RADIOONDE Aperiodico di scienza e tecnica della radio - N. 26, giugno 2002

Fotocopiato in proprio, distribuito gratuitamente, è gradita la collaborazione dei lettori - Il N. 25 è stato inviato a 14 lettori
Redazione: Ezio Mognaschi, v.le Gorizia, 63 - 27100 Pavia PV, tel. 0382 539522, posta elettronica: mognaschi@fisicavolta.unipv.it

Hanno collaborato a questo numero: G. Di Bella, A. Nardi, E. Mognaschi, M. E. Mognaschi ed altri.

Notizie: * Il Gruppo-Radio-Mondiale "Sierra Tango" ha realizzato il sito *http://www.forumradio.cjb.it* dedicato al mondo della radio e spedisce via posta elettronica *Rapporto Radio* contenente notizie sul radioascolto. L'indirizzo postale è C. P. 5, 80010 Quarto (NA). Per iscrizioni mandare un messaggio a: *ForumRadio-subscribe@yahooogroups.com.*
* L'ultimo massimo dell'attività solare si verificò alla metà del 2000 con un numero di macchie solari il più alto degli ultimi 10 anni. Una notevole eruzione solare si verificò il 14 luglio 2000 con un'aurora che fu osservabile anche a basse latitudini e la temporanea messa fuori servizio di alcuni satelliti di telecomunicazione. Successivamente il numero di macchie diminuì lentamente ed il Sole rimase relativamente quieto per mesi. Ma nel 2002 è stato osservato un nuovo aumento dell'attività solare per cui il presente ciclo solare, come già i due precedenti, sembra presentare due picchi. Si attende quindi un ulteriore aumento dell'attività solare per il prossimo anno, in quanto le più intense eruzioni tendono ad addensarsi verso la fine del ciclo.
* La stazione GBR che opera su 16 kHz è stata spenta dal 31 marzo al 21 aprile 2002 per riparazioni all'antenna. A metà del 2003 cesserà definitivamente l'attività dopo 77 anni di servizio.
* Adriano Nardi segnala il sito *http://www.itacom.net/PH/2report.htm* del Comitato Italiano per il Progetto Hessdalen ove è descritta l'attività in VLF di questo gruppo per lo studio delle misteriose luci che appaiono della vallata di Hessdalen.
* Il 28 maggio si è svolto a Milano, organizzato dall'Assessorato all'Ambiente di quella provincia, il convegno *Rischi da esposizione a campi elettromagnetici - Aspetti normativi, tecnici, sanitari ed economici*. Il convegno è stato addirittura pubblicizzato con un inserto sul *Corriere della Sera*, tuttavia solo circa 300 persone hanno seguito le prime relazioni ed alla fine del convegno erano in sala non più di 20 persone. Personaggi più o meno noti del mondo politico locale, di quello tecnico, sanitario, legale e produttivo si sono sforzati per illustrare i vari aspetti del problema. L'osservazione più importante, scaturita dal convegno, è che, nell'immaginario collettivo, il problema dell'inquinamento elettromagnetico è il più sentito dagli italiani, più ancora di problemi ben più gravi per la salute pubblica, come quelli dell'inquinamento atmosferico e di mucca pazza. Quersto spiega l'accanimento dei vari organi di governo, dal governo centrale, a quello regionale di molte regioni ad intervenire a "normare" la situazione; spiega l'intervento della propvincia che si è data da fare ad organizzare il convegno stesso e l'intervento addirittura dell'Associazione Nazionale dei Comuni d'Italia che ha fatto sapere che anche i sindaci vogliono dire la loro in quanto ufficiali sanitari e responsabili della salute pubblica! La conseguenza, per ora, è una difformità tra le leggi di diverse regioni e la gara tra queste a chi è più restrittivo, pur dichiarando di "voler salvaguardare i servizi" [leggi "telefoni cellulari e TV private"] come a dire: botte piena e moglie ubriaca. Altro dato importante emerso è l'accertata caratteristica dei campi magnetici ELF [leggi 50 Hz] di essere "possibilmente cancerogeni" per valori superiori a 0.2 – 0.4 μT; per capirsi il campo prodotto a 30 cm dal motore di un phon può salire a circa 2500 μT, mentre sotto un elettrodotto è tipicamente di 20 μT. Mentre per il phon ciascuno deve arrangiarsi come crede, per gli elettrodotti sono stati calcolati i costi per il risanamento che corrispondono a circa 15 lire in più al kWh per i prossimi 35 anni.
* Giancarlo di Bella, IZ0DGI, informa che si è costituito nel Lazio il Guppo di Lavoro sulle Onde Lunghe che comprende, per ora, oltre a Di Bella, Giancarlo Spagnoli e Marcello Casali.

La misura dell'intensità dei segnali radio

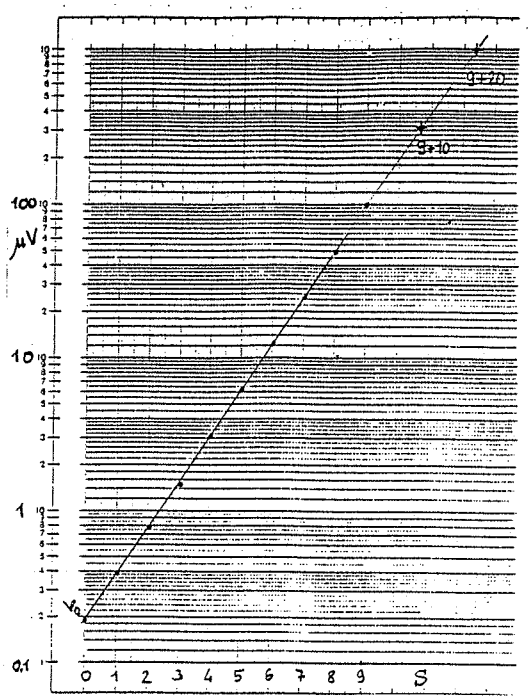
di Ezio Mognaschi

Considerazioni generali e definizioni

I radioricevitori di qualità sono generalmente dotati di un indicatore dell'intensità del segnale ricevuto. Questo indicatore può essere uno strumento analogico, a lancetta, nei vecchi ricevitori a valvole oppure, nei ricevitori più recenti, a stato solido, può essere un indicatore a diodi LED, solitamente a luce rossa, o a barre nei pannelli a cristalli liquidi. L'indicatore dell'intensità del segnale è chiamato *S-meter* in quanto fornisce una misura dell'intensità del segnale in unità S, cioè in unità di segnale. Questa scala si estende da 0 a 9; oltre il 9, come vedremo, la scala continua con intervalli di 10 dB usualmente sino a 60 dB. I segnali radio che vengono misurati dall'*S-meter* si possono trovare in un intervallo amplissimo che va da una piccola frazione di microvolt a qualche centinaio di millivolt. Per misurare una grandezza i cui valori si estendono per parecchi ordini di grandezza, ma soprattutto per fornire una misura direttamente correlabile con la

percezione del nostro udito che non è lineare, bensì logaritmica, si usa appunto una scala logaritmica. Nella definizione della scala dell'intensità del segnale, come per tutte le scale logaritmiche, che, per loro natura non hanno né inizio né fine, si deve innanzitutto scegliere un livello di riferimento e questa scelta è arbitraria: per i segnali radio viene solitamente scelto il valore di 100 μV per S = 9. Questa scelta non è uno standard ed è possibile che diversi costruttori usino diversi livelli di riferimento. Inoltre si deve scegliere il passo della scala ed è stato scelto, sempre arbitrariamente, che ad ogni diminuzione di un'unità S corrisponda il dimezzamento del segnale. Quindi, come si può vedere dalla tabella e dal grafico di pag. 2, ad S = 8 corrisponde un segnale di 50 μV e così via, sino ad S = 0 che corrisponde a circa 0.2 μV. I radioascoltatori sanno che sino ad S = 5 il segnale è debole e il guadagno del ricevitore, determinato dal controllo automatico di volume (il CAV) se non viene escluso, comporta la presenza di rumore; da S = 6 ad S = 9 il segnale è forte; oltre S = 9 il segnale è fortissimo.

S	**Intensità del segnale** V_o	**Potenza del segnale** W_o	**dBV**
0	0.1953 μV	762.94 aW	−134
1	0.3906	3.0517 fW	−128
2	0.7812	1.22	−122
3	1.5625	48.8	−116
4	3.125	195.3	−110
5	6.25	781.25	−104
6	12.5	3.125 pW	−98
7	25	12.5	−92
8	50	50	−86
9	100	200	−80
9 + 10 dB	316	2 nW	−70
9 + 20	1 mV	20	−60
9 + 30	3.1	200	−50
9 + 40	10	2 μW	−40
9 + 50	31	20	−30
9 + 60	100	200	−20
9 + 70	310	2 mW	−10
9 + 80	1 V	20	0



a (atto) = 10^{-18}; f (femto) = 10^{-15}; p (pico) = 10^{-12}; n (nano) = 10^{-9}; μ (micro) = 10^{-6}; m (milli) = 10^{-3} .

I dati mostrati nella seconda colonna della tabella possono essere rappresentati dalla seguente relazione:

$$\log V = \log V_o + k\,S \qquad (1)$$

ove V è l'intensità del segnale in volt corrispondente alla lettura S dell'*S-meter*, V_o è il valore dell'intensità del segnale per S = 0 e k = log 2 ≈ 0.3010. La relazione (1) è rappresentata anche graficamente nella figura in scala semilogaritmica.

Nella terza colonna della tabella sono riportate le potenze che si riferiscono al segnale radio. Per calcolare questa colonna occorre stabilire il valore della resistenza sulla quale viene dissipata la potenza. È stato scelto per la resistenza, convenzionalmente, il valore tipico della resistenza di antenna dei ricetrasmettitori amatoriali che è di 50 Ω. Pertanto la potenza W sviluppata da un segnale S = 9, corrispondente a V = 100 μV, su R = 50 Ω, è

$$W = V^2/R = (100\ \mu V)^2/50\ \Omega = 200\ pW. \qquad (2)$$

I valori di potenza corrispondenti agli altri valori di S si possono ottenere dalla seguente relazione:

$$\log W = \log W_o + 2k\,S \qquad (3)$$

ove W_o è il valore della potenza sviluppata dal segnale corrispondente ad S = 0. Dalla (3) e dalla (1) si deduce che, se per una diminuzione di un'unità nella scala S la tensione si dimezza, la potenza si riduce ad un quarto, come, del resto, è evidente dalla (2).

La quarta colonna riporta il valore del segnale in dBV, cioè in decibel riferiti ad 1V. Questo è un altro modo

convenzionale di misurare le intensità di segnale ed è esprimibile con la relazione:

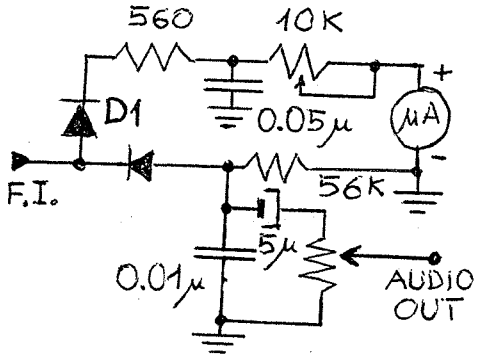
$$dBV = 20 \log (V/1V). \qquad (4)$$

Dalla (4), per V = 1V si ha ovviamente dBV = 0; per V = 100 μV (S = 9), dBV = 20 log (100 μV/1 V) = –80, per S = 8, dBV = 20 log (50 μV/1V) = –86 e così via. Si vede quindi che da S = 9 in giù, alla diminuzione di un'unità S, il segnale diminuisce di 6 dB, mentre sopra S = 9 si usano passi di 10 dB.

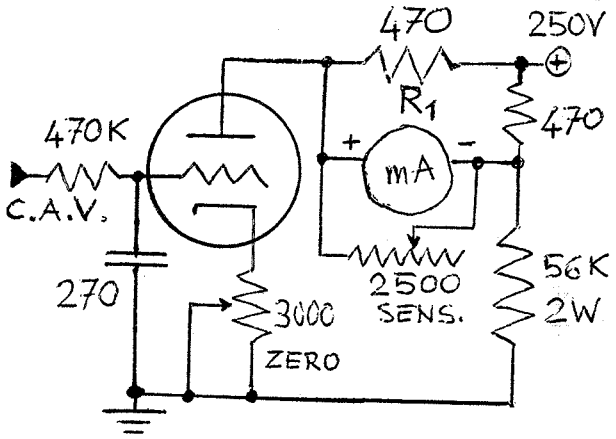
Un ricevitore che presenta un *S-meter* con una scala da S = 0 ad S = 9 + 60 dB ha una dinamica di (54 + 60) dB = 114 dB, cioè può trattare segnali da 0.2 μV a 100 mV.

Esempi di circuiti di S-meter

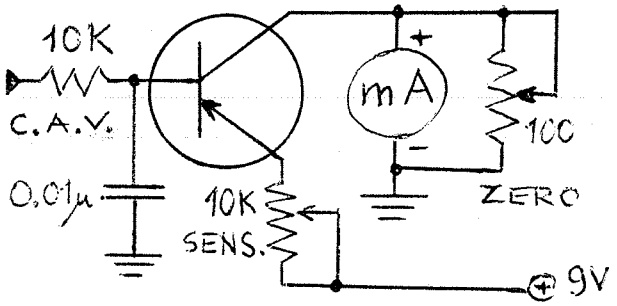
Presentiamo ora alcuni circuiti che realizzano la funzione di *S-meter*. Il primo circuito è il più semplice: viene direttamente collegato all'uscita del trasformatore dell'ultima frequenza intermedia, in parallelo al circuito del rivelatore. Consiste in un secondo circuito di rivelazione formato dal diodo D_1, seguito dal circuito filtro RC. La resistenza da 10 kΩ serve a portare a zero l'indicatore in assenza di segnale e contribuisce a linearizzare la risposta del circuito compensando parzialmente la non linearità del diodo D_1. Lo strumento di misura ha un fondo scala di 50 μA e quindi sottrae parte della corrente che esce dall'ultima frequenza intermedia.



Il secondo circuito, adatto per ricevitori a valvole e più elaborato, consiste in uno stadio di amplificazione del segnale negativo di controllo automatico di volume. All'aumentare di questo segnale negativo che viene presentato alla griglia, la corrente di placca diminuisce e quindi diminuisce la caduta di potenziale ai capi di R_1. Ciò permette un aumento della corrente attraverso lo strumento di misura posto in un circuito a ponte. Il circuito contiene sia un reostato per il controllo dello zero, sia uno per il controllo della sensibilità.



Il terzo circuito è la versione a stato solido del precedente. Un transistor bipolare p-n-p amplifica il segnale del circuito di controllo automatico di guadagno che agisce come polarizzazione diretta variabile sul transistor e causa un aumento della corrente di collettore in presenza di segnale. Nel caso che il segnale di controllo automatico di volume fosse positivo occorre usare un transistor n-p-n ed alimentare il circuito con una tensione negativa, invece che positiva.



La taratura di qualsiasi *S-meter* è un'operazione che richiede un generatore di segnali con taratura di precisione ed uscita con impedenza di 50 Ω. L'operazione di taratura consiste nel collegare l'uscita del generatore all'ingresso di antenna del ricevitore con un corto cavo schermato con impedenza caratteristica di 50 Ω. Fissato il segnale di uscita del generatore ai valori riportati nella seconda colonna della tabella, alla frequenza scelta e sintonizzato il ricevitore alla stessa frequenza, si segna sul quadrante dello strumento il corrispondente valore di S. È possibile che la sensibilità del ricevitore sia diversa a frequenze diverse, anche nella stessa banda. Perciò la taratura dovrebbe essere effettuata a diverse frequenze, a seconda delle necessità. Una procedura più semplice, anche se non rigorosa, è quella di collegare in parallelo al ricevitore da tarare, cioè alla stessa antenna, un altro ricevitore che possieda un *S-meter*, cercare stazioni di diversa intensità di segnale e segnare sull'*S-meter* da tarare i valori letti su quello di riferimento.

convenzionale di misurare le intensità di segnale ed è esprimibile con la relazione:

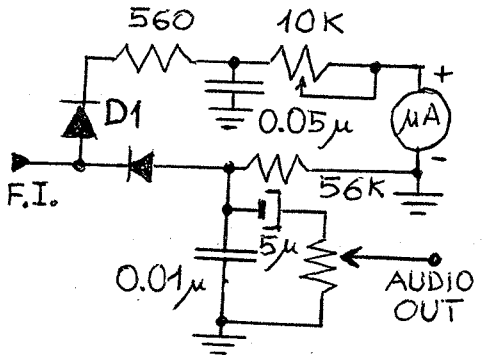
$$dBV = 20 \log (V/1V). \qquad (4)$$

Dalla (4), per V = 1V si ha ovviamente dBV = 0; per V = 100 μV (S = 9), dBV = 20 log (100 μV/1 V) = –80, per S = 8, dBV = 20 log (50 μV/1V) = –86 e così via. Si vede quindi che da S = 9 in giù, alla diminuzione di un'unità S, il segnale diminuisce di 6 dB, mentre sopra S = 9 si usano passi di 10 dB.

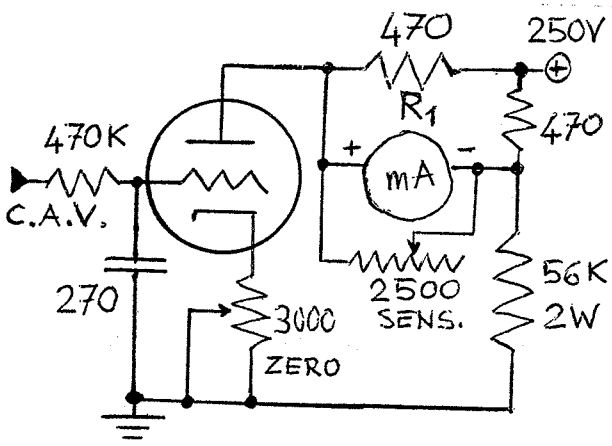
Un ricevitore che presenta un *S-meter* con una scala da S = 0 ad S = 9 + 60 dB ha una dinamica di (54 + 60) dB = 114 dB, cioè può trattare segnali da 0.2 μV a 100 mV.

Esempi di circuiti di S-meter

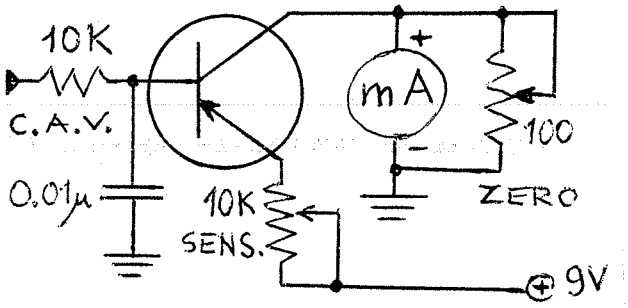
Presentiamo ora alcuni circuiti che realizzano la funzione di *S-meter*. Il primo circuito è il più semplice: viene direttamente collegato all'uscita del trasformatore dell'ultima frequenza intermedia, in parallelo al circuito del rivelatore. Consiste in un secondo circuito di rivelazione formato dal diodo D_1, seguito dal circuito filtro RC. La resistenza da 10 kΩ serve a portare a zero l'indicatore in assenza di segnale e contribuisce a linearizzare la risposta del circuito compensando parzialmente la non linearità del diodo D_1. Lo strumento di misura ha un fondo scala di 50 μA e quindi sottrae parte della corrente che esce dall'ultima frequenza intermedia.



Il secondo circuito, adatto per ricevitori a valvole e più elaborato, consiste in uno stadio di amplificazione del segnale negativo di controllo automatico di volume. All'aumentare di questo segnale negativo che viene presentato alla griglia, la corrente di placca diminuisce e quindi diminuisce la caduta di potenziale ai capi di R_1. Ciò permette un aumento della corrente attraverso lo strumento di misura posto in un circuito a ponte. Il circuito contiene sia un reostato per il controllo dello zero, sia uno per il controllo della sensibilità.

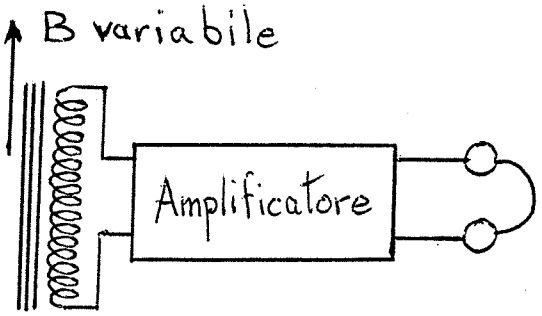


Il terzo circuito è la versione a stato solido del precedente. Un transistor bipolare p-n-p amplifica il segnale del circuito di controllo automatico di guadagno che agisce come polarizzazione diretta variabile sul transistor e causa un aumento della corrente di collettore in presenza di segnale. Nel caso che il segnale di controllo automatico di volume fosse positivo occorre usare un transistor n-p-n ed alimentare il circuito con una tensione negativa, invece che positiva.



La taratura di qualsiasi *S-meter* è un'operazione che richiede un generatore di segnali con taratura di precisione ed uscita con impedenza di 50 Ω. L'operazione di taratura consiste nel collegare l'uscita del generatore all'ingresso di antenna del ricevitore con un corto cavo schermato con impedenza caratteristica di 50 Ω. Fissato il segnale di uscita del generatore ai valori riportati nella seconda colonna della tabella, alla frequenza scelta e sintonizzato il ricevitore alla stessa frequenza, si segna sul quadrante dello strumento il corrispondente valore di S. È possibile che la sensibilità del ricevitore sia diversa a frequenze diverse, anche nella stessa banda. Perciò la taratura dovrebbe essere effettuata a diverse frequenze, a seconda delle necessità. Una procedura più semplice, anche se non rigorosa, è quella di collegare in parallelo al ricevitore da tarare, cioè alla stessa antenna, un altro ricevitore che possieda un *S-meter*, cercare stazioni di diversa intensità di segnale e segnare sull'*S-meter* da tarare i valori letti su quello di riferimento.

Per mettere in evidenza l'effetto Barkausen si può utilizzare il dispositivo, descritto dallo stesso autore, e schematizzato in figura. Un filo di ferro, o di acciaio, AB è posto all'interno di un solenoide di filo di rame collegato ad un amplificatore audio con alto guadagno. Barkausen utilizzò un'amplificazione di 10000 volte ottenuta con una catena di triodi, noi oggi possiamo collegare il solenoide all'ingresso dell'impianto *hi-fi* del salotto. Il numero delle spire del solenoide non è critico, un centinaio va bene, Barkausen ne usò 300, avvolte su di un supporto del diametro di 25 mm. Se ora si avvicina o si allontana dal nucleo di filo di ferro un magnete permanente che magnetizzi o smagnetizzi il nucleo, si ascolterà in altoparlante un fruscio che corrisponde alle variazioni a scatti della magnetizzazione del ferro o dell'acciaio. Questo fruscio, indesiderato nelle riproduzioni ad alta fedeltà, si elimina eliminando i trasformatori dai circuiti di amplificazione.



È interessante osservare che, se al posto di un nucleo di ferro si usa un nucleo di ferrite, l'effetto Barkausen è molto meno evidente in quanto le dimensioni più piccole dei domini ferromagnetici in questi materiali ha come conseguenza la minore altezza dei gradini nella curva del ciclo di isteresi.

Il breve articolo di Barkausen termina con il seguente commento: "Sarebbe auspicabile una ricerca dettagliata anche riguardo alle applicazioni pratiche, al detector magnetico di Marconi ed al telgraphon di von Poulsen".

In questo numero di *Radioonde* viene pubblicata la prima parte di una ricerca sulla crittanalisi, svolta nell'ambito del corso di Sistemi Operativi presso la Facoltà di Ingegneria dell'Università di Pavia. Il seguito nei prossimi numeri.

Crittanalisi (I parte)

di Maria Evelina Mognaschi

Introduzione

La crittanalisi è la disciplina che studia come forzare i cifrari costruiti dai crittografi, ovvero come determinare la chiave (se il sistema crittografico ne ha una) o scovare il metodo di crittografia (qualora il sistema si basi solamente sulla segretezza del metodo) o alterare in maniera conveniente un messaggio crittografato (ad esempio sostituendo parti del testo cifrato con altre valide).

In maniera schematica si può ipotizzare una situazione in cui un soggetto M (mittente) desidera comunicare in maniera protetta con un soggetto D (destinatario) e un terzo soggetto S (spia) voglia intromettersi; S può avere moltissime ragioni per farlo come ad esempio sapere che cosa si dicono o alterare i messaggi in modo da averne un guadagno. Il primo scopo è in genere movente di un comportamento *passivo* da parte di S (ci si limita ad "ascoltare"), mentre il secondo lo spinge ad un comportamento *attivo* (di intrusione nella comunicazione).

Le ipotesi fondamentali della crittanalisi sono due:

- Eventuali attaccanti hanno una perfetta conoscenza dell'algoritmo utilizzato per cifrare il messaggio e di tutti i dettagli della sua realizzazione
- Eventuali attaccanti hanno completo accesso al canale di comunicazione e possono pertanto intercettare, interrompere, creare o modificare qualsiasi flusso di dati

La spia S può sferrare un attacco al testo cifrato in diversi modi, in generale in maniera dipendente dalle informazioni che è riuscito ad ottenere; si distingue allora tra:

Cypher-Text Only Attack: la spia ha a disposizione solo il messaggio cifrato da cui determinare il messaggio in chiaro; la spia deve cercare di ricorrere ad ogni sotterfugio possibile per carpire il significato del messaggio, ad esempio utilizzando ricorrenze statistiche o regole matematiche. Un attacco di questo tipo è sempre possibile e si presuppone che un crittosistema non possa essere considerato sicuro se non vi resiste. In questa trattazione verrà considerato principalmente questo tipo di attacco.

Known Plain-Text Attack: S ha a disposizione una serie di coppie (x_i,y_i) rispettivamente di testo in chiaro e di testo cifrato (non a sua scelta) per poter forzare il sistema. Il testo in chiaro può o meno essere in una posizione nota dalla spia S, ma in generale il messaggio da decifrare è sufficientemente corto da permettere alla stessa spia di assumere che possa trovarsi in ogni possibile posizione e lanciare una serie di controlli in parallelo per ogni caso. In questo caso, il testo in chiaro noto potrebbe essere un qualcosa di così comune da essere sicuri che ci sia nel messaggio.

Nei seguenti tipi di attacchi, la spia S ha, inoltre, la possibilità di alterare il messaggio originale con parti a sua scelta; un codice che resiste a questi attacchi è ovviamente più apprezzato.

Chosen Plain-Text Attack: la spia ha la capacità di trovare il testo cifrato corrispondente ad un arbitrario messaggio di testo in chiaro a sua scelta.

Chosen Cypher-Text Attack: la spia può scegliere arbitrariamente il testo cifrato e trovare il corrispondente testo in chiaro.

Adaptive Chosen Plain-Text Attack: la spia può determinare il testo cifrato di un testo in chiaro da lui scelto in un processo interattivo o iterativo basato su risultati precedentemente acquisiti. Questo è il nome generale per un metodo di attacco chiamato *crittanalisi differenziale*. Più specificamente, se si hanno due coppie di testo in chiaro e testo cifrato, la crittanalisi differenziale consiste nell'eseguire un EXOR bit a bit dei due testi in chiaro e dei due testi cifrati e di confrontarne le differenze (da cui differenziale). In questa trattazione in realtà ci si limiterà alla crittanalisi di cifrari semplici, quindi non si tratteranno algoritmi come il *Data Encryption Standard* (DES) per cui viene utilizzata la crittanalisi differenziale e l'RSA (nome derivato dagli inventori: Ron Rivest, Adi Shamir e Len Adleman).

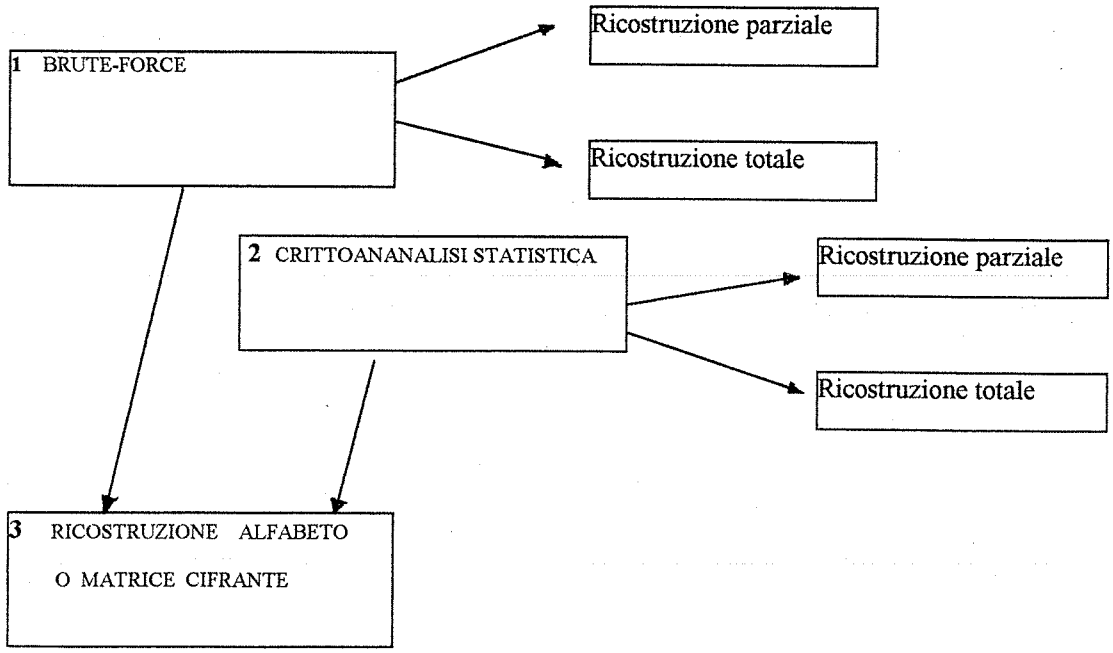
Se ci si limita ad una spia di tipo *passivo* si deve ricordare che il suo scopo è solo quello di capire che cosa voglia dire il messaggio che deve analizzare; questo non porta sempre la spia a svelare la chiave o a ricostruire l'alfabeto o la matrice cifrante, ma il più delle volte le basta capire il senso del messaggio, anche se l'analisi non è risultata perfetta (ad esempio, se si legge "dpmpni vengp p trovprti" si capisce lo stesso cosa voglia dire). Se invece si vuole manomettere il testo cifrato, assumendo quindi un ruolo attivo, è ovvio che bisogna arrivare a scoprire la chiave o a ricostruire gli strumenti cifranti.

Il risultato di un attacco può quindi essere classificato come segue:

- forzatura totale (si è scoperta la chiave o l'algoritmo usato)
- deduzione globale (si è trovato un surrogato che ha portato alla conoscenza del testo in chiaro)
- deduzione locale (solo alcune parti crittogramma sono state decifrate)
- deduzione parziale (si è estratta qualche informazione sul messaggio ma non lo si è scoperto completamente)
- fallimento (nessuna informazione è stata carpita).

Per quanto riguarda la deduzione parziale, locale e globale possono essere il risultato di due metodi: della **crittanalisi statistica** o del **metodo Brute-Force**. Con questi due sistemi si riesce spesso a carpire parte o tutto il testo in chiaro, ma non si riesce scoprire la chiave utilizzata. D'altro canto per riuscire a dedurre l'alfabeto cifrante o le varie matrici utilizzate nel crittare il messaggio è necessario partire da qualcosa di noto per es. da qualche corrispondenza nota tra lettere del testo in chiaro e del testo cifrato (nel caso di cifrari a sostituzione). È proprio in questo caso che tornano utili i due metodi sopra menzionati; possono essere quindi anche utilizzati per ottenere sufficienti informazioni per poter intraprendere un'analisi completa di decifrazione (forzatura totale).

Il seguente schema mostra le possibilità di decifrazione:



Per ricostruzione parziale o totale si intende ricostruzione dell'alfabeto cifrante o della matrice cifrante o comunque della chiave utilizzata e quindi del testo in chiaro.

Nella crittanalisi quindi è possibile intraprendere solo l'attacco 1 o solo il 2 o l'1 + 3 o il 2 + 3. Il 3 da solo è molto improbabile che porti a qualche successo.

(segue)