RATIO MATH. 1.
(1990), 121 - 132

# Analisi Critttografica e Ricerca Scientifica

Giovanni Moro

## 1. PREMESSE

Prima di entrare nel vivo dell'argomento mi sembra opportuno qualche cenno, anche se fugace, sulla "Crittografia", l'arte- scienza che, fin dalle sue origini, ha avuto due obiettivi non solo ben distinti, ma addirittura antitetici:

- uno, quello della tutela del segreto delle comunicazioni, mediante la loro cifratura;
- l'altro, quello della penetrazione (illegale) del segreto delle comunicazioni, a mezzo decrittazione.

L'attività di studio e ricerca, che è alla base dei tentativi di decrittazione dei messaggi cifrati, va sotto il nome ormai universalmente noto di "Analisi Crittografica" o "Criptoanalisi".

LA CRIPTOANALISI.

La criptoanalisi è la scienza composita che, partendo da messaggi cifrati con sistemi di cifratura dei quali può anche non essere noto nulla, si prefigge, in linea di massima, di raggiungere, nell'ordine, i seguenti obiettivi:

(1) determinare l'architettura del sistema di cifratura impiegato, individuandone i "parametri" fondamentali, o di base, che lo governano sul piano operativo;

(2) ricostruire le leggi, se ve ne sono di determinabili, alle quali fa capo la "variazione" dei "parametri base", che, con la loro evoluzione temporale,

dovrebbero assicurare l'impervietà del sistema di cifratura;

(3) ricostruire le "chiavi" dei singoli messaggi;

(4) decrittare i messaggi, possibilmente in tempo utile per poterli sfruttare operativamente;

(5) acquisire una "conoscenza" tanto approfondita del sistema studiato, che consenta di individuare la "filosofia" che è a monte del sistema stesso.

Se questo risultato è raggiunto, in caso di "varianti" sia funzionali che operative al sistema di cifratura, si possono più facilmente individuare le eventuali linee preferenziali di studio-ricerca da seguire per risolvere i problemi che le "varianti" apportate creano.

I moderni sistemi di cifratura, in linea di massima, sono ormai talmente complessi e sofisticati che il loro studio non può essere effettuato da singoli, anche se molto preparati. E' necessario impiegare teams composti da persone di varia estrazione culturale e scientifica; oltre ai "crittografi" più o meno classici che dovrebbero fungere anche da analisti di sistema, è necessario, secondo le varie necessità che si possono presentare, impiegare anche: statistici, matematici, spesso specializzati in teoria dei numeri; eletronici; linguisti; programmatori; tecnici delle trasmissioni.

L'impiego di sistemi di elaborazione elettronica di adeguata potenza è dato per scontato.

I dati ricavati dalla "Criptoanalisi" sono di grandissima utilità anche per la ideazione, progettazione, realizzazione dei moderni sistemi di cifratura elettronici che, oltre che efficienti, devono essere sicuri.

La "Criptoanalisi" deve quindi essere una attività di studio- ricerca non considerata a sè stante, ma inquadrata nel più ampio contesto della "Crittografia", intesa nel suo più ampio significato.

## CRIPTOANALISI E RICERCA SCIENTIFICA

Normalmete si pensa alla "Crittografia" come ad una scienza tributaria di altre scienze, ma non anche come ad una scienza autonoma, che possa essere di ausilio alle altre.

La mia esperienza quarantennale di lavoro in tale campo, mi porta a ritenere questo modo di pensare non valido in assoluto. Cercherò di dimostrare la correttezza di questo mio convincimeto:

(1) Illustrando, anche se solo a grandi linee, la "logica" che è alla base del lavoro crittografico, facendo vedere come l'"Analisi Crittografica", considerata nei suoi aspetti generali, non sia altro che ricerca scientifica, talvolta pura.

(2) Riportando, come pratico esempio di applicazione dei principi di cui

sopra, i risultati da me ottenuti studiando da "crittografo" l'equazione a numeri interi: $M^2 = N^2 - P^2$.

## 2. CENNI SULL'"ANALISI CRITTOGRAFICA"

L'"Analisi crittografica", in sintesi, si sviluppa attraverso le seguenti fasi successive, fra di loro strettamente collegate da legami di retroazione, a quasi tutti i livelli.

(1) Si assume una base numerica, su modulo/i opportuno/i , con la quale tradurre in numeri i dati oggetto di studio. Si ricavano "blocchi" di "numeri", che costituiscono la base per le successive fasi di sviluppo delle ricerche.

(2) Sui "blocchi" di "numeri" così trovati, considerati singolarmente e, o opportunamente raggruppati, si va alla ricerca di "fenomeni", di natura generalmente "logico-matematica", che escono, "ragionevolmente", al di fuori della fascia della "casualità".

(3) Si cerca di dare una interpretazione "logico-matematica" ai fenomeni "non casuali" rilevati, facendo, se necessario, ipotesi "attendibili". Si verifica l'attendibilità delle eventuali ipotesi fatte.

(4) Si cerca di inserire e coordinare in un unico "modello logico-funzionale", i singoli "fenomeni" rilevati e le eventuali "ipotesi", che gli stessi hanno originato.

(5) Si procede all'esame critico (sperimentale, quando necessario) del "modello" trovato ed alla verifica finale della sua validità.

(6) Si applica il "modello finale" al caso studiato.

*Il lavoro, quando necessario, procede per approssimazioni successive.*

Nello sviluppo delle singole fasi dello studio è spesso, per non dire quasi sempre, specialmente nei problemi molto complessi, necessario ritornare nelle "fasi" precedenti per apportare correzioni alle interpretazioni date dai "fenomeni" rilevati e, o alle "ipotesi logiche", o di altro tipo, che si sono fatte.

*Nel caso di "ricostruzione" di sistemi di cifratura, il "modello" ricavato può essere "fittizio" e, o "reale".*

Se si esaminano le "fasi" attraverso le quali si sviluppa la "criptoanalisi", sembra di poter pervenire alla conclusione che segue.

L'"analisi crittografica" non è altro che un "metodo" di "ricerca scientifica" pura, che si può applicare anche in campi, che ben poco, per quel che può

sembrare, hanno a che fare con la "crittografia".

*La cosa non deve stupire più di tanto, perchè, in ultima analisi, l'"analisi crittografica" e la "ricerca pura", hanno come obiettivo finale comune la ricerca di "informazioni", nei casi in cui esistano, indipendantemente dalla loro natura e dal fatto che siano, o meno, determinabili.*

## 3. RADICI DELL'EQUAZIONE $M^2 = N^2-P^2$, PER: M, N, P INTERI.

### 3.1 PREMESSE.

Per l'equazione:

$$M^2 = N^2 - P^2 = (P + Z)^2-P^2 \tag{1}$$

(M, N, P, Z interi), *con "procedimenti" di lavoro "crittografico"*, sono stati trovati i seguenti tre metodi per calcolarne le infinite radici.

**(I)**

$$\begin{cases} M = \{2^{(1+r)}GZ + Z^2\}; \; N = \{2^{(1+r)}GZ + 2^{(1+2r)}G^2\}; \\ P = \{2^{(1+r)}GZ + 2^{(1+2r)}G^2\} \end{cases} \tag{2}$$

ove: $Z \geq 1$, intero dispari qualsiasi; G intero dispari ( $\lesseqgtr 0$), primo con Z, qualsiasi; $r \geq 0$, intero qualsiasi. *La (1) è verificata per qualsiasi terna di valori di M, N, P definita da un "blocco" di valori qualsiasi di Z; G; r.*

**(II)** *L'equazione:*

$$M^2 = \{(M^2 + Z^2) / 2Z\}^2 - \{(M^2-Z^2) / 2Z\}^2 \tag{3}$$

*ammette soluzione:*

- *per:* $Z = 1$, per qualsiasi valore intero di $M \geq 3$, dispari;
- *per:* $Z = 2$, per qualsiasi valore intero di $M \geq 4$, *pari.*

**(III)** *Ricostruendo sistematicamente, a catena*, nell'ambito di un prefissato valore qualsiasi di Z, *i valori, crescenti, degli: M- N-P, omologhi nelle rispettive successioni, costituenti le infinite terne soluzioni della (1)*, caratterizzate dal

prescelto valore di Z.

*Come terna di partenza, terna numero 1, è stata scelta la:*

$$M^2 = N^2 - P^2 = Z^2-(0)^2 \tag{4}$$

Omesso un approfondimento dei casi (1) e (2), passiamo al caso (III).

### 3.2 CASO (III).

La ricostruzione (calcolo), a catena, dei termini omologhi delle tre successioni degli M, N, P, noti i quali sono determinate le infinite terne M, N, P soluzioni della (1), si può effettuare tenendo presenti:

(a) Il seguente schema:

| | | | | | |
|---|---|---|---|---|---|
| M | $M_1 = Z$ | $M_2 - M_3$ - | | $M_s$ | successione M crescenti |
| | $D_1M$ | $D_1M - D_1M$ - | | | successione $1^e$ Differenze M |
| N | $N_1 = Z$ | $N_2 - N_3$ - | | $N_s$ | successione N crescenti |
| | $D_1N$ | $D_1N - D_1N_2$ - | | | successione $1^e$ Differenze N |
| | $D_2N$ | $D_2N$ - | | | successione $2^e$ Differenze N |
| P | $P_1 = 0$ | $P_2 - P_3$ - | | $P_s$ | successione P crescenti |

(5)

Ove:

$S \geq 1$, intero qualsiasi;

$D_1M = \{M_{(s+1)}-M_s\}$ = costante - $1^e$ Differenze succ. M;

$D_1N = \{M_{(s+1)}-N_s\}$ - $1^e$ Differenze succ. N;

$D_2N = \{D_1N_{(s+1)}-D_1N_s\}$ = costante - $2^e$ Differenze succ. N.

Dal quadro (5) risulta chiaramente come, partendo da:

$-M_1 = Z$ e $D_1M$, mediante somme successive a catena, da sinistra a destra, si possono ricostruire tutti i termini della successione degli M.

$-N_1 = Z$, $D_1N_1$ e $D_2N$, mediante somme successive a catena, sempre da sinistra a destra, si possono ricostruire tutti i termini e della successione ausiliaria dei $D_1N$ e di quella degli N.

I valori dei $P_s$ sono dati da: $(N_s - Z)$.

Z è noto perchè il suo valore viene prefissato in partenza: gli altri elementi base per lo sviluppo del procedimento, e cioè: $M_1$- $D_1M$-$N_1$-$D_1N_1$-$D_2N$ sono calcolabili con le:

(b) Seguenti formule:

| | Z | | | |
|---|---|---|---|---|
| | $(2H+1)^2$ | $\{(2K)^2:2\}$ | $(2H_1+1)$ | $(2K_1)$ |
| | $H \geq 0$ | $K \geq 1$ | $H_1 \geq 1$ | $K_1 \geq 2$ |
| $M_1$ | $(2H+1)^2 = Z$ | $\{(2K)^2:2\} = Z$ | $(2H_1+1) = Z$ | $(2K_1) = Z$ |
| $D_1M$ | $2(2H+1)$ | $2K$ | $2(2H_1+1) = 2Z$ | $(2K_1) = Z$ |
| $N_1$ | $(2H+1)^2 = Z$ | $\{(2K)^2:2\} = Z$ | $(2H_1+1) = Z$ | $(2K_1) = Z$ |
| $D_1N_1$ | $2(2H+1)+2$ | $(2K+1)$ | $4(2H_1+1) = 4Z$ | $3K_1$ |
| $D_2N$ | 4 | 2 | $4(2H_1+1) = 4Z$ | $(2K_1) = Z$ |
| $P_s$ | $(N_s$-$Z)$ | $(N_s$-$Z)$ | $(N_s$-$Z)$ | $(N_s$-$Z)$ |

(6)

Nelle quali:

H, intero qualsiasi;
K, intero qualsiasi;
$H_1$, intero per cui $(2H_1+1)$ diverso $(2H+1)^2$;
$K_1$, intero per cui $(2K_1)$ diverso $\{(2K)^2:2\}$.

La configurazione caratteristica delle formule di cui sopra, suggerisce l'idea di considerare, per l'insieme dei valori di Z, i seguenti quattro sottoinsiemi caratteristici:

- $S_z(2H+1)^2$-$S_z(1)$: sottoinsieme dei valori di Z, dei quadrati dei numeri dispari.
- $S_z\{(2K)^2:2\}$-$S_z(2)$: sottoinsieme dei valori di Z, delle metà dei quadrati dei numeri pari.
- $S_z(2H_1+1)$-$S_z(3)$: sottoinsieme dei valori di Z, dei numeri dispari, esclusi i quadrati.
- $S_z(2K_1)$-$S_z(4)$: sottoinsieme dei valori di Z, dei numeri pari, escluse le metà dei quadrati dei pari.

### 3.3 PROPRIETA' DI MAGGIOR INTERESSE DELLE SOLUZIONI DELLA (1)

Nell'allegato 1, sono riportati, a titolo di esempio, raggruppati in funzione di Z, blocchi di valori di M - N - P costituenti terne di interi soluzioni della (1), determinate con il "procedimento" di cui al caso (III).

Definite come soluzioni "primitive", quelle che possono essere ricavate "esclusivamente" come soluzioni della (1):

- applicando uno qualsiasi dei metodi sopra visti;
- e che presentano valori di P - "pari";

l'unico dei quattro sottoinsiemi dei valori di Z, che contiene anche soluzioni "*primitive*" è $S_z(1)$.

Considerando le soluzioni della (1) raggruppate in funzione di: $S_z(1)$ - $S_z(2)$ - $S_z(3)$ - $S_z(4)$, si rileva quanto di seguito specificato, per ciascuno dei quattro sottoinsiemi citati.

a) *Sottoinsieme* $S_z(1)$.
$H = 0$ - $Z = 1$: *tutte le soluzioni sono "primitive"*.
$H \geq 1$ - $Z = (2H+1)^2$. Se:

$$(7) \qquad \begin{cases} (M_1)^2 = (P_1+1)^2 - (P_1)^2 \\ (M_2)^2 = (P_2+1)^2 - (P_2)^2 \end{cases} \qquad M_1 < M_2$$

sono soluzioni, del gruppo $Z = 1$; si ha che gli: $M_3$ - $N_3$ - $P_3$ dati da:

$$(8) \qquad \begin{cases} M_3 = M_1 M_2 \\ N_3 = (P_2+1) + P_1 = ((M_2)^2 + (M1)^2)/2 = (N2) + (P_1) \\ P_3 = (P_2) - (P_1) = ((M_2)^2 - (M_1)^2)/2 \end{cases}$$

sono soluzioni della (1), del gruppo $Z = (M_1)^2 = (2P_1 + 1)$.
(9) *Regola di derivazione* A.

Le soluzioni nelle quali M - N - P sono tra loro "non" - "primi", oltre che con la (9), sono sicavabili ("derivabili") anche da opportune soluzioni (terne M - N - P), che chiameremo soluzioni "base", moltiplicate per opportune costanti.
(10) *Regola di derivazione* B.

Nei quadri $S_z(1)$ dell'Allegato 1 vicino a ciascuna terna "derivata" sono indicate le relative regole: A - B di "derivazione".

"A", è seguito da due numeri, che indicano i numeri d'ordine delle due terne "base" - entrambe del gruppo di soluzioni $Z = 1$ - che danno origine alla terna "derivata".

"B", è seguita da tre numeri che indicano nell'ordine:

- valore di Z al quale appartiene la terna base;
- numero d'ordine, in tale gruppo di soluzioni, della terna "base";
- valore della costante moltiplicativa degli M - N - P della terna "base" che sono serviti per ricavare la terna "derivata".

Da rilevare, come già detto in altro punto, che per $S_z(1)$, qualsiasi sia il valore di Z, tutti i valori di P sono "pari".

b) Sottoinsieme $S_z(2)$

*Le soluzioni sono tutte "derivate".*

Le regole di "derivazione", applicando le quali, a seconda dei casi, si ricavano le varie terne di M - N - P soluzioni della (1) sono le seguenti tre:

(a) Si scambiano di posto i valori di M e P, mantenedo fisso quelo di N, di una soluzione di $S_z(1)$.

(11) *Regola di derivazione* C.

(b) Si moltiplicano per 2 i valori degli M - M - P di una soluzione di $S_z(1)$.

(12) *Regola di derivazione* D.

(c) Si moltiplicano per 4 i valori degli M - N - P di una soluzione di $S_z(2)$, stesso.

(13) *Regola di derivazione* E.

Nei quadri di $S_z(2)$, dell'allegato1, vicino a ciascune terna soluzione, sono indicate le relative regole: C - D - E, di derivazione.

C, è seguito da due numeri, che indicano nell'ordine:

- valore di Z, al quale appartiene la terna "base";
- numero d'ordine, in tale gruppo di soluzioni, della terna "base";

che sono serviti per ricavare la terna "derivata".

Tali due elementi sono riportati anche dopo D ed E, in tali casi sono poi seguito da un terzo: la costante moltiplicativa.

c) Sottoinsieme $S_z(3)$

*Le soluzioni sono tutte "derivate".*

Regola impiegata: si moltiplicano per $Z=(2H_1+1)$ i valori di M - N - P della soluzione omologa - terna "base" - di $Z=1$.

(14) *Regola di derivazione* F.

Nel quadro, dell'allegato 1 di $S_z$ (3), accanto ad F è riportata la costante

moltiplicativa.

d) Sottoinsieme $S_z(4)$

*Le soluzioni sono tutte "derivate".*

Regola impiegata: si moltiplicano per $K_1$ i valori di M - N - P della soluzione omologa - terna "base" - di $Z=2$.

(15) *Regola di derivazione* G.

Nel quadro, dell'allegato 1, di $S_z$ (4), accanto a G è riportata la costante moltiplicativa.

**3.4 Vedere, nell'allegato 2, un "procedimeto", diverso da quelli già sopra descritti, per ricavare le terne di: M - N - P soluzioni della (1) - caso $Z=(N-P)=1$.**

## ALLEGATO 1

ESEMPI DI RISULTATI OTTENUTI CON L'APPLICAZIONE DELLE: (5) - (6) PER LA RICOSTRUZIONE A CATENA DELLE SOLUZIONI DELLA (1).

1. *Sottoinsieme* $S_z$ (1)

| $H=0; Z=1$ | | | | $H=1; Z=3^2=9$ | | | REGOLE | | |
|---|---|---|---|---|---|---|---|---|---|
| S | M | N | P | M | N | P | A | B | S |
| 1 | 1 | 1 | 0 | 9 | 9 | 0 | 2-2 | 1-1-9 | 1 |
| 2 | 3 | 5 | 4 | 15 | 17 | 8 | 2-3 | - | 2 |
| 3 | 5 | 13 | 12 | 21 | 29 | 20 | 2-4 | - | 3 |
| 4 | 7 | 25 | 24 | 27 | 45 | 36 | 2-5 | 1-2-9 | 4 |
| 5 | 9 | 41 | 40 | 33 | 65 | 56 | 2-6 | - | 5 |
| 6 | 11 | 61 | 60 | 39 | 89 | 80 | 2-7 | - | 6 |
| 7 | 13 | 85 | 84 | 45 | 117 | 108 | 2-8 | 1-3-9 | 7 |
| 8 | 15 | 115 | 112 | 51 | 149 | 140 | 2-9 | - | 8 |
| 9 | 17 | 145 | 144 | 57 | 185 | 176 | 2-10 | - | 9 |
| 10 | 19 | 181 | 180 | 63 | 225 | 216 | 2-11 | 1-4-9 | 10 |

## NOTE

(1) I valori di: $M_s$ - $N_s$ - $P_s$, costituenti la $S^a$ terna soluzione della (1) - per $Z=(2H+1)^2$, $H\geq 0$ qualsiasi - si possono calcolare anche applicando le seguenti tre formule:

(16) $M_s=(2H+1)\{2(H+S)-1\}$; $N_s=\{(2H+S)^2+(S-1)^2\}$; $P_s=2(S-1)(2H+S)$

(2) I "guadri", intestati a: $Z=(2H+1)^2$ - per $H \geq 1$ - delle terne: M - N - P soluzioni della (1), si possono ricavare applicando la regola di "derivazione" - A (vedere (9)), facendo giocare la terna $S=(H+1)$, successivamente con le terne:

(17) $S_{\bullet}=(H+1)\text{-}(H+2)\text{-}(H+3)\text{-}(H+4)\text{-}\ldots$

del gruppo di soluzioni di $Z=1$ -$(H=0)$.

## 2. Sottoinsieme $S_z$ (2)

K = 1

Z = 2 REGOLE

| S | M | N | P | C | D |
|---|---|---|---|---|---|
| 1 | 2 | 2 | 0 | - | 1-1-2 |
| 2 | 4 | 5 | 3 | 1-2 | - |
| 3 | 6 | 10 | 8 | - | 1-2-2 |
| 4 | 8 | 17 | 15 | 9-2 | - |
| 5 | 10 | 26 | 24 | - | 1-3-2 |
| 6 | 12 | 37 | 35 | 25-2 | - |
| 7 | 14 | 50 | 48 | - | 1-4-2 |
| 8 | 16 | 65 | 63 | 49-2 | - |
| 9 | 18 | 82 | 80 | - | 1-5-2 |

K = 2

Z = 8 REGOLE

| M | N | P | C | E | S |
|---|---|---|---|---|---|
| 8 | 8 | 0 | - | 2-1-4 | 1 |
| 12 | 13 | 5 | 1-3 | - | 2 |
| 16 | 20 | 12 | - | 2-2-4 | 3 |
| 20 | 29 | 21 | 9-3 | - | 4 |
| 24 | 40 | 32 | - | 2-3-4 | 5 |
| 28 | 53 | 45 | 25-3 | - | 6 |
| 32 | 68 | 60 | - | 2-4-4 | 7 |
| 36 | 85 | 77 | 49-3 | - | 8 |
| 40 | 104 | 96 | - | 2-5-4 | 9 |
| 44 | 125 | 117 | 81-3 | - | 10 |

3. Sottoinsieme $S_z(3)$

$H_1 = 1$

$Z = 3$ R.

| S | M | N | P | F |
|---|---|---|---|---|
| 1 | 3 | 3 | 0 | 3 |
| 2 | 9 | 15 | 12 | 3 |
| 3 | 15 | 39 | 36 | 3 |
| 4 | 21 | 75 | 72 | 3 |
| 5 | 27 | 123 | 120 | 3 |
| 6 | .. | ... | ... | 3 |

4. Sottoinsieme $S_z(4)$

$K_1 = 2$

R. $Z = 4$

| G | M | N | P | S |
|---|---|---|---|---|
| 2 | 4 | 4 | 0 | 1 |
| 2 | 8 | 10 | 6 | 2 |
| 2 | 12 | 20 | 16 | 3 |
| 2 | 16 | 34 | 30 | 4 |
| 2 | 20 | 52 | 48 | 5 |
| 2 | .. | .. | .. | 6 |

## ALLEGATO 2

**Schema di calcolo delle terne: M, N, P (interi) soluzioni della $M^2 = N^2 - P^2$, per $Z = (N - P) = 1$, partendo dalla successione: $0^2$, $1^2$, $2^2$, $3^2$, $4^2$, ...**

$\{(n+1)^2 - n^2\}$ $n^2$ $[(n+1)^2 + n^2]$ $\{[(n+1)^2 + n^2] - 1\}$

$\{M\}$ $[N]$ $\{P\}$

| | | | | | |
|---|---|---|---|---|---|
| 1 | 1 | 0 | 1 | 0 | 1 |
| 2 | 3 | 1 | 5 | 4 | 2 |
| 3 | 5 | 4 | 13 | 12 | 3 |
| 4 | 7 | 9 | 25 | 24 | 4 |
| 5 | 9 | 16 | 41 | 40 | 5 |
| 6 | 11 | 25 | 61 | 60 | 6 |
| 7 | 13 | 36 | 85 | 84 | 7 |
| 8 | 15 | 49 | 113 | 112 | 8 |
| 9 | 17 | 64 | 145 | 144 | 9 |
| 10 | 19 | 81 | 181 | 180 | 10 |
| 11 | 21 | 100 | 221 | 220 | 11 |
| 12 | 23 | 121 | 265 | 264 | 12 |
| 13 | 25 | 144 | 313 | 312 | 13 |
| 14 | 27 | 169 | 365 | 364 | 14 |
| 15 | .. | 196 | ... | ... | 15 |
| .. | .. | ... | ... | ... | .. |

n = 0, 1, 2, 3, 4, 5, ..., ecc., ....

**SOMMARIO.** Viene illustrata la possibilità che la tecnica di lavoro legata all'"Analisi crittografica", sia impiegabile in campi della ricerca, che, poco, sembrano avere in comune con la "Crittografia". Come esempio di realizzazione di tale possibilità vengono presentati i risultati ottenuti nello studio dell'equazione a numeri interi: $M^2 = N^2 - P^2$