Il presente volume è stato pubblicato con il contributo dell'Alma Mater Studiorum Università degli Studi di Bologna e del Centro interdipartimentale di ricerca in Storia del diritto, Filosofia e Sociologia del diritto e Informatica giuridica "A. Gaudenzi – G. Fassò"

Michele Martoni

Firme elettroniche

profili informatico-giuridici

www.aracneeditrice.it
info@aracneeditrice.it

via Raffaele Garofalo, 133/A–B
00173 Roma
(06) 93781065

isbn 978–88–548–3652–5

I edizione: novembre 2010

a Eleonora e Margherita

Quando il tempo è maturo per certe cose, queste appaiono in diversi luoghi, proprio come le violette sbocciano dappertutto quando comincia la primavera.

Farkas Bolyai, *1830*

Indice

Prefazione

di Monica Palmirani

Dopo oltre dieci anni dalla nascita della firma digitale in Italia ancora tale argomento anima il dibattito scientifico, legislativo e dottrinale in modo assolutamente non artificioso ma guidato da una genuina necessità di raggiungere la quadratura del cerchio fra tecnologia, diritto e semplificazione applicativa. Questo controverso e fluido cammino, che pare debba presto vedere una nuova tappa con l'attesa emanazione delle modifiche al CAD, è dovuto essenzialmente a tre motivi.

Il primo risiede nel peccato originale con cui il diritto storicamente affronta l'utilizzo della tecnologia ossia con una metodologia *ex-post* invece che *ex-ante*, tentando di regolamentare l'introduzione del mezzo informatico ingabbiandolo spesso all'interno di processi organizzativi tradizionali e istituti giuridici sorti per la carta.

Il secondo motivo deve essere ricercato nella continua evoluzione tecnologica, evoluzione che sollecita nuove prospettive e quindi mette in crisi le regole poste in essere, che con lentezza vengono adeguate. Questo impedisce di fatto allo strumento giuridico di agire come volano dell'innovazione nella pubblica amministrazione e di liberare quelle potenzialità di semplificazione, razionalizzazione e miglioramento che invece gli strumenti tecnologici, se ben condotti anche sul lato organizzativo, sono in grado di produrre.

Il terzo aspetto risiede nell'insieme di applicazioni concrete che negli ultimi tre anni sono fiorite in ambito eGov accompagnate da un'analisi organizzativa, di processo e di servizio. L'esigenza di risolvere dei problemi fattuali ha portato a definire scenari nuovi neppure immaginati dal mondo giuridico e quindi non modellati nella normativa (e.g. il timbro digitale, le firme remote, le firme multiple, etc.).

Per questi motivi il presente elaborato affronta con energia nuova e con un approccio metodologico inconsueto la materia in oggetto, iniziando da una comprensione dei fenomeni tecnologici per poterne liberare tutta la potenza di azione mediante il corredo essenziale di un adeguato impianto normativo. Il ruolo del diritto in questa ottica è di creare una cassa di risonanza delle potenzialità inespresse dalla tecnologia, ipotizzando anzi tempo scenari nuovi e processi lavorativi ancora inesplorati.

Il presente elaborato non dimentica però la funzione contenitiva e regolativa del diritto, il quale deve nel contempo impedire usi illeciti o non appropriati del mezzo tecnologico, salvaguardare i principi fondanti il diritto, preservare l'identità dei documenti giuridici, evitare ogni abuso e distorsione da parte del nuovo *media* digitale.

L'analisi condotta quindi dall'Autore segue questa duplice funzione assegnata al diritto delle nuove tecnologie, propositiva e contenitiva, fornendo una lettura inedita della disciplina delle firme elettroniche alla luce anche dei molti casi che l'Autore ha avuto modo di affrontare e modellare nelle applicazioni concrete a servizio dell'eGov.

Introduzione

In quest'opera si affronterà il tema delle firme elettroniche. Rispetto all'attuale stato dell'arte si è, però, prescelto un diverso angolo prospettico.

Il corretto inquadramento dell'istituto delle firme elettroniche richiede di avviare la propria disamina dall'essenza tecnica del medesimo, per, poi, trarne le conseguenti implicazioni giuridiche. Le firme elettroniche sono, infatti, essenzialmente, applicazioni moderne e complesse della crittografia, scienza antica caratterizzata da una continua e rapida evoluzione.

L'analisi delle tecniche crittografiche condurrà, quindi, all'approfondimento delle implicazioni giuridiche che da esse discendono ed agli effetti che l'ordinamento attribuisce alle firme elettroniche.

In quest'ottica si procederà ad una ricostruzione in chiave storico-evolutiva dell'istituto. Ricorre, peraltro, proprio quest'anno, il tredicesimo anniversario dal riconoscimento, formale ed esplicito, della piena rilevanza giuridica della forma elettronica degli atti. Recitava, infatti, il comma 2 dell'art. 15 della legge 15 marzo 1997 che «*gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge*».

Prima di procedere oltre si ritiene doveroso chiarire la ragione che induce ad occuparsi di questi temi e della loro disciplina giuridica.

La motivazione deve individuarsi nel ruolo sempre maggiore che la "*rete*" riveste nelle relazioni interpersonali, il ruolo sempre maggiore assunto dall'identità digitale di ciascuno.

Il fatto che le relazioni interindividuali trovino, sempre più, la loro espressione in Internet rende imprescindibile per il legislatore – e, quindi, per lo studioso del diritto – addentrarsi negli elementi che determinano e caratterizzano dette interazioni.

L'efficacia ed il valore del documento informatico, l'identificazione della persona, le modalità di espressione della volontà, gli effetti a quest'ultima riconducibili, la riservatezza e la prote-zione del dato personale, sono soltanto alcuni dei temi che nelle nuove relazioni telematiche devono trovare una loro collocazione e definizione.

La normativa, per quanto qui in argomento, nel definire gli effetti ed il valore giuridico del documento informatico si sofferma sugli aspetti più strettamente tecnici che caratterizzano le diverse tipologie di firma elettronica, attribuendo uno specifico rilievo giuridico quale diretta conseguenza della diversa caratterizzazione tecnica.

Rebus sic stantibus, al fine di consentire una compiuta e non frammentaria comprensione del quadro giuridico in esame, si analizzeranno, innanzi tutto, le nozioni tecnologiche di base. Le quali consentiranno, pertanto, di meglio orientarsi nel contesto normativo che verrà, indi, secondariamente, e da ultimo, dettagliatamente illustrato.

Mi sia consentito spendere ancora poche righe per illustrare la scelta dell'immagine di copertina. L'Autore del dipinto con la propria opera vuole significare la soggettiva rappresentazione dell'identità individuale. Il tratto dell'Artista identifica, nel suo *animus*, un soggetto ben preciso e individuato, ancorché lo stesso non venga nominato. Il tratto impresso sulla tela, a sua volta, è tale da identificare univocamente colui che lo ha tracciato, ancorché l'Artista non abbia impresso la propria firma. Le nuove tecnologie, analogamente, mediante un'attività "di processo", sono oggi in grado di ricondurre ad una certa rappresentazione di dati, l'identità di una persona determinata. Di ciò si tratterà nel presente contributo, di come la tecnica possa ricondurre un segno, un dato, un processo, ad un soggetto preciso e di come, conseguentemente, i concetti tradizionali della teoria documentale giuridica debbano necessariamente evolversi e adattarsi a questa nuova epoca culturale.

Infine, ringrazio la prof.ssa Monica Palmirani, mia maestra e guida e il prof. Enrico Pattaro che costantemente mi sostiene nell'attività di ricerca.

Capitolo I

Dalla crittografia alle firme elettroniche

1.1. Premessa

Il corretto inquadramento dell'istituto delle firme elettroniche richiede di avviarne la disamina dalla sua essenza.

Le firme elettroniche altro non sono che applicazioni moderne e complesse della crittografia.

Si prenderanno, pertanto, in esame, ancorché in termini generali, le principali tecniche crittografiche. Ciò che condurrà a porre in risalto le implicazioni giuridiche che ne discendono e, più nello specifico, gli effetti che il legislatore ha attribuito alle firme elettroniche.

La nascita e l'evoluzione delle tecniche crittografiche trova il proprio *incipit* nei libri di storia antica: «*per migliaia di anni, re, regine e generali hanno avuto bisogno di comunicazioni efficienti per governare i loro paesi e comandare i loro eserciti* […] *essi compresero quali conseguenze avrebbe avuto la caduta dei loro messaggi in mani ostili* […] *fu il pericolo dell'intercettazione* […] *a promuovere lo sviluppo di codici e cifre, tecniche di alterazione del messaggio destinate a renderlo comprensibile solo alle persone autorizzate*»[1].

La crittografia, svolta la propria importante funzione storica, è oggi un fattore, consapevolmente o meno, del vivere comune.

Dati di ogni genere, quotidianamente, sono oggetto di comunicazione, di diffusione e di ogni altro tipo di trattamento.

---

[1] S. SINGH, Codici e segreti, Rizzoli, Milano 1999, p. IX.

Ogni giorno cresce l'esigenza che tali azioni siano trasparenti, sicure e riconducibili ad un soggetto determinato o determinabile. Si rende, sempre più, necessario identificare – direttamente o indirettamente – l'attore delle "transazioni".

La crittografia, anche per queste ragioni, è divenuta un importante strumento per la persona, per la sua tutela, per la sua privacy e per la sua corretta salvaguardia.

Scriveva Philip Zimmermann[2]: «*se la privacy diviene fuorilegge, solo i fuorilegge avranno la privacy. I servizi segreti hanno accesso a buone tecniche crittografiche. Così come i grandi trafficanti di droga e di armi. Così come industrie del settore difesa, compagnie petrolifere o altri colossi finanziari. Ma la gente comune e le organizzazioni politiche nascenti non hanno mai avuto accesso a tecnologie crittografiche a chiave pubblica di livello militare. Non fino ad ora. PGP permette alla gente di avere la loro privacy a portata di mano. C'è un bisogno sociale crescente di questo. Ecco perché l'ho scritto*»[3].

---

[2] Philip Zimmermann, come pubblicato nel suo sito personale, è il creatore di: «*Pretty Good Privacy, an email encryption software package. Originally designed as a human rights tool, PGP was published for free on the Internet in 1991. This made Zimmermann the target of a three-year criminal investigation, because the government held that US export restrictions for cryptographic software were violated when PGP spread worldwide. Despite the lack of funding, the lack of any paid staff, the lack of a company to stand behind it, and despite government persecution, PGP nonetheless became the most widely used email encryption software in the world. After the government dropped its case in early 1996, Zimmermann founded PGP Inc. That company was acquired by Network Associates Inc (NAI) in 1997, where he stayed on for three years as Senior Fellow. In 2002 PGP was acquired from NAI by a new company called PGP Corporation, where Zimmermann served as special advisor and consultant until its acquisition by Semantec in 2010. Zimmermann currently is consulting for a number of companies and industry organizations on matters cryptographic, and is also a Fellow at the Stanford Law School's Center for Internet and Society. He was a principal designer of the cryptographic key agreement protocol for the Wireless USB standard. His latest project is Zfone, which provides secure telephony for the Internet. Before founding PGP Inc, Zimmermann was a software engineer with more than 20 years of experience, specializing in cryptography and data security, data communications, and real-time embedded systems. His interest in the political side of cryptography grew out of his background in military policy issues. Zimmermann has received numerous technical and humanitarian awards for his pioneering work in cryptography*», in www.philzimmermann.com, visitato il 20 agosto 2010.

[3] P. ZIMMERMANN, Why I wrote PGP, in www.philzimmermann.com, visitato il 30 agosto 2010.

1.2. Terminologia ed evoluzione

Lo studio approfondito delle tecniche crittografiche richiede, innanzi tutto, di soffermarsi sul lessico generalmente utilizzato in questo contesto scientifico.

La "crittologia" è definita come la scienza che studia le scritture segrete. La stessa ricomprende al proprio interno la "crittografia" e la "crittoanalisi".

La crittografia, in particolare, è rivolta all'implementazione di sistemi di protezione dei messaggi, mentre la crittoanalisi si concentra sui metodi per violare questi ultimi.

Nel parlare comune il termine crittografia è generalmente impiegato indifferentemente per indicare ambedue le scienze menzionate.

Il messaggio è, poi, indicato come "testo in chiaro" (*plain* o *clear text*).

Il messaggio che ha subito il procedimento crittografico viene, invece, denominato "testo cifrato" (*cipher text*).

Il procedimento inverso alla cifratura può essere differentemente rubricato come "decifrazione" o come "decrittazione".

Con il primo termine si indica l'operazione posta in essere sfruttando la trasformazione inversa che muta il testo da cifrato a chiaro.

Con il secondo termine si indica, invece, l'attività di violazione, di forzatura del sistema, tecnicamente, di rottura del cifrario.

Una particolare tecnica di protezione del contenuto del messaggio è la "steganografia", dalle parole greche "*steganós*" che significa "coperto" e "*graphein*" che significa "scrivere".

Si tratta di una forma di comunicazione segreta basata sull'occultamento "fisico" del messaggio.

Il limite intrinseco della steganografia è la perdita, o quanto meno il grave pregiudizio, della segretezza del messaggio nell'ipotesi in cui lo stesso sia intercettato.

È per tale ragione che, in parallelo allo sviluppo della steganografia, si è assistito alla nascita della crittografia, dal greco *kriptós* che significa "nascosto". La crittografia non mira a nascondere fisicamente il messaggio, ad occultarlo, ma a celarne il contenuto – che, quindi, per l'effetto, è visibile ma non comprensibile – mediante un procedimento prefissato ed invertibile.

Il crittoanalista pur intercettando il messaggio non sarà in grado di accedere al contenuto se non mediante il procedimento inverso di alterazione.

Proseguendo la disamina, la crittografia può essere suddivisa in due distinte categorie: la crittografia *trasposizionale* e la crittografia *sostitutiva*.

La tecnica trasposizionale prevede che le lettere del messaggio siano mutate di posizione secondo un schema predefinito. Vi sono diverse tipologie di metodi trasposizionali. Tutti ubbidiscono ad un criterio che consente la cifratura del messaggio e la successiva decifratura.

Un esempio storico ed autorevole di crittografia trasposizionale è la "scitale spartana" risalente al V secolo a.C. La scitale (asta lignea) consisteva in un cilindro attorno al quale veniva arrotolata una striscia di pelle. Il mittente scriveva un messaggio sulla striscia avvolta attorno al cilindro, quindi svolgeva la striscia. Il destinatario poteva comprendere il testo del messaggio solo avvolgendo la striscia di pelle attorno ad un cilindro del medesimo diametro.

Diversa dalla trasposizione è la cosiddetta "sostituzione alfabetica" che si ottiene abbinando alle lettere dell'alfabeto le lettere di un diverso alfabeto, individuato *ad hoc*, e sostituendo a ciascuna lettera del testo (formulato con il primo alfabeto) quella corrispondente in base al predetto accoppiamento[4].

Il metodo sostitutivo comporta, quindi, la determinazione di un "alfabeto cifrante", da utilizzarsi per la sostituzione delle lettere dell'alfabeto comunemente impiegato.

Qualunque scrittura segreta può essere analizzata in termini di metodo crittografico generale (algoritmo) ed in termini di chiave. Se si considera ad esempio il *De bello gallico*, l'algoritmo prescrive che ogni lettera dell'alfabeto chiaro sia sostituita da una lettera dell'alfabeto cifrante e che l'alfabeto cifrante consista in una riorganizzazione dell'alfabeto chiaro. La chiave consiste nell'alfabeto cifrante da impiegare[5].

---

[4] Giulio Cesare nel *De bello gallico* racconta l'applicazione del metodo sostitutivo (cosiddetta sostituzione di Cesare).

[5] La netta separazione concettuale fra chiave ed algoritmo è un cardine della crittografia ed è nota come Principio di Kerckhoffs (1883). In base a quest'ultimo, l'affidabilità di un si-

Illustrato il concetto di crittografia si impone ora di prendere in esame la cosiddetta "crittoanalisi".

«*Si può ben dubitare che l'ingegno umano sia mai capace di costruire un enigma di questo tipo* [un crittogramma] *tale che l'ingegno umano stesso non possa, applicandovisi appropriatamente, risolverlo*»[6].

La crittoanalisi è la scienza dell'interpretazione di un messaggio di cui si ignora la chiave per l'accesso al contenuto in chiaro. La "chiave crittografica" è l'elemento che consente di trasformare il testo (da *cipher* a *clear* e/o viceversa).

I crittografi hanno l'obiettivo di implementare i sistemi per la scrittura segreta mentre i crittoanalisti, come dianzi osservato, operano per individuarne le vulnerabilità.

È una costante rincorsa che, in ultima analisi, conduce alla realizzazione di sistemi sempre più sicuri.

Tra i crittoanalisti spiccarono gli arabi. Nell'XI secolo lo studioso al-Kindī[7] individuò, infatti, il punto debole della crittografia (con sostituzione monoalfabetica) basata sul summenzionato metodo sostitutivo[8]. In un breve passaggio della sua opera *Sulla decifrazione dei messaggi crittati* l'Autore riporta il procedimento applicato: «*Un modo di svelare un messaggio crittato, se conosciamo la lingua dell'originale, consiste nel trovare un diverso testo chiaro nella stessa lingua, abbastanza lungo da poter calcolare la frequenza di ciascuna lettera. Chiamiamo "prima" quella che compare più spesso, "seconda" quella che la segue per frequenza, "terza" la successiva, e così via, fino ad esaurire tutte le lettere del campione di testo chiaro. Esaminiamo poi il testo in cifra che vogliamo interpretare, ordinando* [in base alla frequenza] *anche i suoi simboli. Troviamo il simbolo più comune, e rimpiazziamolo con la "prima" lettera dell'esempio chiaro; il*

---

stema crittografico deve essere fondata "non" sulla segretezza del metodo di cifratura utilizzato bensì sulla segretezza della chiave.

[6] E. A. POE, *Lo scarabeo d'oro*, Einaudi, Torino 2004 (1843).

[7] A. AL-KINDĪ, studioso arabo del IX secolo a.C. Si veda l'opera *Sulla decifrazione dei messaggi crittati*, ritrovata nel 1987 nell'archivio ottomano Sulaimaniyyah di Istanbul.

[8] Il punto debole della crittografia *monoalfabetica* è stato rintracciato nell'unicità dell'alfabeto cifrante. Ciò comportava che ad una certa lettera del testo in chiaro corrispondesse sempre una sola lettera del testo cifrante. Come si vedrà successivamente detto limite è stato superato grazie all'impiego della crittografia *polialfabetica*.

simbolo che lo segue per frequenza sia rimpiazzato dalla "seconda" lettera, il successivo simbolo più comune sia rimpiazzato dalla "terza", e così via, fino ad aver preso in considerazione tutti i simboli del crittogramma che intendevamo svelare».

Un tentativo di rinforzare la cifratura per sostituzione monoalfabetica portò all'introduzione di parole in codice.

Tra il 1460 ed 1470 fu essenziale la spinta innovativa portata dal Leon Battista Alberti. Egli propose di utilizzare non uno ma più alfabeti cifranti, sostituendoli durante la fase di cifratura.

Questa intuizione fu, poi, sviluppata dall'abate tedesco Johannes Trithenius (1462), dall'italiano Porta (1535) ed, infine, dal francese Vigenère[9] (1523), il quale ultimo la teorizzò nella cosiddetta "cifratura di Vigenère".

La cifratura di Vigenère postulava l'utilizzo di ventisei alfabeti cifranti per cifrare un solo messaggio (cosiddetta "cifratura polialfabetica").

I ventisei alfabeti prescelti venivano raccolti nella "tavola di Vigenère", nella quale, ad ogni riga, corrispondeva un diverso alfabeto determinato con una trasposizione (o *spostamento di Cesare*)[10].

Per comprendere quale riga utilizzare per la cifratura di una lettera, e quindi per la decifratura, poteva essere fissata una parola chiave con il compito di indicare la sequenza delle righe della tavola utilizzata.

La cifratura di Vigenère, rispetto ai metodi preesistenti, era estremamente più resistente alla crittoanalisi (ivi compresa l'analisi delle frequenze). Essa non riscosse però grande successo a causa della complessità del suo utilizzo. Per tale ragione si svilupparono maggiormente altri metodi monoalfabetici più semplici da impiegare[11].

Fra le cifrature monoalfabetiche della nuova generazione merita una menzione particolare la *Gran Cifra di Luigi XIV*. Ideata dai Ros-

[9] B. VIGENERE, *Traicté des Chiffres*, 1586.

[10] La tavola consiste in un alfabeto chiaro di ventisei lettere seguito da ventisei alfabeti cifranti, ciascuno spostato a sinistra di una lettera rispetto al precedente. Pertanto, la riga numero uno è rappresentata da un alfabeto cifrante con uno spostamento di Cesare pari a uno, e così via fino all'ultima riga, la ventiseiesima.

[11] Un esempio è rappresentato dalla "cifratura per sostituzione omofonica" che comporta la sostituzione di ogni lettera con più elementi cifranti il cui numero è determinato in modo proporzionale alla frequenza della lettera da sostituire.

signol[12], padre e figlio, era utilizzata per le comunicazione segrete del Re Sole. Essa è rimasta irrisolta fino al XIX secolo quando fu vinta dall'opera del crittoanalista Bazeries[13].

Nel XIX secolo ritroverà ampia applicazione la "tavola di Vigenère" e la cifratura polialfabetica, applicate in particolare alle prime comunicazioni moderne tramite telegrafo e con alfabeto *Morse*[14]. Il messaggio, nello specifico, veniva cifrato e poi convertito in codice *Morse*.

La decrittazione fece un notevole balzo in avanti nella gara contro la crittografia quando Charles Babbage (1854) scoprì il punto debole della cifratura di Vigenère.

«*Risolvere un crittogramma ben fatto è un po' come scalare una parete di roccia ripida e senza appigli: il crittoanalista deve sfruttare ogni minima crepa o asperità. Nella cifratura monoalfabetica si aggrappa alla frequenza delle lettere,* […] *In una cifratura polialfabetica alla Vigenère le differenze di frequenza sono drasticamente ridotte, perché la chiave è usata per mettere in gioco più alfabeti cifranti. Perciò, a prima vista la parete sembra liscia* […]»[15].

Nella tavola di Vigenère la stessa lettera è cifrata in modi diversi all'interno dello stesso messaggio. La stessa parola è cifrata in tanti modi diversi quante sono le lettere della parola chiave, se ad esempio la parola chiave è ROMA ogni lettera del testo chiaro sarà cifrata in quattro modi diversi. Se la parola cifrata compare più volte nel messaggio è molto probabile che vi siano delle ripetizioni[16].

Proprio queste ripetizioni rappresentarono l'appiglio che consentì a Babbage di scalare la tavola di Vigenère. Ufficialmente il merito di ta-

---

[12] Antoine e Bonaventure Rossignol (1626). Per un maggiore approfondimento si veda E. LERVILLE, *Les Cahiers secrets de la cryptographie*, Monaco, Ed. du Rocher, 1972.

[13] Etienne Bazeries, ufficiale del dipartimento crittografico dell'esercito francese. Si veda R. CANDELA, *The Military Cipher of Commandant Bazeries*, New York, Cardanus Press, 1938.

[14] L'alfabeto *Morse*, o meglio il codice *Morse*, è un alfabeto/codice alternativo ma *non* cifrante.

[15] S. SINGH, *op. cit.*, p. 67.

[16] In estrema sintesi il *test* era in primo luogo rivolto a determinare la chiave. A tal fine si ricercavano le stringhe uguali ripetute nel messaggio. Individuata la lunghezza della chiave si utilizzava il calcolo delle frequenze per determinare lo spostamento di Cesare. Fatto ciò la crittoanalisi era terminata ed il messaggio svelato.

le impresa fu riconosciuto a Friedrich Wilhelm Kasiski[17], ufficiale in pensione dell'esercito prussiano. Il metodo implementato da Babbage è per tale ragione noto come *test di Kasiski*.

Sul finire del XIX secolo la crittografia dovette affrontare un grave periodo di crisi. Babbage e Kasiski avevano minato la fiducia nella cifratura di Vigenère. I crittografi erano alla ricerca di un sistema in grado di ripristinare la sicurezza delle comunicazioni anche alla luce delle recenti invenzioni.

In particolare Guglielmo Marconi (1894) aveva iniziato i propri studi concernenti le comunicazioni radio. Fu proprio il fascino della radio, del nuovo sistema di comunicazione, che pose ancor più l'accento sulla necessità di un livello di sicurezza appropriato.

Questa esigenza fu particolarmente sentita nel corso della prima guerra mondiale.

Uno dei sistemi crittografici più forti del periodo fu l'ADFGVX. Sistema inaugurato il 5 marzo 1918 in occasione del tentativo tedesco di prendere Parigi. Tentativo sfumato proprio per opera della crittoanalisi, ed in particolare del crittoanalista George Painvin.

L'ADFGVX così come le altre cifrature del periodo consisteva in varianti o combinazioni dei metodi in uso nel secolo precedente. I principi di base erano, pertanto, noti e, dunque, i sistemi utilizzati non erano in grado di garantire una resistenza sufficiente agli attacchi crittoanalitici.

Mentre la guerra volgeva al termine il maggiore Mauborgne, capo delle ricerche crittografiche dell'esercito degli Stati Uniti, introdusse nelle procedure in atto l'impiego di "chiavi casuali" di crittografia, al fine di incrementare la sicurezza delle comunicazioni.

Questa nuova tecnica consisteva in una chiave formata da una serie di lettere in sequenza casuale da applicarsi al sistema di Vigenère. Il primo passo del metodo[18] di Mauborgne consisteva nel preparare una pila di fogli. Ciascun foglio conteneva una chiave diversa. La pila doveva essere realizzata in almeno due esemplari identici, uno per il mittente ed uno per il destinatario. I fogli e le relative chiavi dovevano essere utilizzati in sequenza, una chiave diversa per ogni messaggio fino

[17] F. W. KASISKI, *Die Geheimschriften und die Dechiffrir-kunst*, 1863.
[18] La cosiddetta "crittografia a blocco monouso".

all'esaurimento della pila.

Il sistema comportava una resistenza pressoché assoluta anche se i problemi pratici non ne consentirono la diffusione e l'utilizzo auspicati.

Dopo il primo conflitto mondiale la ricerca di nuovi sistemi di protezione proseguì giungendo nel 1918 alla creazione della macchina crittografica *Enigma*[19]. I vertici militari tedeschi commissionarono uno studio volto ad accrescere la sicurezza delle comunicazioni. Al termine di dette ricerche (1926) si decise di adottare la macchina Enigma inventata da Scherbius.

La macchina Enigma disponeva di diversi elementi combinati per formare un dispositivo elettromeccanico per la creazione di scritture cifrate. Il dispositivo consisteva in una serie di "scambiatori" e "rotatori", in una "unità scambiatrice" ed in un "pannello a prese multiple". La posizione, il setting, di questi componenti determinava la "chiave di cifratura". Nella versione predisposta per l'esercito i possibili settaggi e quindi le possibili chiavi di cifratura erano circa *dieci milioni di miliardi*!

Una volta accordatisi sui collegamenti del pannello, sull'anello, sull'ordine dei rotori e sul loro orientamento, e, quindi, una volta determinata la chiave, mittente e destinatario potevano crittare e decrittare i messaggi.

L'esercito aveva predisposto un blocco di chiavi, cosiddetto "cifrario". Era prevista una chiave diversa per ogni giorno. Il blocco così realizzato era poi distribuito alle varie stazioni di comunicazione.

La sicurezza di Enigma[20] non risiedeva, pertanto, nella segretezza

---

[19] L'invenzione della macchina *Enigma* è stata merito degli inventori tedeschi Arthur Scherbius e Richard Ritter.

[20] L'inizio della fine della macchina *Enigma* si sviluppò in Polonia. I polacchi erano stretti fra la Russia e la Germania e necessitavano pertanto di una potente *Intelligence* in grado di sapere anticipatamente le intenzioni avversarie. Francia e Inghilterra approfittando del periodo di relativa quiete avevano decisamente allentato la ricerca crittoanalitica delegandola, di fatto, agli studiosi polacchi. In primo luogo il governo polacco costituì un ufficio cifre, il *Biuro Szyfrów*. La sorveglianza delle comunicazioni tedesche diede i primi frutti nel 1926 con l'intercettazione dei primi messaggi *Enigma*. I messaggi parvero inizialmente una parete insormontabile e solo grazie al tradimento del tedesco Hans-Thilo Schmidt, impiegato alla *Chiffrierstelle* – ufficio amministrativo preposto alle comunicazioni crittate, fu possibile fare i primi passi nel procedimento di crittoanalisi. Schmidt fornì le fotografie dei manuali di istruzioni per l'uso della macchina cifratrice. Grazie al materiale così ottenuto fu possibile costrui-

del dispositivo quanto piuttosto nella segretezza delle impostazioni della macchina e, quindi, nella segretezza della chiave. E ciò in perfetta attuazione del menzionato principio di Kerckhoffs.

Un cenno merita, da ultimo, il sistema di sicurezza utilizzato dagli Stati Uniti durante la campagna del Pacifico contro il Giappone. Esso portò ad una nuova evoluzione della crittografia. L'esigenza era quella di individuare un sistema di comunicazione sicuro ed al tempo stesso veloce ed agile, adatto a comunicazioni improvvise e non programmate, in condizioni spesso precarie. Da tale necessità prese spunto l'intuizione dell'ingegnere Philip Johnston che pensò di utilizzare come alfabeto cifrante la lingua *navajo*.

I marconisti navajo (*code talkers*), furono addestrati ed arruolati per poi essere impiegati negli scontri armati (in particolare per la presa di Guadalcanal)[21].

Fu implementato un vero e proprio cifrario che ricomprendeva le parole di uso comune tradotte in navajo. Laddove non esisteva una parola corrispondente se ne indicava una convenzionale[22].

---

re una replica di *Enigma*. D'altra parte la sola conoscenza del dispositivo non consentiva comunque la crittoanalisi, occorreva la "chiave", il settaggio della macchina, la posizione delle sue diverse componenti. Fu in tale prospettiva che prese il via la ricerca di tutti quei possibili appigli in grado di consentire la determinazione delle chiavi. Massimo esponente in materia fu il matematico polacco Marian Rejewski. Rejewski si concentrò principalmente sull'analisi delle concatenazioni, giungendo in tal modo all'implementazione di una macchina – la "bomba di Rejewski" – in grado di controllare automaticamente e velocemente il settaggio e quindi la chiave di *Enigma*. Nel dicembre 1938 i crittografi tedeschi aumentarono il livello di sicurezza delle loro comunicazioni aggiungendo nuove componenti ed aumentando così il numero delle possibili combinazioni e quindi delle possibili chiavi. Per far fronte a questa nuova rivale i polacchi coinvolsero francesi ed inglesi e fu così fondato il centro di Bletchley Park (1939) dove trovò sede la *Government Code and Cypher School*. I crittoanalisti di Bletchley Park in breve tempo riuscirono a padroneggiare *Enigma*, in particolare grazie allo sfruttamento dei cosiddetti *cillies*. Artefice della vittoria finale su *Enigma* fu lo scienziato Alan Turing con la cosiddetta "macchina di Turing".

[21] Il regista J. Woo, nel novembre 2001, traendo spunto dagli eventi storici descritti, realizzò il film *Windtalkers* che rispecchia fedelmente la posizione ed il ruolo strategico degli indiani navajo all'interno dell'esercito statunitense.

[22] Il codice navajo non è mai stato decifrato. Questo è conseguenza del fatto che l'utilizzo di una lingua specifica è completamente priva di senso per il crittoanalista che non la conosca. Detto utilizzo non consente alcun appiglio, alcun elemento, alcun dato comparativo.