UNIVERSITÀ DEGLI STUDI DI TRENTO

Dipartimento di Matematica

Corso di Laurea in Matematica

ELABORATO FINALE

SUL GRUPPO GENERATO DAL CRITTOSISTEMA PGM

Relatore:
Professor
Andrea Caranti

Candidato:
Paolo Piasenti
Matr. 178638

Anno Accademico 2017/2018

Ai miei genitori,
a mio fratello Stefano
e a Chiara

Se l'uomo non sapesse di matematica
non si eleverebbe di un sol palmo da terra

Galileo Galilei

Indice

Prefazione

Fine e *inizio*. Questo elaborato nasce come ponte di collegamento tra due cammini, come spiaggia d'approdo di un percorso triennale in Matematica orientato perlopiù verso l'Algebra e al contempo come molo d'imbarco in direzione Crittografia.

Come giovane matematico in procinto di conseguire il titolo di laurea breve, i miei intenti nella battitura di questo testo sono quelli di vedere applicate in un mio personale approfondimento le più importanti – e più affascinanti – nozioni algebriche imparate durante questi anni di alfabetizzazione, nell'ottica di intraprendere il Corso di Laurea Magistrale curriculum *Cryptography* offerto dall'Università degli Studi di Trento.

Fulcro dell'intera dissertazione è senza dubbio il corso di Teoria dei Gruppi tenuto dal Professor Caranti e frequentato dal sottoscritto durante il primo semestre dell'anno accademico 2017/2018.

L'argomento trattato in questa tesi è il sistema crittografico PGM (*Permutation Group Mappings*), ideato nei tardi anni '70 dal matematico greco (naturalizzato statunitense) Spyros Simos Magliveras e il cui funzionamento è imperniato sul concetto di gruppo di permutazioni. Nel corso degli anni, diversi sono stati i professori e i crittografi che si sono occupati di studiarne le buone proprietà e che, come molto spesso accade in matematica, si sono domandati se alcuni risultati o proprietà sussistessero sotto condizioni più deboli e generali.

Ad un'introduzione alla teoria coinvolta e al funzionamento stesso del PGM farà proprio seguito un teorema concernente la sicurezza e la chiusura del crittosistema, dimostrato dallo stesso Professor Caranti e da una sua collaboratrice, la Professoressa Dalla Volta.

Il primo capitolo è dedicato a definizioni, richiami e risultati di Teoria dei Gruppi e di Crittografia, per fissare le idee circa il dominio della trattazione. Segue poi un secondo capitolo sul PGM: dopo la sua definizione e il suo funzionamento è presentato un esempio di situazione concreta con le due fasi di cifratura e decifrazione. Il lavoro si chiude con un terzo capitolo in cui, dopo alcune premesse di inquadramento, viene enunciato e dimostrato il teorema risolutivo della teoria esposta che generalizza il Teorema di Magliveras - Memon, e in cui si discute circa le sue implicazioni sulla sicurezza e l'efficacia stessa del PGM.

Capitolo 1

Nozioni preliminari

Presentiamo dapprima alcune definizioni e risultati importanti di Teoria dei Gruppi e di Crittografia di base; questi concetti costituiranno un prerequisito essenziale per poter costruire la complessa architettura del PGM.

1.1 Gruppi di permutazioni

Definizione 1.1. Un *gruppo* è un insieme non vuoto G munito di un'operazione binaria interna $* : G \times G \to G$ che ad ogni coppia di elementi $a, b \in G$ associa un elemento di G che indichiamo con $a * b$ tale che siano soddisfatti i seguenti assiomi:

1. *proprietà associativa*: $\forall\, a, b, c \in G$ vale che $(a * b) * c = a * (b * c)$;
2. *esistenza dell'elemento neutro*: $\exists\, 1 \in G$ tale che $\forall\, a \in G$ vale $a * 1 = 1 * a = a$;
3. *esistenza dell'inverso*: $\forall\, a \in G\ \exists\, a' \in G$ tale che $a * a' = a' * a = 1$; tale elemento è detto *inverso* di a ed è denotato con a^{-1}.

Se poi in G vale la *proprietà commutativa* per cui $\forall\, a, b \in G$ si ha che $a * b = b * a$ allora il gruppo è detto *abeliano* (o *commutativo*).

Definizione 1.2. Dato un gruppo G, un suo *sottogruppo* è un suo sottoinsieme non vuoto H che sia ancora un gruppo rispetto alla stessa operazione $*$ di G. In altre parole vale che:

1. $1 \in H$;
2. se $a \in H$ allora $a^{-1} \in H$;
3. se $a, b \in H$ allora $a * b \in H$.

In simboli, si scrive $H \leq G$ per dire che H è un sottogruppo di G.

Definizione 1.3. Sia G un gruppo. L'*ordine* di G è definito come la sua cardinalità $|G|$. G è detto *finito* se ha ordine finito, *infinito* altrimenti.

Definizione 1.4. Siano dati $(G, *)$ e $(G', \circ)$ due gruppi. Una funzione $f : G \to G'$ è detta *omomorfismo* (talvolta *morfismo*) *di gruppi* se vale che $f(a * b) = f(a) \circ f(b)$ per ogni $a, b \in G$. Un omomorfismo biiettivo è detto *isomorfismo*.

Dato un sottogruppo H di un gruppo G, possiamo definire su G una relazione mediante

$$a \sim b \iff ab^{-1} \in H$$

ed è immediato verificare che tale relazione è di equivalenza e che le sue classi di equivalenza, per $a \in G$, sono

$$[a]_\sim = \{ha : h \in H\} =: Ha$$

Quest'ultima riga costituisce la definizione di *classe laterale sinistra di H in G di rappresentante a*. In modo speculare si definiscono le classi laterali *destre*, indicate con aH per $a \in G$. Fissato un sottogruppo $H \leq G$ le classi laterali sinistre formano, in quanto classi di equivalenza, una partizione di G. Il numero di classi che formano la partizione è detto *indice* di H in G e denotato con $[G : H]$.

Il prossimo teorema mette in relazione gli indici di una catena di tre sottogruppi e ricorda la cosiddetta Formula dei Gradi per le estensioni di campi.

Teorema 1.5 (Formula degli Indici)**.** *Sia G un gruppo e H, K sottogruppi di G tali che $K \leq H \leq G$. Se $[G : K]$ è finito allora anche $[G : H]$ e $[H : K]$ lo sono. Se $[G : H]$ e $[H : K]$ sono finiti allora anche $[G : K]$ lo è e vale la formula*

$$[G : K] = [G : H] \cdot [H : K]$$

Dimostrazione. Per la prima parte, è chiaro che le classi laterali di K in H sono un sottoinsieme delle classi laterali di K in G e si verifica facilmente che la funzione $Kg \mapsto Hg$ è ben definita e suriettiva. Dunque se il numero $[G : K]$ di classi laterali di K in G è finito lo sono necessariamente anche il numero $[G : H]$ di classi laterali di H in G e il numero $[H : K]$ di classi laterali di K in H.

Per dimostrare la seconda parte, cominciamo col definire un *trasversale* di K in G come un sistema completo di rappresentanti per le classi laterali di K in G, cioè un insieme che consiste di un elemento per ogni classe laterale, e in modo analogo per gli altri casi. Siano dunque $T(H : K)$ e $T(G : H)$ trasversali per le varie classi laterali. Si afferma che gli elementi di

$$T(H : K) \cdot T(G : H)$$

sono distinti e formano un trasversale $T(G : K)$ di K in G. Questo proverà banalmente il risultato annunciato. La dimostrazione è analoga a quella della Formula dei Gradi per le estensioni di campi. Siano $x, x' \in T(G : H)$ e $y, y' \in T(H : K)$. Teniamo a mente che, per definizione di trasversale, $H \cdot T(G : H) = G$ in modo unico. Se $yx = y'x'$ allora $Hx = Hyx = Hy'x' =$

Hx' dunque $x = x'$ da cui anche $y = y'$. Sia ora Kg una classe laterale di K in G. Allora $Hg = Hx$ per un unico $x \in T(G : H)$. Dunque $gx^{-1} \in H$, e quindi $Kgx^{-1} = Ky$ per un unico $y \in T(H : K)$, da cui in definitiva segue $Kg = Kyx$. □

La semplice proprietà per cui tutte le classi laterali di H in G hanno la stessa cardinalità di H permette di dimostrare il seguente teorema.

Teorema 1.6 (Lagrange)**.** *Sia G un gruppo finito e H un suo sottogruppo. Allora vale $|G| = [G : H] \cdot |H|$ e l'ordine di H divide l'ordine di G.*

Di fondamentale importanza nella Teoria dei Gruppi è il concetto di sottogruppo normale.

Definizione 1.7. Sia G un gruppo. Un sottogruppo N di G si dice *normale* (e si indica con $N \trianglelefteq G$) se soddisfa una delle seguenti quattro proprietà equivalenti:

1. $\forall\, a \in G$ si ha che $aN = Na$;
2. $\forall\, a \in G$ si ha che $a^{-1}Na \subseteq N$;
3. $\forall\, a \in G$ si ha che $a^{-1}Na = N$;
4. $\forall\, a \in G$, $\forall\, n \in N$ si ha che $a^{-1}na \in N$.

La dimostrazione dell'effettiva equivalenza delle proprietà è un classico esercizio di applicazione delle definizioni ed è dunque lasciata al lettore. Dalla definizione appena data risulta ovvio che tutti i sottogruppi di un gruppo abeliano sono normali. Esistono però controesempi che mostrano che il viceversa è falso in generale: da qui il senso della prossima definizione.

Definizione 1.8. Sia G un gruppo non abeliano. Esso è detto *hamiltoniano* se ogni suo sottogruppo è normale.

Se abbiamo un gruppo G e un suo sottogruppo normale N, è triviale dimostrare che l'insieme delle classi laterali di N in G, denotato con $G/N := \{Ng : g \in G\}$ è in realtà un gruppo, detto *gruppo quoziente*, con l'operazione $Na \cdot Nb = N(ab)$. Il punto cruciale è che se N è normale, allora tale operazione è ben definita.

Teorema 1.9 (Primo Teorema di Isomorfismo per Gruppi)**.** *Siano G e H gruppi e $f : G \to H$ un omomorfismo di gruppi suriettivo. Consideriamo il nucleo di f ovvero $ker(f) := \{x \in G : f(x) = 1\} = K$. Allora esso è un sottogruppo normale di G. Considerato il gruppo quoziente G/K, si ha che la proiezione al quoziente $\pi : G \to G/K$ tale che $\pi(g) = Kg$ è un morfismo di gruppi; inoltre esiste ed è unica la funzione $g : G/K \to H$ tale che $f = g \circ \pi$ e tale g è un isomorfismo di gruppi.*

Definizione 1.10. Sia G un gruppo e S un suo sottoinsieme non vuoto. Si dice *sottogruppo di G generato da S* e si indica con $\langle S \rangle$ il più piccolo sottogruppo di G che contenga S.

Naturalmente dalla definizione non segue l'esistenza, ma si vede in effetti che $\langle S \rangle$ esiste sempre ed è uguale all'intersezione di tutti i sottogruppi di G contenenti S:

$$\langle S \rangle = \bigcap \{H \leq G : S \subseteq H\}$$

Un caso particolare si ha scegliendo $S = \{g\}$. In questo caso, il gruppo $C = \langle \{g\} \rangle = \langle g \rangle$ è detto *gruppo ciclico di generatore g* ed è facile vedere che $C = \{g^i : i \in \mathbb{Z}\}$ ove g^i sono le potenze del generatore, usando la notazione moltiplicativa. Se G è finito, anche $\langle g \rangle$ lo sarà. Esiste quindi $n := min\{i > 0 : g^i = 1\}$, che è detto *ordine* (o *periodo*) dell'elemento $g \in G$. Non è un caso l'uso di questo termine: in effetti si vede che $|\langle g \rangle| = n$, ossia che il sottogruppo ciclico di G generato da g ha ordine n, che è appunto l'ordine di g.

Teorema 1.11 (Cauchy)**.** *Sia G un gruppo finito e p un primo che divide l'ordine di G. Allora $\exists\, g \in G$ di ordine p e G possiede un sottogruppo di ordine p.*

Tra tutti i gruppi, siamo interessati a studiare i gruppi di permutazioni.

Definizione 1.12. Sia X un insieme. Una *permutazione* su X è una funzione biiettiva $p : X \to X$. L'insieme delle permutazioni su X è indicato con $\mathscr{S}_X$.

Vale la seguente, la cui dimostrazione è banale e dunque omessa.

Proposizione 1.13. *Sia X un insieme non vuoto. Allora l'insieme $\mathscr{S}_X$ delle funzioni biiettive (permutazioni) su X forma un gruppo rispetto alla composizione fra funzioni, con elemento neutro l'identità.*

Nel caso in cui X sia un insieme finito non vuoto, diciamo di cardinalità $n \in \mathbb{N}^*$, senza perdita di generalità (a meno di funzioni biunivoche) possiamo pensare che esso sia $X = \{1, 2, \ldots, n-1, n\}$. In questo caso, il gruppo G delle permutazioni di X è detto *gruppo simmetrico su n lettere* e viene denotato con $\mathscr{S}_n$.

É facile mostrare che ogni permutazione di $\mathscr{S}_n$ può essere scritta come composizione di un numero finito di *trasposizioni*, ossia permutazioni che scambiano solamente due lettere e lasciano invariate le altre. Benché la scrittura di una permutazioni mediante trasposizioni non sia in generale unica, quello che invece può essere dimostrato è che se una permutazione ammette due scritture mediante trasposizioni, allora il numero di trasposizioni che compaiono nella prima e nella seconda scrittura hanno la stessa parità. Grazie a questa proprietà, è ben definita la *parità* di una permutazione (che verrà di conseguenza detta o *pari* o *dispari*) ed è dunque ben

definito quello che è detto il *segno* di una permutazione, che altro non è che la funzione

$$sgn : \mathscr{S}_n \longrightarrow \{1, -1\}$$

che assegna ad una permutazione il valore 1 se essa è pari o il valore -1 se essa è dispari. Si vede immediatamente che la funzione sgn è un omomorfismo di gruppi, il cui nucleo è il sottogruppo normale di $\mathscr{S}_n$ delle permutazioni pari. Questo è detto *gruppo alterno* e viene indicato con $\mathscr{A}_n$.

Applicando il Primo Teorema di Isomorfismo per Gruppi al morfismo sgn, si vede che l'indice di $\mathscr{A}_n$ in $\mathscr{S}_n$ è $[\mathscr{S}_n : \mathscr{A}_n] = 2$ e quindi dal Teorema di Lagrange segue che $|\mathscr{A}_n| = \frac{|\mathscr{S}_n|}{2}$.

Definizione 1.14. Sia $n \in \mathbb{N}^*$ un numero naturale positivo fissato. Un *gruppo di permutazioni* è un sottogruppo di $\mathscr{S}_n$. Il numero n è detto *grado* del gruppo di permutazioni.

1.2 Segnature logaritmiche

Introduciamo ora un nuovo concetto, che assomiglia molto al concetto di base di uno spazio vettoriale riadattato al caso dei gruppi.

Definizione 1.15. Sia G un gruppo di permutazioni di grado n. Una *segnatura logaritmica* per G è una collezione finita ordinata $\alpha = \{B_i : i = 1, \ldots, s\}$ di insiemi finiti ordinati $B_i = \{u(i,1), u(i,2), \ldots, u(i,r_i)\}$ tali che:

1. $u(i,j) \in \mathscr{S}_n$ per ogni $1 \leq j \leq r_i$ e $1 \leq i \leq s$;
2. ogni $g \in G$ può essere espresso in modo unico come prodotto (di composizione) della forma

$$g = q_s \cdot q_{s-1} \cdots q_2 \cdot q_1$$

per certi $q_i \in B_i$ e dove la composizione è da sinistra a destra.

I B_i sono detti *blocchi* di α e il vettore delle lunghezze dei blocchi $\boldsymbol{r} = (r_1, \ldots, r_s)$ è detto *tipo* di α. Definiamo *lunghezza* di una segnatura logaritmica α il numero $\sum_{i=1}^{s} r_i$. Indichiamo con Λ la collezione di tutte le segnature logaritmiche di G.

Si noti che i q_i non sono necessariamente elementi di G, bensì potrebbero appartenere a un gruppo più largo in cui G è immerso (a priori l'intero $\mathscr{S}_n$).

Definizione 1.16. Sia G un gruppo di permutazioni di grado n e α una sua segnatura logaritmica. Allora α è detta:

1. *non banale* se $s \geq 2$ e $r_i \geq 2$ per ogni $1 \leq i \leq s$, *banale* altrimenti;
2. *docile* (*tame*) se la fattorizzazione che essa garantisce può essere portata a termine in tempo $poly(n)$, ossia in un numero di operazioni che dipende da n in maniera polinomiale;

3. *super-docile* (*supertame*) se la fattorizzazione che essa garantisce può essere portata a termine in tempo $O(n^2)$, ossia in un numero di operazioni che dipende da n come un polinomio di secondo grado;

4. *selvaggia* (*wild*) se non è docile.

C'è un modo intelligente per procurarsi segnature logaritmiche per un dato gruppo di permutazioni G. Supponiamo di avere una *catena* (o *torre*) γ di sottogruppi di G della forma

$$\gamma : \{1\} = G_s < G_{s-1} < \ldots < G_2 < G_1 < G_0 = G$$

con $s \geq 2$. Una segnatura non banale τ può essere costruita nella seguente maniera: per ogni $i \in \{1, \ldots, s\}$ consideriamo l'insieme delle classi laterali sinistre di G_i in G_{i-1}, ne prendiamo un trasversale, che come anticipato in precedenza altro non è che un sistema (insieme) completo di rappresentanti per ogni classe, e lo ordiniamo. Detto T_i il trasversale ordinato di G_i in G_{i-1} si nota che $\tau = \{T_i : i = 1, \ldots, s\}$ è una segnatura logaritmica per G. Infatti, preso un qualunque $g \in G$, esso starà in una delle classi laterali sinistre di G_1 in G. Dal momento che T_1 è un trasversale di G_1 in G allora $\exists!\ t_1 \in T_1$ tale che $g = g' \cdot t_1$ con $g' \in G_1$, in quanto t_1 è l'unico rappresentante della classe cui appartiene g. Ora, g' si scrive a sua volta in modo unico come $g' = g'' \cdot t_2$ con $g'' \in G_2$ e $t_2 \in T_2$ unico rappresentante della classe laterale sinistra di G_2 in G_1 cui g' appartiene. Iterando il discorso (più formalmente: procedendo per induzione), si arriva a concludere che $g = t_s \cdot t_{s-1} \cdots t_2 \cdot t_1$ con $t_i \in T_i$ e la scrittura è unica per costruzione. Chiaramente in questo caso il tipo $\boldsymbol{r} = (r_1, \ldots, r_s)$ di τ è tale che $r_i = [G_i : G_{i-1}]$.

Non è difficile capire perché una segnatura logaritmica siffatta è detta *segnatura logaritmica trasversale*. Denotiamo con Γ_G l'insieme di tutte le catene di sottogruppi di G della forma poc'anzi descritta, con $\Lambda(\gamma)$ l'insieme di tutte le segnature logaritmiche trasversali di G generabili a partire dalla catena di sottogruppi γ e indichiamo con $\mathcal{E}$ l'insieme di tutte le segnature logaritmiche trasversali per un dato gruppo G, pertanto

$$\mathcal{E} := \bigcup_{\gamma \in \Gamma_G} \Lambda(\gamma)$$

Senza addentrarsi troppo nel merito della questione, è di fondamentale importanza sottolineare come studi approfonditi in questo settore abbiano messo in luce la possibilità di testare l'appartenenza ad un gruppo di permutazioni in tempo polinomiale nel grado e nel numero di generatori del gruppo (per eventuali ulteriori approfondimenti si consulti [5] in bibliografia). L'esistenza di un tale algoritmo consente, dato $g \in G$ e una segnatura logaritmica trasversale come descritto sopra (quindi $\tau = \{T_i : i = 1, \ldots, s\}$), di trovare quell'unico $q_1 \in T_1$ tale che

$$g \in G_1 q_1 \iff g q_1^{-1} \in G_1$$

banalmente testando per ogni elemento t di T_1 (al più r_1 operazioni) se gt^{-1} appartiene o meno al sottogruppo G_1, e questa procedura è computazionalmente efficiente (sotto ovvie assunzioni sull'ordine i grandezza di n) in quanto l'algoritmo termina in tempo polinomiale nel grado n e nel numero di generatori di G_1. Possiamo iterare questa procedura, definendo $g_1 := gq_1^{-1} \in G_1$ e calcolando nella stessa maniera quell'unico $q_2 \in T_2$ tale che

$$g_1 \in G_2 q_2 \iff g_1 q_2^{-1} = g q_1^{-1} q_2^{-1} \in G_2$$

e più in generale continuando fino a trovare quell'unico $q_s \in T_s$ tale che

$$g_{s-1} \in G_s q_s \iff g_{s-1} q_s^{-1} = g q_1^{-1} q_2^{-1} \cdots q_{s-1}^{-1} q_s^{-1} \in G_s = \{1\}$$

ossia continuando finchè non abbiamo trovato quei $q_i \in T_i$ tali che

$$g q_1^{-1} q_2^{-1} \cdots q_{s-1}^{-1} q_s^{-1} = 1 \iff g = q_s q_{s-1} \cdots q_2 q_1$$

Quello che abbiamo ottenuto altro non è che la fattorizzazione del generico elemento $g \in G$ rispetto alla segnatura logaritmica trasversale τ, in un numero di operazioni che dipende da n in maniera polinomiale grazie all'algoritmo sopracitato. Dunque, data per assodata la teoria descritta in [5], abbiamo appena dimostrato la seguente proposizione.

Proposizione 1.17. *Sia G un gruppo di permutazioni di grado n e sia τ una segnatura logaritmica trasversale per G. Allora essa è docile.*

1.3 Azioni

Definizione 1.18. Sia G un gruppo e X un insieme. Si dice *azione di gruppo* (ovvero *G-azione*) una funzione

$$\begin{aligned} \theta : X \times G &\longrightarrow X \\ (x, g) &\longmapsto x^g \end{aligned}$$

tale che siano soddisfatte le sue seguenti condizioni:

1. $(x^g)^h = x^{gh}$ per ogni $x \in X$ e per ogni $g, h \in G$;
2. $x^1 = x$ per ogni $x \in X$.

In letteratura si dice che G *agisce* su X mediante θ o che X è un *G-insieme*.

Data un'azione, possiamo considerare la relazione $\sim$ su X data da

$$x \sim y \iff x^g = y$$

per qualche $g \in G$. É banale verificare che si tratta di una relazione di equivalenza.

Definizione 1.19. Se G agisce su X e $x \in X$ l'insieme $x^G := \{x^g : g \in G\} = [x]_\sim$ si dice *orbita di x sotto G*.

Dal momento che le orbite sono le classi di equivalenza della relazione $\sim$ esse formano, per motivi generali, una partizione di X.

Definizione 1.20. Un'azione è detta *transitiva* se possiede un'unica orbita.

Definizione 1.21. Se G agisce su X, dato $x \in X$, l'insieme $G_x := \{g \in G : x^g = x\}$ si dice *stabilizzatore di x in G.*

Definizione 1.22. Sia G un gruppo che agisce transitivamente su un insieme X. G è detto *imprimitivo* se esiste una partizione $\mathcal{P}$ di X, che chiameremo *sistema di blocchi*, i cui elementi, detti *blocchi*, soddisfano le seguenti proprietà:

1. l'azione di G su X mappa un blocco di $\mathcal{P}$ in un altro blocco di $\mathcal{P}$ (segue in particolare che tutti i blocchi hanno la stessa cardinalità);
2. tutti i blocchi di $\mathcal{P}$ sono sottoinsiemi propri di X contenenti almeno due elementi.

Se G è imprimitivo su X, si dice che G *rispetta* il sistema di blocchi $\mathcal{P}$. Il gruppo transitivo G è detto *primitivo* se non è *imprimitivo.*

Con un po' di rammarico si ammonisce il lettore riguardo all'ambiguità di notazione: nel secondo capitolo verranno introdotti nuovi oggetti algebrici che purtroppo sono designati con lo stesso termine "blocchi". Ad ogni modo, dovrebbe essere chiaro dal contesto a cosa ci si sta riferendo.

Definizione 1.23. Sia G un gruppo che agisce su un insieme X con almeno due elementi. G è detto 2-*transitivo* se per ogni coppia di coppie $(x, y), (z, w) \in X \times X$ con $x \neq y$ e $z \neq w$ esiste $g \in G$ tale che $(x, y)^g := (x^g, y^g) = (z, w)$.

Vale la seguente facile proposizione.

Proposizione 1.24. *Un gruppo G che agisce 2-transitivamente su un insieme X è primitivo.*

1.4 Crittografia: concetti base

Iniziamo questa sezione definendo cosa si intende per crittosistema. La crittografia non è altro che la branca della matematica che studia e progetta crittosistemi, pertanto è necessario darne una definizione formale.

Definizione 1.25. Un *crittosistema* (o *sistema crittografico*) è una 4-upla ordinata $(\mathscr{M}, \mathscr{K}, \mathscr{C}, \mathscr{T})$ ove:

1. $\mathscr{M}$ è un insieme finito, detto *spazio dei messaggi*;
2. $\mathscr{K}$ è un insieme finito, detto *spazio delle chiavi*;
3. $\mathscr{C}$ è un insieme finito, detto *spazio dei testi cifrati*;

4. $\mathscr{T}$ è una famiglia di trasformazioni $\{E_k : \mathscr{M} \to \mathscr{C}\}_{k\in\mathscr{K}}$ dette *trasformazioni crittografiche* tali che per ogni $k \in \mathscr{K}$ la mappa E_k sia invertibile; denotiamo tale inversa con D_k.

Implicitamente, un crittosistema presenta anche una mappa $E : \mathscr{K} \to \mathscr{T}$ che agisce associando $k \mapsto E_k$. Il crittosistema è detto *fedele* se E è iniettiva, in altre parole se a chiavi diverse corrispondono trasformazioni crittografiche diverse.

I sistemi crittografici vengono classificati sulla base delle differenze sostanziali che intercorrono tra i quattro insiemi appena citati e sul loro impiego.

Definizione 1.26. Sia C un crittosistema. C è detto:

1. *asimmetrico* (o *a chiave pubblica*) se la chiave di cifratura è diversa dalla chiave di decrittazione. In questo tipo di crittografia il destinatario possiede una chiave privata, che nasconde segretamente, e una chiave pubblica, che distribuisce a chiunque voglia comunicare con lui. Per mezzo della chiave pubblica, un qualsiasi mittente critta il suo messaggio, che potrà venir decrittato solamente dal destinatario mediante la chiave privata. I crittosistemi di questo tipo evitano il problema connesso alla necessità di uno scambio sicuro di unica chiave di cifratura/decifrazione (presente invece nella classe di crittosistemi che segue), ma sono solitamente un po' più macchinosi;

2. *simmetrico* (o *a chiave privata*) se la chiave di cifratura e la chiave di decifrazione coincidono. In questo tipo di crittografia si presuppone che le due parti siano già in possesso della chiave (per esempio dopo essersela scambiata di persona o mediante un sistema a chiave pubblica), tuttavia questi crittosistemi sono solitamente più rapidi e agevoli.

Molto frequenti sono i crittosistemi descritti nella seguente definizione.

Definizione 1.27. Un crittosistema C è detto *endomorfo* se $\mathscr{M} = \mathscr{C}$. Un sistema endomorfo è detto *chiuso* se $\mathscr{T}$ forma un gruppo rispetto alla composizione.

Se C è endomorfo, lo spazio dei messaggi coincide con lo spazio dei testi cifrati, e ricordando che le trasformazioni crittografiche sono biiezioni, possiamo concludere che esse sono permutazioni di $\mathscr{M}$.

In generale, per un crittosistema endomorfo C, possiamo considerare il gruppo $\mathscr{G}_C = \langle\mathscr{T}\rangle$ generato dalle trasformazioni di C (se C è chiuso si avrà $\langle\mathscr{T}\rangle = \mathscr{T}$). Per le considerazioni fatte, si avrà che $\mathscr{G}_C \leq \mathscr{S}_{|\mathscr{M}|}$. Molte delle questioni che riguardano la sicurezza dei sistemi crittografici endomorfi sotto certi tipi di attacchi (primo fra tutti il *brute force*) sono legate al gruppo $\mathscr{G}_C$, in particolare alla sua dimensione. Di ciò parleremo più nel dettaglio nel caso particolare del gruppo generato dalle trasformazioni del PGM.

Capitolo 2

Il crittosistema PGM

Questo capitolo è interamente dedicato al sistema crittografico che prende il nome da quelle che, di fatto, sono le trasformazioni crittografiche che sfrutta, ovvero le *Permutation Group Mappings* (letteralmente: le mappature dei gruppi di permutazioni). Nella prima sezione è esposta la costruzione che porta alla definizione del sistema stesso e delle sue chiavi, mentre nella seconda è illustrato un classico esempio di situazione concreta, in cui i classici personaggi della crittografia Alice e Bob vogliono scambiarsi un messaggio adoperando il PGM.

2.1 Costruzione e definizione

Prima di passare alla descrizione del PGM introduciamo alcune notazioni. Di seguito α è una segnatura logaritmica trasversale per il gruppo di permutazioni G.

Con $\mathbb{Z}_n$ si intende $\mathbb{Z}/n\mathbb{Z}$ dunque $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Con $\alpha[i, j]$ intendiamo il j-esimo elemento dell'i-esimo blocco di α, con $i \in \{1, \ldots, s\}$ e $j \in \{0, \ldots, r_i - 1\}$. Inoltre, se il tipo di α è $\boldsymbol{r} = (r_1, \ldots, r_s)$ e consideriamo $(p_1, \ldots, p_s) \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s}$ allora definiamo la permutazione

$$\alpha(p_1, \ldots, p_s) := \alpha[s, p_s] \cdots \alpha[2, p_2]\, \alpha[1, p_1]$$

sempre utilizzando la notazione di composizione da sinistra a destra.

Quello che andiamo ora a descrivere è il PGM nella sua formulazione più immediata e naturale, ovvero quella a chiave privata, nonché quella che per prima fu ideata. Alcune altre varianti a chiave pubblica (come MST1 e MST2, dal nome degli ideatori Magliveras, Stinson e van Trung) vennero proposte successivamente e fondano il loro funzionamento sempre sulle segnature logaritmiche, in particolare sulla difficoltà di a riuscire portare a termine la fattorizzazione garantita da una segnatura selvaggia (sulla falsa riga dell'esempio fornito dall'RSA).

Consideriamo ora un gruppo di permutazioni G di grado n (pertanto $G \leq \mathscr{S}_n$) e supponiamo di disporre di una segnatura logaritmica trasversale

α per G. Ricordando la Formula degli Indici dimostrata nel primo capitolo e applicandola iterativamente, si ha che

$$\prod_{i=1}^{s} r_i = \prod_{i=1}^{s} [G_i : G_{i-1}] = |G|$$

ove $\boldsymbol{r} = (r_1, r_2, \ldots, r_s)$ è il tipo della segnatura α. L'obiettivo è costruire una biiezione tra $\mathbb{Z}_{|G|}$ e se stesso a partire da α. Le biiezioni siffatte interpreteranno poi il ruolo di trasformazioni crittografiche del PGM. Vediamo come fare.

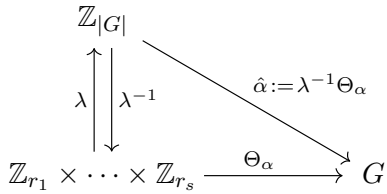
Tenuto conto delle proprietà del tipo $\boldsymbol{r}$ di una qualunque segnatura logaritmica trasversale per G, c'è un modo interessante per costruire una biiezione tra $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s}$ e $\mathbb{Z}_{|G|}$ (che, per l'appunto, hanno la stessa cardinalità finita). Definiamo i numeri naturali m_i con $i \in \{1, 2, \ldots, s\}$ come

$$m_1 = 1 \qquad m_i = \prod_{j=1}^{i-1} r_j \qquad i = 2, \ldots, s$$

e consideriamo la funzione $\lambda : \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s} \to \mathbb{Z}_{|G|}$ definita da

$$\lambda(p_1, \ldots, p_s) = \sum_{i=1}^{s} p_i m_i$$

Innanzitutto è ben definita in quanto assume valori compresi tra $0 \in \mathbb{Z}_{|G|}$ in corrispondenza di $(0, \ldots, 0) \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s}$ e $(\prod_{i=1}^{s} r_i) - 1 \in \mathbb{Z}_{|G|}$ in corrispondenza di $(r_1 - 1, \ldots, r_s - 1)$. É poi facile verificare che si tratta di una biiezione. Infatti, essa è banalmente iniettiva; inoltre, preso $x \in \mathbb{Z}_{|G|}$ è possibile trovare $(p_1, \ldots, p_s)$ tale che $\lambda(p_1, \ldots, p_s) = x$ rappresentando x sulla "base mista" $(m_1, \ldots, m_s)$ mediante divisioni e sottrazioni successive (l'idea di fondo è prendere il quoziente della divisione di x per m_s, assegnarlo a p_s, prendere il resto della divisione e procedere in questa maniera; questa procedura ha senso in quanto il quoziente è, ad ogni passo, banalmente compreso tra 0 e $r_i - 1$ inclusi). Pertanto, essendo λ una biiezione, possiamo considerare $\lambda^{-1} : \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s} \to \mathbb{Z}_{|G|}$ che agisce precisamente nel modo appena considerato per dimostrare la suriettività. In letteratura la funzione λ^{-1} è detta *knapsack transformation*. Osserviamo ora il seguente diagramma.



Le due funzioni λ e λ^{-1} sono una l'inversa dell'altra e dunque biiezioni. A questo punto, preso $g \in G$, dal momento che α è una segnatura logaritmica trasversale per G, esistono indici $0 \leq p_i \leq r_i - 1$ tali che

$g = \alpha[s, p_s] \cdots \alpha[2, p_2]\, \alpha[1, p_1]$ e, viceversa, in corrispondenza di ogni scelta di indici siffatti la permutazione ottenuta componendo in modo opportuno gli elementi dei blocchi contrassegnati dagli indici è chiaramente una permutazione in G. Abbiamo sostanzialmente definito un'altra funzione

$$\Theta_\alpha : \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s} \longrightarrow G$$

che agisce secondo

$$\Theta_\alpha(p_1, \ldots, p_s) = \alpha(p_1, \ldots, p_s)$$

e che è, per ogni $\alpha \in \mathcal{E}$, una biiezione, proprio per definizione di segnatura logaritmica.

A questo punto, per ogni $\alpha \in \mathcal{E}$, definiamo la mappa $\hat{\alpha} : \mathbb{Z}_{|G|} \to G$ componendo λ^{-1} con Θ_α quindi $\hat{\alpha} = \lambda^{-1}\Theta_\alpha$ come è bene illustrato in figura. Abbiamo così trovato un modo per associare ad ogni elemento del gruppo G uno e un solo elemento di $\mathbb{Z}_{|G|}$ in maniera biunivoca mediante $\hat{\alpha}$ che, in qualità di composizione di biiezioni, è anch'essa una biiezione.

Le trasformazioni della forma $\hat{\alpha}$ sono facilmente invertibili, infatti vale che la funzione $\hat{\alpha}^{-1} : G \to \mathbb{Z}_{|G|}$ si ottiene calcolando

$$\hat{\alpha}^{-1} = \Theta_\alpha^{-1}\lambda$$

ossia trovando la fattorizzazione del generico elemnto del gruppo in termini della segnatura logaritmica e poi mappando la s-upla ottenuta con la funzione λ.

Possiamo finalmente definire il crittosistema PGM. L'obbiettivo che ci eravamo prefissati era quello di costruire una mappa biunivoca da $\mathbb{Z}_{|G|}$ in se stesso: ora che sappiamo costruire una mappa biunivoca da $\mathbb{Z}_{|G|}$ in G il gioco è presto fatto. Siano dati $n \in \mathbb{N}^*$ e un gruppo di permutazioni $G \leq \mathscr{S}_n$; siano date due segnature logaritmiche trasversali α e β per G. Allora la funzione

$$E_{\alpha,\beta} = \hat{\alpha} \circ \hat{\beta}^{-1}$$

è una biiezione tra $\mathbb{Z}_{|G|}$ e se stesso, dunque una sua permutazione (qui abbiamo usato la notazione della composizione "da sinistra a destra" per cui la prima funzione ad agire è $\hat{\alpha}$). Il crittosistema PGM è un sistema endomorfo in cui lo spazio dei messaggi e lo spazio dei testi cifrati sono $\mathbb{Z}_{|G|}$ e le cui trasformazioni crittografiche sono le funzioni del tipo $E_{\alpha,\beta} = \hat{\alpha} \circ \hat{\beta}^{-1}$ ove α e β sono pescati dall'insieme $\mathcal{E}$ delle segnature logaritmiche trasversali di G. Per comodità, denotiamo con $\hat{\mathcal{E}}$ l'insieme delle applicazioni di tale forma, ossia

$$\hat{\mathcal{E}} := \{\hat{\alpha} \circ \hat{\beta}^{-1} : (\alpha, \beta) \in \mathcal{E} \times \mathcal{E}\}$$

Tutto quanto detto si può dunque riassumere in una sola espressione:

$$\mathrm{PGM} = (\mathbb{Z}_{|G|},\, \mathcal{E} \times \mathcal{E},\, \mathbb{Z}_{|G|},\, \hat{\mathcal{E}})$$

Ci si accorge facilmente del fatto che il PGM non è fedele: prese due segnature logaritmiche trasversali distinte $\tau, \rho \in \mathcal{E}$, le due chiavi distinte $(\tau, \tau), (\rho, \rho) \in \mathcal{E} \times \mathcal{E} = \mathscr{K}$ corrispondono alla stessa trasformazione crittografica $\hat{\tau} \circ \hat{\tau}^{-1} = \hat{\rho} \circ \hat{\rho}^{-1} = id_{\mathscr{S}_n}$, cioè la permutazione identica.

2.2 Un esempio: Alice e Bob

In questa sezione vediamo come effettivamente si svolgono le procedure di codifica e decodifica per il PGM da parte dei due classici protagonisti della crittografia. In particolare sono presentate in dettaglio tutte le operazioni e i calcoli delle funzioni che il mittente e il destinatario devono svolgere rispettivamente per cifrare e decifrare il messaggio.

Sia dunque $n = 5$ e consideriamo $\mathscr{S}_5$ il gruppo simmetrico su 5 lettere. Come gruppo di permutazioni su cui imperniare il sistema di comunicazione crittata scegliamo $G = \mathscr{A}_5$ ossia il gruppo alterno su 5 lettere. Chiaramente si ha che $G \leq \mathscr{S}_5$. Il gruppo simmetrico $\mathscr{S}_5$ ha cardinalità $|\mathscr{S}_5| = 5! = 120$ e dunque il gruppo G ha cardinalità $|G| = |\mathscr{A}_5| = \frac{120}{2} = 60$.

In questo particolare caso si ha quindi che lo spazio dei messaggi e quello dei testi cifrati sono $\mathscr{M} = \mathscr{C} = \mathbb{Z}_{60} = \{0, 1, \ldots, 58, 59\}$. Consideriamo ora le due segnature logaritmiche trasversali descritte nella tabella che segue:

α	*knapsack*	β
(1)(2)(3)(4)(5)	0	(1 4 2 3 5)
(1 2 3 4 5)	1	(1)(2)(3 4 5)
(1 3 5 2 4)	2	(1 2 5 4 3)
(1 4 2 5 3)	3	(1 3)(2 4)(5)
(1 5 4 3 2)	4	(1 5 3 4 2)
(1)(2)(3)(4)(5)	0	(1)(2 3)(4 5)
(1)(2 3)(4 5)	5	(1)(2 5 3)(4)
(1)(2 4 3)(5)	10	(1)(2 4 3)(5)
(1)(2 5 3)(4)	15	(1)(2)(3)(4)(5)
(1)(2)(3)(4)(5)	0	(1)(2)(3)(4)(5)
(1)(2)(3 4 5)	20	(1)(2)(3 5 4)
(1)(2)(3 5 4)	40	(1)(2)(3 4 5)

Qui, come d'altronde sempre quando si tratta di permutazioni, abbiamo usato la notazione dei *k-cicli*, che altro non sono che permutazioni di $\mathscr{S}_n$ indicate con $(i_1\ i_2\ \cdots\ i_k)$ che agiscono mandando i_m in i_{m+1} con la convenzione che i_k viene mandato in i_1. Quindi, per esempio, la permutazione $\alpha[1, 3]$ è un 5-ciclo, mentre $\beta[2, 0]$ è composizione di due 2-cicli e un 1-ciclo.

Gli 1-cicli, dal momento che di fatto non scambiano nulla e agiscono quindi come l'identità, vengono spesso omessi.

É interessante sottolineare come α sia stata ricavata da una torre di due stabilizzatori, il primo della lettera $1 \in X = \{1, 2, 3, 4, 5\}$ e il secondo della lettera $2 \in X$, dell'azione di $\mathscr{A}_5$ su X, e come β sia stata ottenuta a partire da α applicando delle trasformazioni che saranno descritte e di cui si farà largo uso nel prossimo capitolo. Come anticipazione, le due operazioni sono o la scelta di un altro rappresentante per la stessa classe laterale oppure il rimescolamento dei rappresentanti all'interno dello stesso blocco, considerati quindi in un altro ordine (oppure una combinazione di queste due). Degno di nota è il fatto che è possibile dimostrare in modo abbastanza agile che le segnature logaritmiche trasversali ricavate da una catena di stabilizzatori sono sempre super-docili.

In questo caso si hanno tre blocchi in quanto $s = 3$ e il tipo delle due segnature è dato da $\boldsymbol{r} = (5, 4, 3)$. I naturali m_i sono invece

$$m_1 = 1 \qquad m_2 = 5 \qquad m_3 = 20$$

sicché nella seconda colonna della tabella è stato possibile riportare gli abbinamenti tra i valori della knapsack trasformation e gli opportuni elementi dei blocchi.

Ebbene, supponiamo che Alice e Bob si siano scambiati in un qualche modo le due segnature α e β, e vediamo come, mediante queste ultime, riescano a scambiarsi segretamente un messaggio. Ipotizziamo che Alice voglia mandare a Bob il messaggio $m = 49 \in \mathbb{Z}_{60}$. Allora Alice calcola la rappresentazione di 49 sulla "base mista" $(1, 5, 20)$ computando

$$49 = \mathbf{2} \cdot 20 + 9 = \boxed{40} + 9$$

$$9 = \mathbf{1} \cdot 5 + 4 = \boxed{5} + 4$$

$$4 = \mathbf{4} \cdot 1 + 0 = \boxed{4} + 0$$

di modo che $49 = 40 + 5 + 4$ e quindi $\lambda^{-1}(49) = (4, 1, 2)$. Successivamente si passa al calcolo di $\Theta_\alpha(4, 1, 2)$ che si ottiene componendo le opportune permutazioni, in pratica

$$\Theta_\alpha(4, 1, 2) = \alpha(4, 1, 2) = \alpha[3, 2]\, \alpha[2, 1]\, \alpha[1, 4] =$$

$$= (1)(2)(3\ 5\ 4) \circ (1)(2\ 3)(4\ 5) \circ (1\ 5\ 4\ 3\ 2) = (1\ 5\ 4)(3)(2)$$

e abbiamo quindi calcolato $\hat{\alpha}(49) = (1\ 5\ 4)(3)(2)$. Si badi al fatto che, una volta ottenuta la scrittura di 49 come somma dei naturali messi in evidenza nei box, grazie alla seconda colonna della tabella, è sufficiente comporre nel giusto ordine le permutazioni di α corrispondenti alla stessa riga in cui compaiono gli interi.

A questo punto facciamo intervenire la segnatura β, e dovendo calcolare $\hat{\beta}^{-1} = \Theta_\beta^{-1}\lambda$ cominciamo col determinare $\Theta_\beta^{-1}\big((1\ 5\ 4)(3)(2)\big)$, ossia la rappresentazione della permutazione appena ottenuta su β. Riguardo a questo passaggio, che è chiaramente il più delicato in quanto si tratta di invertire una funzione che invece è molto facile da calcolare direttamente e proprio per il quale sono state spese diverse parole circa gli algoritmi che permettono di assolvere a questa fattorizzazione e la loro efficienza (si veda, nel primo capitolo, la Proposizione 1.15 e il preambolo ad essa, che afferma che ogni segnatura logaritmica trasversale è docile), è palese come, nel caso generale, sia necessario l'ausilio di un calcolatore su cui siano stati implementati gli opportuni algoritmi e le opportune procedure (reperibili, come già sottolineato, in [5]). Ad ogni modo, grazie anche alla super-docilità delle segnature del nostro caso particolare, la questione è molto più semplice e può essere sbrigata "a mano".

Prima di tutto notiamo che, visto che tutte le permutazioni del secondo e terzo blocco di β fissano 1 in quanto elementi del suo stabilizzatore, e visto che la permutazione $\pi := (1\ 5\ 4)(3)(2)$ di cui dobbiamo calcolare la rappresentazione manda 1 in 5, segue necessariamente che essa sarà il prodotto di composizione di una certa σ con l'unica permutazione del primo blocco di β che manda 1 in 5, ossia $\beta[1,4]$. Pertanto $\pi = \sigma\,\beta[1,4]$ e risolvendo in σ si ottiene

$$\sigma = \pi\,\beta[1,4]^{-1} = (1\ 5\ 4)(3)(2) \circ (1\ 2\ 4\ 3\ 5) = (1)(2\ 4)(3\ 5)$$

che come ci aspettavamo fissa 1 e sta nello stabilizzatore. Continuando nella stessa maniera, dal momento che tutte le permutazioni del terzo blocco di β fissano 2 in quanto elementi del suo stabilizzatore e dal momento che la permutazione σ mappa 2 in 4, è inevitabile che essa sarà il prodotto di composizione di una certa ρ con l'unica permutazione del secondo blocco di β che manda 2 in 4, ossia $\beta[2,2]$. Perciò $\sigma = \rho\,\beta[2,2]$ e risolvendo in ρ si ottiene

$$\rho = \sigma\,\beta[2,2]^{-1} = (1)(2\ 4)(3\ 5) \circ (1)(2\ 3\ 4)(5) = (1)(2)(3\ 5\ 4) = \beta[3,1]$$

che come ci aspettavamo, dato che ci trovavamo al livello più basso della catena di sottogruppi, è proprio un elemento del terzo blocco della segnatura β. Pertanto, risalendo per sostituzione a π, si ha che

$$\pi = \beta[3,1]\,\beta[2,2]\,\beta[1,4]$$

e la controprova è immediata per calcolo diretto. Da questa scrittura ricaviamo $\Theta_\beta^{-1} = (4,2,1) \in \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_3$ e di conseguenza

$$\lambda(4,2,1) = 4 \cdot 1 + 2 \cdot 5 + 1 \cdot 20 = 4 + 10 + 20 = 34$$

risultato a cui potevamo pervenire utilizzando nuovamente la seconda colonna della tabella e andando a sommare gli interi in corrispondenza delle stesse righe in cui compaiono le permutazioni che fattorizzano π. Questo

conclude il calcolo di $\beta^{-1}(\pi) = 34$

Quindi, in definitiva, abbiamo ottenuto che $E_{\alpha,\beta}(49) = 34$ e quindi Alice manda a Bob il messaggio cifrato $c = 34 \in \mathbb{Z}_{60}$.

A questo punto, come fa Bob a capire qual è il messaggio originale che Alice gli ha voluto mandare? Il gioco è presto fatto: dal momento che anche Bob dispone delle segnature logaritmiche trasversali α e β, altro non gli resta che calcolare

$$D_{\alpha,\beta}(34) = E_{\beta,\alpha}(34)$$

ossia compiere le operazioni che abbiamo appena mostrato per Alice, ma con α e β a ruoli invertiti. La verifica del fatto che $D_{\alpha,\beta} = 49$ è un mero esercizio di calcolo e di imitazione di quanto appena esposto, ed è dunque lasciato ad ogni lettore interessato. Si osservi che anche in questo caso, nel momento del calcolo di α^{-1} in particolare di Θ_α^{-1}, Bob sarà certo di poter adempiere alla fattorizzazione in tempi rapidi grazie alla super-docilità della segnatura α, in quanto trasversale in relazione a una torre di stabilizzatori.

Capitolo 3

Le proprietà del gruppo $\langle \hat{\mathcal{E}} \rangle$

Dopo aver definito il PGM, sorge spontanea la domanda su quali siano le sue buone proprietà algebriche. In [1] Magliveras e Memon sono giunti a risposte parziali e piuttosto restrittive: in particolare, come già anticipato nei capitoli precedenti, l'interesse è stato focalizzato sullo studio di $\mathscr{G}_C = \langle \mathscr{T} \rangle$, il gruppo generato dall'insieme delle trasformazioni crittografiche $\mathscr{T}$, che nel caso del PGM è $\mathscr{G}_{\text{PGM}} = \langle \hat{\mathcal{E}} \rangle$, e i due matematici sono riusciti a dimostrare che quest'ultimo coincide con tutto il gruppo simmetrico su $|G|$ lettere, ossia che $\langle \hat{\mathcal{E}} \rangle = \mathscr{S}_{|G|}$ e che dunque è il più grande possibile. Tuttavia il loro risultato sussiste solamente sotto certe ipotesi piuttosto limitative: è in quest'ottica che, con il paper di cui in [3], Caranti e Dalla Volta hanno dimostrato la validità di tale risultato anche sotto ipotesi minime.

3.1 Premesse

Nel 1988 i tre crittoanalisti Kaliski, Rivest e Sherman pubblicarono un paper dal titolo "*Is the data encryption standard a group? (Results of cycling experiments on* DES*)*", che avrebbe di lì a poco cambiato le sorti di quello che era ormai diventato l'algoritmo di cifratura per antonomasia, adottato pressoché da tutte le organizzazioni governative e le compagnie informatiche, ossia il DES (*Data Encryption Standard*, appunto).

Come per il PGM, le trasformazioni del DES sono permutazioni dello spazio dei messaggi $\mathscr{M} = \{0,1\}^{64}$. La lunghezza di ogni chiave è pari a 56 bit, e l'insieme delle chiavi ha dunque cardinalità 2^{56}. A partire dal 1977, vari crittoanalisti iniziarono ad avanzare a livello teorico varie proposte per un computer in grado di violare il DES, sulla scia dello scetticismo generale circa la brevità delle sue chiavi. Si scoprirono vari tipi di attacchi possibili, alcuni dei quali sufficientemente efficaci, e proprio nel lavoro sopracitato venne evidenziata l'esistenza di una procedura capace di rompere una chiave DES in $2^{28} \approx 10^8$ operazioni medie (relativamente poche) nel caso in cui l'insieme generato dalle trasformazioni crittografiche fosse stato un gruppo.

La questione di fondamentale importanza era quindi studiare le proprietà algebriche dell'insieme $\mathscr{T}$ delle trasformazioni del DES, in primo luogo per far chiarezza sulla pericolosità del potenziale attacco poc'anzi accennato, e

in secondo luogo per tentare di rafforzare il DES mediante cifratura multipla. Infatti, nel caso in cui l'insieme $\mathscr{T}$ del DES non fosse stato un gruppo, allora componendo due permutazioni crittografiche sarebbe stato possibile "uscire" da $\mathscr{T}$ ottenendo una permutazione appartenente a un gruppo più grande contenente $\mathscr{T}$. Questo, di contro, sarebbe stato impossibile nella sfortunata eventualità in cui $\mathscr{G}_{\text{DES}} = \mathscr{T}$, in quanto componendo due permutazioni di un gruppo si sarebbe "ricaduti" nel gruppo stesso, e quindi la cifratura multipla sarebbe stata perfettamente equivalente a quella singola. Da qui l'importanza dello studio di $\langle \mathscr{T} \rangle$, della sua dimensione, delle sue proprietà.

La risposta arrivò da Campbell e Wiener, che nel 1992 pubblicarono l'articolo "DES *is not a group*" e diedero una svolta definitiva alle sorti del crittosistema in questione. Nella loro ricerca, oltre a dimostrare che il DES non è chiuso, i due dimostrarono che il gruppo generato dalle permutazioni del DES ha cardinalità superiore a 10^{2499}. Nacque così il Triple DES (TDES o 3DES), basato sull'interazione della cifratura DES per tre volte, e per quello che abbiamo appena commentato venne quindi assunto, per l'epoca, praticamente impenetrabile tramite forza bruta, considerando anche che le sue chiavi crebbero in numero da 2^{56} a $(2^{56})^3 = 2^{168} \approx 10^{50}$. Ciononostante il TDES passò quasi immediatamente in secondo piano in quanto debole contro certi tipi di attacchi specificatamente architettati per esso, e venne rimpiazzato da quello che ancora oggi è il crittosistema ufficialmente riconosciuto come standard: l'AES (*Advanced Encryption Standard*).

Questa premessa fa trapelare quanto importante sia conoscere l'insieme $\mathscr{T}$ e il gruppo $\mathscr{G}_C$ per ogni crittosistema C. Proprio per questo motivo, gli stessi quesiti sono stati posti e risolti per il PGM, e in questo capitolo vedremo come.

Innanzitutto vediamo come il PGM non presenta il problema della scarsità delle chiavi. Infatti, si potrebbe andare a calcolare la cardinalità di $\mathcal{E}$, ma in effetti si vede che in $\mathcal{E}$ sussiste il problema di equivalenza di segnature, per cui due segnature $\alpha, \beta \in \mathcal{E}$ sono dette equivalenti se $\hat{\alpha} = \hat{\beta}$. Pertanto, quello a cui si è veramente interessati è in realtà in numero di $\alpha \in \mathcal{E}$ che conducano a trasformazioni $\hat{\alpha}$ tutte distinte fra di loro, sostanzialmente all'insieme quoziente $\mathcal{E}/\!\sim$ ove $\sim$ è la relazione di equivalenza fra segnature logaritmiche. In [7] si dimostra che il numero di segnature inequivalenti in relazione a una catena di sottogruppi γ come quelle finora considerate è

$$\prod_{i=1}^{s} \left(\left(\prod_{j=1}^{i-1} r_j \right)^{r_i - 1} \cdot r_i! \right)$$

ove $\boldsymbol{r} = (r_1, \ldots, r_s)$ è il tipo di ogni segnatura ricavata da γ. É chiaro che anche per un gruppo di permutazioni G di relativamente basso grado n come $\mathscr{A}_{10}$ la cui cardinalità è $\frac{10!}{2} \approx 10^6$, il numero di segnature logaritmiche inequivalenti rispetto a un'unica torre è già di per sé astronomico. In più si tenga conto di tutte le torri che è possibile generare, e si tenga conto della

cifratura multipla. Insomma è evidente che il numero di chiavi è davvero spropositato e che ogni attacco sulle chiavi è realmente impossibile.

Resta quindi da capire come è fatto l'insieme $\mathscr{T}$ del PGM. In [1] Magliveras e il suo collega Memon hanno provato abbastanza comodamente che esso non è chiuso e, sempre nello stesso lavoro, hanno dimostrato il seguente risultato.

Teorema 3.1 (Magliveras - Memon)**.** *Se G è un gruppo di permutazioni finito, non abeliano e non hamiltoniano tale che $|G|$ è diverso da $q, (1+q^2)$, $(1+q^3), (q^m-1)/(q-1), 2^{m-1}(2^m \pm 1), 11, 12, 15, 22, 23, 24, 28, 176, 276$ dove q è una potenza di un primo e m è un intero positivo, allora il gruppo $\langle \hat{\mathcal{E}} \rangle$ generato da $\hat{\mathcal{E}}$ è 2-transitivo su $\mathbb{Z}_{|G|}$ e coincide con tutto il gruppo simmetrico $\mathscr{S}_{|G|}$.*

In chiusura del lavoro, i due matematici lasciano però aperta la questione riguardo alla possibilità che il risultato sussista anche sotto condizioni meno stringenti di quelle da loro imposte. E infatti così è: quello che andiamo a provare in questo capitolo è il seguente risultato, di Caranti e Dalla Volta.

Teorema 3.2 (Caranti - Dalla Volta)**.** *Sia G un gruppo di permutazioni finito e supponiamo che non sia ciclico di ordine un primo o il quadrato di un primo. Allora il gruppo $\langle \hat{\mathcal{E}} \rangle$ generato da $\hat{\mathcal{E}}$ coincide con tutto il gruppo simmetrico $\mathscr{S}_{|G|}$*

Come si può constatare, le ipotesi in questo caso sono drasticamente più essenziali del caso precedente. Usando la Teoria dei Gruppi applicata a operazioni elementari i due matematici italiani sono riusciti ad aggirare un sacco di anomalie e casi particolari che comportavano invece la lista di eccezioni nel Teorema 3.1.

Questo risultato ha, come per il DES, un risvolto assai importante, che si traduce in un sensibilmente rafforzamento del sistema tramite cifratura multipla: permettendo cifratura multipla, è possibile ottenere ogni permutazione dello spazio dei messaggi, e ogni sequenza di k messaggi cifrati distinti può a priori scaturire da ogni sequenza di k messaggi in chiaro. In questo modo un crittoanalista o un potenziale origliatore non ottiene nessuna informazione sulla corrispondenza tra parole in chiaro e parole cifrate, e l'unica alternativa che gli resta è un attacco a forza bruta su tutte le $|G|!$ permutazioni di $\mathscr{S}_{|G|}$. Questa strategia non ha ovviamente nessuna speranza già a partire da gruppi piccoli come $\mathscr{A}_5$ del nostro esempio, in cui sarebbero richieste $60! \approx 10^{81}$ prove, e ne ha ancora meno quando il grado del gruppo adoperato è un po' (ma non troppo) più grande, come $\mathscr{A}_{10}$, in cui si dovrebbero eseguire $(\frac{20!}{2})!$ tentativi. Non credo si riesca nemmeno a immaginare o a calcolare l'ordine di grandezza di tale numero, per quanto sia spaventosamente enorme.

3.2 Trasformazioni di segnature logaritmiche

In questa sezione iniziamo a delineare l'assetto algebrico che verrà poi impiegato nella dimostrazione del Teorema 3.2 nelle prossime pagine, e a definire alcune trasformazioni applicabili alle segnature logaritmiche trasversali. Anche qui si continuerà ad utilizzare la notazione di composizione da sinistra a destra.

Per i nostri scopi, ci limitiamo a considerare una catena di sottogruppi di G molto semplice, ottenuta prendendo $s = 2$ nella scrittura di una catena generica, che quindi diventa

$$\delta : \{1\} < H < G$$

Chiaramente questa costruzione non è legittima nel caso in cui G sia ciclico di ordine un primo, in quanto l'unico suo sottogruppo proprio sarebbe quello banale e verrebbe quindi a mancare il gruppo intermedio H. A noi però non interessa questo caso, poiché esso è escluso dalle ipotesi del teorema che vogliamo andare a provare. Scriviamo $|H| = \mu$ e $[G : H] = \lambda$, sicché $|G| = \lambda\mu$.

Un accorgimento molto utile consiste nel notare che, se fissiamo una segnatura logaritmica trasversale α per G con riferimento alla catena δ, allora il gruppo $\mathscr{G}_{\mathrm{PGM}} = \langle \hat{\mathcal{E}} \rangle$ coincide con il gruppo generato dall'insieme di trasformazioni crittografiche

$$\hat{\mathcal{E}}_\alpha := \{\hat{\alpha} \circ \hat{\beta}^{-1} : \beta \in \mathcal{E}\}$$

Infatti, se $\gamma \in \mathcal{E}$ è una qualsiasi altra segnatura logaritmica trasversale per G, allora

$$(\hat{\alpha} \circ \hat{\gamma}^{-1})^{-1} \circ (\hat{\alpha} \circ \hat{\beta}^{-1}) = \hat{\gamma} \circ \hat{\beta}^{-1}$$

e perciò $\hat{\mathcal{E}}_\alpha$ contiene pure tutte le trasformazioni della forma $\hat{\gamma} \circ \hat{\beta}^{-1}$, dove γ e β sono segnature logaritmiche trasversali per G. In definitiva vale dunque $\langle \hat{\mathcal{E}} \rangle = \langle \hat{\mathcal{E}}_\alpha \rangle$. Per questo motivo fissiamo una segnatura α rispetto alla catena δ (dove H dipenderà caso per caso dalle proprietà del gruppo G) una volta per tutte, e per comodità prendiamo $\alpha[1, 0] = \alpha[2, 0] = id_G$, ovvero la permutazione identica, unità del gruppo G. Questo espediente faciliterà i ragionamenti giacché permette di lavorare con $\langle \hat{\mathcal{E}}_\alpha \rangle$ anziché con $\langle \hat{\mathcal{E}} \rangle$.

Cominciamo ora ad analizzare alcune trasformazioni della forma $\hat{\alpha} \circ \hat{\beta}^{-1}$, con $\beta \in \mathcal{E}$ ricavata da α in maniere che ora andiamo a descrivere, da un punto di vista dell'imprimitività.

Una prima operazione che possiamo effettuare è quella di riordinare i rappresentanti delle classi laterali sinistre di H in G, ossia compiere un rimescolamento all'interno del primo blocco della segnatura α. Quella che otteniamo altro non è che una nuova segnatura logaritmica trasversale β di G che, presa $\tau \in \mathscr{S}_\lambda$, è definita settando $\beta[2, x_2] := \alpha[2, x_2]$ per ogni $x_2 \in \mathbb{Z}_\mu$ e $\beta[1, x_1] := \alpha[1, x_1\tau]$ per ogni $0 \leq x_1 \leq \lambda - 1$. Quindi, dato

$x \in \mathbb{Z}_{\lambda\mu}$ e decomposto con la knapsack transformation in $x = x_1 + \lambda x_2$ con $(x_1, x_2) \in \mathbb{Z}_\lambda \times \mathbb{Z}_\mu$ si ha che

$$x\hat{\beta} = \beta[2, x_2]\,\beta[1, x_1] = \alpha[2, x_2]\,\alpha[1, x_1\tau]$$

In altre parole, $x\hat{\beta} = (x\check{\tau})\hat{\alpha}$, dove $x\check{\tau} = (x_1+\lambda x_2)\check{\tau} := x_1\tau+\lambda x_2$ e quindi $\hat{\beta} = \check{\tau}\circ\hat{\alpha}$. Si badi che la funzione $\check{\tau}$ agisce come permutazione su $\mathbb{Z}_{\lambda\mu}$ e non è una funzione derivata da una segnatura logaritmica trasversale come $\hat{\alpha}$ e $\hat{\beta}$, che operano da $\mathbb{Z}_{\lambda\mu}$ su G. É per questo motivo che è stata contrassegnata con il simbolo *check* ($\check{}$) invece che con quello *hat* ($\hat{}$). Si vede che le trasformazioni del tipo $\check{\tau}$, agendo su $\mathbb{Z}_{\lambda\mu}$ rispettano un sistema di blocchi ben preciso, dato da

$$B_{x_1} = \{x_1 + \lambda x_2 : x_2 \in \mathbb{Z}_\mu\}$$

al variare di $x_1 \in \mathbb{Z}_\lambda$, e si nota che $\hat{\alpha} \circ \hat{\beta}^{-1} = \hat{\alpha} \circ \hat{\alpha}^{-1} \circ \check{\tau}^{-1} = \check{\tau}^{-1} \in \hat{\mathcal{E}}_\alpha$ e dunque $(\check{\tau}^{-1})^{-1} = \check{\tau} \in \langle\hat{\mathcal{E}}_\alpha\rangle$. Possiamo a questo punto dimenticarci di α e β e considerare solo le mappe $\check{\tau}$ che operano come definito sopra, e che chiamiamo *permutazioni blocco a blocco* in riferimento al sistema di blocchi B_i.

Il secondo tipo di operazioni che possiamo effettuare sulla segnatura logaritmica trasversale α si realizza all'interno di una singola classe laterale sinistra di H in G, e consiste nel sostituire il rappresentante di tale classe con un altro elemento della stessa. Formalmente, scelto un elemento del primo blocco della segnatura logaritmica trasversale α, diciamo $\alpha[1, z_0]$ per qualche $z_0 \in \mathbb{Z}_\lambda$, e un elemento $h \in H$, una nuova segnatura logaritmica trasversale β di G è ottenuta definendo $\beta := \alpha$ dappertutto tranne che $\beta[1, z_0] := h \cdot \alpha[1, z_0]$. Pertanto abbiamo che $x\hat{\beta} = x\hat{\alpha}$ sempre eccetto quando $x = z_0 + \lambda x_1$ nel cui caso si ha

$$x\hat{\beta} = \beta[2, x_2]\,\beta[1, z_0] = \alpha[2, x_2]\,(h \cdot \alpha[1, z_0]) = (\alpha[2, x_2] \cdot h)\,\alpha[1, z_0]$$

Ora, dato un gruppo H, l'omomorfismo di gruppi $H \to \mathscr{S}_H$ dato da $h \mapsto (k \mapsto k \cdot h)$ è chiamato *rappresentazione regolare* di H. Chiamiamo $\tau_h \in \mathscr{S}_\mu$ la permutazione di $\mathbb{Z}_\mu$ indotta dall'immagine di h sotto la rappresentazione regolare, mediante la biiezione tra $\mathbb{Z}_\mu$ e H data dal secondo blocco di α. Più concretamente, per $x_2 \in \mathbb{Z}_\mu$, scriviamo $\alpha[2, x_2] \cdot h = \alpha[2, x_2\tau_h]$ per cui la scrittura precedente diventa $x\hat{\beta} = \alpha[2, x_2\tau_h]\,\alpha[1, z_0]$. In questa configurazione, si ha che $\hat{\beta} = \check{\tau}_{z_0,h} \circ \hat{\alpha}$, dove $\check{\tau}_{z_0,h}$ è l'identità su tutti i blocchi tranne che sul blocco B_{z_0}, su cui lavora producendo $(z_0+\lambda x_2)\check{\tau}_{z_0,h} := z_0+\lambda(x_2\tau_h)$. Chiara mente $\hat{\alpha} \circ \hat{\beta}^{-1} = \hat{\alpha} \circ \hat{\alpha}^{-1} \circ \check{\tau}_{z_0,h}^{-1} = \check{\tau}_{z_0,h}^{-1} \in \hat{\mathcal{E}}_\alpha$ e dunque $(\check{\tau}_{z_0,h}^{-1})^{-1} = \check{\tau}_{z_0,h} \in \langle\hat{\mathcal{E}}_\alpha\rangle$. Chiamiamo questo genere di mappe *permutazioni regolari* del blocco B_{z_0}. Per la costruzione esposta, anche queste mappe rispettano il sistema di blocchi B_i.

Il terzo e ultimo tipo di operazioni attuabili su segnature logaritmiche trasversali interviene quando costruiamo la nuova segnatura logaritmica trasversale β permutando il secondo blocco $\alpha[2, x_2]$ della segnatura α. Di fatto β è definita ponendo $\beta[1, x_1] := \alpha[1, x_1]$ per ogni $x_1 \in \mathbb{Z}_\lambda$ e ponendo

$\beta[2, x_2] := \alpha[2, x_2\rho]$ dove $\rho \in \mathscr{S}_\mu$. Questo comporta che

$$x\hat{\beta} = \beta[2, x_2]\,\beta[1, x_1] = \alpha[2, x_2\rho]\,\alpha[1, x_1]$$

e, come nei casi precedenti, questa costruzione porta alla trasformazione $x\hat{\beta} = (x\check{\rho})\hat{\alpha}$, dove $x\check{\rho} = (x_1 + \lambda x_2)\check{\rho} := x_1 + \lambda(x_2\rho)$ e quindi $\hat{\beta} = \check{\rho} \circ \hat{\alpha}$. Come nei casi precedenti, quello che otteniamo è che $\hat{\alpha} \circ \hat{\beta}^{-1} = \hat{\alpha} \circ \hat{\alpha}^{-1} \circ \check{\rho}^{-1} = \check{\rho}^{-1} \in \hat{\mathcal{E}}_\alpha$ e dunque $(\check{\rho}^{-1})^{-1} = \check{\rho} \in \langle \hat{\mathcal{E}}_\alpha \rangle$. Le mappe di questo genere sono dette *permutazioni diagonali* e rispettano ancora una volta il sistema di blocchi B_i.

La verifica del fatto che il gruppo generato dall'insieme contenente le trasformazioni dei tre tipi appena illustrati agisce transitivamente su $\mathbb{Z}_{\lambda\mu}$ è un semplice esercizio ed è lasciato al lettore. Inoltre, per quanto evidenziato per ogni tipo di trasformazione, si ha che tale gruppo è anche imprimitivo su $\mathbb{Z}_{\lambda\mu}$ in quanto preserva il sistema di blocchi B_i.

3.3 La dimostrazione del teorema

In questa sezione finale proviamo il Teorema 3.2 enunciato nella prima sezione di questo capitolo. Ci sarà necessario ricordare alcuni risultati di Teoria dei Gruppi, ma li citeremo e discuteremo nel momento del loro intervento.

Dimostrazione. Il primo passo della prova consiste nel mostrare che il gruppo $\langle \hat{\mathcal{E}}_\alpha \rangle$ agisce 2-transitivamente su $\mathbb{Z}_{\lambda\mu}$. Per farlo, consideriamo un sottogruppo non banale H di G e consideriamo la costruzione fatta nella sezione immediatamente precedente. Come già sottolineato, questo passo è lecito in quanto il gruppo G non è banale e non è ciclico di orgine un primo, e quindi ammette per il Teorema di Cauchy un sottogruppo non banale (è sufficiente prendere un divisore non banale di $|G|$ per generarlo).

Consideriamo quindi $(x, y), (z, w) \in \mathbb{Z}_{\lambda\mu} \times \mathbb{Z}_{\lambda\mu}$ con $x \neq y$ e $z \neq w$ e mostriamo che esiste una permutazione di $\langle \hat{\mathcal{E}}_\alpha \rangle$ che porta x in z e y in w. Distinguiamo alcuni casi.

Se x e x' sono in blocchi differenti e y e y' sono anch'essi in blocchi differenti, prima di tutto applichiamo una permutazione blocco a blocco che porta x nello stesso blocco di y e x' nello stesso blocco di y'. Continuando a usare gli stessi nomi degli elementi al posto delle loro immagini sotto questa permutazione per non appesantire troppo la notazione, possiamo applicare una permutazione regolare all'interno del blocco di x e y che porta x in y, e una all'interno del blocco di di x' e y' che porta x' in y'. Chiaramente la composizione di queste funzioni sta in $\langle \hat{\mathcal{E}}_\alpha \rangle$.

Se invece x e x' sono nello stesso blocco B e y e y' sono nello stesso blocco C, per prima cosa applichiamo una permutazione blocco a blocco che muove B in C e poi applichiamo all'interno del blocco in cui ora giacciono x, y, x', y' una permutazione diagonale (l'insieme delle quali è tutto il gruppo simmetrico su ogni blocco, per costruzione) che porta x in y e x' in y'. Anche in questo caso la composizione di queste funzioni sta in $\langle \hat{\mathcal{E}}_\alpha \rangle$.

L'ultimo caso che rimane da provare è quello in cui x e x' sono nello stesso blocco B mentre y e y' sono in blocchi differenti. Chiaramente, non possiamo pretendere di riuscire a risolvere questo caso utilizzando solo le trasformazioni dei tre tipi fin'ora utilizzati, in quanto arriveremmo ad avere che il gruppo generato dall'insieme contenente tali trasformazioni è contemporaneamente imprimitivo e 2-transitivo, assurdo tenuto conto della Proposizione 1.23. Comunque, per sbrogliare questa situazione, è sufficiente trovare una permutazione di $\langle \hat{\mathcal{E}}_\alpha \rangle$ che fissa x' e muove x fuori da B, in modo tale da ricondursi al primo caso considerato. Applicando una permutazione blocco a blocco seguita da una permutazione diagonale possiamo supporre quindi che $B = B_0 = \{0 + \lambda x_2 : x_2 \in \mathbb{Z}_\mu\}$ e che $x' = 0$. Ricordiamo ora la scelta compiuta sulla segnatura α: avendo presente la sua natura, si ha che la classe laterale sinistra $H\alpha[1,0]$ è esattamente H, e $x'\hat{\alpha} = 0\hat{\alpha} = id_G$. Invece $x\hat{\alpha}$ sarà un certo $\tilde{h} \in H$. Consideriamo ora un altro sottogruppo proprio non banale K di G diverso da H, e consideriamo un'altra segnatura logaritmica trasversale β con riferimento alla catena $\{1\} < K < G$ e tale che $\beta[1,0] = \beta[2,0] = id_G$. Siano B'_i i blocchi relativi a β.

Anzitutto ci chiediamo se questo passaggio sia legittimo o meno. Si nota che poiché G è non banale, non ciclico di ordine un primo o il quadrato di un primo, esso ha sempre almeno due sottogruppi propri, distinti e non banali. Infatti, se l'ordine non è una potenza di un primo, allora esso sarà divisibile per due primi distinti q ed r che per il Teorema di Cauchy origineranno due sottogruppi propri, distinti e non banali, fra l'altro di ordine differente. Se invece l'ordine è una potenza di un primo p, ovvero p^k con $k \geq 3$, si ha che anche in questo caso esistono due sottogruppi propri, distinti e non banali: uno è quello di ordine p garantito ancora una volta dal Teorema di Cauchy, e l'altro ci è garantito dalla teoria dei gruppi di Sylow (reperibile in [4]), in cui si mostra un risultato che afferma che ogni gruppo di ordine p^k ha sottogruppi propri non banali di ordine p^i per ogni $0 < i < k$. Quindi, se $k \geq 3$, troviamo certamente due sottogruppi propri, distinti e non banali di ordine differente (per esempio in corrispondenza degli ordini p e p^{k-1}). L'unico caso non contemplato è quello in cui si ha $k = 2$. Qui usiamo l'ipotesi su G di non essere ciclico di ordine il quadrato di un primo: se così fosse, per la teoria sui gruppi ciclici sapremmo che c'è uno e un solo sottogruppo per ogni divisore dell'ordine, quindi l'unica catena possibile sarebbe $\{1\} < \langle g \rangle < G$ per qualche $g \in G$ di ordine p e non esisterebbe quindi un altro sottogruppo intermedio. Quindi, escluso questo caso, si ha che nel gruppo non ciclico G di ordine p^2 esiste, nuovamente per il Teorema di Cauchy, un elemento $h \in G$ di ordine p. Definiamo $H := \langle h \rangle$ e prendiamo un elemento qualsiasi $k \in G \setminus H$, che chiaramente non avrà ordine né 1 né p^2, poiché altrimenti sarebbe o l'unità (che stava già in H) oppure sarebbe un elemento che genera tutto G e quindi esso sarebbe ciclico. Dunque l'unica possibilità per k è che abbia ordine p e dunque $K := \langle k \rangle$ è un altro sottogruppo proprio, non banale di G e distinto da H. In effetti si vede che se ci troviamo nella situazione in cui tutti i sottogruppi propri di un gruppo non ciclico hanno lo stesso ordine o, allora o è un primo e il gruppo è un

o-gruppo elementare abeliano di ordine o^2.

In accordo con quanto appena esaminato, distinguiamo due casi. Supponiamo prima che G abbia due sottogruppi propri H e K tali che, senza perdita di generalità, $|H| < |K|$. Segue che $|B'_i| = |K| > |H| = |B_0|$ per ogni i. Tornando a considerare $\tilde{h} \in H$, se $\tilde{h} \in K$, sicché $\tilde{h}\hat{\beta}^{-1} \in B'_0$, possiamo modificare β mediante una permutazione diagonale, ottenendo una nuova segnatura logaritmica che chiamiamo con lo stesso nome β e che preservi ancora la condizione $0\hat{\beta} = id_G$, ma tale che $\tilde{h}\hat{\beta}^{-1} \notin B_0$, in quanto $|B_0| < |B'_0|$. Quindi in questo caso la permutazione di $\langle\hat{\mathcal{E}}_\alpha\rangle$ che fissa $x' = 0$ e muove x fuori da B_0 è data da $(\hat{\alpha}\circ\hat{\beta}^{-1})$ in quanto $0(\hat{\alpha}\circ\hat{\beta}^{-1}) = id_G\hat{\beta}^{-1} = 0$ e $x(\hat{\alpha}\circ\hat{\beta}^{-1}) = \tilde{h}\hat{\beta}^{-1} \notin B_0$ proprio per costruzione.

Nel caso in cui H e K siano invece sottogruppi propri, non banali, distinti ma di ordine uguale, abbiamo che i due sistemi di blocchi che a essi corrispondono sono tali che $B_i = B'_i$ per ogni i. Visto che l'intersezione dei due gruppi è banale ossia $H \cap K = \{1\}$, si ha che $\tilde{h} \notin K$, sicché $\tilde{h}\hat{\beta}^{-1} \notin B_0$ e la permutazione di $\langle\hat{\mathcal{E}}_\alpha\rangle$ cercata è di nuovo $(\hat{\alpha}\circ\hat{\beta}^{-1})$ per costruzione.

Questo chiude la prima parte della dimostrazione, dal momento che abbiamo provato che $\langle\hat{\mathcal{E}}_\alpha\rangle$ è 2-transitivo su $\mathbb{Z}_{|G|}$.

Per chiudere definitivamente la dimostrazione, dobbiamo destreggiarci utilizzando un paio di escamotage interessanti sulle permutazioni. Ricordiamo che, dato un gruppo G, è possibile definire su di esso la relazione di *coniugio*, mediante $a\,R\,b \Leftrightarrow \exists\, x \in G : b = x^{-1}ax$. Si vede facilmente che tale relazione è di equivalenza; il *coniugato di a mediante x* è l'elemento di G definito da $a^x := x^{-1}ax$. Il coniugio nel caso in cui G sia un gruppo di permutazioni ha una proprietà abbastanza utile e interessante, la cui verifica è lasciata per esercizio a tutti gli appassionati: se σ è una permutazione di G e $(a_1\ a_2\ \ldots\ a_k)$ è un k-ciclo di G, allora $(a_1\ a_2\ \ldots\ a_k)^\sigma = \sigma^{-1}(a_1\ a_2\ \ldots\ a_k)\sigma = (a_1\sigma\ a_2\sigma\ \ldots\ a_k\sigma)$.

Distinguiamo a questo punto due casi. Se $|G|$ è pari allora, usando per l'ennesima volta il Teorema di Cauchy, G ammette un sottogruppo H di ordine 2. Quindi, rispetto alla torre $\{1\} < H < G$, si ha che le mappe che abbiamo chiamato permutazioni regolari sono in realtà trasposizioni in $\langle\hat{\mathcal{E}}_\alpha\rangle$. Pertanto $\langle\hat{\mathcal{E}}_\alpha\rangle$ contiene almeno una trasposizione. In realtà le contiene tutte, dal momento che $\langle\hat{\mathcal{E}}_\alpha\rangle$ è 2-transitivo su $\mathbb{Z}_{|G|}$. Infatti, supponiamo che la trasposizione che sappiamo stare in $\langle\hat{\mathcal{E}}_\alpha\rangle$ sia $(i\ j)$ e prendiamo una qualsiasi altra trasposizione $(k\ l)$. Per la 2-transitività sappiamo che in $\langle\hat{\mathcal{E}}_\alpha\rangle$ esiste una permutazione σ che manda i in k e j in l, dunque coniugando $(i\ j)$ con σ si ha $(i\ j)^\sigma = (i\sigma\ j\sigma) = (k\ l) \in \langle\hat{\mathcal{E}}_\alpha\rangle$. A questo punto, visto che $\langle\hat{\mathcal{E}}_\alpha\rangle$ contiene tutte le permutazioni, allora esso coincide banalmente con tutto $\mathscr{S}_{|G|}$.

Se invece $|G|$ è dispari, vogliamo dimostrare che $\langle\hat{\mathcal{E}}_\alpha\rangle$ contiene un 3-ciclo. Partiamo dal considerare una permutazione diagonale σ che agisce contemporaneamente su ogni blocco come una trasposizione $(a\ b)$ per opportuni a e b in ogni blocco. Essa sarà quindi un prodotto di trasposizioni disgiunte. Fissiamo poi un blocco B e consideriamo quella permutazione regolare π di B indotta da quel particolare elemento $h \in H$ tale che $\pi = (a\ b\ c\ \ldots)$

per qualche $c \in B$ Ora, coniugando σ con π otteniamo la permutazione $\sigma^\pi = \pi^{-1}\sigma\pi$ appartenente a $\langle\hat{\mathcal{E}}_\alpha\rangle$ che è la trasposizione $(a\ b)$ su tutti i blocchi eccetto B, dove è $(a\ b)^{(a\ b\ c\ \ldots)} = (b\ c)$. Infine, componendo $\sigma^\pi\sigma$ otteniamo una permutazione che si comporta come l'identità su tutti i blocchi eccetto B, dove è il 3-ciclo cercato $(b\ c)(a\ b) = (a\ b\ c)$. Sulla falsa riga del caso precedente, mostriamo ora che in realtà $\langle\hat{\mathcal{E}}_\alpha\rangle$ contiene tutti i possibili 3-cicli. Sia dunque $(a\ b\ c)$ un generico 3-ciclo, e $(x\ y\ z)$ il 3-ciclo che sappiamo appartenere a $\langle\hat{\mathcal{E}}_\alpha\rangle$. Per 2-transitività sappiamo che $\exists\,\rho \in \langle\hat{\mathcal{E}}_\alpha\rangle$ tale che $x\rho = b$, $y\rho = a$ e $z\rho = d$ per qualche $d \in \mathbb{Z}_{\lambda\mu}$. Inoltre, sempre per 2-transitività, sappiamo anche che $\exists\,\sigma \in \langle\hat{\mathcal{E}}_\alpha\rangle$ tale che $x\sigma = b$, $y\sigma = c$ e $z\sigma = e$ per qualche $e \in \mathbb{Z}_{\lambda\mu}$. Coniugando opportunamente si ha che $(x\ y\ z)^\rho = (x\rho\ y\rho\ z\rho) = (b\ a\ d) \in \langle\hat{\mathcal{E}}_\alpha\rangle$ e che $(x\ y\ z)^\sigma = (x\sigma\ y\sigma\ z\sigma) = (b\ c\ e) \in \langle\hat{\mathcal{E}}_\alpha\rangle$. Se per caso $d = e$ allora $(b\ c\ d)(b\ a\ d)^{-1} = (a\ b\ c) \in \langle\hat{\mathcal{E}}_\alpha\rangle$. Altrimenti, se $d \neq e$, si ha che $(b\ a\ d)^{(b\ c\ e)} = (c\ a\ d) \in \langle\hat{\mathcal{E}}_\alpha\rangle$ e di conseguenza $(b\ a\ d)^{-1}(c\ a\ d) = (a\ b\ c) \in \langle\hat{\mathcal{E}}_\alpha\rangle$. Da ciò segue che $\langle\hat{\mathcal{E}}_\alpha\rangle$ è un sottogruppo di $\mathscr{S}_{|G|}$ contenente $\mathscr{A}_{|G|}$, quindi $\langle\hat{\mathcal{E}}_\alpha\rangle = \mathscr{A}_{|G|}$ oppure $\langle\hat{\mathcal{E}}_\alpha\rangle = \mathscr{S}_{|G|}$. É sufficiente accorgersi che $\langle\hat{\mathcal{E}}_\alpha\rangle$ contiene una permutazione dispari per concludere che $\langle\hat{\mathcal{E}}_\alpha\rangle = \mathscr{S}_{|G|}$.

□

Conclusioni

Giunto a queste pagine di epilogo e dovendo quindi tirare un po' le fila di tutto quanto il lavoro svolto, quello che più mi preme sottolineare e con cui mi piacerebbe chiudere questo elaborato può essere riassunto all'insegna di tre aggettivi che appieno descrivono il percorso maturato: *stimolante*, *concreto* e *insolito*.

Stimolante in quanto per tutta la durata del lavoro, comprensivo di studio delle fonti e battitura della tesi, ho sempre avuto la sensazione di star imparando qualcosa di affascinante, qualcosa di stuzzicante per quella parte della mia mente che non si accontenta di fermarsi in superficie, insomma qualcosa che sapevo sarei riuscito a far totalmente mio.

Concreto perché a questo punto del mio cammino – seppur breve – di matematico, credo sia necessario fare una scelta e prendere una decisione sulla strada da imboccare e su cui proseguire. Addentrarsi in modo più radicale nel mondo dell'algebra avanzata e prettamente teorica o muoversi verso il dominio delle applicazioni? Io ho scelto la seconda opzione, e questa trattazione ne è prova: dopo tre anni passati ad imparare le regole del gioco, ho ritenuto opportuno iniziare a giocare, a maneggiare gli oggetti algebrici che fino a prima di questa circostanza sono sempre rimasti sul piano dell'astrazione come sterili protagonisti di definizioni e proposizioni ma che mai sono stati visti all'opera.

Insolito per un semplice motivo, che trapela in particolare nell'ultimo capitolo della tesi: per quel che mi riguarda (e che, in realtà, riguarda anche un paio di amici e colleghi di università) è stato davvero molto inusuale ritrovarsi a dover studiare e approfondire una pubblicazione del proprio docente di Algebra, lo stesso che ti ha insegnato delle banalità come cosa siano gruppi e anelli e sul quale ti sei sempre posto la domanda: su cos'è che fa ricerca, in realtà? Ecco quindi una possibile risposta, che sfocia poi in una riflessione più ampia sul ruolo del ricercatore, su come in verità il mondo sia pieno di nuove sfide da scoprire e controversie da risolvere e su come in settori pionieristici e di nicchia come quello affrontato ci si possa specializzare a tal punto da dimostrare veri e propri teoremi, come appunto è riuscito il Professor Caranti.

Un ultimo punto su cui volevo fare chiarezza è quello per cui mi si potrebbe contestare il fatto di non aver approfondito più di tanto alcune dimostrazioni costruttive o aver dato per assodato proprietà fondamentali (per dirne una, la possibilità di testare l'appartenenza a un gruppo di permutazioni in tempo polinomiale). Quello che tengo a precisare è che, dopo tutto, si tratta di una tesi di laurea in Matematica e per questo ho ritenuto più importante mettere in luce le questioni algebriche rispetto a quelle pseudo-informatico, computazionali e algoritmiche, di cui comunque ho riportato le referenze in bibliografia.

Per chiudere definitivamente, ci tengo a ringraziare i miei genitori Lina e Gianfranco, che di fatto hanno permesso tutto ciò; mio fratello Stefano, per la sua curiosità e per aver sempre avuto il consiglio pronto; i miei compagni di università, per avermi dato preziose dritte per la comprensione di alcuni argomenti in tutti questi anni; *dulcis in fundo* la mia fidanzata Chiara, per aver creduto in me e avermi sempre dato la forza per affrontare nuove sfide.

Bibliografia

[1] S. S. Magliveras & N. D. Memon, *Algebraic properties of cryptosystem* PGM, J. Cryptology 5 (1992), no. 3, 167-183.

[2] S. S. Magliveras, D. R. Stinson & Tran van Trung, *New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups*, J. Cryptology 15 (2002), no. 4, 285-297.

[3] A. Caranti & F. Dalla Volta, *The round functions of cryptosystem* PGM *generate the symmetric group*, Des Codes Crypt 38 (2006), 147-155.

[4] A. Caranti, *Alcune note per un corso di Teoria dei Gruppi*, disponibile a `http://www.science.unitn.it/~caranti/Didattica/Gruppi/static/Note/Note_Gruppi.pdf`.

[5] M. Furst, J. Hopcroft & L. Eugene, *Polynomial-time algorithms for permutation groups*, Proceedings of the 21st IEEE Symposium on Foundations of Computer Science (1980), 36-41.

[6] A. Languasco, A. Zaccagnini, *Manuale di Crittografia*, Ulrico Hoelpi Editore (2015), 1-36.

[7] D. Riechl, *Group factorisations and cryptology*, Ph.D. thesis (2015), University of Tübingen, 40-44, disponibile a `https://bibliographie.uni-tuebingen.de/xmlui/bitstream/handle/10900/65399/Dissertation_DominikReichl.pdf?sequence=1&isAllowed=y`.