Cryptography
6CCS3CIS / 7CCSMCIS

Prof. Luca Viganò

Department of Informatics
King's College London, UK

First term 2019/20

Tutorial 2

Encryption scheme (possible exam questions)

1. Give a generic mathematical formalisation of an encryption scheme that maps plaintexts into ciphertexts and vice versa. (Remember to define the message spaces and all the other ingredients and properties.)
2. How can one define symmetric-key and asymmetric-key encryption in such a generic mathematical formalisation?
3. Define the key space $\mathcal{K}$ for each the following pairs of message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$:
   - $\mathcal{M} = \{m_1, m_2\}$ and $\mathcal{C} = \{c_1, c_2\}$
   - $\mathcal{M} = \{m_1, m_2, m_3\}$ and $\mathcal{C} = \{\text{apple}, \text{orange}, \text{peach}\}$
   - $\mathcal{M} = \{m_1, m_2, m_3, m_4\}$ and $\mathcal{C} = \{c_1, c_2, c_3\}$

Caesar Cipher: Exercise

Use the following relative frequencies in an English text of 1000 letters:

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
73	9	30	44	130	28	16	35	74	2	3	35	25	78	74	27	3	77	63	93	27	13	16	5	19	1

to decide the most likely shift used to obtain:

K DKVO DYVN LI KX SNSYD, PEVV YP CYEXN KXN PEBI, CSQXSPISXQ XYDRSXQ.

Don't just use "brute force" but proceed strategically: tally the frequencies of letters in the ciphertext

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

and then try a shift so that there is a correspondence between *English Language Frequencies* and *Enciphered Message Frequencies*.
Why is this not a very good example for the use (and decryption) of an advanced Caesar cipher by frequency analysis?
As a comparison, decrypt the following ciphertext and explain why it is better suited for frequency analysis

QBB JXU MEHBT YI Q IJQWU QDT QBB JXU CUD QDT MECUD CUHUBO FBQOUHI

Additive and multiplicative substitution ciphers (possible exam question)

The Caesar Cipher is an additive cipher, meaning that if we assign integer values to the letters ($A = 0$, $B = 1$, $C = 2$, etc.) then encryption with a shift K can be represented mathematically as an addition modulo 26:

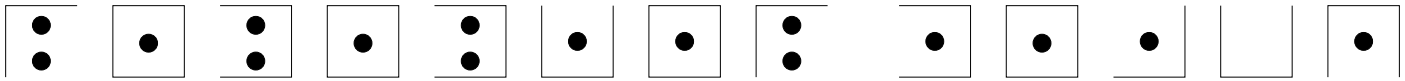
$$C = E(K, P) = (P + K) \bmod 26 \,.$$

Suppose that instead we encrypted messages by multiplying by 2 still using arithmetic modulo 26, i.e.

$$C = (P \times 2) \bmod 26 \,.$$

Could this cipher be used for encryption?
Justify your answer, arguing for “yes” or for “no”.

The Churchyard cipher (simplified): Exercise



- History:
  - This ciphertext appeared engraved on a tombstone in Trinity Churchyard (New York) in 1794.
  - First published solution: 1896.
- Questions:
  - What kind of cipher is it?
  - Why is it so difficult to break? (Especially without the hint!)
  - What is the plaintext message?
  - What is the key?
- HINT: TIC TAC TOE

- Similar cipher: the Pigpen Cipher.

The Playfair Cipher: Exercise

Use the keyword “CHARLES" to encrypt the plaintext

MEET ME AT HAMMERSMITH BRIDGE TONIGHT

Another cipher: The Polybius Chequerboard (not examinable)

The Greek Polybius (∼200–118 b.C.) invented a monoalphabetic cipher that converts alphabetic characters into numeric characters. Used to signal messages by holding different combinations of torches in each hand.

A Polybius Chequerboard using the English alphabet:

#	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Each letter may be represented by two numbers by looking up the row the letter is in and the column. For instance h=23 and r=42.
Note that i and j share the same position. But thjs wjll not cause much of a problem when decoding as jt wjll usually be obvjous from the context whjch was jntended!

Vigenère Cipher: Exercise

Use the Vigenère tableau and the keyword RELATIONS to encrypt

TO BE OR NOT TO BE THAT IS THE QUESTION

and then use them again to decrypt the ciphertext (showing the steps and discussing the strength of Vigenère against frequency attacks)

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Ciphers: Exam question

Alice wants to send the plaintext RIVER to Bob. She encrypts the plaintext and sends the ciphertext EVIRE. Select all the correct statements from the following list.

1. Alice used a Caesar cipher with shift 12.
2. Alice used a Caesar cipher with shift 13.
3. Alice used a Caesar cipher with shift 39.
4. Alice used a Vigenère cipher with keyword NNNN.
5. Alice used a Vigenère cipher with keyword NN.
6. Alice used a ROT13 cipher.
7. Alice used a transposition cipher.
8. Alice did not use a transposition cipher.
9. Alice used a Caesar cipher with shift 13 followed by a Vigenère cipher with keyword AAAAA.
10. Alice used a Caesar cipher with shift 13 followed by a ROT13.

One-time pad: Exercise

- Example:
  - If message is ONETIMEPAD and the key sequence from the pad is TBFRGFARFM, then the ciphertext is IPKLPSFHGQ.
    O + T mod 26 = I, N + B mod 26 = P ...
  - Every key sequence is equally likely, so attacker has no chance!
  - Key sequence could be

$$\begin{aligned} \texttt{POYYAEAAZX} &\Longrightarrow \texttt{SALMONEGGS} \\ \texttt{BXFGBMTMXM} &\Longrightarrow \texttt{GREENFLUID} \\ \texttt{ABCDEFGHIJ} &\Longrightarrow \ldots \end{aligned}$$

- Caveats:
  - Key letters have to be generated randomly.
  - No reuse of key sequence.
  - Length of key sequence must be equal to length of message.
  - Synchronization sender-receiver is needed.

One-time pad: Exercise

- Ciphertexts encrypted according to a one-time pad cipher are unbreakable.
- However, this relies on each one-time pad being used once and only once.
- If an attacker intercepts two distinct ciphertexts which have been encrypted with the same one-time pad, he could (quite easily) decipher them.
- Question: which strategy could he adopt to decipher them?
- As a concrete example, decipher the two following texts, which were encrypted with the same one-time pad (mod 26):
  - UJHANTAMAWMUZVGKTERRYKUB
  - BPGXMKYMBBPYXMOGOEHDEFGH

  Which is the one-time pad that was used?