ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea in Matematica

LA STORIA DELLA CRITTOGRAFIA: APPUNTI E RIFLESSIONI

Tesi di Laurea in Storia della Scienza

Relatore:
Chiar.mo Prof.
Giuliano Pancaldi

Presentata da:
Chiara Giberti

Correlatore:
Chiar.mo Prof.
Davide Aliffi

II Sessione
Anno Accademico 2010/2011

Dedicato a chi ha qualcosa da nascondere,
ma anche agli spioni…

“Se Gauss fosse vivo oggi, sarebbe un hacker.”
Peter Sarnak, prof della Princeston University.

Indice

Introduzione

Il problema di scambiarsi informazioni private, che risultino indecifrabili da terze persone, è

più che mai attuale. Se per secoli la crittografia è stata associata ad aspetti ben lontani dalla vita ordinaria e fino a pochi decenni fa veniva utilizzata soprattutto in ambito militare e governativo, al giorno d'oggi ciascuno di noi ne fa uso quotidianamente anche se spesso inconsapevolmente.
L'informatica e internet hanno fatto sì che il problema della segretezza delle comunicazioni diventi sempre più rilevante.
Azioni che svolgiamo ogni giorno come chiamare con il cellulare, aprire l'auto con il telecomando o fare bancomat, fanno si che noi trasmettiamo informazioni che potrebbero essere captate e sfruttate a nostro svantaggio. Per evitare che ciò accada bisogna far sì che anche se una potenziale terza persona dovesse intercettare il messaggio, questo gli appaia incomprensibile. Lo stesso ricevente avrà quindi la certezza non solo che le informazioni siano rimaste segrete, ma potrà anche essere sicuro che le informazioni non siano state manomesse da terzi.
La crittografia si occupa proprio dell'insieme dei sistemi in grado di rendere incomprensibile un messaggio a chiunque ne venga in possesso ad eccezione del legittimo destinatario. La crittoanalisi, al contrario, è l'arte di forzare tali sistemi. Numerosi matematici in diversi periodi storici, si sono cimentati nella crittoanalisi: è famoso il caso della violazione della cifratura della macchina Enigma, il sistema crittografico usato dall'esercito nazista durante la II guerra mondiale, dovuta, primariamente, al matematico polacco Marian Rejewski e completata poi da un gruppo di scienziati inglesi, tra i quali ruolo prominente ebbe il celeberrimo logico Alan Turing.

La matematica ha svolto un ruolo fondamentale nello sviluppo della crittografia e

della crittoanalisi, soprattutto dopo gli anni 70 con l'introduzione della crittografia a chiave pubblica e di altri simili protocolli.
La necessità di scambiarsi informazioni segrete, però, non riguarda solo i tempi più recenti ma anche il passato. Si ritiene infatti che la crittografia sia antica quanto la scrittura e già nella Bibbia vengono utilizzati tre diversi tipi di cifratura per nascondere alcune specifiche parole: il Codice Atabash (che verrà analizzato nel secondo capitolo), il Codice Albam e il Codice Atbah. Il più antico esempio di crittografia consiste in un bastoncino su cui veniva arrotolata una strisciolina di cuoio chiamata Scitala lacedemonica in uso intorno al 400 a.C..

Questa tesi si propone di ripercorrere le tappe più importanti della storia della crittografia dall'antichità fino ai giorni nostri, mettendo in relazione le nuove tecniche con le teorie matematiche che ne sono alla base.
I primi quattro capitoli esporranno quindi lo sviluppo dei sistemi crittografici dal IV secolo a.C. fino alle nuove tecniche utilizzate durante la prima guerra mondiale. Il quinto capitolo si concentrerà sul ruolo di primo piano che la crittografia ha avuto durante la seconda guerra mondiale e, in particolare, sull'importanza della decifratura dei messaggi cifrati dai tedeschi tramite la macchina Enigma. Il sesto capitolo tratterà brevemente i metodi moderni di cifratura, cercando i rapporti che intercorrono al giorno d'oggi tra crittografia, matematica e informatica.
In appendice saranno analizzati alcuni"termini tecnici"della crittografia e, infine, saranno approfonditi gli argomenti di algebra e teoria dei numeri utilizzati nei sistemi crittografici esposti.
Il fine di questa tesi vuole essere quello di dare un'immagine della crittografia come di una disciplina in continua evoluzione e nella quale la matematica (l'algebra e la teoria dei numeri in particolare) svolge un ruolo di primaria importanza, in quanto strumento sempre più necessario man mano che avanza lo sviluppo di nuovi sistemi di cifratura. La matematica vista in questa ottica non appare quindi più come materia prettamente teorica, avendo nella crittografia una applicazione pratica e utilizzata nella vita di tutti i giorni.

Capitolo 1

Cos'è la crittografia?

Il termine "crittografia" deriva dal greco "kryptó-s" che significa "nascosto" e "graphìa" che significa "scrittura. La crittografia è quindi l'arte di scrivere messaggi segreti.

Con crittografia si intende quindi un insieme di metodi, tecniche e algoritmi che consentono di trasformare un messaggio in modo da renderlo intellegibile solamente alle persone che condividono maggiori informazioni riguardo al metodo tramite cui si è codificato il messaggio.

Ipotizziamo che due persone vogliano scambiarsi a distanza informazioni che devono restare riservate: il messaggio scambiato non deve essere accessibile da terze persone. Quando ciò si verifica diremo che il canale di trasmissione è sicuro, in realtà nessun canale può considerarsi veramente sicuro.

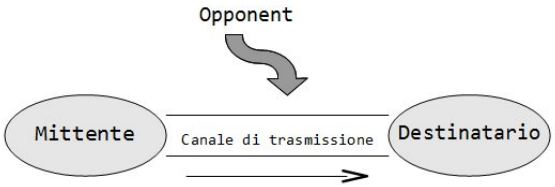


Figura 1.1: Schema di trasmissione del messaggio

Il mittente deve quindi cercare di mantenere la riservatezza"nascondendo"l'informazione

contenuta nel messaggio e per fare ciò adopera un sistema di cifratura che trasforma il testo in chiaro (plain text) in un crittogramma (cyper text), apparentemente privo di significato e tale che solamente al legittimo destinatario, sia possibile estrarre l'informazione trasmessa.

Se il canale di trasmissione non è sicuro una terza persona (avversario/opponent) può cercare di intercettare il messaggio e decifrarlo (ruolo passivo) o, addirittura, di intromettere suoi messaggi nel canale(ruolo attivo).
Il sistema funziona se mittente e destinatario condividono un segreto, di cui l'avversario non deve essere a conoscenza: questo segreto costituisce la **chiave del sistema**.

Capitolo 2

Crittografia antica

Fino dall'antichità l'uomo ha sentito l'esigenza di trasmettere messaggi segreti; infatti i primissimi esempi di crittografia sono stati scoperti in alcuni geroglifici egiziani risalenti a più di 4500 anni fa.
Dagli scritti di Plutarco si è

venuti a conoscenza dell'uso della *scitala lacedemonica* intorno al 400 a.C., un rudimentale sistema crittografico che veniva sfruttato dagli spartani, in particolare in tempo di guerra , per brevi comunicazioni. La scitala era un piccolo bastone di legno, il messaggio veniva scritto su una striciolina di pelle arrotolata intorno a essa. Una volta srotolata la striscia di pelle dalla scitala era impossibile decifrare il messaggio. La chiave del sistema consisteva nel diametro della scitala, la decifrazione era possibile solo se si era in possesso di una bacchetta identica a quella del mittente, si tratta perciò di un sistema crittografico a chiave simmetrica (vedi appendice).

Figura 2.1: Scitala

2.1 Il codice Atbash

Anche nei testi sacri si possono ritrovare numerosi esempi di scritture segrete, spesso adoperate per attaccare la cultura dominante o le autorità politiche. Nell'Antico Testamento sono stati trovati diversi tipi di codici cifranti tra i quali il Codice Atbash utilizzato nel libro di Geremia per cifrare il nome della città di Babilonia.
Il Cifrario Atbash è un esempio di codice monoalfabetico (cfr appendice) molto semplice e consiste nel sostituire la prima lettera dell'alfabeto ebraico (aleph) con l'ultima (taw), la seconda (beth) con la penultima (shin) e così via. Applicandolo al nostro alfabeto si ottiene:

plain text	A B C D ... W X Y Z
crittogramma	Z Y X W ... D C B A

L'uso della crittografia negli scritti religiosi dei primi Cristiani terminò solo con l'avvento dell'imperatore Costantino I, convertitosi al Cristianesimo.

2.2 Il codice di Cesare (II sec d.C.)

Questo antico sistema crittografico, in uso fino al rinascimento, è il più semplice codice simmetrico possibile. Consideriamo l'alfabeto latino di 26 caratteri e numeriamoli da 0 a 25:

Fissiamo un numero da 0 a 25 che sarà la chiave segreta K. L'operazione di cifratura tramite il Codice di Cesare consiste nel sommare K ad ogni carattere del messaggio in chiaro: il crittogramma, cioè, si ottiene spostando"in avanti"di K posti ogni carattere del messaggio in chiaro. Grazie alla testimonianza di Svetonio sappiamo che Cesare utilizzava come chiave di cifratura K=3.

m ="JULIUS CAESAR
c = m+3 ="MXOLXVFDHVDU

Questa stringa costituiva quindi il messaggio affidato al corriere e, teoricamente, anche se fosse caduto in mano nemica, la riservatezza restava garantita dal fatto che il nemico non conosceva la chiave K. Solo il legittimo destinatario,

che conosceva la chiave, poteva recuperare il messaggio originale dal crittogramma eseguendo l'operazione inversa, cioè spostando ogni lettera del crittogramma"indietro"di K posti.

Per la cifratura secondo il Codice di Cesare, si deve immaginare l'alfabeto scritto su di una corona circolare (...XYZABC...) senza soluzione di continuità. Matematicamente, la cifratura di Cesare è una operazione di **somma modulo 26** e la decifrazione è un'operazione di **differenza modulo 26**. (cfr aritmetica modulare in appendice)

Se l'avversario riesce a impadronirsi del crittogramma e sospetta trattarsi di un Codice di Cesare, può tentare un attacco di tipo"forza bruta"(ricerca esaustiva nello spazio delle chiavi), provando a decifrare il messaggio con tutte le possibili chiavi da K=1 (per K=0 si ha una cifratura banale che lascia inalterato il messaggio) a K=25, sperando di imbattersi in un messaggio di senso compiuto. Questo elementare tipo di attacco è reso possibile dal numero estremamente esiguo di chiavi; il Codice di Cesare garantisce ora, perciò, una sicurezza assai scarsa, invece al tempo di Cesare questo tipo di sistema crittografico era abbastanza sicuro, considerando che spesso i nemici non erano neanche in grado di leggere un testo in chiaro, men che mai uno cifrato e inoltre non esistevano metodi di crittanalisi in grado di rompere tale codice, per quanto banale.

Capitolo 3

Crittografia medievale e rinascimentale

Fino all'anno mille la crittograqfia fu usata quasi esclusivamente per celare nomi propri nei manoscritti; spesso per fare ciò ogni lettera dell'alfabeto veniva, sempilicemente, scambiata con la successiva, cifrando quindi seguendo il metodo di Cesare con chiave 1.
Intorno al IX secolo avviene una delle maggiori scoperte della crittoanalisi che permise di violare molto più facilmente i codici a sostituzione monoalfabetici adoperati fino a quel periodo.
Al matematico e filosofo arabo Al-Kindi viene infatti attribuito lo sviluppo di un nuovo metodo secondo il quale la frequenza dell'occorrenza delle lettere può essere analizzata ed utilizzata per rompere un codice (crittoanalisi per **analisi delle frequenze**, cfr. appendice).
In seguito all'esigenza di trovare nuovi metodi non vulnerabili all'analisi delle frequenze, nascono quindi **cifrari polialfabetici**.
I cifrari polialfabetici si differenziano dai monoalfabetici in quanto un dato carattere del testo chiaro non viene cifrato sempre con lo stesso carattere, ma con caratteri diversi in base ad una qualche regola, in genere legata ad una parola segreta da concordare.
Dei primi cifrari polialfabetici possiamo giá leggere nel"Manoscritto per la decifrazione dei messaggi crittati" scritto da Al-Kindi intorno all'800 d.C., ma il vero padre dei cifrari polialfabetici viene considerato **Leon Battista Alberti**.

Fino alla fine del XIV erano in uso quasi esclusivamente cifrari monoalfabetici tutti violabili tramite l'analisi frequenziale, nel 1495 Leon Battista Alberti nel suo *De Cifris* illustra una nuova tecnica di criptatura polialfabetica che produce un crittogramma di fronte al quale il crittanalista si trova disorientato dal continuo, erratico cambiamento di valori e non può assolutamente mettere a frutto eventuali equivalenze chiaro-cifrato già scoperte.
Per i successivi tre secoli il codice di Leon Battista Alberti costituì il basamento dei sistemi crittografici.

In Europa la crittografia assunse notevole importanza come conseguenza della competizione politica e della rivoluzione religiosa. Durante e dopo il Rinascimento, molti matematici e studiosi di diversi stati diedero vita a una rapida proliferazione di tecniche crittografiche, alcune delle quali riflettevano la conoscenza degli studi dell'Alberti sulle tecniche di sostituzione polialfabetiche.
Nel 1586 il diplomatico e crittografo francese Blaise de Vigenè

re pubblicò uno dei più semplici cifrari polialfabetici, considerato per secoli inattaccabile. Il **cifrario di Vigenère** aveva come punto di forza quello di utilizzare non uno ma 26 alfabeti per cifrare un solo messaggio, seguendo un metodo che può essere considerato una generalizzazione del codice di Cesare. Da tale metodo deriva il **cifrario di Vernam**, considerato teoricamente perfetto e che sarà approfondito nel prossimo capitolo.

3.1 Il disco di Leon Battista Alberti

Intorno al 1467 Leon Battista Alberti descrive nel suo trattato"De cifris" un nuovo metodo di cifratura polialfabetica che rappresenterà una vera svolta nella storia della crittografia occidentale.
Il nuovo metodo ha bisogno di un dispositivo meccanico, chiamato *disco cifrante*. Quest'ultimo è costituito da due dischi concentrici in rame. Il disco maggiore (disco stabile) viene suddiviso in 24 parti uguali, dette anche *Case*. Su queste vengono poi riportate le lettere dell'alfabeto in chiaro: 20 lettere in ordine alfabetico, escludendo le lettere"inutili"(H,K,Y,W) e considerando J=I e V=U e i numeri da 1 a 4.
Sulle case del cerchio interno (disco mobile) sono invece riportate tutte le 24 lette-

re dell'alfabeto (solo considerando I=J e U=V) ma in ordine sparso e un simbolo speciale end (o"et).

Figura 3.1: Disco di Leon Battista Alberti

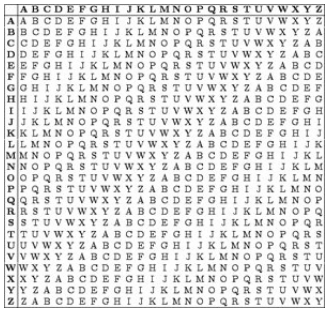
Mittente e destinatario devono essere in possesso dello stesso disco e aver concordato una chiave cifrante, costituita da una coppia di lettere che determinano la corrispondenza iniziale fra i caratteri dei due dischi. Per cifrare il messaggio, il mittente scrive il messaggio in chiaro senza spazi e inserendo a caso numeri da 1 a 4 all'interno del testo. Quindi, ad ogni lettera del messaggio in chiaro, lettera che va letta sul disco più grande, associa la lettera corrispondente nel disco più piccolo. Questo avviene fino a che non si incontra uno dei numeri: a quel punto la lettera corrispondente al numero determina una nuova disposizione: alla lettera A (la prima lettera della chiave) si fa corrispondere quella dedotta dal numero. Si considera il disco dell'Alberti una delle cifrature polialfabetiche più sicure, che non ottenne il successo meritato anche per la decisione dell'ideatore stesso di tenerla segreta (il suo trattato fu pubblicato solo un secolo più tardi a Venezia e passò quasi inosservato).

3.2 Il codice di Vigenère

Alla fine del XVI secolo il francese Vigenère propone un nuovo metodo di cifratura polialfabetica e a chiave simmetrica. Questo metodo era basato sull'idea che la debolezza del codice monoalfabetico si può superare rendendo la cifratura di un carattere dipendente dalla posizione che il carattere occupa nel testo.
La chiave, detta anche *verme*, è una stringa la cui lunghezza determina quella dei"blocchi"in cui viene diviso il testo in chiaro. Il verme viene quindi scritto ripetutamente sotto il messaggio fino a coprirne tutta la lunghezza. Ogni lettera

del messaggio va sostituita con un'altra di n-1 posizioni più avanti nell'alfabeto, dove n è il valore ordinale della lettera corrispondente nella chiave. Il cifrario di Vigenère può essere considerato un'evoluzione del codice di Cesare, infatti la cifratura consisterà nella somma modulo 26 (come per il codice di Cesare) di ogni lettera del testo in chiaro con la sottostante lettera della chiave. Si avranno quindi N cifrari di Cesare, dove N è la lunghezza della chiave.

È da notare che non c'è più una corrispondenza biunivoca fra caratteri del testo



	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

Figura 3.2: Schema per la cifratura tramite il metodo di Vigenèr

in chiaro e del crittogramma, non permettendo quindi un'analisi delle frequenze.
Per la decifrazione si procede in modo analogo ordinando ripetutamente la chiave sotto il testo cifrato, ed eseguendo la differenza modulo 26 coppia per coppia dei caratteri.
Per facilitare la cifratura Vigenère utilizzò una tavola in cui per trovare il carattere cifrato è sufficiente individuare il carattere in chiaro sulla prima riga e poi il carattere del verme sulla prima colonna. L'incrocio delle due posizioni individuerà automaticamente il carattere cifrato.

Capitolo 4

Crittografia dal 1800 alla prima guerra mondiale

Fino alla prima metà del XIX secolo la corrispondenza era esclusivamente cartacea ed era recapitata dai servizi postali. Tra la seconda metà del XIX secolo e il XX secolo, l'invenzione del telegrafo, del telefono e della radio hanno cambiato radicalmente il modo di comunicare, rendendo possibile la trasmissione di messaggi pressochè istantanea anche da luoghi molto distanti. Questi nuovi mezzi di comunicazione, la radio in particolare, rendevano però ancora più facili e frequenti le intercettazioni da parte di nemici; il ricorso alla crittografia diventa, quindi, inevitabile, come la necessità di cifrari sempre più sofisticati.

Nel 1863 il colonnello prussiano Friedrich Kasiski pubblica il primo metodo di decrittazione del cifrario di Vigenère basandosi sulla seguente osservazione: porzioni ripetute di messaggio cifrate con la stessa porzione di chiave risultano segmenti di testo cifrato identici.
In Italia la crittografia in questo periodo viene pressochè ignorata, si dovrà attendere l'entrata in Guerra nel 1915 per rendersi conto del ritardo accumulato in campo crittografico, e porvi rimedio.
In questo periodo si sviluppano anche le prime macchine cifranti che permettono di ridurre notevolmente i tempi di cifratura e decifratura trasformando automaticamente le lettere del testo chiaro in quelle del testo cifrato e viceversa. Si può considerare come primissima e rudimentale macchina cifrante il disco di Leon

Battista Alberti, ma è nella prima metà del Novecento che le macchine cifranti hanno il loro massimo sviluppo.

4.1 La crittografia nella prima Guerra Mondiale

I Francesi furono i primi a capire i grandi cambiamenti dettati dalle invenzioni del telegrafo e della radio. All'inizio della Guerra erano giá organizzati con un efficiente Ufficio Cifra e nel 1914 i crittoanalisti francesi erano in grado di decifrare i messaggi radio tedeschi. Un ulteriore passo avanti dei francesi si ebbe quando, nel 1918, il migliore crittoanalista francese, il professor Painvin, riuscì a decrittare la cifra campale germanica, metodo utilizzato dall'esercito tedesco nella Grande Guerra già dall'inizio del 1918.
Gli unici paesi organizzati con veri e propri uffici cifra allo scoppio della guerra erano Francia e Austria, quest'ultima riusciva già nel 1914 a decrittare i radiomessaggi russi.
I Russi in un primo momento non si preoccuparono nemmeno di cifrare i propri messaggi radio, permettendo così ai Tedeschi di intercettare ogni informazione e anche quando i Russi iniziarono a utilizzare messaggi cifrati, i tedeschi riuscirono a decrittarli.
I crittografi britannici si riunivano nella Stanza 40, nome della stanza dell'ammiragliato inglese sede dell'ufficio crittografico preposto alla violazione dei codici cifrati tedeschi. Da questa stanza si decrittavano migliaia di radiomessaggi della marina tedesca. Il più noto di questi fu il"telegramma Zimmermann"con il quale i Tedeschi offrivano un'alleanza ai Messicani in chiave anti-USA. Letto al Congresso degli Stati Uniti, questo messaggio fu uno dei fattori che spinsero gli USA a entrare in guerra nel 1917.
Negli USA fu adoperato come ufficio cifra il reparto crittologico dei laboratori Riverbanks di Chicago, nel quale lavorava anche William Friedmann destinato a divenire il massimo crittologo e crittanalista USA.
Del tutto impreparati in campo crittologico erano gli Italiani che dovettero in un primo tempo appoggiarsi all'ufficio cifra francese; solo in un secondo tempo fu costituito un ufficio cifra autonomo sotto la guida di Luigi Sacco.

In definitiva fu proprio la Grande Guerra a far scoprire a molti Stati l'importanza della crittografia, il cui ruolo diventerà assolutamente fondamentale nella II guerra mondiale.

4.2 Il metodo Kasiski

L'attacco alla Kasiski si basa sull'osservazione che in un crittogramma alla Vigenère si trovano spesso sequenze identiche di caratteri a una certa distanza l'una dell'altra; infatti una stessa lettera del testo in chiaro viene, generalmente, cifrata con caratteri diversi nelle sue varie occorrenze, ma se due lettere identiche si trovano a una distanza pari a quella della chiave, o a un suo multiplo, vengono cifrate allo stesso modo. Per individuare la lunghezza della chiave sarà quindi sufficiente calcolare il massimo comun divisore tra le distanze tra sequenze ripetute. Una volta trovata la lunghezza della chiave, disponendo di un numero significativo di crittogrammi, si può applicare l'analisi delle frequenze a sottoinsiemi di caratteri che occupano la medesima posizione all'interno di un blocco.
Questa tecnica viene anche chiamata *metodo Babbage-Kasiski* in quanto, già nel 1854, l'eccentrico matematico e inventore Charles Babbage aveva individuato un criterio di decifrazione del tutto analogo a quello successivamente elaborato dal Kasiski, ma mai pubblicato.

4.3 Il codice di Vernam

Il codice di Vernam è una generalizzazione del Codice di Vigenère, sviluppato tenendo conto delle debolezze del codice messe in luce da Kasiski.
Queste debolezze del codice di Vigenère si possono superare cambiando frequentemente la chiave e scegliendo chiavi molto lunghe, tali da"coprire"qualunque messaggio si prevede di trasmettere, inoltre, per rendere ancora più sicuro il metodo, le chiavi possono essere generate come sequenze di lettere, senza alcuna struttura linguisticamente significativa.
Il codice di Vernam, detto anche **Codice One Time Pad** (blocco"usa e getta), prevede l'edizione tipografica di blocchi cartacei uguali, tipo calendario a strappo, con un foglio per ogni giorno, sui quali sono stampate lunghe sequenze di

caratteri casuali. Mittente e destinatario possiedono ciascuno un blocco, da custodire segretamente in quanto il blocco riporta l'insieme delle chiavi da utilizzare giorno dopo giorno.
L'unico modo per decifrare il messaggio per l'avversario è quindi quello di impadronirsi della chiave; per questo motivo il Codice di Vernam è il primo sistema crittografico a chiave simmetrica totalmente sicuro.
Nel 1949 Claude Shannon pubblicò la prima dimostrazione matematica dell'inviolabilitá del Codice di Vernam, che, essendo l'unico sistema crittografico la cui sicurezza sia comprovata da una dimostrazione, si è guadagnato il titolo di"cifrario perfetto.
Questo schema in teoria perfetto risulta però difficilmente realizzabile. Presenta, infatti, diversi problemi pratici non facili da risolvere. Innanzi tutto una comunicazione abbastanza massiccia tramite l'uso del codice One Time Pad necessiterebbe di una chiave di dimensioni spropositate e questo aggraverebbe ancora di più il problema di come scambiarsi la chiave tra mittente e destinatario. Altro inconveniente di questo sistema è dato dal fatto che la chiave utilizzata dovrebbe essere generata in maniera totalmente casuale, cosa anche oggi praticamente impossibile, infatti i generatori di numeri casuali (ad esempio) sono in realtà detti *pseudocasuali* in quanto generano numeri con proprietà non del tutto casuali.

Capitolo 5

Macchine cifranti e crittografia nella seconda guerra mondiale

La ricerca di nuovi sistemi crittografici diede un grande impulso alla crittografia durante il periodo antecedente la Seconda Guerra Mondiale. Già dall'inizio del XX sec, infatti, stava nascendo l'esigenza di poter usufruire di una crittografia sicura e, soprattutto, veloce e facilmente utilizzabile: per questo nacquero le prime macchine cifranti.

5.1 Le macchine cifranti

Fin dalla fine del XIX sec, lo sviluppo della crittografia rese necessaria una progressiva automatizzazione dei metodi di cifratura e decifratura, le macchine cifranti nacquero quindi non tanto per rendere i sistemi crittografici più sicuri ma semmai per velocizzarli.
La prima macchina cifrante fu inventata dal comandante francese Etienne Bazières già nel 1891. Da questa prima macchina furono sviluppate molte altre che permettevano metodi di cifratura sempre più rapidi e sicuri; la più famosa di queste macchine è sicuramente **Enigma**, brevettata dall'ingegnere tedesco Arthur Scherbius nel 1918 e adottata dell'esercito e dalla marina tedesca durante la Seconda Guerra Mondiale.
Il funzionamento di queste macchine si basa sull'ultilizzo di uno o più dischi cifranti, detti anche rotori. Ogni rotore ha inciso sopra una permutazione dell'al-

fabeto a 26 lettere e gira attorno a un asse: questo permette di cifrare ogni lettera immessa con un alfabeto diverso. Le macchine cifranti possono quindi essere ritenute una versione meccanica del cifrario di Vigenère.
Il rotore rappresenta la caratteristica principale delle macchine cifranti ma, al contempo, anche il punto debole, in quanto dopo 26 rotazioni il disco torna nella posizione iniziale. Una macchina cifrante ad un rotore solo ripete il suo schema di crittografia ogni 26 lettere, avendo quindi un periodo T = 26. È possibile superare questo problema aggiungendo altri rotori, una macchina a 2 rotori, ad esempio, ha periodo 26*26=676 lettere prima che il testo venga cifrato con lo stesso schema.
Possiamo dunque dire che la sicurezza aumenta esponenzialmente con l'aumentare dei rotori e il periodo T di una macchina a n rotori è uguale a 26^n.

Nel 1915, due ufficiali della marina olandese inventarono una nuova macchina per cifrare i messaggi, destinata a diventare una delle più famose di tutti i tempi: la **macchina cifrante Enigma**. Arthur Scherbius la brevettò nel 1918 e cominciò a venderla alle banche e alle aziende. Il posto di Enigma nella storia, però, venne garantito nel 1924, quando le forze armate tedesche iniziarono ad utilizzarne una versione adattata alle esigenze militari per cifrare le loro comunicazioni. E continuarono a fare affidamento su questa macchina anche durante la seconda guerra mondiale, credendo che fosse assolutamente sicura.
Le macchine Enigma nella versione per l'esercito avevano, inizialmente, tre rotori che potevano essere estratti e cambiati. Il primo compito per un operatore di Enigma era di decidere in quale posizione andava impostato ogni singolo rotore. C'erano cinque rotori tra cui scegliere e che potevano essere inseriti nei tre alloggiamenti di Enigma.
Ogni carattere del testo in chiaro veniva digitato su una tastiera, l'*unità scambiatrice*, costituita principalmente dai rotori, cifrava la lettera trasformandola nel corrispondente elemento del crittogramma e, infine, una lampadina posta sul *pannello luminoso* (o visore), accendendendosi, indicava la lettera da inserire nel crittogramma.
La particolarità di Enigma stava nel fatto che ogni volta che una lettera veniva battuta sulla tastiera, le parti mobili della macchina ruotavano, cambiando la loro posizione in modo che una successiva pressione del tasto corrispondente alla stes-

sa lettera quasi certamente sarebbe stata cifrata in altro modo.
La macchina venne poi arricchita ulteriormente con un *pannello a prese multiple* che permetteva di"scambiare"coppie di lettere all'inizio della cifratura e un anello che regolava i tempi di rotazione dei rotori. Tutto questo rendeva impossibile la crittoanalisi tramite i metodi tradizionali di analisi frequenziale e fece sì che Enigma potesse permette un enorme numero di chiavi, ovvero di configurazioni iniziali della macchina.
L'unico modo per decifrare il crittogramma era quindi quello di possedere una macchina Enigma configurata esattamente come quella con cui si era cifrato il messaggio e batterne le lettere sulla tastiera, allora le lettere del testo in chiaro si sarebbero illuminate sul pannello.
La configurazione delle macchine tedesche veniva cambiata ogni 24 ore seguendo un determinato protocollo da tenere in totale segretezza in quanto, se gli alleati ne fossero venuti in possesso, avrebbero potuto decifrare facilmente ogni messaggio.

5.2 La crittografia nella seconda Guerra Mondiale

Fino alla prima metà degli anni venti, i crittoanalisti americani e francesi erano in grado di decifrare molto spesso i messaggi criptati dai tedeschi. Questo avvenne solo fino al 1926 quando, l'impiego massiccio da parte dei tedeschi di Enigma, mise in crisi l'intero apparato di contro-spionaggio inglese e francese. Il metodo crittografico tedesco appariva insormontabile. Solo i polacchi, che intuivano le mire espansionistiche della Germania ai loro danni, non si diedero per vinti.
Molti anni dopo la fine della guerra si seppe che, in effetti, già nel 1932 l'ufficio cifra polacco, guidato dal matematico Rejewski, era riuscito a trovare il modo di forzare la macchina Enigma.
Nell'agosto del 1939 i Britannici costituirono la scuola dei codici e dei cifrari a Bletchley Park, dove reclutarono i migliori crittoanalisti, matematici e scienziati. Sfruttando anche le conoscenze raggiunte dagli alleati polacchi, durante la guerra, gli inglesi continuarono a forzare sistematicamente i messaggi cifrati con Enigma e dal 1941 anche quelli cifrati con la più sofisticata macchina Lorenz.
La crittografia giocò quindi un ruolo di fondamentale importanza durante tutta la

Figura 5.1: Macchina cifrante Enigma

durata della guerra e, ad esempio, fu fondamentale per lo Sbarco in Normandia. Infatti Eisenhower e Montgomery erano in grado di leggere tutti i messaggi degli alti comandi tedeschi, che usavano la macchina Lorenz; ebbero così conferma che Hitler aveva creduto alla falsa notizia di un imminente sbarco alleato nei pressi di Calais, e aveva concentrato le sue migliori truppe in quella zona. Poterono quindi ordinare lo sbarco in Normandia sicuri che avrebbe incontrato ben poca resistenza.

Fin dal 1940 gli americani avevano realizzato **Magic**, una macchina in grado di decrittare i messaggi giapponesi cifrati con la **macchina Purple**. Questa consentì, ad esempio, agli americani di vincere la Battaglia delle Midway, conoscendo fin nei dettagli i piani dell'esercito nipponico. È possibile che gli americani fossero già a conoscenza anche dell'attacco di Pearl Arbour e decisero di non impedirlo, forse per convincere l'opinione pubblica della necessità dell'entrata in guerra. Una teoria più prudente sostiene che gli Americani sapevano che il Giappone stava per attaccare, ma non sapevano dove. Certo è che al momento dell'attacco nella baia di Pearl Harbour non c'era nemmeno una portaerei e, in definitiva, furono affondate solo alcune navi vecchie e di importanza non fondamentale per la guerra. Alla fine della guerra il gen. Marshall ammise che in molti casi di importanza"non vitale"gli alleati dovettero fingere di non conoscere i messaggi cifrati nemici, anche al costo di perdite umane, tale era il timore che tedeschi e giapponesi si accorgessero che i loro cifrari venivano sistematicamente decrittati.

Capitolo 6

Cenni di crittografia moderna

La crittografia moderna si differenzia notevolmente dalla crittografia di cui si è parlato fin ora; l'avvento dei computer infatti ha rivoluzionato profondamente sia i sistemi crittografici sia il modo di vedere e utilizzare la crittografia.
Molti sistemi crittografici analizzati in precedenza e considerati ragionevolmente sicuri fino al XIX sec, possono oggi essere forzati in tempi brevissimi grazie alla velocità di elaborazione del computer. Inoltre possono essere ora utilizzati sistemi crittografici molto complessi e che, un tempo, avrebbero richiesto tempi di cifratura"a mano"troppo lunghi (come il DES e l'RSA).
Nell'era dei computer la crittografia è"uscita dai campi di battaglia"e viene utilizzata da ogni persona, più o meno consapevolmente, nella vita di tutti i giorni: per prelevare soldi con un bancomat, nell'effettuare acquisti su internet o, semplicemente, chiamando con un telefono cellulare. La crittografia è quindi diventata uno strumento di massa, atto a proteggere i segreti di stato tanto quanto i dati che noi vogliamo, o almeno vorremmo, rimanessero privati.

6.1 Il codice DES: un sistema crittografico moderno a chiave simmetrica

Nell'epoca dei computer la crittografia non utilizza più l'alfabeto a 26 lettere, ma lavora con file binari basati sul codice ASCII. Il codice ASCII prevede 128 caratteri di cui solo 96 sono i cosiddetti *printable characters*; ogni carattere è codificato

con un byte, ovvero con 8 bit (cifre binarie 0,1). Il testo in chiaro viene suddiviso in blocchi, tipicamente di 8 caratteri ciascuno, scrivendo la codifica ASCII da ogni blocco si otterrà una stringa di 64 cifre.

Il codice DES (Data Encryption Standard) è stato progettato dall'IBM nel 1975, per poi essere introdotto nel 1977 come sistema ufficiale di cifratura del Governo degli USA.
Si tratta di un cifrario misto che prevede 16 trasformazioni successive (trasposizioni e sostituzioni) applicate a ogni blocco del messaggio, per mezzo di una chiave simmetrica. La chiave ha una lunghezza di 64 bit, ma 8 di questi sono di controllo. Si ha quindi un numero di chiavi possibili pari a 2^{56} sufficiente fino agli anni '70 per porre il sistema al riparo da un attacco"forza bruta"ma non più oggi con l'avvento dei calcolatori moderni. Per questo motivo il DES è stato aggiornato con il più robusto sistema crittografico AES, che costituisce oggi il modello crittografico a chiave simmetrica più diffuso.

6.2 Sistemi crittografici a chiave pubblica: il protocollo di Diffie-Hellman

Un problema di tutti i sistemi crittografici a chiave simmetrica, dai più rudimentali ai più sofisticati, è dato dalla necessità della distribuzione delle chiavi in modo sicuro tra mittenti e destinatari.
Fin dagli anni '70 si cercò di concepire un sistema crittografico che non richiedesse la condivisione delle chiavi, la cosa si dimostrò concettualmente possibile tramite il *protocollo dei due lucchetti*. Secondo questo protocollo se A vuole inviare un messaggio a B, si procederà nel seguente modo:

- A mette il messaggio in una scatola, la chiude con il suo lucchetto e la spedisce a B
- B riceve la scatola chiusa, la chiude ulteriormente con il suo lucchetto e la rispedisce a A
- A toglie il primo lucchetto e rispedisce la scatola a B che possiederà quindi la chiave dell'ultimo lucchetto

Il protocollo dei due lucchetti costituisce il primo esempio di **crittografia asimmetrica**, con l'utilizzo cioè di due lucchetti.
In questo modo è quindi possibile comunicare in sicurezza senza un preventivo scambio di chiavi tra mittente e destinatario.
Bisogna notare però che la scatola contenente il messaggio ha dovuto compiere tre viaggi invece che uno, offrendo quindi all'attaccante una maggiore possibilità di impadronirsi del messaggio. Inoltre, il protocollo dei due lucchetti, per funzionare, richiede l'utilizzo di funzioni commutative per cifratura e decifrazione.

Nel 1976 i ricercatori americani Diffie ed Hellman furono i primi a proporre un sistema crittografico a chiave pubblica, per risolvere il problema dello scambio delle chiavi.
La novità del protocollo Diffie-Hellman (DH) sta nel fatto che ogni utente ha due chiavi distinte: una pubblica e una privata. Si tratta quindi di un sistema crittografico asimmetrico in cui la **chiave pubblica** serve per la cifratura del messaggio, mentre per la decifrazione il destinatario deve utilizzare la sua **chiave privata**, che deve restare totalmente segreta.
La cifratura del messaggio (chiusura del lucchetto) dovrà essere alla portata di tutti con l'utilizzo della chiave pubblica; mentre la decifrazione (apertura del lucchetto) sarà possibile, in tempi accettabili, solo al possessore della chiave privata corretta. Solitamente il protocollo D-H viene utilizzato da mittente e destinatario solo in un primo momento per lo scambio della chiave in modo sicuro, quest'ultima potrà essere quindi impiegata per criptare le comunicazioni successive tramite uno schema di crittografia simmetrica.

L'idea si basa quindi sul concetto di *funzione unidirezionale*: esistono funzioni che sono agevoli da calcolare in una direzione ma che diventano computazionalmente pesantissime nella direzione opposta (funzione inversa). Nella Teoria dei Numeri, nell'aritmetica modulare si trovano diverse funzioni di questo tipo come ad esempio l'elevamento a potenza modulo n: $y = f(x) = (z^x) mod n$. Il calcolo di $f(x)$, data x, risulta semplice e rapido mentre la funzione inversa (**logaritmo discreto**) $x = f^{-1}(y) = (D \log_z y) mod n$ è molto più difficile da calcolare, in quanto non esiste un algoritmo efficiente.

Se Alice (A) e Bob (B) vogliono comunicare segretamente utilizzando il protocollo D-H dovranno procedere nel modo seguente:

- Alice e Bob si accordano pubblicamente su un numero primo p molto elevato e quindi su un numero g, generatore del gruppo moltiplicativo degli interi modulo p
- Alice sceglie un numero a ($1 \leq a \leq p-1$) e calcola $A = g^a mod p$ e lo invia a Bob
- Bob sceglie un numero b ($1 \leq b \leq p-1$) e calcola $B = g^b mod p$ e lo invia a Alice
- Alice calcola $K_a = B^a mod p$ e Bob calcola $K_b = A^b mod p$
- Alice e Bob potranno quindi iniziare a comunicare sfruttando la chiave segreta $K = K_a = K_b = g^{ab} mod p$

Il protocollo D-H è però vulnerabile a attacchi del tipo ”man in the middle”: un malintenzionato, infatti, avendo a disposizione le informazioni pubbliche potrebbe intromettersi e cercare di modificarle o falsificarle.

6.3 Il metodo RSA

L'RSA è il più conosciuto sistema crittografico a chiave pubblica (asimmetrica) e fu proposto dai ricercatori Rivest, Shamir e Adelman nel 1978.
Supponiamo di voler scambiare un messaggio M con un nostro conoscente utilizzando il metodo RSA.
Per prima cosa trasformiamo il messaggio M in un vettore di numeri interi $m = (m_1, ...m_k)$. Scegliamo due numeri primi casuali p e q abbastanza grandi da garantire la sicurezza dell'algoritmo e calcoliamo $n = pq$. Sappiamo (si veda capitolo 7) che: $\Phi(n) = \Phi(pq) = (p-1)(q-1)$.
Prendiamo quindi, sempre a caso, un numero e che sia primo con $\Phi(n)$. Abbiamo quindi ottenuto la chiave pubblica che sarà formata dalla coppia (n, e). La chiave segreta consisterà invece nel numero d, inverso di e modulo $\Phi(n)$: $ed \equiv 1 mod(\Phi(n))$.

Possiamo infine distruggere i numeri p, q e $\Phi(n)$.
Per criptare il messaggio ottenendo il messaggio cifrato c si calcolerà:
$c = m^e mod(n)$
Nell'operazione di cifratura sarà quindi sufficiente conoscere la chiave pubblica del destinatario, il quale per decrittare c e tornare al messaggio in chiaro procederà nel seguente modo:
$m = c^d mod(n)$
Infatti:
$c^d = (m^e)^d = m^{ed}(modn)$
ma sappiamo che $ed \equiv 1mod((p-1)(q-1))$ quindi $ed \equiv 1mod(p-1)$ e $ed \equiv 1mod(q-1)$
quindi per il Piccolo teorema di Fermat: $m^{ed} \equiv mmod(p)$ e $m^{ed} \equiv mmod(q)$
Siccome $p \neq q$ e sono numeri primi, applicando il teorema cinese del resto, otteniamo:
$m^{ed} \equiv mmod(pq)$ e perciò $c^d \equiv mmod(n)$.

Se l'avversario riuscisse a impadronirsi del crittogramma c, per calcolarlo dovrebbe saper calcolare la radice e-esima di c modulo n:
$m = \sqrt[e]{c}modn = c^{e^-1 mod \Phi(n)}modn$
La sicurezza del sistema RSA si basa sulla inesistenza di algoritmi efficienti per calcolare le radici e-esime modulo n. Oppure, equivalentemente, l'avversario potrebbe provare a fattorizzare n per poi calcolare $\Phi(n)$ ed invertire $\Phi(n)$, trovando così la chiave segreta d. Ma nemmeno per la fattorizzazione si conoscono algoritmi efficienti.
Anche ipotizzando, in futuro, computer con una potenza di calcolo molto superiore a quella odierna che favorisca i crittoanalisti, questa potenza di calcolo crescente aiuterebbe molto di più i crittografi.

Infine non bisogna ritenere che la crittografia a chiave simmetrica sia stata superata dagli algoritmi del sistema RSA, in quanto questi ultimi sono efficienti ma molto più lenti di sistemi come il DES. Come detto anche in precedenza, quindi, la moderna crittografia utilizza entrambi i due tipi di sistemi, sfruttando un sistema asimmetrico come l'RSA solamente per permettere lo scambio sicuro di una chiave simmetrica con cui vengono trattati tutti i messaggi successivi.

Capitolo 7

La matematica dietro la crittografia

Tutti i sistemi crittografici fin ora descritti, dai più antichi ai moderni metodi implementati su computer, hanno le loro radici in concetti matematici e soprattutto algebrici che verranno spiegati in quest'ultimo capitolo.
È inoltre interessante notare come nell'era dei computer è la"vecchia"Teoria dei Numeri da Euclide (IV-III sec a.C.) a Fermat, Eulero e Gauss (XVII-XIX) a fornire le basi sulle quali si sviluppa la crittografia moderna.

7.1 Gruppi

Definizione Un gruppo è una struttura algebrica formata da un insieme G e da un operazione binaria $\star$, definita sugli elementi dell'insieme e che deve godere delle seguenti proprietà:

- chiusura: $\forall a,b \in G,\ a \star b \in G$
- associativa: $\forall a,b,c \in G,\ (a \star b) \star c = a \star (b \star c)$
- elemento neutro: $\exists \varepsilon \in G$ t.c. $\forall a \in G,\ a \star \varepsilon = a = \varepsilon \star a$
- elemento inverso: $\forall a \in G,\ \exists a^{-1}\ t.c.\ a \star a^{-1} = \varepsilon.$

Definizione Un gruppo abeliano è un gruppo in cui vale anche la proprietà commutativa ($\forall a,b \in G,\ a \star b \in G$)

Definizione L'ordine di un gruppo è il numero di elementi da cui è costituito l'insieme.

Definizione Una permutazione é un modo di ordinare in successione n oggetti distinti, come nell'anagrammare una parola. In termini matematici una permutazione di un insieme X si definisce come una funzione biiettiva $p : X \to X$.

Osservazione L'insieme delle possibili permutazioni delle 26 lettere dell'alfabeto con l'operazione di composizione tra permutazioni costituiscono un gruppo particolarmente interessante in crittografia; molti cifrari si basano infatti su sostituzioni di una lettera con un altra e, cioè, su permutazioni delle lettere dell'alfabeto.

7.2 Divisibilità e numeri primi

Definizione Siano a, b due numeri interi. Si dice che a divide b ($a \mid b$) se esiste un intero q t.c $b = q \cdot a$.

Lemma di divisione Dati due interi a, b, con $a \neq 0$, esistono e sono unici due interi q, r t.c. : $b = q \cdot a + r$ con $0 \leq r < a$
(q e r sono detti rispettivamente quoziente e resto)

Definizione Dati due interi a, b non entrambi nulli, si dice massimo comune divisore il più grande intero che divide entrambi:
$D = MCD(a,b) = max\{d \ \ t.c. \ \ d \mid a \ \ e \ \ d \mid b\}$

Osservazione Il $MCD(a,b)$ è anche la più piccola combinazione lineare di a e b: $d = sa + tb$

Definizione a e b sono relativamente primi se $MCD(a,b) = 1$

Per calcolare il *MCD*, è noto fin dall'antichità l'Algoritmo Euclideo: si applica inizialmente il lemma di divisione ai dati a e b ottenendo quoziente e resto; successivamente si compie lo stesso procedimento prendendo ogni volta come nuovo dividendo il divisore precedente e come nuovo divisore il resto precedente, fino

ad ottenere resto nullo; l'ultimo resto non nullo trovato è il *MCD*.

Definizione Un numero intero p si dice primo se:

- $p \geq 2$
- i soli divisori positivi di p sono 1 e p

Definizione Un numero intero $a \geq 2$ è composto (non primo) se esistono due interi $b, c > 1$ t.c. $a = bc$

Teorema Fondamentale dell'aritmetica Unicità della scomposizione in fattori primi: Ogni numero intero $a \geq 2$ si può scrivere in modo unico come prodotto di numeri primi $a = p_1 p_2 ... p_r$

Proprietà Esistono infiniti numeri primi: Ammettiamo per assurdo che l'insieme dei numeri primi sia finito, di ordine n: $p_1, ..., p_n$. Costruiamo il numero $a = p_1 p_2 ... p_n + 1$ è primo e > 1, inoltre non è divisibile per nessuno degli n numeri primi. Allora a è primo.

Pricipio di Euclide Se un primo p divide un prodotto ab, allora $p \mid a$ o $p \mid b$.

Frequenza dei numeri primi : Osservando la successione di numeri primi, si osserva che al crescere del modulo, i numeri primi diventano sempre meno frequenti.
La funzione $\pi(N)$ conta quanti sono i numeri primi $p \leq$ di un numero intero N.
Oggi sappiamo grazie agli studi di Legendre e Gauss riguardanti la funzione $\pi(N)$ che l'intervallo tra due primi consecutivi è approssimativamete $logN$; questo risultato è molto importante per la necessità della crittografia moderna di generare grandi numeri primi.

Definizione Dato un numero a, si dice inverso di a (a^{-1}), il numero b t.c. $ab = 1$.

Definizione Un gruppo in cui tutti gli elementi non nulli sono invertibili viene detto campo.

7.3 Aritmetica modulare

Siano a, b due interi e n un intero positivo detto modulo.

Definizione a e b sono congruenti modulo n ($a \equiv b(mod n)$) se n divide $(a-b)$, ovvero se la divisione per n sia di a, sia di b dà lo stesso resto.

Fissato un modulo n la classe di equivalenza modulo n è l'insieme di tutti gli interi che hanno tutti lo stesso resto rispetto al divisore n. L'insieme delle classi di equivalenza realizza una partizione dell'insieme dei numeri interi. Si potrà quindi parlare di operazioni di addizione e moltiplicazione tra questi nuovi oggetti matematici.

Teorema di Fermat Sia p primo, a intero t.c. p non divide a.
Allora: $a^{p-1} \equiv 1(mod p)$

Teorema di Eulero Il teorema di Eulero è una generalizzazione del teorema di Fermat.
Fissato un modulo n qualunque, si determinano quanti sono gli interi positivi a minori di n relativamente primi rispetto a n. Chiamiamo $\phi(n)$ questo numero. $\phi(n)$ è detta funzione di Eulero.
Fissato ora un intero a e un modulo n, con $MCD(a,n) = 1$,
vale che: $a^{\phi(n)} \equiv 1(mod n)$.

Osservazione In aritmetica modulare si parla di inverso modulo n e si può notare che sono invertibili solo i numeri relativamente primi rispetto a n.
Se il modulo è un numero primo p allora qualunque numero a t.c. $a(mod p) \neq 0$ é invertibile modulo p. L'insieme delle classi di equivalenza modulo p formano quindi un campo.

7.4 Criteri di primalità

Una delle necessità maggiori della crittografia moderna è la generazione di numeri primi. Esistono vari metodi di generazione elaborati dall'antichità ai giorni

nostri.

Crivello di Eratostene Il metodo più antico per la generazione di numeri primi era stato inventato da Eratostene già nel III sec a.C..
Si scrivono in una tabella tutti i numeri interi da 2 a N, quindi si "setacciano" eliminando tutti i multipli dei numeri rimanenti procendendo in ordine crescente fino a che l'ultimo numero considerato risulta $\leq \sqrt{N}$. I numeri "superstiti" saranno i numeri primi cercati.

Nella crittografia moderna metodi come quello di Eratostene non possono essere utilizzati efficacementente, in quanto le complessitá computazionali richieste (tempo di calcolo, memoria) eccedono quelle ragionevolmente disponibili.

I nuovi metodi seguono la seguente strategia:

- si sceglie un possibile candidato N
- si esegue un test di primalità su N: se il test riesce, N è il numero primo cercato, se fallisce, si modifica N e si ripete il test

Test di primalità **deterministici**:

- Criterio di Wilson
  p è primo se e solo se $(p-1)! \equiv -1(mod\, p)$

- Criterio di Fermat
  p è primo se $a^{p-1} \equiv 1(mod\, p)$ per ogni intero $a = 1, 2, ...p-1$

Anche questi criteri però richiedono costi computazionali troppo elevati, che li rendono difficilmente utilizzabili.
Per questo motivo il test di primalità più utilizzato è il Criterio di Miller Rabin di tipo **probabilistico**.
Sia N il numero da testare:

- si genera un numero casuale a, $2 \leq a \leq N-1$

- calcolo $d = MCD(a,N)$
- se $d > 1$, N non è primo: test fallito prematuramente, si cerca un altro N
- se d=1:
  1. scriviamo $N-1 = 2^s \cdot t$ con $s \geq 1$, t dispari
  2. se $a^t modN = 1 \rightarrow N$supera il test
  3. oppure, detto $e = 2^r \cdot t$, se $a^e \equiv -1(modN)$ per qualche $r = 0,1...s-1 \rightarrow N$ supera il test

Si può dimostrare che la possibilità che N non sia primo ma superi ugualmente il test di Miller Rabin, è al massimo del 1/4. Se allora eseguiamo il test consecutivamente su k basi random diverse $a_1, a_2, ..., a_k$, e questo risulta superato tutte le volte, allora la probabilità di una falsa conclusione è inferiore a $(1/4)^k$.

Capitolo 8

Conclusioni

8.1 La crittografia come matematica applicata

Come si è potuto osservare l'impiego della matematica nella crittografia ha avuto un forte impulso durante la Seconda Guerra Mondiale e, ulteriormente, con l'inizio dell'era dell'informatica, intorno agli anni '70-'80 del secolo scorso.
Infatti, fino all'avvento delle prime macchine cifranti, la matematica utilizzata in crittografia si limitava praticamente solo alle basi dell'aritmetica modulare e ad alcuni metodi di analisi statistica atti a facilitare la decifrazione.
Nel 1940 il famoso matematico Godfrey H. Hardy scriveva in un suo saggio: $\ll$La vera matematica non ha alcun effetto sulla guerra. Nessuno ha ancora scoperto un uso bellico della teoria dei numeri o della relatività, e sembra molto improbabile che se ne scopra uno ancora per molti anni.$\gg$. Ottimo matematico, Hardy, ma pessimo profeta. Infatti solo cinque anni più tardi il mondo potè vedere l'orribile smentita della sua affermazione sugli usi bellici della relatività, sotto forma di bomba atomica. Per quanto riguarda l'altro suo esempio, la teoria dei numeri, era considerata, giustamente, nel 1940 un un settore della matematica di grandissima bellezza e valore intrinseco, ma di nessuna utilità esterna alla matematica stessa. Oggi però sappiamo che questa disciplina è alla base di ogni moderno sistema crittografico ed è quindi anche ampiamente sfruttata in campo militare. Il campo di ricerca di Hardy era, guarda caso, proprio la teoria dei numeri, e parte del suo lavoro si è rivelata di utilità pratica proprio nella crittografia.
In questa tesi ho cercato di presentare la crittografia come esempio di matemati-

ca applicata che, anche se spesso inconsapevolmente, utilizziamo tutti quotidianamente. Lo studio della sua storia e della sua evoluzione, inoltre, permette di capire l'importanza che ha avuto nei secoli passati e, in particolare, quanto le intense lotte tra crittografi e crittoanalisti abbiano stimolato la ricerca matematica e tecnologica.
La matematica come scienza pura ha una sua ragion d'essere autonoma dalla matematica applicata. Non si può però negare che gli sviluppi applicativi hanno contribuito molto al progresso teorico, fornendo stimoli per ricerche innovative. La crittografia, in particolare negli ultimi decenni, ha costituito una importante sfida intellettuale per molti ricercatori. Questa componente di sfida deriva dalla necessità continua, della crittografia, di trovare nuovi sistemi che garantiscano sempre una maggiore sicurezza e, al contempo, dalla consapevolezza del fatto che questi, per quanto sicuri siano, potranno sempre essere messi in crisi anche dall'evoluzione delle macchine, sempre più potenti nel portare attacchi del tipo"forza bruta.
Al giorno d'oggi inoltre la crittografia è divenuta anche un prodotto commerciale. Per questo motivo i tempi della matematica e quelli della crittografia, sono parecchio diversi. Da un lato, un matematico scrive poco, e solo quando è sicuro di quello che dice. Mentre dall'altro le ifluenze dell'informatica e del commercio sulla crittografia hanno portato a una diminuzione dei tempi di ricerca, portando a scrivere di più in meno tempo e con conseguente minore controllo su quello che si scrive.

8.2 Crittografia e open source

L'informatica e in particolare lo sviluppo del web ha, negli ultimi anni, sollevato una nuova disputa dividendo i crittoanalisti tra favorevoli e contrari all'open source. Esistono, infatti, due visioni diametralmente opposte su come garantire la sicurezza di un sistema crittografico. La contrapposizione è tra chi sostiene che tenere segreto il funzionamento interno di un sistema lo renda più sicuro (sicurezza tramite segretezza) e chi invece afferma che la sicurezza debba essere affidata esclusivamente alla conoscenza della chiave, dando quindi per scontato

che il"nemico"sia a conoscenza delle specifiche del cifrario.
Quest'ultima filosofia è alla base dell'open source e si fonda sulla **legge di Kerkhoffs**:
≪In un sistema crittografico è importante tener segreta la chiave, non l'algoritmo di crittazione.≫
Seguendo questa linea di pensiero, la sfida della crittografia è proprio questa: rendere noti i particolari tecnici, i codici sorgenti, ma essere sicuri che nessuno riuscirà a violarli, almeno in tempi utili. Tutti i sistemi descritti in questa tesi basano infatti la loro sicurezza sulla segretezza della chiave inoltre andando ad analizzare i moderni sistemi si osserva che la sicurezza è affidata alla matematica, in particolare allo studio di funzioni unidirezionali. La matematica però, in quanto scienza pura, non sempre si adatta perfettamente alla realtà e in tutti i casi viene applicata da persone, che possono sbagliare. Ricordando le parole del crittografo e saggista americano Bruce Schneier: *≪è di gran lunga più facile trovare punti deboli nelle persone che non trovarli nei sistemi crittografici≫*. Schneier è un convinto sostenitore dell'open source in quanto ritiene che la crittografia come scienza può esssere considerata sicura ma i sistemi crittografici, in quanto applicazioni dell'uomo, hanno i loro problemi. Grazie alla vasta collaborazione della comunità, però, le falle possono venir scoperte più facilmente e altrettanto rapidamente corrette, con il risultato di rendere intrinsecamente più sicuro il sistema.

8.3 Crittografia e didattica

Infine vorrei sottolineare come la crittografia possa essere un utile strumento didattico per invogliare gli studenti ad avvicinarsi a una disciplina come la matematica, spesso considerata arida, difficile e distante dai problemi quotidiani.
La crittografia, come esempio di matematica applicata nella tecnologia, può essere ultilizzata come catalizzatore dell'attenzione degli studenti, per facilitare l'apprendimento di alcuni aspetti elementari di teoria dei numeri. Come ho già osservato in questa tesi, la necessità di scambiarsi informazioni segrete è sempre stata una necessità dell'uomo e sicuramente continuerà ad esserlo anche in futuro. La storia della crittografia permette proprio di capire come i metodi si siano evoluti nei secoli e di come questa evoluzione sia stata il frutto di una lotta serrata tra crit-

tografi e crittoanalisti di ogni epoca. Questa sfida continua ancora oggi sfruttando conscenze matematiche sempre più avanzate, intrecciandosi sempre di più con le nuove tecnologie e il mondo dell'informatica.
Anche se i nuovi orizzonti della crittografia richiedono conoscenze matematiche e informatiche molto approfondite, la crittografia analizzata in questa tesi e la matematica utilizzata in essa possono essere comprese anche da studenti delle scuole superiori. Lo scopo è proprio quello di dare agli studenti, alle prese con le prime nozioni di algebra e teoria dei numeri, un riscontro abbastanza immediato di come la matematica abbia applicazioni pratiche di grande utilità nel mondo tecnologico: vi è una spendibilità culturale della matematica, aspetto, questo, che purtroppo spesso viene trascurato.
Inoltre il fascino del "mistero"presente nella crittografia e nella sua storia, funge facilmente da stimolo per l'intaresse dello studente.
A coloro che considerano la matematica"inutile"la crittografia mostra come, invece, essa sia del tutto indispensabile connettersi con un computer, fare una telefonata con il cellulare o prelevare soldi al bancomat.

Infine, il bello della matematica è che ci si può anche giocare. Presentare alcuni sistemi crittografici come enigmi, rompicapi da risolvere permette ancora una volta di avvicinare lo studente al vero fascino della matematica e aiuta ad assumere un modo di ragionare che poi sarà utile anche nello studio della matematica più avanzata. Una punta di malizia, un tocco di logica e una manciata di perseveranza, infatti, costituiscono la migliore ricetta per affrontare un gioco matematico.
Concludo citando il celebre matematico statunitense Martin Gardner:

≪I giochi matematici sono un veicolo quanto mai utile per diffondere la bellezza e l'utilità della matematica e per far capire che bellezza e utilità vanno ben al di là dei confini delle aule scolastiche.≫

Appendice A

Nozioni di Crittografia

Questa appendice ha lo scopo di approfondire alcuni concetti generali di crittografia, già descritti nello svolgimento della tesi.

A.1 Sistemi crittografici a chiave simmetrica

Un sistema crittografico che usa la stessa chiave sia per cifrare sia per decifrare si dice **sistema a chiave simmetrica**.
La Scitala lacedemonica e il codice di Cesare sono perciò esempi di cifratura a chiave simmetrica.
Schema di un sistema crittografico a chiave simmetrica:

- **m** :“plain text”che Chiara vuole fare pervenire a Luca
- **K** : chiave segreta
- **E** : funzione di cifratura eseguita da Chiara
- **c=E(m,K)** :“cyper text”(crittogramma)
- **D** : funzione di decifrazione eseguita da Luca
- **D(c,K)=m** : recupero del messaggio in chiaro

A.2 Codici monoalfabetici

Nei sistemi crittografici monoalfabetici lettere uguali del messaggio in chiaro vengono cifrate con lettere uguali nel crittogramma. Lo schema generale di cifratura-decifrazione di un codice monoalfabetico è perciò rappresentato da una matrice quadrata NxN, con N=numero di lettere dell'alfabeto considerato. La chiave del sistema è costituita dalla tavola stessa delle corrispondenze, ed essendo difficile da memorizzare, deve essere conservata come documento cartaceo, con maggiori rischi di trafugamento.
Il codice di Cesare e il Codice Atabash sono esempi di codici monoalfabetici molto semplici.

Una implementazione interessante è quella del **Codice monoalfabetico affine**, nel quale le funzioni di cifratura e decifrazione sono costituite da trasformazioni lineari. In questo codice la chiave (sempre simmetrica) è costituita da una coppia di numeri interi: $K = (f,t)$ con:

- $0 < f < 26$: fattore moltiplicativo invertibile modulo 26
- $0 \leq t < 26$: offset di traslazione

Ciò significa che f deve essere relativamente primo rispetto a 26. Allora esistono 12 scelte possibili per f: $f \in 1,3,5,7,9,11,15,17,19,21,23,25$.
La funzione di cifratura si scrive: $c = E(m,K) = (m * f + t) mod 26$
Quella di decifrazione: $m = [f^{-1}(c-t)] mod 26$

Nell'**attaccare un codice monoalfabetico** decifrare un singolo messaggio significa sostanzialmente aver in mano la chiave del sistema e quindi avere anche la possibilità, per l'avversario, di giocare un ruolo attivo immettendo dei messaggi depistanti nel canale.
Un codice di Cesare (**traslazione**) è facilissimo da violare in quanto lo spazio delle chiavi è molto ridotto mentre il codice monoalfabetico affine (**trasformazione lineare**) è un po' più resistente in quanto lo spazio delle chiavi ha ordine 12x26-1=311 (12 possibili f, 26 possibili t, meno la cifratura banale f=1, t=0). Infine lo spazio delle chiavi di un sistema monoalfabetico generalizzato (**permutazione**) ha ordine 26! (circa $4x10^{26}$ che renderà impraticabile un attacco"forza bruta.

A.3 Analisi delle frequenze

I codici monoalfabetici hanno un grave difetto: lo stesso carattere del messaggio in chiaro viene cifrato sempre nello stesso modo. In ogni lingua è possibile studiare la frequenza con cui si presenta una determinato carattere in un testo, ad esempio nell'italiano le lettere"a" ed"e" sono le più frequenti e perciò, nel crittogramma, le corrispondenti cifrature appariranno con la medesima frequenza. L'analisi delle frequenze rappresenta quindi l'efficace grimaldello per violare un codice monoalfabetico, a condizione di essere in possesso di un testo cifrato abbastanza lungo.

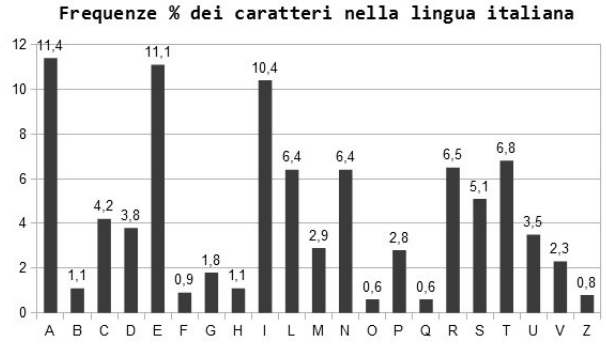


Figura A.1: Grafico frequenze

A.4 Codici polialfabetici

I cifrari polialfabetici si differenziano dai monoalfabetici in quanto ogni occorrenza di un carattere nel messaggio in chiaro può essere sostituita con diverse lettere nel crittogramma. In questo modo la sicurezza del codice dovrebbe aumentare in modo significativo, non è infatti più così semplice individuare le lettere del messaggio in base alla loro frequenza caratteristica in ogni lingua.
Per decifrare un testo cifrato con un codice polialfabetico è necessario, in un primo momento, individuare la lunghezza della chiave. Quindi è sufficiente suddividere il testo in N colonne dove N rappresenta la lunghezza della chiave e applicare l'analisi delle frequenze a ogni colonna, in quanto le lettere appartenenti a una stessa

colonna sono cifrate allo stesso modo.
Con testi sufficientemente lunghi e chiavi abbastanza corte la difficoltà di crittoanalizzare un testo cifrato con più alfabeti, non è quindi di molto superiore a quella che si aveva con il cifrario di Cesare.

A.5 Il funzionamento di Enigma

La prima versione della macchina Enigma, risalente al 1918, possedeva un solo *rotore*. Quest'ultimo ruotava di un ventiseiesimo di giro dopo la cifratura di ogni lettera, permettendo quindi una cifratura polialfabetica.
In questo modo però il meccanismo presentava il problema della ripetizione (a una distanza di 26 caratteri le lettere vengono cifrate con medesimo alfabeto), per superare questo inconveniente vennero introdotti un secondo e un terzo rotore. Il secondo compiva una rotazione parziale soltanto dopo che il primo aveva compiuto un intero giro e allo stesso modo faceva il terzo basandosi sul secondo.
Venne inoltre inserito un altro disco non ruotante e in cui i fili che vi entravano, riemergevano dalla stessa parte, chiamato *riflettore*.
La configurazione dei rotori con cui iniziava la cifratura giornaliera costituiva una vera e propria chiave e l'insieme di tali chiavi veniva distribuito agli operatori mensilmente e in totale segretezza.
Una macchina di questo tipo ammetteva quindi 26^3 chiavi possibili; per aumentarne ancora la sicurezza i rotori divennero rimovibili e ogni mattina l'operatore aveva il compito di scegliere i tre rotori da utilizzare tra 5 rotori possibili (ci sono quindi $5x4x3 = 60$ modi per posizionare i 5 rotori nei 3 alloggiamenti). Infine fu aggiunta un'altra sezione detta *pannello dei collegamenti* che permetteva di collegare tramite 10 cavi, 10 coppie di lettere e scambiarle prima della cifratura. In questo modo il numero di chiavi possibili diventò enorme e i tedeschi iniziarono a considerare, a torto, la macchina Enigma inattaccabile.

Inconsapevolmente, però, gli stessi tedeschi aiutarono i britannici a decifrare Enigma. Alcune disattenzioni quotidiane, infatti, permisero ai crittoanalisti di Bletchley Park di raccogliere degli indizi (*cribs*) su quale fosse la chiave utilizzata. Ad esempio:

- I messaggi spesso presentavano lo stesso testo di apertura, molti cominciavano con la parola *Spruchnummer* (messaggio numero) e molti messaggi dell'aeronautica con la frase *An die Gruppe* (al gruppo)
- I messaggi spesso terminavano con *Heil Hitler!*
- I messaggi spesso contenevano frasi di routine come *Kienebesondere Ereignisse* (niente da segnalare)

Questi crib insieme a nuove procedure e algoritmi per la determinazione della messa a punto di Enigma, e anche a dispositivi di calcolo elettronico sviluppati al Bletchley Park per implementare questi metodi, permisero ai crittoanalisti britannici di decifrare la macchina Enigma e li aiutarono a porre fine alla guerra.

Bibliografia

[1] David Kahn. *The Codebreakers - The Story of Secret Writing* (1976)

[2] Simon Singht. *Codici e Segreti* (1999)

[3] Keith Devlin. *Dove va la matematica* (1994)

[4] Marcus Du Sautoy. *L'enigma dei numeri primi* (2004)

[5] *Dispense: Laboratorio"Numeri primi e crittografia"*

[6] Andrea Centomo, Enrico Gregorio, FrancescaMantese *Crittografia* http://www.webalice.it/andrea.centomo/crittografia_per_studenti.pdf

[7] Giovanni Cutolo. *Matematica e crittografia* http://www.dma.unina.it/cutolo/critto.pdf

[8] Alfredo de Santis *Crittografia classica* http://www.dia.unisa.it/~ads/corso-security/www/CORSO-9900/crittografiaclassica/index.htm

[9] Marco Triverio. *Crittografia: aspetti storici e matematici* http://www.scribd.com/doc/24546830/Crittografia-aspetti-storici-e-matematici

[10] Simone Zuccher. *Tra codici, cifratura e crittografia: il ruolo della matematica nell'arte di nascondere messaggi* http://ebookbrowse.com/zuccher-medi-crittografia-pdf-d56254816

[11] Marco Evangelista, Valentina Testa, Maura Tuzzolo. *Numeri primi e crittografia* http://www.mat.uniroma2.it/pls/corsop/elaborati/crittografia.pdf

[12] *La genesi della crittografia* http://www.rcvr.org/varie/pgp/storia.htm

[13] *Storia della crittografia e delle macchine cifranti* http://www.danielepalladino.it/downloads/uni/slide_storia.della.crittografia.pdf

[14] *La crittografia da Atbash a RSA* http://critto.liceofoscarini.it/index.html

[15] Gabriella Mundo. *Breve storia della crittografia* http://people.na.infn.it/~murano/Abilitanti/Mundo-Crittografia.pdf

[16] *La crittografia* http://www.introni.it/crittografia.html

[17] Franco Eugeni, Raffaele Mascella. *Leon Battista Alberti, crittografia e crittoanalisi* http://www.apav.it/master/alberticritt.pdf

[18] Stefano Cappellini. *La crittografia da Atbash a RSA* http://critto.liceofoscarini.it/index.html

[19] Emanuele Salvador. *Appunti di crittografia, una introduzione all'algebra moderna* http://www2.dm.unito.it/paginepersonali/roggero/Crittografia.pdf

[20] *Storia della crittografia* http://it.wikipedia.org/wiki/Storia_della_crittografia

[21] Bernhelm Boob-Bavnbek. *Matematica e guerra* http://matematica-old.unibocconi.it/matematica-guerra/home.htm

[22] Davide Guidetti. *Codici e Segreti* http://www.cicap.org/new/articolo.php$?$id=101691

[23] Enrico Zimuel. *Riflessioni sulla crittografia open source* http://www.isacaroma.it/html/newsletter/node/71

[24] *Crittografia* http://it.wikipedia.org/wiki/Crittografia

[25] Carlo Toffalori. *Numeri e crittografia* http://www.unicam.it/matinf/pls/Filenuovi/Numeri_e_Crittografia_Docenti.pdf

[26] Claire Ellis. *Exploring the Enigma* http://plus.maths.org/content/os/issue34/features/ellis/index

[27] Alfonso Zecca. *Enigma* http://www.dia.unisa.it/~ads/corso-security/www/CORSO-0203/Enigma.pdf

[28] Andrea Susa. *Crittografia Moderna* http://www.capponcino.it/alessio/files/universita/crittografia_moderna.pdf

[29] *Diffie-Hellman* http://www.linux.it/~davide/doc/tesi_html/node54.html

[30] Neal Koblitz. *The Uneasy Relationship Between Mathematics and Cryptography* http://www.ams.org/notices/200708/tx070800972p.pdf