRYPTOSYSTEM HAVE PERFECT SECRECY?

Exercise 2 – Affine Cipher

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

- Let us consider:
  - $e(x) = ax+b \bmod 26$, with a=9 and b=2
- Is 9 a valid choice for parameter "a"? Why?
- Is b=2 a valid choice ? Why ?
- Encrypt the plaintext "affine"
- Find the decryption function d(y)
- Decrypt the cyphertext "zmimcab"
- Decrypt the cyphertext "ucr"

In practical situations, the « invmodn » function found here can be used
http://www2.math.umd.edu/~lcw/MatlabCode/

Exercise 2 - Solution

- Yes, gcd(9,26)=1, it is a valid choice
- Any choice for b is valid
- *e('affine')=CVVWPM*
- We start with y=9x+2 and solve for x.
  - Since gcd(9,26)=1, the multiplicative inverse of 9 (modulo 26) exists. In fact, it is easy to see that 9*3=1 mod 26, hence 3 is the desired inverse.
  - Therefore we have x=3(y-2)=3y-6=3y+20 (mod 26)
  - d(y) = 3y+20 mod 26
- d('zmimcab') = 'reseaux'
- d('ucr') = 'cat'

Exercise 3 – Affine Cipher

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

- Let us consider:
  - $e(x) = ax+b \bmod 26$, with a=13 and b=4
- Is 13 a valid choice for parameter “a”? Why?
- Is 4 a valid choice for parameter “b”? Why?
- Encrypt the plaintext “input”
- Encrypt the plaintext “alter”

Exercise 3 - Solution

- No, gcd(13,26)=13, it is not a valid choice
- Any choice for b is valid
- *e('input')='ERRER'*
- *e('alter')='ERRER'*
  - *It is impossible to decrypt, since several plaintext yield the same ciphertext.*
  - *Encryption must be one-to-one, and this fails in the present case.*

Exercise 4 – Chosen Plaintext Attack on Affine Cipher

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

- Consider an affine cipher:
  - $e(x) = mx + n \bmod 26$,   with m,n unknown
- You perform a *chosen plaintext* attack using ‘hahaha’. The ciphertext is ‘NONONO’.
- Determine the encryption function.

Exercise 4 - Solution

- Let $mx + n$ be the encryption function.
- Since h = 7 and N = 13, we have
  - $m \cdot 7 + n \equiv 13 \pmod{26}$.
- Using the second letters yields
  - $m \cdot 0 + n \equiv 14 \pmod{26}$. .
- Therefore **n = 14**.
- The first congruence now yields
  - $7m \equiv -1 \pmod{26}$.
- This yields **m = 11**.
- The encryption function is therefore **11x + 14**.

Exercise 5 – Known Plaintext Attack on Affine Cipher

- With a little luck, knowing 2 letters of the plaintext and the corresponding letters of the ciphertext suffices to find the key. In any case, the number of possibilities for the key is greatly reduced and a few more letters should yield the key.
- Suppose the plaintext starts with « if » and te corresponding ciphertext is « PQ ».
- Find the key (i.e., the encryption function).

Exercise 5 - Solution

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

- In numbers we have that 8 (=i) maps to 15 (=P) and 5 maps to 16.
- Let $mx + n$ be the encryption function.
- Therefore we have the equations:
  - $m \cdot 8 + n \equiv 15 \pmod{26}$ and $m \cdot 5 + n \equiv 16 \pmod{26}$. .
- Subtracting we obtain:
  - $m \cdot 3 \equiv -1 \equiv 25 \pmod{26}$, which has the unique solution **m=17**.
- Using the first equation, we find $17 * 8 + n \equiv 15 \pmod{26}$, which yields **n=9**

Exercise 6 – Known Plaintext Attack on Affine Cipher

- Same exercise as before, but now suppose that the plaintext « go » corresponds to the ciphertext « TH ».
- Find the key (i.e., the encryption function).

Exercise 6 - Solution

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

- We have the equations:
  - $m \cdot 6 + n \equiv 19 \pmod{26}$ and $m \cdot 14 + n \equiv 7 \pmod{26}$. .
- Subtracting we obtain:
  - $-8*m \equiv -1 \equiv 12 \pmod{26}$. Since gcd(-8,26)=2, this has two solutions: m=5 and m=18. The corresponding values of n are both **15** (this is not a coincidence, it always happens when the coefficients of m in the equations are even)
- So we have 2 candidates for the key: (5,15) and (18,15). However, gcd(18,26)>1, hence the key is **(m=5,n=15)**

Exercise 7 – Double Ciphering

- Suppose you encrypt using an affine cipher, $mx+n$, then encrypt the encryption using another affine cipher, $ax+b$ (both modulo 26).
- Is there any advantage to doing this, rather than using a single cipher ?
- Why or why not ?

Exercise 7 - Solution

- Let mx+n be one affine function and ax+b be another. Applying the first, then the second, yields the function
  – a(mx+n)+b = (am)x+(an+b) …

  … which is still an affine function.
- Therefore, successively encrypting with two affine functions is the same as encrypting with a single affine function. There is therefore *no advantage* of doing double encryption in this case.

- <u>Technical point</u>: Since gcd(a, 26) = 1 and gcd(m, 26) = 1, it follows that gcd(am, 26) = 1, so the affine function we obtained is still of the required form.)