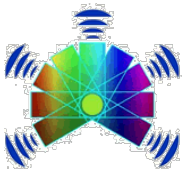
LABORATORIO

Introduzione alla crittografia e alla teoria dei codici

Secondo incontro



Piano Lauree Scientifiche

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Ricordiamo: teoria della informazione e teoria dei codici

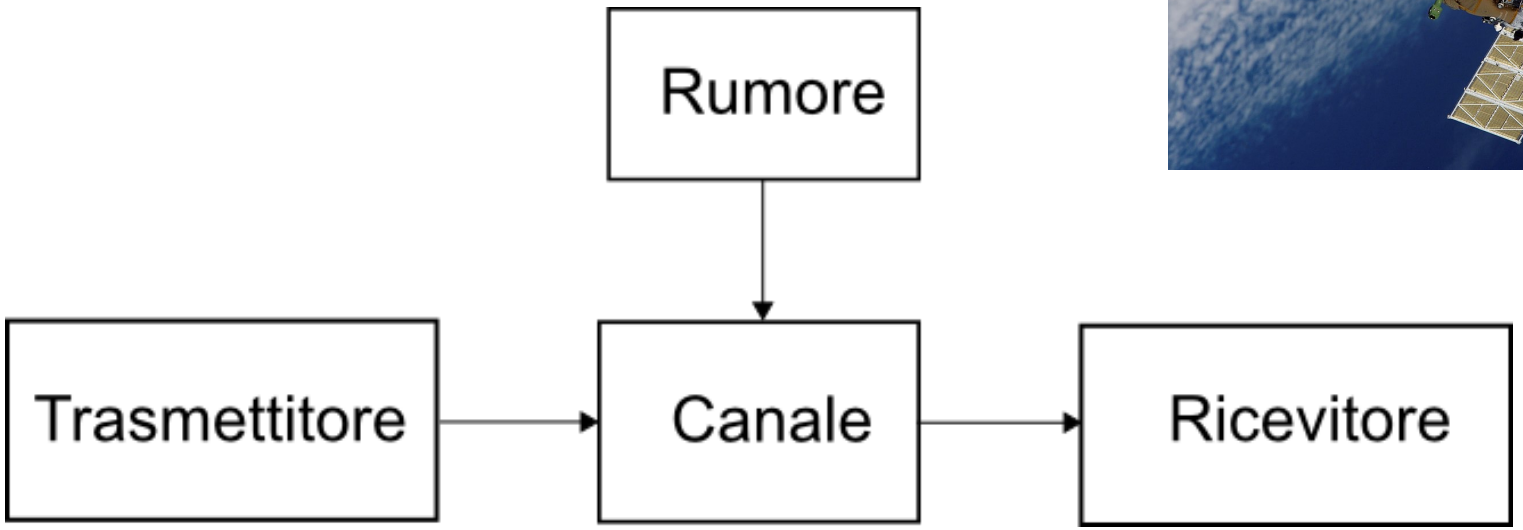
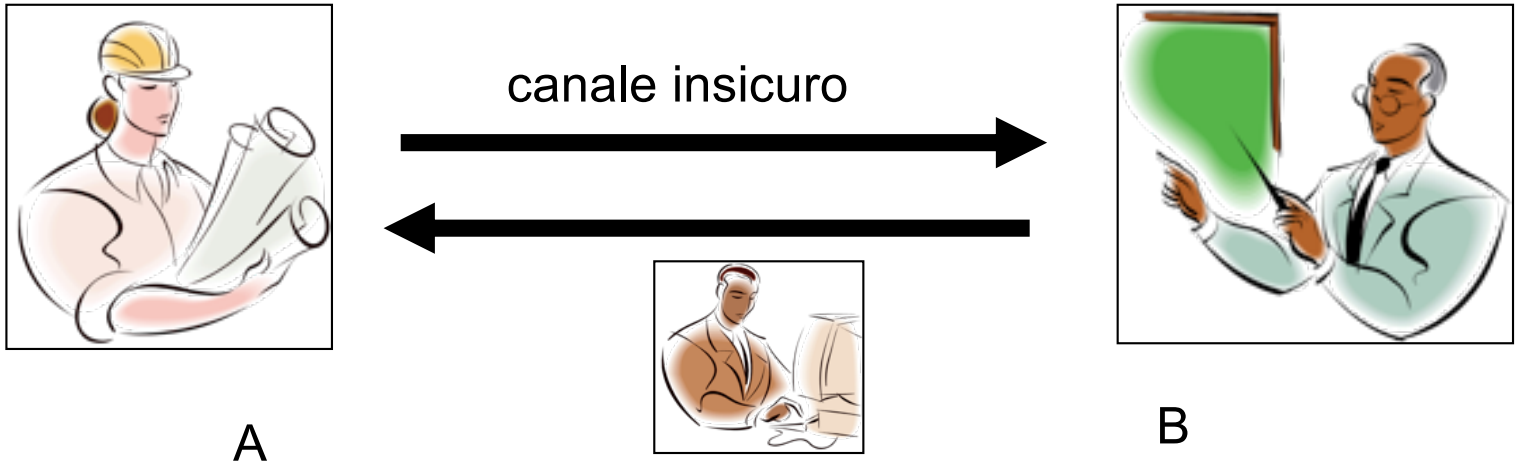


Foto: Soyuz (TMA version) Spacecraft, Wikimedia Commons,
https://commons.wikimedia.org/wiki/File:Soyuz_TMA-7_spacecraft2edit1.jpg

Ricordiamo: La crittografia

come rendere segreta e sicura la comunicazione tra due persone o entità nascondendo il significato del messaggio?



Ricordiamo: La scacchiera di Polibio come sistema crittografico e codice di trasmissione

Ogni lettera è rappresentata dalla coppia di numeri che indica la sua posizione nella scacchiera, cominciando dalla prima riga: B è 12, P è 34, V è 45

Il messaggio viene battuto lasciando una pausa più breve tra i due numeri che si riferiscono ad una lettera e una pausa più lunga tra una lettera e l'altra.

a	b	c	d	e
f	g	h	i	l
m	n	o	p	q
r	s	t	u	v
z	.	,	:	?

Il crittosistema di Cesare

Giulio Cesare utilizzava un sistema di cifrazione molto semplice: ogni lettera va sostituita con quella che si trova tre posti dopo: la *a* viene cifrata con D, la *b* con E, etc.

Usiamo le lettere maiuscole per indicare l'alfabeto cifrante.

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z
D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C

Ad esempio la frase

domani attaccheremo (testo in chiaro),

diventa

Per decifrare, basta tornare indietro di tre passi

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
u	v	z	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t

Il crittosistema di Cesare

Abbiamo visto che Giulio Cesare utilizzava un sistema di cifrazione molto semplice: ogni lettera va sostituita con quella che si trova tre posti dopo

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z
D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C

Ad esempio la frase

domani attaccheremo (testo in chiaro),

diventa **G R P D Q N D Z Z D F F M H U H P R**

Per decifrare, basta tornare indietro di tre passi

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
u	v	z	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t

Il crittosistema di Cesare

Possiamo generalizzare il Sistema di Cesare, spostandoci di un numero *k* arbitrario di passi.

Il numero *k* è detto **chiave.**

Per $k = 7$:

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z
H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C	D	E	F	G

Se *k* è la chiave per cifrare, allora $-k$ è la chiave per decifrare

La chiave $-k$ equivale alla chiave $21 - k$

Tavola 2.1: Decifrare

4) Hai ricevuto il seguente messaggio, cifrato mediante un cifrario di Cesare con chiave cifrante 5.

Messaggio cifrato

M	P	G	Z	F		T	B	B	P	H	F

5) A partire dalla chiave cifrante, ricava la chiave per decifrare, e decifra il messaggio, aiutandoti con la griglia con l'alfabeto.

CHIAVE CIFRANTE 5 CHIAVE PER DECIFRARE ….

Alfabeto per decifrare:

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

6) Decifra il messaggio, aiutandoti con la griglia con l'alfabeto, e riporta il messaggio decifrato nella griglia seguente

Messaggio decifrato

decifrare

4) Hai ricevuto il seguente messaggio, cifrato mediante un cifrario di Cesare con chiave cifrante 5.

Messaggio cifrato

M	P	G	Z	F		T	B	B	P	H	F

5) A partire dalla chiave cifrante, ricava la chiave per decifrare, e decifra il messaggio, aiutandoti con la griglia con l'alfabeto.

CHIAVE CIFRANTE 5 CHIAVE PER DECIFRARE -5 = + 16

Alfabeto per decifrare:

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
s	t	u	v	z	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r

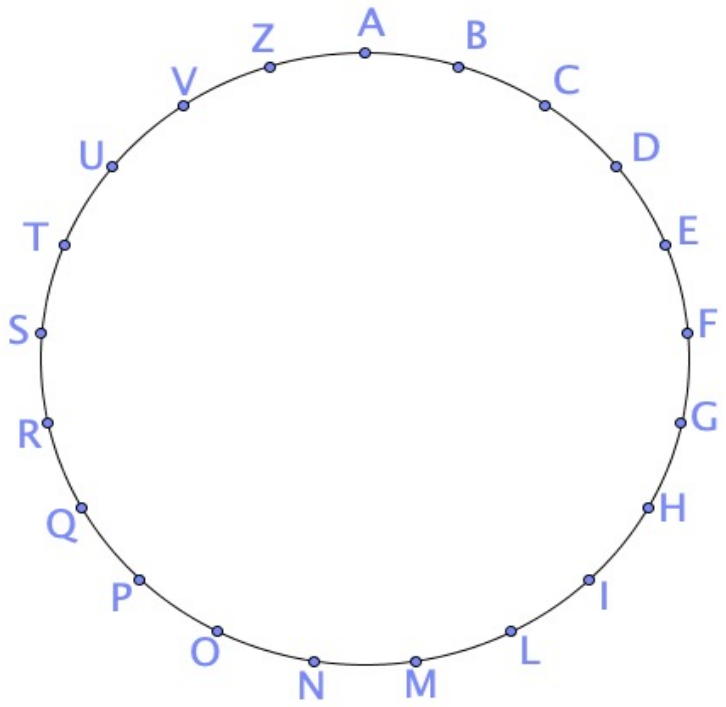
6) Decifra il messaggio, aiutandoti con la griglia con l'alfabeto, e riporta il messaggio decifrato nella griglia seguente

Messaggio decifrato

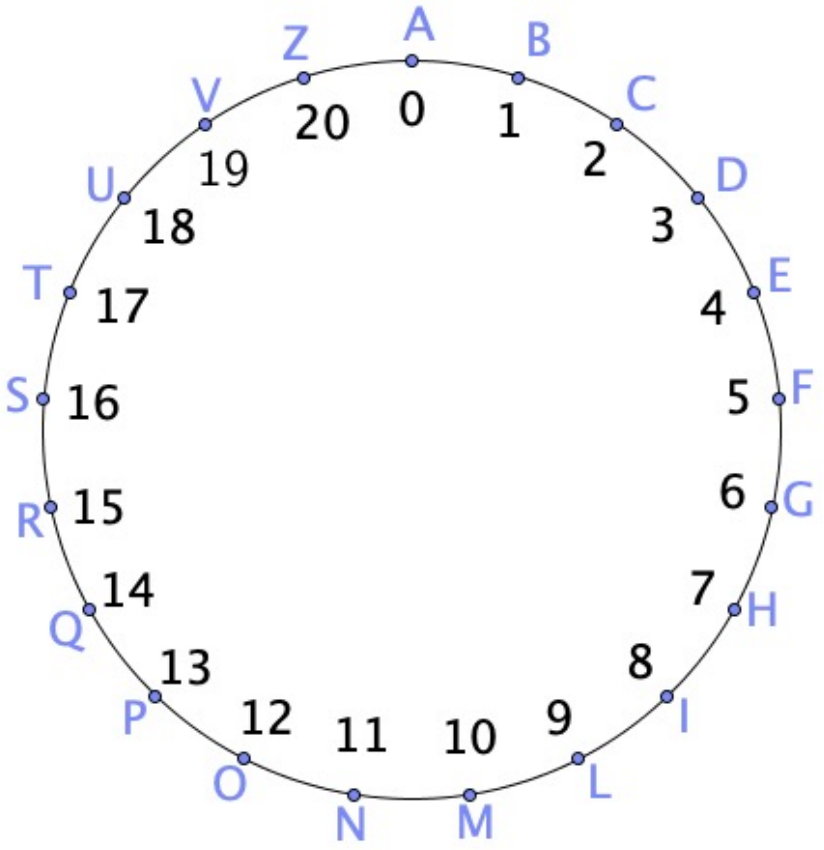
f	i	b	r	a		o	t	t	i	c	a

Semplificare il processo di codifica e decodifica

- Disponiamo le lettere circolarmente



- Sostituiamo le lettere con numeri



Conversione lettere-numeri

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z

a	b	c	d	e	f	g	h	i	l
0	1	2	3	4	5	6	7	8	9

m	n	o	p	q	r	s	t	u	v	z
10	11	12	13	14	15	16	17	18	19	20

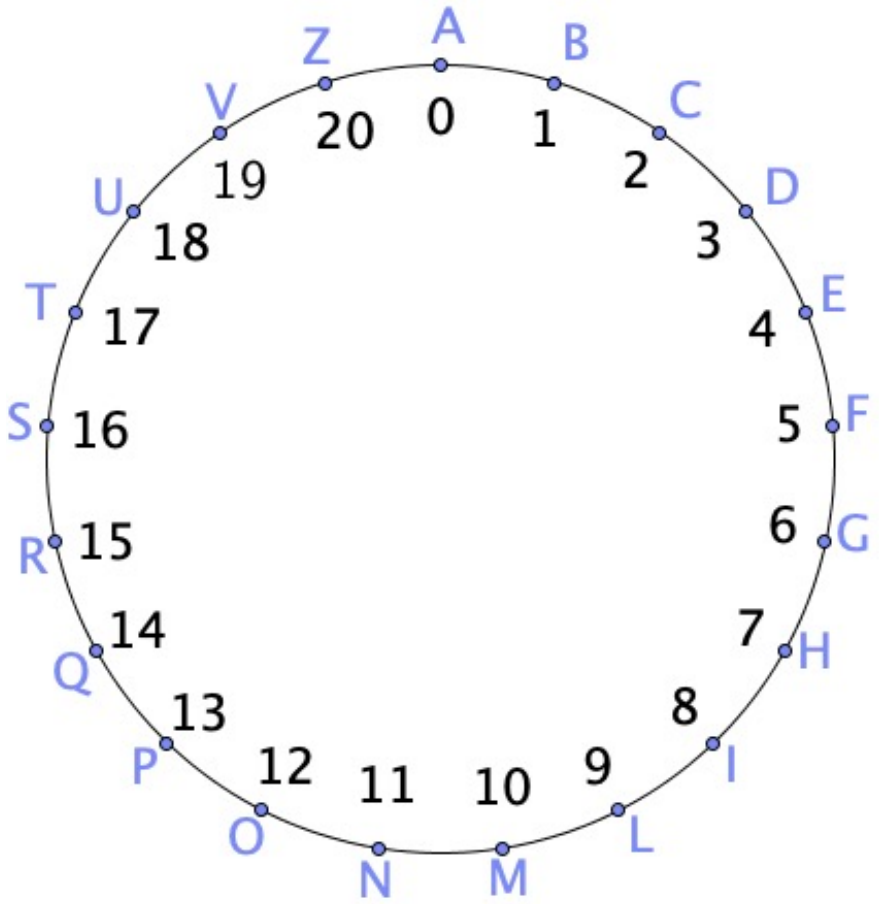
Ancora Cesare

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z

Interpretiamo la procedura seguita nel sistema di Cesare.

Decidiamo un numero (ad esempio 5) che rappresenta la nostra chiave.

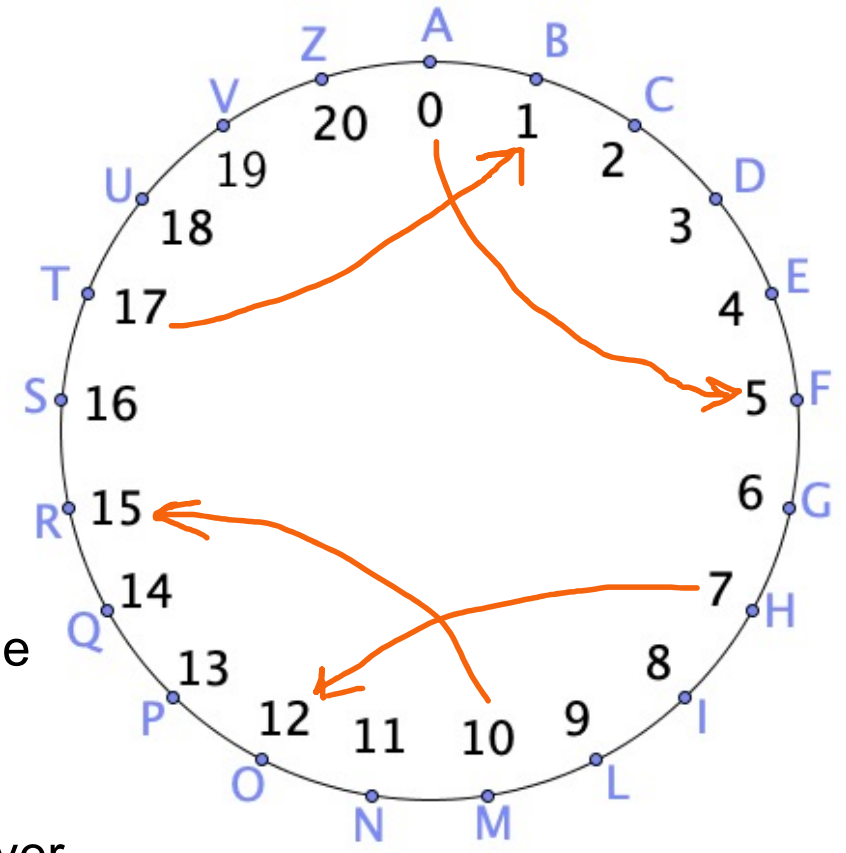
La rotazione di 5 posizioni in senso antiorario ‘corrisponde’ a sommare + 5 a ogni numero dell’alfabeto.



Ancora Cesare

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z

a ⇔ 0 viene cifrata con F ⇔ 5
b ⇔1 viene cifrata con G ⇔ 6
.....
r ⇔ 15 viene cifrata con Z ⇔ 20.
s⇔16 viene cifrata con A⇔0
t⇔17 viene cifrata con B⇔1
u ⇔ 18 viene cifrata con C⇔2
v ⇔19 viene cifrata con D⇔3
z⇔20 viene cifrata con E⇔4



La lettera *t* occupa la posizione 17 e nella rotazione operata si sposta nella posizione

$$17+5=22\,.$$

Poiché $22 = 1 \cdot 21 + 1$, posso dire che 22 corrisponde alla posizione 1, immaginando di aver fatto un giro completo, ma tenendo conto solo della posizione di arrivo.

Ancora Cesare

- Cifrando, operiamo una somma (per traslare): se il risultato è maggiore di 21, ci interessa solo la sua posizione sull'orologio, che è data dal resto della divisione per 21

- Le lettere dell'alfabeto sono in corrispondenza biunivoca con i possibili resti della divisione di un intero per 21.

- Ogni numero intero rappresenta una lettera: per sapere quale, basta calcolare il suo resto nella divisione per 21

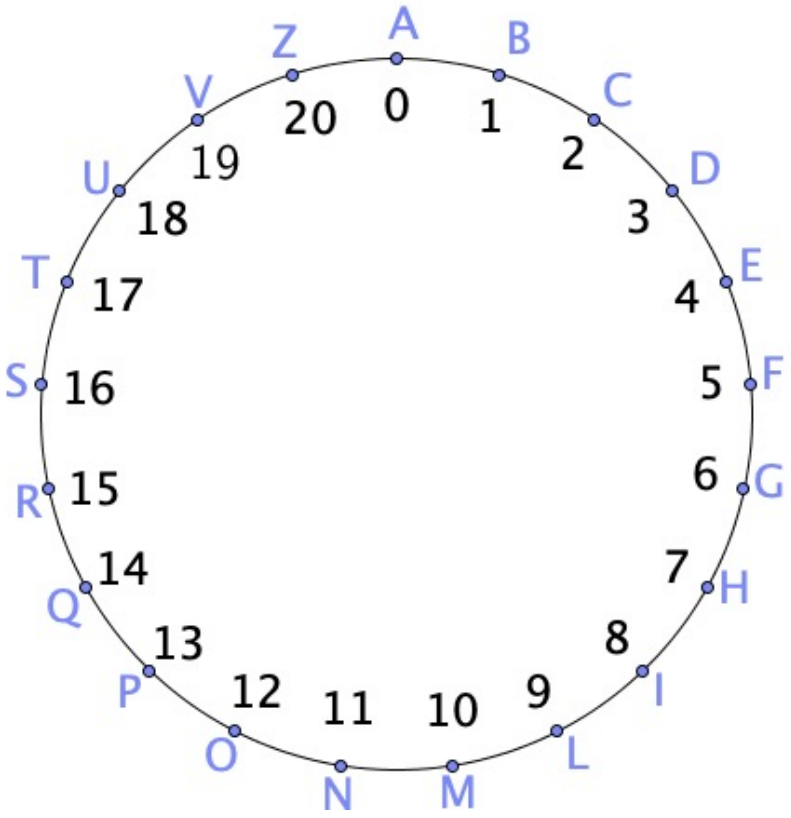


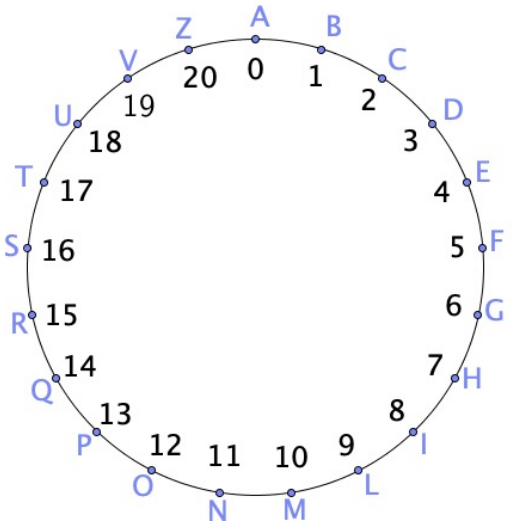
Tavola 2.2

1) Considera la conversione tra numeri e lettere

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z

2) Cifra con cifrario di Cesare con chiave 12 la seguente parola.

g	i	o	v	e	d	i	chiaro
6	8	12	19	4	3	8	numero
18	20	24					Somma da svolgere
		3	10	16	15	20	orologio



3) Decifra il messaggio cifrato con cifrario di Cesare con chiave 5

20	23	0	0	9	14	l4	cifrato
15	18	16		4	9		numero
r	u	s	s	e	l	l	chiaro

Tavola 2.2 : svolgimento

1) Considera la conversione tra numeri e lettere

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z

2) Cifra con cifrario di Cesare con chiave 12 la seguente parola.

g	i	o	v	e	d	i	chiaro
6	8	12	19	4	3	3	numero
6+12	8+12	12+12	19+12	4+12	3+12	3+12	somma
18	20	3	10	16	15	15	cifrato

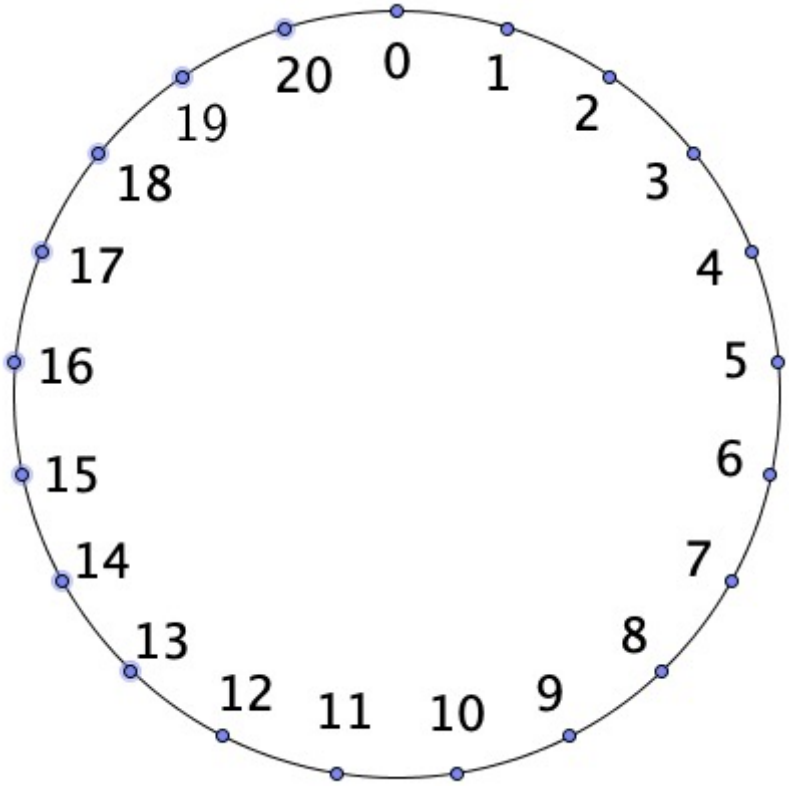
3) Decifra il messaggio cifrato con cifrario di Cesare con chiave 5

20	23	0	0	9	13	l3	
15	18	16	16	4	9	9	
r	u	s	s	e	l	l	

Congruenza modulo *21* : *esercizi*

1) Seguendo l'esempio, determina un numero tra 0 e 20 congruente modulo *21* al numero assegnato:

- 23 è congruente modulo 21 a ...2...
- 30 è congruente modulo 21 a ...9.....
- 40 è congruente modulo 21 a ..19.....
- – 1 è congruente modulo 21 a ...20.....
- 58 è congruente modulo 21 a .....16 ...



2) È vero che 132 è congruente a 257 modulo 21?

Nota: 257-132 = 125 = 21× 5 + 20

Congruenza modulo *21: soluzioni*

1) Seguendo l'esempio, determina un numero tra 0 e 20 congruente modulo *21* al numero assegnato:

- 23 è congruente modulo 21 a 2
- 30 è congruente modulo 21 a 9
- 40 è congruente modulo 21 a 19
- – 1 è congruente modulo 21 a 20
- 58 è congruente modulo 21 a 16

1) Seguendo l'esempio, determina un numero tra 0 e 20 congruente modulo *21* al numero assegnato:

- 23 è congruente modulo 21 a 2
- 30 è congruente modulo 21 a 9
- 40 è congruente modulo 21 a 19
- – 1 è congruente modulo 21 a 20
- 58 è congruente modulo 21 a 16

2) È vero che 132 è congruente a 257 modulo 21?

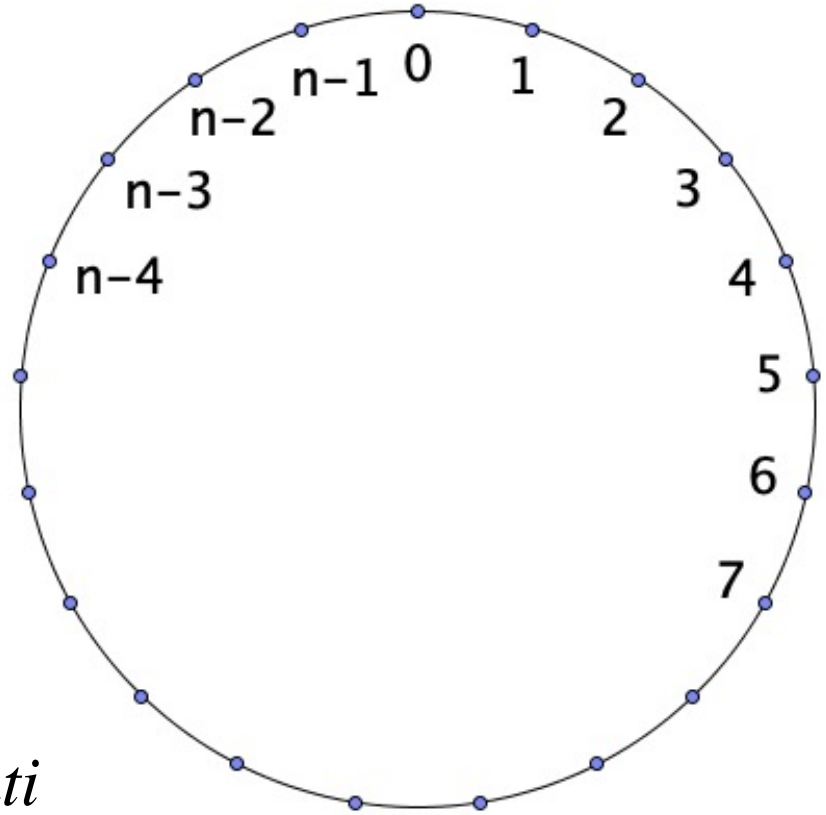
Nota: 257-132 = 125 = 21× 5 + 20

2) È vero che 132 è congruente a 257 modulo 21?

Nota: 257-132 = 125 = 21× 5 + 20

Congruenza modulo *n*

- Lasciamo libero il numero delle lettere dell'alfabeto, che denoteremo con *n (> 0)*
- in un alfabeto di *n* lettere, possiamo chiamare 0, 1, ..., *n–1* le lettere e **identificare due numeri che abbian stesso resto nella divisione per *n***.



- Quando due numeri hanno lo stesso resto nella divisione per *n* sono **congruenti modulo *n* (o mod *n*)** e introduciamo un simbolo:

- se due numeri $a, b \in Z$ sono *congruenti modulo n*, scriviamo
  - $a \equiv b \bmod n$

Congruenza modulo *n*

Ogni numero *a* è congruente mod *n* al suo resto nella divisione per *n,* cioè all'unico intero *c* compreso tra *0* e *n–1* tale che

$$a = n \cdot q + c \quad \text{, con } q \text{ intero.}$$

- Dunque, un qualsiasi numero intero (positivo o negativo) è congruente modulo *n* ad uno e ad uno solo tra i numeri 0, …, *n–1*.