Cryptographia ad usum Delphini

Alessandro Zaccagnini

Parma, 13.4.2005

In questo articolo intendiamo fare una breve storia di alcuni aspetti della Crittografia, dall'antichità classica ai giorni nostri: per raggiungere il nostro scopo ci facciamo aiutare da alcuni famosi racconti o testi letterari che contengono riferimenti a crittogrammi o messaggi nascosti. Nell'illustrare il metodo di risoluzione cercheremo di dare un'idea delle tecniche della crittografia antica, per poi passare ad una descrizione di quella moderna, che ribalta radicalmente le prospettive. Per questo avremo bisogno di richiamare alcuni concetti di statistica, e di sviluppare in piccola parte la matematica delle grandezze discrete, senza alcuna pretesa di generalità o completezza.

1 Edgar Allan Poe, "Lo scarabeo d'oro"

1.1 Il crittogramma

Il racconto "Lo scarabeo d'oro" racconta la ricerca di un tesoro a partire da un pezzo di pergamena che contiene il disegno di un capretto e una serie di caratteri, come quelli qui riprodotti.

5 3 ‡ ‡ † 3 0 5)) 6 * ; 4 8 2 6) 4 ‡
.) 4 ‡) ; 8 0 6 * ; 4 8 † 8 ¶ 6 0))
8 5 ; 1 ‡ (; : ‡ * 8 † 8 3 (8 8) 5 *
† ; 4 6 (; 8 8 * 9 6 * ? ; 8) * ‡ (;
4 8 5) ; 5 * † 2 : * ‡ (; 4 9 5 6 * 2
(5 * – 4) 8 ¶ 8 * ; 4 0 6 9 2 8 5) ;
) 6 † 8) 4 ‡ ‡ ; 1 (‡ 9 ; 4 8 0 8 1 ;
8 : 8 ‡ 1 ; 4 8 † 8 5 ; 4) 4 8 5 † 5 2
8 8 0 6 * 8 1 (‡ 9 ; 4 8 ; (8 8 ; 4 (
‡ ? 3 4 ; 4 8) 4 ‡ ; 1 6 1 ; : 1 8 8 ;
‡ ? ;

Nel vedere questo schema, ci sono di solito due reazioni: la prima, che possiamo descrivere con le parole di Amleto

> HAMLET: "O dear Ophelia, I am ill at these numbers"
> William Shakespeare, "Hamlet," II, 2; 119

si può definire come rassegnazione di fronte a un problema apparentemente insolubile, mentre la seconda, per la quale prendiamo in prestito le parole di Alice,

> ALICE: "Somehow, it seems to fill my head with ideas—only I don't know exactly what they are!"
> Lewis Carroll, "Through the Looking Glass"

si può definire possibilista. Come possiamo aiutare Amleto ed Alice a scoprire il significato dei simboli del crittogramma? Seguiremo abbastanza da vicino la descrizione che l'Autore stesso fa della decifrazione.

La prima cosa da fare è un'ipotesi sulla lingua del testo del crittogramma. L'Autore spiega che il manoscritto è stato rinvenuto in una zona un tempo infestata da pirati, e che uno dei piú famosi pirata si chiamava Kidd: poiché in inglese "kid" vuol dire capretto, in mancanza di altre informazioni la prima ipotesi sulla lingua del crittogramma è che questa sia l'inglese.

1.2 L'analisi di frequenza

Il secondo passo da fare si chiama analisi di frequenza, ed in effetti prescinde dalla conoscenza della lingua in cui è scritto il testo originale: contiamo quante volte compaiono i singoli caratteri.

8	33	*	13	1	8	3	4
;	26	5	12	0	6	?	3
4	19	6	11	2	5	¶	2
‡	16	(	10	9	5	.	1
)	16	†	8	:	4	–	1

È un'osservazione piuttosto banale che in ogni lingua alcune lettere sono molto piú frequenti di altre: in particolare, le vocali tendono a comparire piú spesso delle consonanti. Se la nostra congettura sulla lingua del testo originale è corretta, i dati in questa tabella suggeriscono che il simbolo "8" rappresenti con ogni probabilità la lettera "e" dato che in un normale testo inglese questa lettera da sola compare circa il 13% delle volte. Quando usiamo la parola "normale" intendiamo dire che il testo *non* è stato costruito con l'intento di distorcere appositamente la normale frequenza delle lettere.

Il fatto che il simbolo piú frequente “8” compaia 33 volte su 203 caratteri (con una frequenza relativa del 16% circa) suggerisce anche che lo *spazio* fra le parole è stato probabilmente eliminato, perché in caso contrario sarebbe il carattere di gran lunga piú frequente.

Non potendo sapere dove iniziano e finiscono le parole (cosa che darebbe una miniera di informazioni in lingue come l’italiano nelle quali le lettere finali sono quasi esclusivamente vocali) e neppure quali sono le sillabe piú frequenti, facciamo un altro passo di analisi statistica, basato sull’osservazione che il comportamento delle vocali e delle consonanti è radicalmente diverso: infatti, le vocali hanno la proprietà di poter precedere o seguire qualunque altra lettera dell’alfabeto (con qualche eccezione relativamente infrequente, come nel caso della consonante “q” che è sempre seguita dalla vocale “u” o dalla “q” stessa), mentre le consonanti tendono a precedere o seguire un numero ristretto di altre lettere. In altre parole, la maggior parte di combinazioni consonante-consonante dà luogo a sequenze impronunciabili, mentre ciò non è vero per le combinazioni di vocali e consonanti.

Facciamo dunque una nuova analisi di frequenza, contando questa volta il numero delle occorrenze dei *digrafi*, cioè delle coppie di lettere adiacenti: nella tabella seguente abbiamo raccolto i risultati di questo conteggio, trascurando naturalmente i digrafi meno frequenti, cioè quelli che compaiono meno di 4 volte.

;	4	12	8	5	5	†	8	4
4	8	8	8	8	5	(	;	4
6	∗	5	4	‡	4	8	)	4
)	4	5	;	8	4			

Il risultato conferma la nostra ipotesi a proposito del simbolo “8” che compare in compagnia di molti simboli diversi, precedendoli o seguendoli, e che spesso è raddoppiato: come si sa, il dittongo “ee” è piuttosto frequente nella lingua inglese.

Prima di sostituire il simbolo “8” con la lettera “e” spingiamo la nostra analisi statistica un passo avanti, esaminando anche i *trigrafi*, cioè terne di lettere adiacenti. Compiliamo dunque la tabella che segue, anche in questo caso ignorando i trigrafi meno frequenti.

;	4	8	7	∗	;	4	3
)	4	‡	4	8	†	8	3
				‡	(	;	3

Che cosa possiamo “dedurre” da questa tabella? Considerando il fatto che il simbolo “8” rappresenta probabilmente la lettera “e” e che una delle parole piú frequenti della lingua inglese è l’articolo determinativo “the,” è piuttosto ragionevole supporre che il trigrafo piú frequente rappresenti per l’appunto proprio

questa combinazione di lettere. Non si tratta di una vera e propria deduzione in senso matematico, ma di una ragionevole congettura. Siamo dunque pronti per la

1.3 Prima congettura: “;48” = “the”

Useremo la convenzione di scrivere in nero i simboli di cui non abbiamo ancora stabilito il valore, in blu le lettere sostituite ai simboli già determinati, ed in rosso le lettere su cui si concentra di volta in volta l’analisi di Poe. Il crittogramma originale diventa:

5 3 ‡ ‡ † 3 0 5)) 6 * t h e 2 6) h ‡
.) h ‡) t e 0 6 * t h e † e ¶ 6 0))
e 5 t 1 ‡ (t : ‡ * e † e 3 (e e) 5 *
† t h 6 (t e e * 9 6 * ? t e) * ‡ (t
h e 5) t 5 * † 2 : * ‡ (t h 9 5 6 * 2
(5 * – h) e ¶ e * t h 0 6 9 2 e 5) t
) 6 † e) h ‡ ‡ t 1 (‡ 9 t h e 0 e 1 t
e : e ‡ 1 t h e † e 5 t h) h e 5 † 5 2
e e 0 6 * e 1 (‡ 9 t h e t (e e t h (
‡ ? 3 h t h e) h ‡ t 1 6 1 t : 1 e e t
‡ ? t

Il narratore del racconto di Poe suggerisce di guardare la sequenza di lettere indicata in rosso: vediamo l’articolo “the” seguito da “t(eeth.” L’ipotesi è che il simbolo “(” rappresenti la lettera “r” in modo che questa sequenza indichi la parola “tree” (che vuol dire albero) e sia poi seguita dall’inizio di un’altra parola. Se questa ipotesi, che è ragionevole anche in base alla frequenza relativa del simbolo corrispondente, è vicina alla verità, sostituendo la lettera “r” dovrebbero comparire altri frammenti di parole inglesi plausibili. Passiamo quindi alla

1.4 Seconda congettura: “(” = “r”

Questo è il risultato della sostituzione indicata:

5 3 ‡ ‡ † 3 0 5)) 6 * t h e 2 6) h ‡
.) h ‡) t e 0 6 * t h e † e ¶ 6 0))
e 5 t 1 ‡ r t : ‡ * e † e 3 r e e) 5 *
† t h 6 r t e e * 9 6 * ? t e) * ‡ r t
h e 5) t 5 * † 2 : * ‡ r t h 9 5 6 * 2
r 5 * – h) e ¶ e * t h 0 6 9 2 e 5) t
) 6 † e) h ‡ ‡ t 1 r ‡ 9 t h e 0 e 1 t

e : e ‡ 1 t h e † e 5 t h) h e 5 † 5 2
e e 0 6 * e 1 r ‡ 9 t h e t r e e t h r
‡ ? 3 h t h e) h ‡ t 1 6 1 t : 1 e e t
‡ ? t

Si può forse essere d'accordo con un altro dei personaggi di "Amleto":

> POLONIUS: "Though this be madness,
> yet there is method in't"
> William Shakespeare, "Hamlet," II, 2, 205–206

Guardiamo ora il frammento di testo indicato in rosso: il narratore suggerisce che si tratti della parola "through" (attraverso), seguita dall'articolo determinativo "the." Consultando la tabella delle frequenze dei vari simboli, scopriamo che "‡" compare ben 16 volte, mentre "?" e "3" compaiono rispettivamente 3 e 4 volte ciascuno. Questo è incoraggiante, perché effettivamente la vocale "o" è piuttosto frequente in inglese, mentre "u" e "g" sono lettere relativamente infrequenti. Siamo pronti per la nostra

1.5 Terza congettura: "‡" = "o" "?" = "u" "3" = "g"

Come sempre, riportiamo il risultato della sostituzione dei simboli a cui abbiamo assegnato un, seppur ipotetico, valore.

5 g o o † g 0 5)) 6 * t h e 2 6) h o
.) h o) t e 0 6 * t h e † e ¶ 6 0))
e 5 t 1 o r t : o * e † e g r e e) 5 *
† t h 6 r t e e * 9 6 * u t e) * o r t
h e 5) t 5 * † 2 : * o r t h 9 5 6 * 2
r 5 * – h) e ¶ e * t h 0 6 9 2 e 5) t
) 6 † e) h o o t 1 r o 9 t h e 0 e 1 t
e : e o 1 t h e † e 5 t h) h e 5 † 5 2
e e 0 6 * e 1 r o 9 t h e t r e e t h r
o u g h t h e) h o t 1 6 1 t : 1 e e t
o u t

Per non tediare inutilmente i Lettori, condensiamo gli ultimi passi dell'analisi di Poe: per prima cosa concentriamoci sul primo frammento in rosso qui sopra. Compare quasi per intero la parola "degree" (grado) che possiamo considerare plausibile se la pergamena contiene davvero le indicazioni per trovare un tesoro. La seconda parola in rosso sembra essere "thirteen" (tredici): considerando che

il simbolo “6” compare ben 11 volte e che dopo una parola come “grado” è naturale aspettarsi qualche dato di tipo numerico, ci sentiamo fiduciosi nel fare le congetture seguenti.

1.6 Quarta congettura: “†” = “d” “6” = “i” “∗” = “n”

Continuando allo stesso modo, è possibile determinare il valore dei pochi simboli ancora sconosciuti: di seguito diamo la corrispondenza fra caratteri del testo cifrato e quelli del testo in chiaro.

8	e	*	n	1	f	3	g
;	t	5	a	0	l	?	u
4	h	6	i	2	b	¶	v
‡	o	(	r	9	m	.	p
)	s	†	d	:	y	–	c

Non resta che sostituire gli ultimi simboli con le lettere corrispondenti per ottenere il testo decifrato, o, per usare il gergo dei crittografi, “in chiaro.”

1.7 Il messaggio in chiaro

a g o o d g l a s s i n t h e b i s h o
p s h o s t e l i n t h e d e v i l s s
e a t f o r t y o n e d e g r e e s a n
d t h i r t e e n m i n u t e s n o r t
h e a s t a n d b y n o r t h m a i n b
r a n c h s e v e n t h l i m b e a s t
s i d e s h o o t f r o m t h e l e f t
e y e o f t h e d e a t h s h e a d a b
e e l i n e f r o m t h e t r e e t h r
o u g h t h e s h o t f i f t y f e e t
o u t

Per comodità dei Lettori, riportiamo il messaggio decifrato dotandolo degli spazi e dei normali segni di interpunzione:

> A good glass in the bishop’s hostel in the devil’s seat — forty-one degrees and thirteen minutes — northeast and by north — main branch seventh limb east side — shoot from the left eye of the death’s-head — a bee-line from the tree through the shot fifty feet out.

La sua traduzione in italiano è la seguente:

> Un buon vetro nell'ostello del vescovo sulla sedia del diavolo — quarantun gradi e tredici minuti — nord-nordest — tronco principale settimo ramo lato est — cala dall'occhio sinistro del teschio — una linea retta dall'albero passando per il punto toccato lontano cinquanta piedi.

Come si vede, si tratta della descrizione di una località dalla quale è possibile scorgere un albero, su un ramo del quale c'è un teschio. Muovendosi di cinquanta piedi dall'albero nella direzione del punto che si trova sulla verticale dell'occhio sinistro del teschio, si troverà il luogo dove è stato seppellito il tesoro. Si noti che "vetro" è un'espressione gergale per cannocchiale.

C'è un aspetto poco verosimile nella descrizione, peraltro molto accurata, di Edgar Allan Poe, e cioè che il processo di decifrazione sia unidirezionale, un passo dietro l'altro, sempre piú vicini alla soluzione corretta. In realtà è quasi certo che si commettano numerosi errori, che si finisca in vicoli ciechi, che si debba tornare sui propri passi, come in un labirinto: il filo di Arianna che guida il crittografo è rappresentato in buona parte dal suo intuito e dalla sua conoscenza delle caratteristiche della lingua in cui si suppone sia scritto il testo da decifrare, ma si basa su una solida analisi statistica del testo. Viceversa, un aspetto assolutamente verosimile riguarda la velocità con cui si decifra il messaggio una volta raggiunta una certa "massa critica" di caratteri identificati correttamente: i primi passi sono molto incerti e dubbi, mentre i passi successivi sono sempre piú sicuri e rapidi.

2 Jules Verne, "Viaggio al centro della terra"

Un altro testo letterario molto famoso in cui compare un crittogramma è "Viaggio al centro della terra" di Jules Verne. Il luogo di accesso alla strada che conduce al centro della terra è nascosto in un crittogramma di natura completamente diversa da quello descritto qui sopra: lo riproduciamo nella Figura 1. Per la precisione, ci affrettiamo a ricordare che il crittogramma originale è ulteriormente protetto essendo scritto con l'alfabeto runico: per semplicità, qui abbiamo riprodotto la sua traslitterazione nell'alfabeto latino.

Questo crittogramma è del tipo "trasposizione": questo significa che le lettere del testo in chiaro sono rimescolate (potremmo dire anagrammate) seguendo una certa regola, e cioè cambiate di posto rispetto alla loro sequenza originale, ma non sono cambiate in natura. In altre parole, le "a" rimangono "a," le "b" rimangono "b" e cosí via, ma la posizione delle lettere può essere cambiata. Questo fatto può essere scoperto dal crittanalista intento alla decifrazione per mezzo di una

m . r n l l s	e s r e u e l	s e e c J d e
s g t s s m f	u n t e i e f	n i e d r k e
k t , s a m n	a t r a t e S	S a o d r r n
e m t n a e I	n u a e c t	r r i l S a
A t v a a r	. n s c r c	i e a a b s
c c d r m i	e e u t u l	f r a n t u
d t , i a c	o s e i b o	K e d i i Y

Figura 1: Il crittogramma di Verne. Ci siamo presi la libertà di traslitterare il testo originario che usa l'alfabeto runico in quello latino, ed abbiamo sostituito il simbolo che sta per "mm" in questo alfabeto con "m."

analisi di frequenza: infatti, non essendo stata cambiata la natura delle lettere che costituiscono il testo originale, la frequenza delle lettere del testo cifrato è la stessa della frequenza delle lettere del testo in chiaro, e quindi le lettere come le vocali compariranno con una frequenza prossima a quella attesa per qualche lingua.

Seguendo la trama del romanzo, il primo passo verso la decifrazione è una trasposizione dei blocchi che lo costituiscono: si veda la Figura 2. Il testo risultante viene poi letto in verticale:

```
messunkaSenrA.icefdoK.segnittamurtnecertserrette,rotai
vsadua,ednecsedsadnelacartniiiluJsiratracSarbmutabiled
mekmeretarcsilucoYsleffenSnI
```

e questo viene infine letto dal fondo:

```
InSneffelsYoculiscrateremkemdelibatumbraScartarisJulii
intracalendasdescende,audasviator,etterrestrecentrumat
tinges.Kodfeci.ArneSaknussem
```

2.1 Il testo in chiaro

Inserendo spazi e segni di interpunzione, possiamo finalmente ricostruire il testo originale:

> In Sneffels Yoculis craterem kem delibat umbra Scartaris Julii intra calendas descende, audas viator, et terrestre centrum attinges. Kod feci. Arne Saknussem

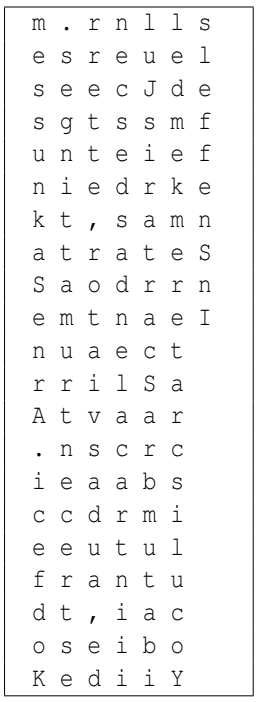

Figura 2: La trasposizione dei blocchi.

Si noti che il latino del testo lascia alquanto a desiderare: infatti, “kem” sta per “quem,” “kod” per “quod,” “audas” per “audax.” La sua traduzione italiana è la seguente:

> Nel cratere dello Yocul dello Sneffels che l’ombra dello Scartaris tocca alle calende di luglio discendi, audace viaggiatore, e raggiungerai il centro della terra. Ciò che io ho fatto. Arne Saknussem

Metodi crittografici di questa natura sono usati molto di rado, perché è molto difficile accordarsi sul metodo di cifratura. In questo caso è stato utilizzato dall’autore per assicurarsi che un messaggio cosí delicato potesse essere decifrato solo da persone sufficientemente abili e determinate da poter intraprendere con successo il viaggio verso il centro della terra.

Una trattazione piú completa con una disamina delle debolezze intrinseche di questi metodi si può leggere nel Capitolo 14 del libro [6]. Un aspetto estremamente importante che vi è trattato è il fatto che l’utilizzazione della stesso procedimento di “trasposizione” a messaggi differenti che hanno in comune qualche parola rivela inevitabilmente al crittanalista le caratteristiche generali della trasposizione stessa e finisce per aiutare la decifrazione. Questo è un caso di interesse pratico, perché con la crittografia classica si tende ad usare a lungo la stessa chiave di cifratura (si veda qui sotto la definizione precisa).

3 Crittografia classica e crittografia moderna

Si considera crittografia classica l'insieme delle tecniche di cifratura e decifratura sviluppate dall'antichità al 1975. Confessiamo che fa un certo effetto a chi scrive pensare di essere nato nell'antichità classica...

I metodi piú antichi di cui abbiamo notizia sono la *skytala* lacedemone, la scacchiera di Polibio, il codice *atbash* e quello di Giulio Cesare. Questi appartengono a quella che consideriamo antichità classica in senso stretto. I successivi risalgono al Rinascimento: i personaggi piú famosi sono Leon Battista Alberti (inventore della cifra polialfabetica e forse dell'analisi di frequenza), Blaise Vigenère, Giovanni Battista Bellaso. Nel ventesimo secolo sono stati sviluppati la macchina Enigma (usata dai tedeschi durante la Seconda Guerra Mondiale), il DES (Data Encryption Standard), ...

La crittografia moderna nasce nel 1975 con un articolo di Diffie & Hellman nel quale si proponeva un nuovo protocollo per lo *scambio delle chiavi*, che è e rimane il vero tallone d'Achille della crittografia classica.[1] Negli anni successivi sono stati proposti metodi crittografici diversi, fra i quali ricordiamo RSA, ElGamal, Massey-Omura, con cui si cambia radicalmente la prospettiva della crittografia classica: un aspetto fondamentale del nuovo approccio è la possibilità dell'applicazione al commercio elettronico e, piú in generale, alla trasmissione sicura di dati fra entità che non hanno concordato preventivamente delle chiavi, e che non necessariamente si fidano l'una dell'altra. Parleremo di questi aspetti nella seconda parte di questo articolo.

4 Il metodo di Giulio Cesare

> Quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A, et perinde reliquas commutet.
> Svetonio, "De Vita Duodecim Caesarum. Divus Julius" Cap. 56

Uno dei piú antichi metodi crittografici è attribuito a Giulio Cesare. Nella versione originale, si disponevano le lettere dell'alfabeto intorno ad un cerchio e ciascuna lettera del testo in chiaro veniva rimpiazzata da quella che la seguiva di

[1] Informalmente, la chiave di un sistema crittografico è una particolare informazione, nota esclusivamente al mittente e al destinatario legittimo di un messaggio segreto, che permette ai due corrispondenti di dialogare in sicurezza. Infatti, si ritiene che sia sostanzialmente impossibile tenere nascosto il *procedimento generale* o meglio il *metodo crittografico* utilizzato per mascherare il messaggio: è dunque necessario che questo procedimento generale sia utilizzabile in un gran numero di modi differenti, e la chiave concordata serve per l'appunto a scegliere quale caso particolare sarà usato concretamente. Gli esempi piú avanti serviranno a chiarire il concetto.

tre posizioni. Piú in generale, oggi si chiama “metodo di Cesare” la trasformazione crittografica nella quale l’alfabeto, che eventualmente conterrà anche spazi ed altri segni di interpunzione, è disposto ad anello, ed ogni lettera è rimpiazzata da quella che la segue di un numero fissato di posti (7 nella nostra Figura 3).

4.1 Esempio di cifratura con il metodo di Cesare con chiave “h”

Riportiamo la cifratura del testo del crittogramma di Poe, completo di spazi e segni di interpunzione, con il metodo di Cesare: per semplificare il confronto, scriviamo il testo in chiaro e subito sotto quello cifrato.

```
a good glass in the bishop's hostel in the devil's sea
t forty-one degrees and thirteen minutes northeast and
 by north main branch seventh limb east side shoot fro
m the left eye of the death's-head a bee-line from the
 tree through the shot fifty feet out.

hgnvvkgnshzzgpug-olgipzovwfzgovz-lsgpug-olgkl'psfzgzlh
-gmvy-bdvulgklnyllzghukg-opy-llugtpu.-lzguvy-olhz-ghuk
gibguvy-ogthpugiyhujogzl'lu-ogsptiglhz-gzpklgzovv-gmyv
tg-olgslm-glblgvmg-olgklh-ofzdolhkghgilldspulgmyvtg-ol
g-yllg-oyv.nog-olgzov-gmpm-bgmll-gv.-e
```

Il metodo di Cesare ha due principali debolezze: per cominciare, è sensibile all’*analisi di frequenza* come il crittogramma nel racconto di Poe. La seconda debolezza è che sono possibili solo *poche* codifiche diverse, e precisamente $n-1$ se n è il numero di caratteri dell’alfabeto. Chi intercetta un messaggio cifrato con il metodo di Cesare può limitarsi a provare successivamente *tutte* le possibili chiavi di cifratura e trovare il testo in chiaro in un tempo ragionevolmente breve. Questo è un esempio di *attacco a forza bruta*.

Un rimedio a questa debolezza è stato proposto dal francese Blaise Vigenère: l’idea è di scrivere il testo da cifrare in *blocchi* di lunghezza fissata, e cifrare la prima lettera di ogni blocco con il metodo di Cesare con chiave a_1, la seconda lettera con il metodo di Cesare con chiave $a_2 \neq a_1$, ... Nella Figura 4 illustriamo la codifica di un piccolo frammento del testo di Poe con chiave “chiave.” Abbiamo indicato la lettera “s” del testo in chiaro in rosso per evidenziare il fatto che viene codificata in modo diverso da colonna a colonna.

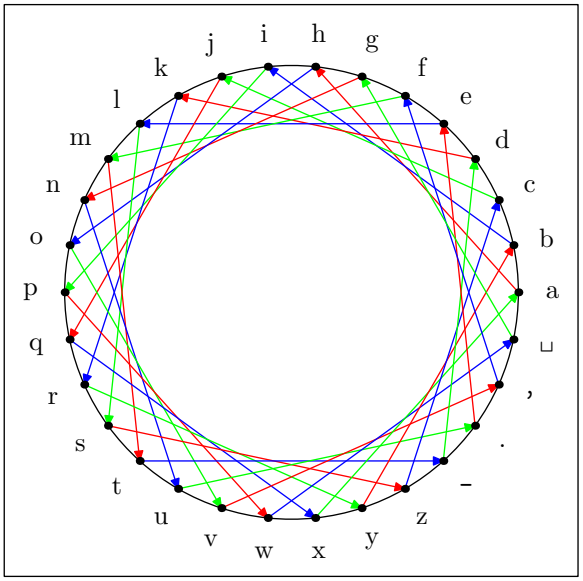

Figura 3: Il metodo di Cesare. Il colore delle frecce non ha un significato particolare: serve solo a rendere piú visibile la relazione fra lettere del testo in chiaro e lettere del testo cifrato. Si dice che la *chiave di cifratura* è “h” perché la lettera “a” viene trasformata in “h”. Chi conosce la chiave di cifratura può facilmente *decifrare*: per questo si parla di cifra *simmetrica*. Si può anche dire che la chiave di decifratura è “x” perché è la lettera che viene trasformata in “a” dalla cifratura, ed è la lettera che *precede* la “a” di 7 posti. Il simbolo “␣” indica lo spazio, che sarebbe altrimenti invisibile.

4.2 Esempio di cifratura con il metodo di Vigenère con chiave “chiave”

Codifichiamo di nuovo il messaggio di Poe usando il metodo di Vigenère: anche in questo caso riportiamo il testo in chiaro e subito dopo il testo cifrato.

```
a good glass in the bishop's hostel in the devil's sea
t forty-one degrees and thirteen minutes northeast and
 by north main branch seventh limb east side shoot fro
m the left eye of the death's-head a bee-line from the
 tree through the shot fifty feet out.

cgoofhbntajwbpv klggjijlqwgsulqz.ecdkuht'ibkmv pazhsze
vgnoix-dwnzdflorziuginydvoqrkiguhm rw-msurqy.hzeu-haeh
bic est-p dekuhbiepjp jixlvt'dnpubuicz. jmflhs'sq-hfis
og.hzdnlntui-lho-dvom yic-p'jajliduebimerpkum -vqtht'i
b-zezdvozolkjg.hzduowtujkm.yujgl. fybg
```

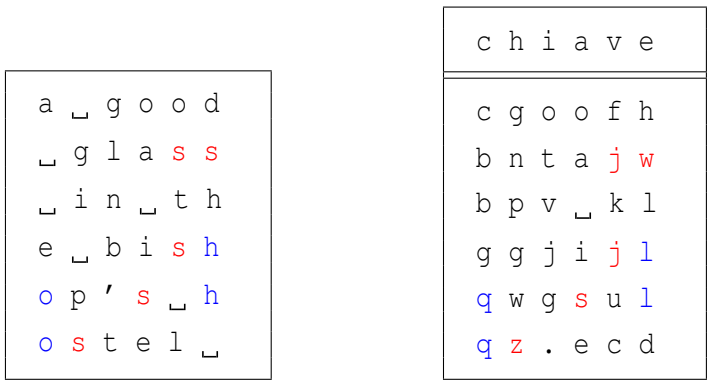

Figura 4: Il metodo di Vigenère: per prima cosa scriviamo il testo in chiaro in blocchi di uguale lunghezza, 6 nel nostro esempio, che disponiamo ordinatamente uno sopra all'altro. Il numero di caratteri in ogni blocco è uguale al numero di caratteri della parola chiave, concordata in anticipo fra chi trasmette e chi riceve: il primo carattere "c" della parola chiave si interpreta come l'istruzione di codificare tutti i caratteri della prima colonna con il metodo di Cesare con parametro "c," e lo stesso avviene per il secondo carattere e la seconda colonna, e cosí via.

L'effetto della cifratura con il metodo di Vigenère è quello di rendere impossibile l'analisi di frequenza che abbiamo descritto qui sopra, perché le lettere piú frequenti saranno codificate con lettere diverse da colonna a colonna, con il risultato di rendere quasi uguali le frequenze relative delle lettere del testo cifrato.

Il metodo di Vigenère sembra essere molto piú robusto di quello di Cesare perché ora il crittografo ha due problemi: determinare la lunghezza k della chiave e poi la chiave stessa. Se l'alfabeto ha n caratteri, vi sono n^k possibili chiavi di cifratura, mentre sono solo $n!/(n-k)!$ se vogliamo che i caratteri siano tutti diversi fra loro. Come si vede, anche da questo punto di vista il metodo di Vigenère è migliore di quello di Cesare.

In effetti questo metodo è stato considerato sicuro per alcuni secoli, finché un'analisi statistica piú raffinata, di Kasinski, mostrò che è possibile "indovinare" (o quanto meno, determinare pochi valori molto probabili) la lunghezza k della chiave di cifratura, riducendo il problema della decifratura a k problemi di decifratura del metodo di Cesare. Questa analisi si basa sul fatto che in ogni lingua vi sono alcune combinazioni di due lettere piuttosto frequenti: se due istanze di questa coppia di lettere compaiono nel testo in chiaro ad una distanza che è un multiplo della lunghezza della chiave, saranno cifrate allo stesso modo, perché vanno a finire nelle stesse colonne. Nel frammento della Figura 4 c'è effettivamente una ripetizione del digrafo "ho" nel testo in chiaro a distanza di 6 caratteri, che genera il digrafo ripetuto "lq" nel testo cifrato: i caratteri corrispondenti sono indicati in blu. Ci sono anche due casi di digrafi ripetuti nel testo in chiaro e

cioè "␣g" e "s␣" che non danno luogo a digrafi ripetuti nel testo cifrato perché la ripetizione avviene ad una distanza che non è un multiplo della lunghezza della chiave. Il crittanalista cerca nel testo cifrato tutte le ripetizioni di coppie di lettere non necessariamente consecutive, compila una lista di "distanze," e ripete la stessa analisi per le terne o addirittura per le quaterne di caratteri. Se molte di queste distanze hanno un fattore comune, è abbastanza probabile che questo fattore rappresenti proprio la lunghezza della chiave di cifratura. Si noti che è ragionevole considerare anche ripetizioni di *singole* lettere: i risultati ottenuti sono altrettanto significativi di quelli calcolati con coppie, terne, ..., di caratteri.[2]

Pur essendo un'attività estremamente tediosa per un essere umano, non è difficile scrivere un programma per computer per eseguire automaticamente questo tipo di analisi su un testo dato. Una possibile contromisura per evitare questo tipo di attacco è la scelta di un alfabeto con moltissimi simboli. Lo stesso metodo si applica in generale alle cosiddette *cifre periodiche*, nelle quali il testo in chiaro è suddiviso in blocchi di lunghezza fissata e ciascun blocco viene codificato come unità singola. Si tratta di cifre in cui, come per il metodo di Vigenère, si deve suddividere il testo in blocchi di k caratteri ciascuno, piú un eventuale blocco di lunghezza minore. La differenza principale risiede nel fatto che, in generale, la codifica di ogni singolo carattere dipende anche da quelli che si trovano nello stesso blocco, mentre questo non avviene per il metodo di Vigenère.

4.3 Mettiamo i puntini sulle i

Prima di passare a discutere la crittografia moderna, è il caso di fissare qualche definizione e concetto importante, che non abbiamo ancora dato in modo rigoroso. I messaggi visti finora erano tutti scritti nel normale alfabeto di 26 lettere piú alcuni segni di interpunzione. Dobbiamo dunque in generale scegliere un alfabeto $\mathfrak{A}$ che contenga tutti i segni che possono essere utilizzati nel messaggio, incluse maiuscole e minuscole, lo spazio, le cifre, i punti e le virgole, ... Siccome per la crittografia moderna si usano esclusivamente computer, deve esistere un metodo per convertire i simboli dell'alfabeto in numeri interi: per esempio se ne può usare il codice ASCII, ma evidentemente non è obbligatorio.

Il metodo di Cesare è un procedimento per trasformare *singoli* caratteri dell'alfabeto in altri caratteri dell'alfabeto, ma abbiamo visto che, per contro, il metodo

[2] In effetti per testi molto brevi questa può essere l'unica analisi a disposizione del crittanalista. I testi brevi sono, comunque, difficili da attaccare. Un esempio concreto di questo fenomeno proviene dai tentativi di decifrazione della lingua etrusca: sebbene siano conosciute migliaia di iscrizioni, queste sono in grande maggioranza epitaffi, per i quali sono utilizzate formule stereotipate che rendono difficile il lavoro del glottologo. Questo è un esempio curioso, perché lo scrivente non aveva intenzione di rendere inintelligibile il suo testo: in alcuni casi le tecniche della crittanalisi si applicano anche alla decifrazione delle lingue antiche.

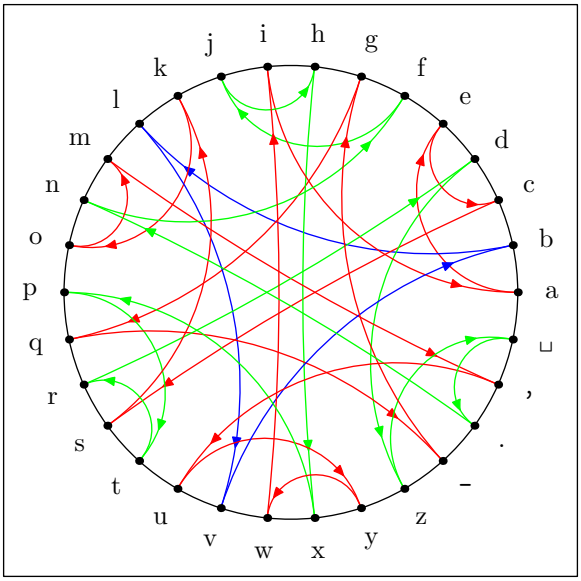

Figura 5: Una variante del metodo di Cesare/Vigenère: il crittosistema affine. Consideriamo $a = 0$, $b = 1, \ldots$ Ogni simbolo dell'alfabeto viene trasformato mediante la funzione $x \mapsto 7x + 4 \bmod 30$. Quindi $a \to e \to c \to s \to k \to o \to m \to , \to u \to y \to w \to i \to a$.

di Vigenère trasforma blocchi di caratteri in altri blocchi della stessa lunghezza. In generale, le unità su cui agiscono le *funzioni crittografiche* sono sequenze di k caratteri dell'alfabeto: chiameremo $\mathfrak{M}$ l'insieme di tutte queste sequenze, e scriveremo $\mathfrak{M} = \mathfrak{A}^k$ per indicare che si tratta di k elementi non necessariamente distinti tratti dall'insieme $\mathfrak{A}$, tenendo conto dell'*ordine* con cui sono scelti. Una funzione crittografica è una trasformazione dell'insieme $\mathfrak{M}$ in sé stesso, con la ragionevole proprietà che elementi distinti hanno immagini distinte, e cioè che testi in chiaro diversi danno luogo a testi cifrati diversi.

Di solito si considerano *famiglie* di trasformazioni crittografiche, che differiscono solo nella scelta di uno o piú *parametri* che nel gergo dei crittografi si chiamano *chiavi*. Nel caso del metodo di Cesare il parametro per cifrare è uguale al numero di posti di cui si deve avanzare a partire da ogni lettera del testo in chiaro per ottenere la corrispondente lettera del testo cifrato. Se l'alfabeto $\mathfrak{A}$ ha n caratteri, la chiave di cifratura è un intero m compreso fra 1 ed $n-1$, e la chiave di decifratura è l'intero $n-m$. Nel caso del metodo di Vigenère, la chiave è costituita da k interi nell'intervallo da 0 ad $n-1$: nel nostro esempio uno dei caratteri della chiave è "a" che significa che i caratteri dell'alfabeto non devono essere modificati, ed infatti è sensato che una delle colonne non venga cambiata. Anche in questo caso, la chiave di decifratura si può calcolare facilmente a partire dalla chiave di cifratura, e viceversa. Nel caso del *crittosistema affine* illustrato nella Figura 5 la chiave di cifratura è costituita dalla coppia di interi $(7,4)$, mentre

la chiave di decifratura è costituita dalla coppia $(13, 8)$: lasciamo la verifica come esercizio per i Lettori.

Per la crittografia classica, il problema di comunicare con sicurezza è dunque ridotto a quello, famosissimo, dello *scambio delle chiavi*. Apparentemente siamo di fronte ad un circolo vizioso: per comunicare in modo sicuro abbiamo bisogno della crittografia, per usare la crittografia dobbiamo assicurare un efficiente scambio delle chiavi, e per effettuare lo scambio delle chiavi dobbiamo poter comunicare in modo sicuro. Nell'antichità (intesa in senso crittografico) lo scambio delle chiavi avveniva tramite corriere, con tutti i rischi insiti un una tale operazione. Nel caso in cui questo non fosse possibile, si pensi per esempio agli U-boote tedeschi, i sommergibili usati nella seconda guerra mondiale e dotati della macchina Enigma, era necessario distribuire ad ogni vascello una copia dell'elenco delle chiavi per un lungo periodo di tempo, tipicamente un mese. Si noti che questa operazione è molto rischiosa, perché se uno di questi elenchi cade in mano nemica, l'avversario potrà decifrare tutte le comunicazioni future; questo è in effetti realmente accaduto durante la Seconda Guerra Mondiale. Inoltre, la possibilità di decifrare messaggi passati, anche se non aiuta a prevenire azioni ostili, può spesso servire ad ottenere informazioni preziose. Per esempio, i tedeschi non usavano le coordinate geografiche standard per indicare i luoghi dove portare l'attacco, ma un loro sistema convenzionale segreto. La decifrazione *a posteriori* di alcuni messaggi cifrati ha permesso agli Alleati di "decifrare" anche questo sistema, che inizialmente ha garantito ai tedeschi un ulteriore livello di sicurezza.

Riassumiamo informalmente alcune caratteristiche peculiari della crittografia classica: due interlocutori si accordano su un metodo crittografico, cioè su un alfabeto e su una famiglia di funzioni crittografiche dipendenti da alcuni parametri detti *chiavi*. La conoscenza della chiave di cifratura permette di ricavare in modo relativamente facile la chiave di decifratura, e viceversa. La sicurezza dipende quindi dalla assoluta segretezza della chiave di cifratura: affinché questa sia garantita, deve essere possibile effettuare lo *scambio delle chiavi* servendosi di un qualche canale che sia al sicuro da attacchi da parte di eventuali avversari.

Nel prossimo paragrafo vedremo come la crittografia moderna fornisca un'elegante soluzione al problema dello scambio delle chiavi. Bisogna aggiungere che la crittografia moderna non ha mandato in pensione quella classica: infatti, a causa della maggiore lunghezza delle chiavi necessarie a garantire un adeguato livello di sicurezza, l'efficienza di cifratura della crittografia moderna è piú bassa di quella della crittografia classica. Paradossalmente, dunque, oggi si usa la crittografia moderna piú che altro per effettuare in modo sicuro proprio lo scambio delle chiavi, mentre si usa la crittografia classica per crittografare grandi moli di dati.

Concludiamo il paragrafo osservando che la crittografia moderna rende possibili anche applicazioni non tradizionali della crittografia, quali il commercio

elettronico: in questo caso, infatti, è impensabile che venditore ed acquirente predispongano un elaborato sistema crittografico per un'operazione che potrebbe anche avvenire *una tantum*. Fra le applicazioni piú comuni della crittografia moderna citiamo il prelievo di denaro dagli sportelli bancomat; fra quelle per cui è prevedibile una rapida diffusione citiamo la certificazione dell'identità e la firma digitale dei documenti.

5 Crittografia moderna o asimmetrica o a chiave pubblica

Già l'ultimo nome della crittografia moderna mostra quanto questa differisca da quella classica: infatti, uno dei dogmi indiscussi della crittografia classica è che le chiavi di cifratura e decifratura debbano essere mantenute segrete. Per il momento ci proponiamo di rispondere alle domande seguenti, avvertendo che queste non esauriscono certo l'insieme dei possibili usi della crittografia moderna.

- Come è possibile che due persone che non si conoscono e non si fidano una dell'altra si mettano d'accordo sulla chiave di un sistema simmetrico, utilizzando Internet?
- Come è possibile *dialogare in modo sicuro* su Internet?
- Come è possibile *certificare l'identità*?

Qui parliamo di Internet per indicare un qualsiasi canale di comunicazione intrinsecamente non sicuro, come anche una linea telefonica o una trasmissione radiofonica: evidentemente si tratta sempre dello stesso problema.

5.1 Il protocollo del "doppio lucchetto"

Si può dire che la crittografia moderna nasce nel 1975 quando Diffie ed Hellman hanno dimostrato, in astratto, che è possibile per due persone comunicare in modo sicuro senza aver preventivamente concordato una chiave. Illustriamo la loro idea per mezzo della Figura 6.

- A mette il suo messaggio per B in una scatola, che chiude con un lucchetto e invia a B.
- B mette il suo lucchetto alla scatola e la rispedisce ad A.
- A toglie il suo lucchetto e rispedisce la scatola a B.

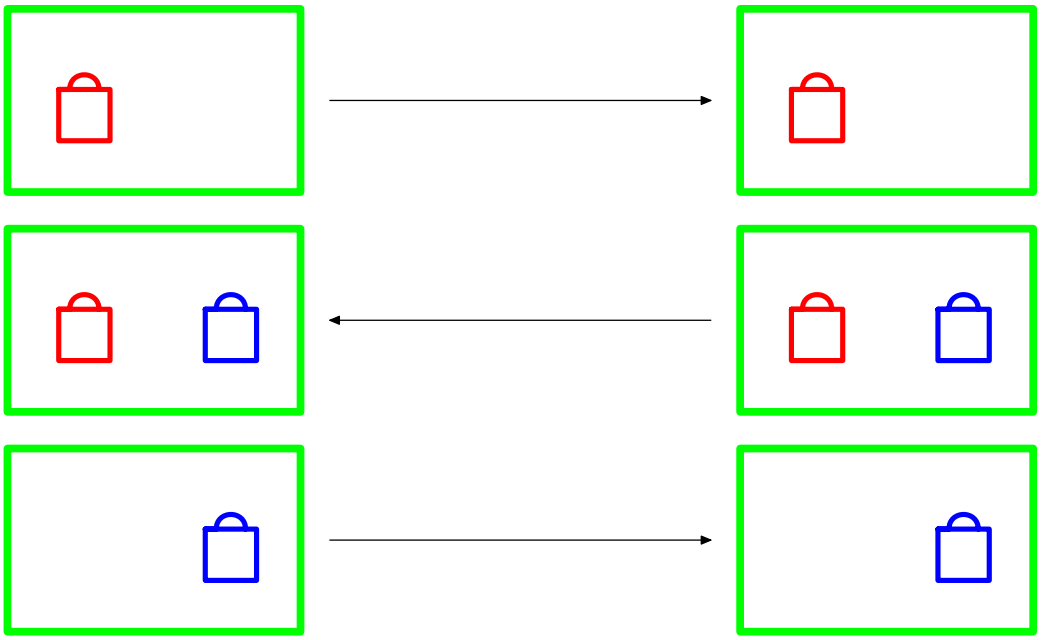

Figura 6: Il protocollo di Diffie ed Hellman.

- B toglie il suo lucchetto e legge il messaggio.

Si noti che la scatola non viaggia mai senza lucchetto, e che né A né B ha dovuto inviare all'altro la chiave del proprio lucchetto. Questo protocollo mostra, in astratto, che è possibile comunicare con sicurezza senza dover effettuare un preventivo *scambio delle chiavi*: questo è il problema che ha afflitto la crittografia classica fin dalla sua nascita, e l'esempio di Diffie ed Hellman mostrò per la prima volta che questo problema poteva essere risolto, nei fatti eliminandolo.

5.2 La matematica discreta

Naturalmente, alla dimostrazione astratta di questa possibilità segue inevitabilmente una domanda: come è possibile realizzare in pratica questo protocollo? Per esempio, sapendo che ormai tutte le comunicazioni o quasi avvengono mediante trasmissione di dati digitali, che cosa è l'analogo *digitale* di una scatola? Ci viene in aiuto la *matematica discreta*, che è adatta alle applicazioni crittografiche. Si tratta dell'Aritmetica Superiore, o Teoria dei Numeri.

> Mathematica regina omnium scientiarum
> et Arithmetica regina omnium mathematicarum
> C. F. Gauss

n	0	1	2	3	4	5	6	7	8	9	10
$7n \bmod 11$	0	7	3	10	6	2	9	5	1	8	4

Figura 7: I multipli di 7 ridotti modulo 11.

L'aritmetica che si usa è la stessa dell'orologio: fissato un numero intero $n > 0$, si fanno tutti i calcoli in $\mathbb{Z}$ e poi si prende il resto del risultato diviso per n. Questa operazione si chiama *riduzione modulo n*. Si tratta di una generalizzazione del concetto di *pari* e *dispari*, o della procedura che si usa nella *prova del nove*. Per esempio, quando $n = 10$, allora $6+9 = 5$ e $3 \cdot 7 = 1$. Scriveremo piuttosto $6+9 \bmod 10 = 5$ e $3 \cdot 7 \bmod 10 = 1$, per sottolineare che non si tratta di vere e proprie uguaglianze e per ricordare il valore del numero n, in questo caso 10.

In questo modo si hanno a disposizione *infiniti* sistemi numerici finiti, molti dei quali sono adatti alle applicazioni crittografiche. Il sistema numerico associato all'intero n si indica con $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. Sono particolarmente adatti alle applicazioni crittografiche i sistemi numerici finiti in cui n è un *numero primo*, cioè è un intero ≥ 2 con esattamente 2 divisori, come 2, 3, 5, 7, 11, 13, 17, 19, ..., 101, 103, ..., 1997, 1999, 2003, 2011, ..., 65537, ...

Euclide ha dimostrato che esistono infiniti numeri primi: siccome la dimostrazione è un piccolo gioiello della matematica antica, la riproduciamo qui. Sia $p_1, p_2, \ldots, p_n$ una lista finita di numeri primi; calcoliamo il numero $N = 1 + p_1 p_2 \cdots p_n$. Sia p un qualsiasi fattore primo di N: dato che N non è divisibile per nessuno dei numeri primi della lista, abbiamo trovato un nuovo numero primo, e quindi nessuna lista *finita* può esaurire tutti i numeri primi.

Oggi sappiamo anche che i numeri primi sono piuttosto *densi* fra gli interi, e che è relativamente semplice determinare numeri primi grandi, come quelli che si usano nelle applicazioni alla crittografia, che tipicamente hanno un centinaio di cifre o piú.

Se p è un numero primo, nel sistema numerico $\mathbb{Z}_p$ non solo si possono eseguire addizioni e moltiplicazioni come in $\mathbb{Z}$, ma è sensato parlare di *divisione* per un intero m, purché questo non sia un multiplo di p. Piú precisamente, dato un numero primo p ed un intero m non divisibile per p, esiste un intero a tale che $m \cdot a - 1$ è multiplo di p: dato che in $\mathbb{Z}_p$ i multipli di p corrispondono a 0, questo intero a, a tutti gli effetti, è il *reciproco* di m nel sistema numerico $\mathbb{Z}_p$.

Formalmente, se m non è divisibile per p, allora l'applicazione $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ definita da $f(x) = m \cdot x \bmod p$ è una biiezione, cioè un rimescolamento degli elementi di $\mathbb{Z}_p$: nella Figura 7 vediamo il caso $p = 11$ ed $m = 7$. In particolare, ogni elemento di $\mathbb{Z}_p \setminus \{0\}$ ha un reciproco nello stesso insieme.

In altre parole, il reciproco di 7, modulo 11, è 8, e, come si vede bene, la moltiplicazione per 7 *rimescola* l'insieme $\mathbb{Z}_{11}$.

Per brevità, scriveremo l'operazione di riduzione di x modulo p nella forma $x \bmod p$, e il reciproco dell'elemento $x \in \mathbb{Z}_p \setminus \{0\}$ con x^{-1}.

5.3 Il protocollo del doppio lucchetto (?)

Ingenuamente, si potrebbe pensare di utilizzare queste proprietà per realizzare una versione del protocollo del doppio lucchetto: prima di cominciare lo scambio di messaggi, A e B concordano un numero primo grande p e un modo per trasformare un qualsiasi messaggio alfanumerico in uno o piú elementi di $\mathbb{Z}_p$.

Per esempio, se $p = 257$ è possibile, ma non certo obbligatorio, utilizzare il codice ASCII dei singoli caratteri, e crittografarli uno alla volta. Questo corrisponde ad usare $\mathfrak{M} = \mathfrak{A} = \mathbb{Z}_p$, e quindi risulta sensibile agli attacchi con analisi di frequenza. Se $\mathfrak{A}$ ha n elementi, cioè se il nostro alfabeto ha n caratteri distinti, allora conviene scegliere per esempio $p > n^2$, ed $\mathfrak{M} = \mathfrak{A}^2$, oppure, piú in generale, $p > n^k$ ed $\mathfrak{M} = \mathfrak{A}^k$. In quest'ultimo caso, si suddivide il messaggio da cifrare in blocchi di lunghezza k, con un eventuale blocco residuo di lunghezza piú piccola. Poi si trasforma ciascuna unità di messaggio $(c_1, c_2, \ldots, c_k) \in \mathfrak{M}$ come se fosse un numero scritto "in base n": poniamo dunque $m = c_1 \cdot n^{k-1} + c_2 \cdot n^{k-2} + \cdots + c_k$. Per costruzione $m \in \{0, \ldots, n^k - 1\}$ e quindi $m < p$ e possiamo crittografarlo usando la funzione crittografica da $\mathbb{Z}_p$ in sé. La decodifica avviene in modo inverso: per esempio, c_k è il resto della divisione di m per n. Poi si rimpiazza m con $(m - c_k)/n$, e c_{k-1} è il resto della divisione di questo nuovo valore di m per n, e cosí via.

Tutto ciò può apparire macchinoso, ma è molto semplice da realizzare per mezzo di un normale computer domestico. Si noti che per motivi di sicurezza è necessario prendere k e di conseguenza p piuttosto grande, ma che questo significa che le operazioni da eseguire, per quanto siano tutte elementari, coinvolgeranno numeri grandi e saranno quindi piuttosto onerose. In definitiva, è necessario un compromesso fra il livello di sicurezza richiesto e la velocità delle operazioni di cifratura/decifratura.

Il nostro primo tentativo di realizzare concretamente il protocollo del doppio lucchetto si basa sulle operazioni che seguono:

- A prende il suo messaggio $M \in \mathbb{Z}_p$, sceglie un altro elemento $a \in \mathbb{Z}_p \setminus \{0\}$ (il suo lucchetto), calcola $M_1 = (a \cdot M \bmod p)$, e trasmette M_1 a B
- B sceglie un elemento $b \in \mathbb{Z}_p \setminus \{0\}$ (il suo lucchetto), calcola $M_2 = (b \cdot M_1 \bmod p)$ e trasmette M_2 ad A

- A toglie il suo lucchetto *dividendo* M_2 per a: in altre parole A calcola a^{-1}, il reciproco di a modulo p, lo moltiplica per M_2 modulo p ottenendo M_3, che invia a B
- B toglie il suo lucchetto *dividendo* M_3 per b: in altre parole B calcola b^{-1}, il reciproco di b modulo p, lo moltiplica per M_3 modulo p ottenendo il messaggio originale M

Sfortunatamente questo metodo non è sicuro: infatti, un eventuale intruso che intercetti i tre messaggi M_1, M_2 ed M_3 può leggere il messaggio originale:

$$M = (M_1 \cdot M_3) \cdot M_2^{-1} \bmod p$$

dove con M_2^{-1} abbiamo indicato il reciproco di M_2 modulo p. Analogamente, A può determinare il lucchetto di B, e viceversa B può determinare quello di A, calcolando $M_2 \cdot M_1^{-1} \bmod p$. Notiamo per inciso che esiste un modo molto semplice ed efficiente per calcolare questo tipo di reciproco, che si basa su una variante dell'Algoritmo di Euclide per calcolare il massimo comun divisore fra due numeri interi: curiosamente *NON* si tratta del metodo insegnato nelle Scuole Medie! Lo stesso procedimento permette di calcolare la chiave di decifratura di un sistema affine come quello illustrato nella Figura 5 data la chiave di cifratura, e viceversa.

5.4 Intermezzo: il calcolo delle potenze

Abbiamo appena incontrato la necessità di calcolare il reciproco di un elemento dell'insieme $\mathbb{Z}_p$, inteso come un altro elemento dello stesso insieme tale che il prodotto dei due dia l'unità. Per non allungare eccessivamente la lunghezza di questa conferenza, rimandiamo la discussione ad altra sede (si vedano le letture consigliate alla fine), ma il problema del calcolo delle potenze con esponente *positivo* ha importanti applicazioni pratiche alla crittografia moderna.

Prima di descrivere dettagliatamente il meccanismo di funzionamento di un metodo crittografico moderno particolare, osserviamo dunque che calcolare potenze, anche con esponenti grandi, non è un'operazione onerosa dal punto di vista computazionale. Con questo intendiamo dire che il calcolo di a^n, che per definizione è un prodotto con n fattori tutti uguali ad a, non richiede $n-1$ moltiplicazioni come potrebbe sembrare a prima vista, ma un numero estremamente piú piccolo. Per esempio, possiamo calcolare a^{400} con solamente 10 moltiplicazioni, come segue:

$$a^{400} = \Big(\Big(\Big(\big(a \cdot \big(((a \cdot a^2)^2)^2\big)^2\big)^2\Big)^2\Big)^2\Big)^2.$$

Infatti, sono sufficienti 6 moltiplicazioni per calcolare la parte colorata di rosso

$$a \cdot \left(((a \cdot a^2)^2)^2\right)^2 = a^{25}$$

e quindi otteniamo a^{400} con quattro ulteriori elevamenti al quadrato. Notiamo che $400 = (110010000)_2$: in un certo senso, possiamo dire che i singoli *bit* possono essere interpretati come *istruzioni*. Infatti, cominciando dal primo "1" a sinistra e partendo dal valore 1, possiamo associare ai bit "1" il comando "eleva al quadrato l'ultimo risultato e moltiplica il nuovo risultato per a", e ai bit "0" il comando "eleva al quadrato l'ultimo risultato." Per esempio, dato che $25 = (11001)_2$, si ha

$$1 \xrightarrow{1} a \xrightarrow{1} a^3 \xrightarrow{0} a^6 \xrightarrow{0} a^{12} \xrightarrow{1} a^{25}.$$

È quindi chiaro che il numero massimo di moltiplicazioni necessarie per calcolare a^n non supera il doppio del numero di bit di n, cioè, approssimativamente, il doppio del logaritmo di n in base 2, oppure, se si preferisce, circa 6.7 volte il numero delle cifre decimali di n.

5.5 Il crittosistema di Massey–Omura

Vediamo ora una effettiva realizzazione pratica del protocollo del doppio lucchetto, supponendo sempre che il messaggio alfabetico originale sia stato trasformato in qualche modo in un equivalente numerico. Tutti gli utenti di questo crittosistema scelgono di comune accordo un numero primo grande p, che viene reso pubblico. L'insieme dei messaggi $\mathfrak{M}$ è dunque $\mathbb{Z}_p$.

Ciascun utente poi sceglie due interi d ed $e \in \mathbb{Z}_{p-1}$ con la proprietà che

$$d \cdot e \bmod (p-1) = 1.$$

Questi costituiscono la sua *chiave privata*, che deve rimanere segreta. L'utente A sceglierà gli interi $d(A)$ ed $e(A)$. Analogamente l'utente B sceglierà gli interi $d(B)$ ed $e(B)$. Anche in questo caso, l'Algoritmo di Euclide fornisce un metodo pratico molto efficiente per effettuare queste scelte.

5.5.1 Comunicare in modo sicuro

Se A vuole spedire a B il messaggio $M \in \mathbb{Z}_p$

- A calcola $M_1 = M^{d(A)} \bmod p$ e lo spedisce a B (A mette il suo lucchetto)
- B calcola $M_2 = M_1^{d(B)} \bmod p$ e lo spedisce ad A (B mette il suo lucchetto)
- A calcola $M_3 = M_2^{e(A)} \bmod p$ e lo spedisce a B (A toglie il suo lucchetto)

- B calcola $M_4 = M_3^{e(B)} \mod p$ e questo coincide con M !!!

Può sembrare miracoloso che l'operazione di rimozione del lucchetto coincida con quella di chiusura del lucchetto stesso, e cioè sia il calcolo di una potenza: i matematici chiamano questi miracoli col nome di teoremi.

6 Le basi matematiche della crittografia moderna

6.1 Il Teorema di Fermat

Vediamo ora una breve descrizione della matematica che sta dietro il meccanismo di funzionamento del crittosistema di Massey–Omura: curiosamente, si tratta di un teorema noto dalla prima metà del Seicento.

Teorema 1 (Fermat) *Sia p un numero primo qualsiasi, ed a un intero non divisibile per p; allora*

$$a^{p-1} \mod p = 1, \qquad \textit{cioè} \qquad a^{p-1} - 1 \qquad \textit{è divisibile per } p.$$

Questo significa che le potenze di a, ridotte modulo p, formano una successione periodica con periodo al piú $p-1$. Per esempio, presi $p = 7$ ed $a = 3$ abbiamo che $3^6 - 1 = 728 = 7 \cdot 104$, e le potenze di 3, ridotte modulo 7, formano la successione periodica 1, 3, 2, 6, 4, 5, 1, 3, 2, ..., mentre le potenze di 2 formano la successione periodica 1, 2, 4, 1, 2, 4, ...

Alla fine del calcolo precedente, abbiamo dunque

$$\begin{aligned} M_4 = M^{d(A)e(A)d(B)e(B)} \mod p &= M^{\left(1+k_1(p-1)\right)\left(1+k_2(p-1)\right)} \\ = M^{1+k_3(p-1)} = M \cdot \left(M^{p-1}\right)^{k_3} &= M \cdot 1 = M \mod p, \end{aligned}$$

dove k_1, k_2, k_3 sono interi opportuni.

Un'altra conseguenza interessante del Teorema di Fermat è il fatto che $a \cdot a^{p-2} \mod p = 1$: dunque il reciproco di a è $a^{p-2} \mod p$ e quindi questo reciproco può essere calcolato in modo efficiente come abbiamo spiegato sopra. Si noti che questo metodo di calcolo differisce dell'Algoritmo di Euclide, che è leggermente piú efficiente.

Dimostreremo un'affermazione equivalente al Teorema di Fermat: qualunque sia l'intero a, se p è un numero primo allora p divide $a^p - a$. Esistono molte dimostrazioni differenti di questo Teorema: ne vedremo una di natura combinatoria che non richiede calcoli e dipende dal conteggio del numero di collane costruite con perline di diverso colore.

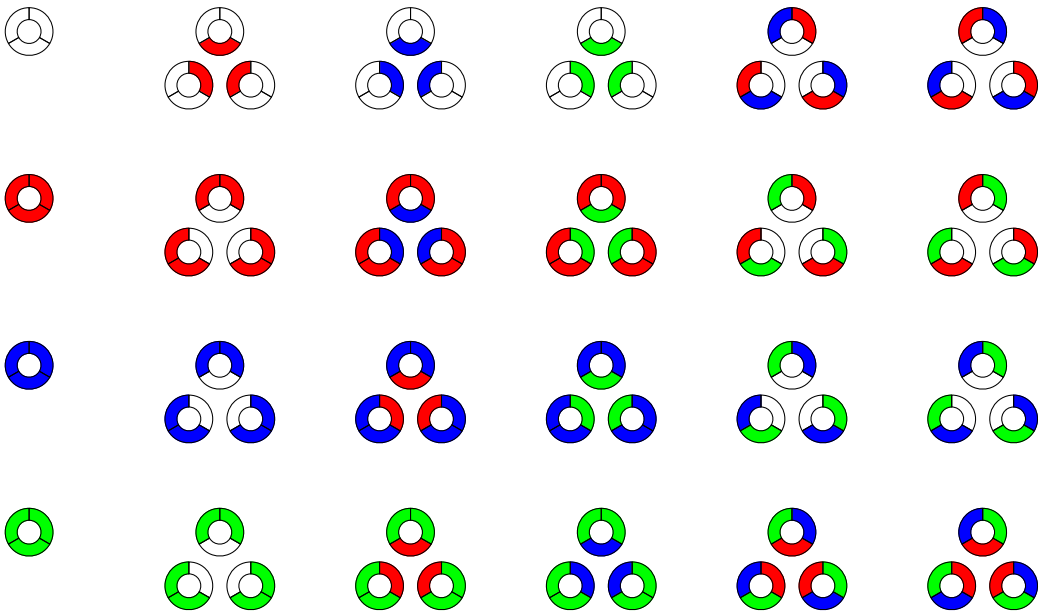

Figura 8: Dimostrazione del Teorema di Fermat: a sinistra le 4 collane monocrome con 3 perline, a destra le $4^3 - 4$ collane policrome con 3 perline, suddivise in classi di collane *equivalenti* per rotazione. Ogni classe contiene *esattamente* 3 collane, e quindi 3 deve dividere $4^3 - 4$.

Ci limiteremo ad illustrare il caso $p = 3$ ed $a = 4$ perché dobbiamo considerare tutte le possibili collane che si possono costruire a partire da p perline di a colori diversi, e queste sono a^p: per poter fare il disegno dobbiamo prendere a e p piuttosto piccoli. La Figura 8 illustra la nostra dimostrazione nel caso particolare citato: la dimostrazione vera e propria si trova nella didascalia.

Per la precisione, per concludere la dimostrazione abbiamo bisogno di un risultato intermedio (un Lemma, nel gergo matematico), e cioè del fatto che ogni classe contiene esattamente p collane: certamente non può contenerne di piú, ma potrebbe contenerne di meno. La Figura 9 dà una dimostrazione di questo fatto: se una collana policroma con n perline è uguale ad una propria rotazione non banale, allora n non è un numero primo.

Questa dimostrazione deve essere piuttosto antica e ci ricorda un brano di uno dei piú importanti teorici dei numeri della prima parte del Ventesimo Secolo.

> A mathematician, like a painter or a poet, is a maker of patterns. If his patterns are more permanent than theirs, it is because they are made with *ideas*. A painter makes patterns with shapes and colors, a poet with words. . . . A mathematician, on the other hand, has no material to work with but ideas, and so his patterns are likely to last longer, since

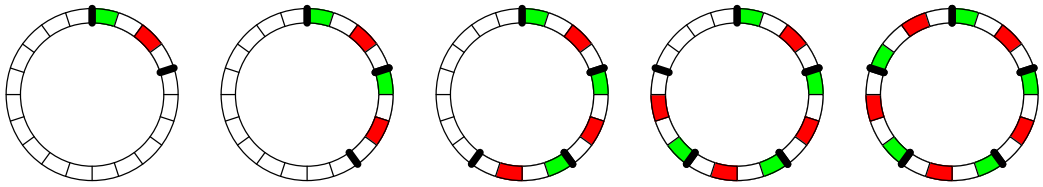

Figura 9: Dimostrazione del Teorema di Fermat. Nell'esempio, supponiamo che la collana sia uguale alla propria rotazione di 4 perline: scelto un qualsiasi blocco di 4 perline consecutive, questo è seguito da un blocco identico, dato che vanno a coincidere dopo la rotazione. Ripetendo lo stesso ragionamento, il secondo blocco è a sua volta seguito da un altro blocco identico, e cosí via, fino ad esaurire completamente tutte le perline. In definitiva, il numero delle perline della collana è divisibile per 4.

> ideas wear less with time than words. The mathematician's patterns, like the painter's or the poet's, must be *beautiful*; the ideas, like the colours or the words, must fit together in a harmonious way. Beauty is the first test: there is no permanent place in the world for ugly mathematics. ... It may be very hard to define mathematical beauty, but that is just as true of beauty of any kind—we may not know quite what we mean by a beautiful poem, but that does not prevent us from recognizing one when we read it.
> G. H. Hardy
> A Mathematician's Apology, 1940

> The artist is the creator of beautiful things.
> Oscar Wilde, "The Picture of Dorian Gray," Preface, 1891

6.2 Il Teorema di Gauss

Il Teorema di Fermat garantisce che le potenze di ogni elemento $a \in \mathbb{Z}_p \setminus \{0\}$ danno luogo ad una successione periodica di periodo che non supera $p-1$, o, piú precisamente, con periodo che divide $p-1$. È importante osservare che esistono elementi dello insieme il cui periodo è *esattamente* uguale a $p-1$.

Teorema 2 (Gauss) *Sia p un numero primo qualsiasi. Esiste $g \in \mathbb{Z}_p$ le cui potenze, ridotte modulo p, hanno periodo $p-1$. In altre parole, i numeri g, $g \bmod p$, $g^2 \bmod p$, ..., $g^{p-1} \bmod p$ sono tutti distinti.*

Questo Teorema è interessante perché è un risultato semplice da capire, ma allo stesso tempo profondo e ricco di conseguenze importanti. La dimostrazione

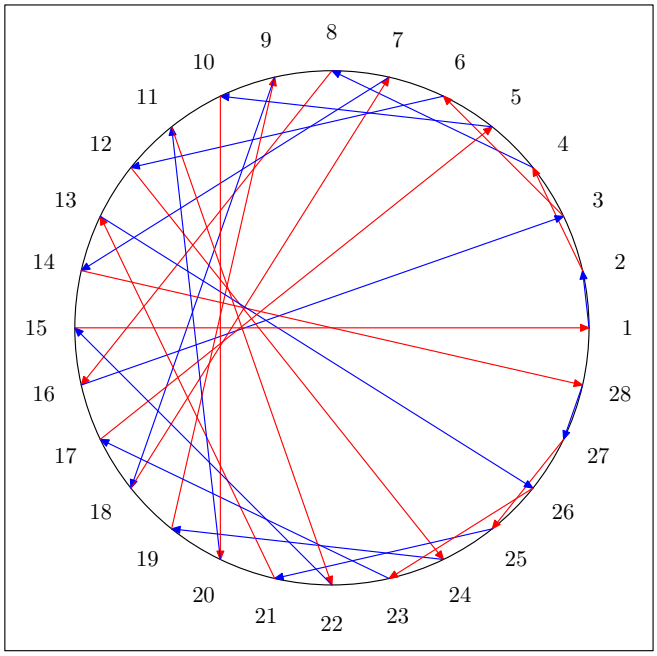

Figura 10: Il teorema di Gauss: le potenze di 2, ridotte modulo 29, toccano tutti i numeri interi fra 1 e 28: infatti valgono 1, 2, 4, 8, 16, 3, 6, 12, 24, 19, 9, 18, 7, 14, 28, 27, 25, 21, 13, 26, 23, 17, 5, 10, 20, 11, 22, 15, 1.

usa il Teorema di Fermat, alcune proprietà dei polinomi e si basa sulla classificazione degli elementi di $\mathbb{Z}_p \setminus \{0\}$ in base alla lunghezza del periodo delle loro potenze. Come sottoprodotto, la dimostrazione garantisce che, per p grande, gli interi $g \in \mathbb{Z}_p$ con la proprietà di Gauss sono piuttosto numerosi, e questo ha una notevole rilevanza crittografica.

Per i numeri primi piccoli, si può scegliere g come indicato qui sotto.

p	2	3	5	7	11	13	17	19	23	29	31	37
g	1	2	2	3	2	2	3	2	5	2	3	2

7 Il crittosistema di ElGamal

Tutti gli utenti di questo crittosistema scelgono di comune accordo un numero primo grande p, e un elemento $g \in \mathbb{Z}_p$ che abbia la proprietà dell'enunciato del Teorema di Gauss. Ogni utente sceglie un elemento $x \in \mathbb{Z}_{p-1}$ che mantiene segreto (la sua *chiave privata*) e rende pubblica la quantità g^x (la sua *chiave pubblica*). Si

tenga presente il fatto che al giorno d'oggi si usano numeri primi di 80–100 cifre, e, in mancanza di un buon algoritmo per ricavare x conoscendo solo g e g^x, questo sistema è da considerarsi sicuro. Abbiamo dunque

- A con chiave privata $\alpha \in \mathbb{Z}_{p-1}$ e chiave pubblica $a = g^\alpha \in \mathbb{Z}_p$
- B con chiave privata $\beta \in \mathbb{Z}_{p-1}$ e chiave pubblica $b = g^\beta \in \mathbb{Z}_p$

Per spedire il messaggio M a B, A sceglie una *chiave di sessione* $k \in \mathbb{Z}_{p-1}$, e spedisce a B la coppia $(g^k, M \cdot b^k)$. Per leggere il messaggio, B calcola

$$(M \cdot b^k) \cdot (g^k)^{-\beta} = M \cdot g^{k\beta} \cdot g^{-k\beta} = M,$$

dove tutte le uguaglianze sono intese modulo p. In altre parole, A mette una *maschera* al messaggio che vuole spedire ed invia a B il messaggio cosí mascherato e un'infomazione che permetta a B (e *solo* a B) di togliere la maschera. La chiave di sessione può includere ad esempio la data e l'ora di invio del messaggio, per garantire che non verrà usata piú di una volta.

8 Conclusioni

Concludiamo con un'ultima citazione di Hardy, il quale si vantava del fatto che, almeno nel suo campo, le scoperte fatte non avevano alcuna applicazione pratica. Come abbiamo visto, è stato presto smentito dai fatti.

> I have never done anything "useful." No discovery of mine has made, or is likely to make, directly or indirectly, for good or ill, the least difference to the amenity of the world. I have helped to train other mathematicians, but mathematicians of the same kind as myself, and their work has been, so far at any rate as I have helped them to it, useless as my own.
> G. H. Hardy
> A Mathematician's Apology, 1940

Ricordando l'altra citazione qui sopra, non siamo molto lontani dall'atteggiamento di un altro scrittore quasi contemporaneo di Hardy.

> All art is quite useless.
> Oscar Wilde, "The Picture of Dorian Gray," Preface, 1891

9 Approfondimenti e letture consigliate

In questa conferenza abbiamo appena sfiorato alcuni dei problemi della crittografia classica e di quella moderna. In particolare, risulta evidente che per realizzare nella pratica i crittosistemi che qui abbiamo descritto, garantendo un adeguato livello di sicurezza, è necessario poter riconoscere i numeri primi fra gli interi "grandi" in modo efficiente, e poter determinare un intero $g \in \mathbb{Z}_p$ con la proprietà dell'enunciato del Teorema di Gauss. Non abbiamo neppure accennato ad alcuni problemi importanti, quali ad esempio la certificazione dell'identità. Per questo rimandiamo ai lavori in italiano descritti appresso.

I racconti citati sono rispettivamente [5] e [8]. Una storia della crittografia, ma senza molto spazio ai suoi aspetti matematici si trova in [7], mentre [2] è un manuale di crittografia, con particolare enfasi sulla crittografia moderna e sui suoi aspetti matematici e informatici. Per una introduzione piú abbordabile, si consulti l'articolo di Alberti [1], dove è discusso anche l'Algoritmo di Euclide. Gli articoli [3], [4] e [9] contengono alcune proprietà dei numeri primi, e qualche loro applicazione alla crittografia moderna.

Riferimenti bibliografici

[1] G. Alberti. Aritmetica finita e crittografia a chiave pubblica – Un percorso didattico per gli studenti delle Scuole Medie Superiori. In A. Abbondandolo, M. Giaquinta, F. Ricci (a cura di), *Ricordando Franco Conti*, pagine 1–29. Scuola Normale Superiore, Pisa, 2004.

[2] A. Languasco, A. Zaccagnini. *Introduzione alla crittografia*. Ulrico Hoepli Editore, Milano, 2004.

[3] A. Languasco, A. Zaccagnini. Alcune proprietà dei numeri primi, I. *Sito web Bocconi-Pristem*, 2005. http://matematica.unibocconi.it/LangZac/zaccagnini.pdf.

[4] A. Languasco, A. Zaccagnini. Alcune proprietà dei numeri primi, II. *Sito web Bocconi-Pristem*, 2005. http://matematica.unibocconi.it/LangZac/LangZacc2.pdf.

[5] E. A. Poe. The Gold Bug. In *The complete tales and poems of Edgar Allan Poe*, pagine 42–70, New York, 1975. Random House. Trad. it. *Lo scarabeo d'oro*, in *Racconti*, L'Unità–Einaudi. Si veda http://web.tiscali.it/no-redirect-tiscali/manuel_ger/ita/bug_ita.htm.

[6] W. W. Rouse-Ball, H. S. M. Coxeter. *Mathematical Recreations and Essays*. Dover, New York, tredicesima edizione, 1987.

[7] S. Singh. *Codici & Segreti*. Rizzoli, Milano, 1999.

[8] J. Verne. *Viaggio al centro della Terra*. Einaudi, Torino, 1989.

[9] A. Zaccagnini. L'importanza di essere primo. In A. Abbondandolo, M. Giaquinta, F. Ricci (a cura di), *Ricordando Franco Conti*, pagine 343–354. Scuola Normale Superiore, Pisa, 2004. http://www.math.unipr.it/~zaccagni/psfiles/papers/importanza.pdf.

Alessandro Zaccagnini
Dipartimento di Matematica
Parco Area delle Scienze, 53/a
Campus Universitario
43100 Parma
e-mail: alessandro.zaccagnini@unipr.it
pagina web: http://www.math.unipr.it/~zaccagni/home.html