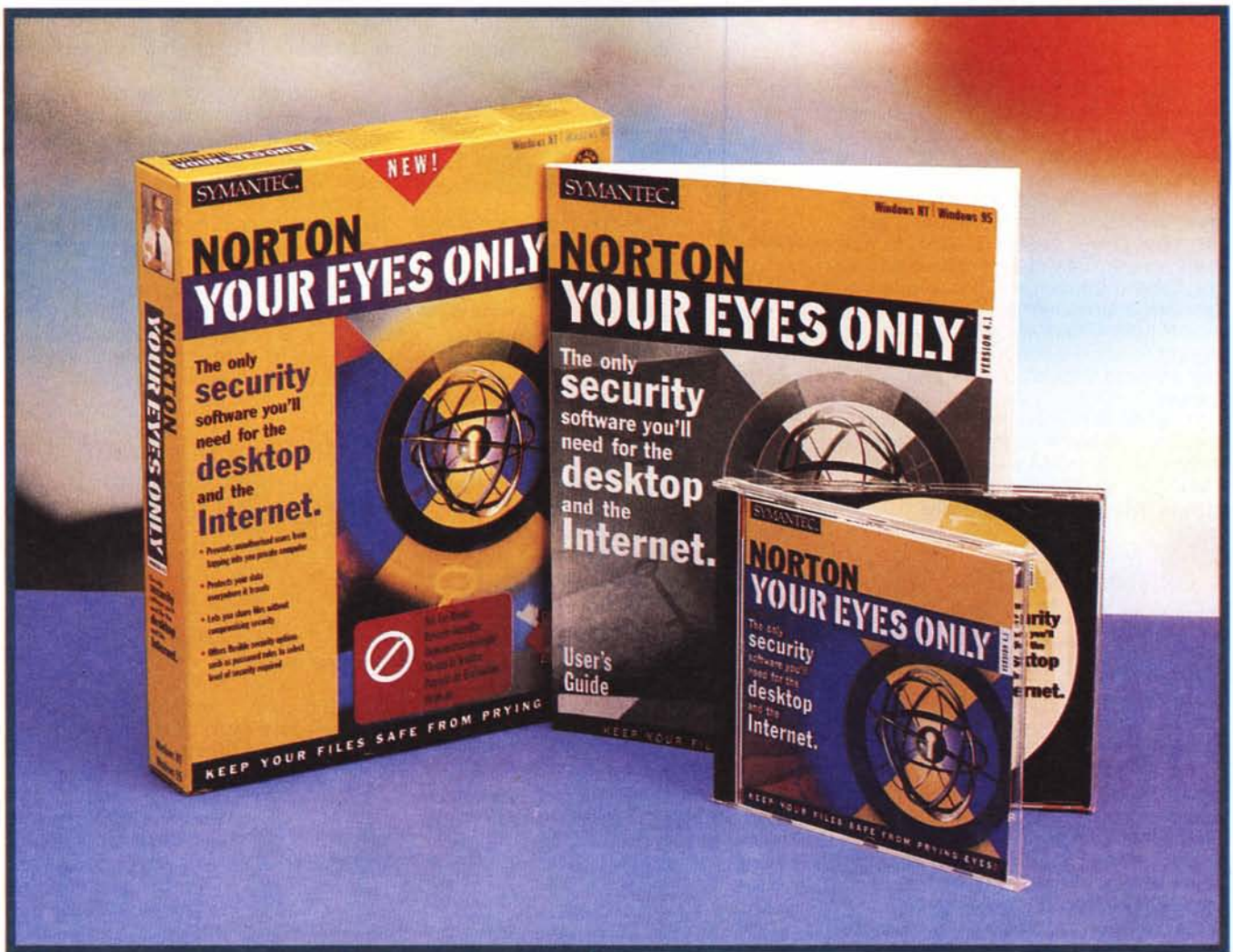
Prova

di Raffaello De Masi



Symantec Norton Your Eyes Only 4.1

Ognuno di noi ha avuto, per un verso o per l'altro, necessità, nella vita, di tenere segrete certe informazioni; le ragazzine scrivono lettere a Leonardo Di Caprio sul loro diario chiuso con un lucchetto, giovincelli focosi scaricano da Internet immagini di donnine scollacciate, poco esponibili al pubblico, diafane fanciulle nascondono nei recessi segreti della propria stanza poesie d'amore da far impallidire Prevert. Insomma, per un motivo o per un altro ognuno, per i motivi anche più innocenti di questo mondo, ha da nascondere qualcosa.

Anche io, confesso, ho da nascondere qualcosa; sono riuscito a procurarmi una barra di cioccolato fondente da quattro chili, un mostro di quelli utilizzati dai pasticcieri professionisti, che non si può neppure mordere, tanto è grossa e dura.

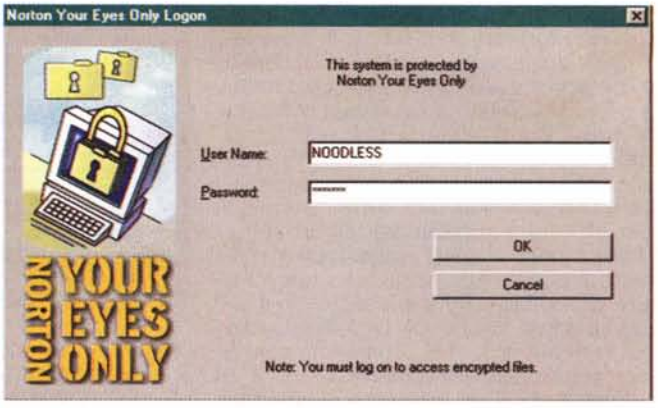
Ogni tanto le faccio una visitina disinteressata, e a botte di scalpello e martello mi rimetto in pari con la mia razione di trigliceridi; e poi, i latini dicevano "Gutta cavat lapidem, non vi, sed saepe cadendo". Quando ero ragazzo, vittima di una mamma più "tosta" di un maresciallo, ero costretto a nascondere ogni cosa ai suoi occhi; figuratevi che era capace di andare a spiare nel mio portafogli, fino a quando ci lasciai un biglietto che recitava: "Ma perché non ti fai i... tuoi?". Allora smise, ma veniva ad ascoltare dietro la porta quando telefonavo a qualche ragazza, telefonava ai miei amici per sapere di questa o di quella mia amicizia femminile, era una vera ossessione, povera donna! Se qualcuno, ovviamente molto più giovane di me, mi sta leggendo e immagina che possa dargli una soluzione contro mamme del genere, purtroppo sono costretto a disilluderlo; bisogna tenersela, ma vi posso assicurare che, poi, non è il male più grande del mondo.

Symantec Norton Your Eyes Only

Produttore :
Symantec Corporation
10201 Torre Avenue
Cupertino (CA) 95014
http://www.symantec.com

Distribuito in Italia da:
Symantec s.r.l.
Via Abbadese, 40
20124 - Milano.Tel. 02/695521
http: //www.symantec.it

Prezzo (IVA esclusa):
Lit. 169.000



La finestra offerta da NYEO all'accensione del computer; non indicando la password non sarà possibile aprire documenti protetti.

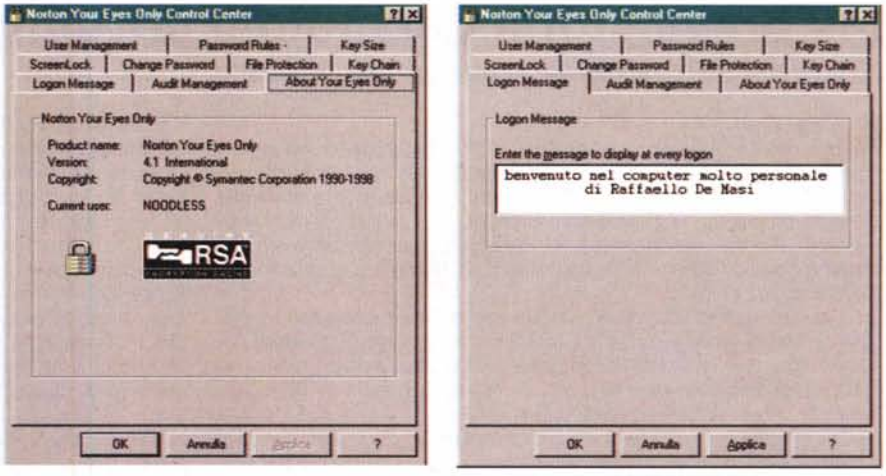
Fortunatamente invece la soluzione è più rosea per il mondo informatico; pacchetti che difendono il contenuto dei nostri dischi da occhi indiscreti ce ne sono, e anche parecchi. E ci si rende conto che l'esigenza di segretezza che ha animato questo mondo è di vecchissima data, visto che fin dagli albori della microinformatica (parlo della fine degli anni '70) sono immediatamente comparsi sulla scena pacchetti e utility destinate allo scopo.

All'inizio si trattava di applicazioni rudimentali, che, senza troppe raffinatezze, affrontavano il problema ad esempio facendo sparire i file dalle directory, nascondendoli sotto altro nome, rendendoli illeggibili con qualche forma di crittazione.

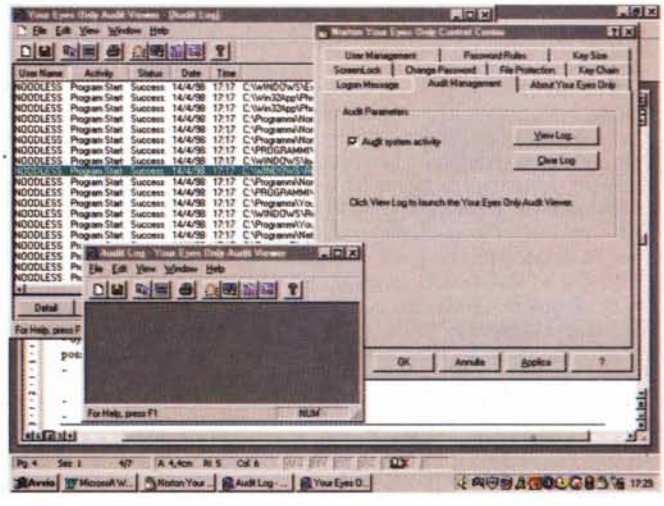
Ricordo che Mino, un mio amico che è per me più di un fratello mi chiese, tanti anni fa, come fare per nascondere una serie di dati in alcune caselle di Excel. Escogitammo allora un sistema non proprio raffinatissimo, ma che funzionava alla perfezione. Poiché le caselle contenevano solo dati numerici, fu sufficiente indicare come formato del numero un carattere "blank" per far sparire, come d'incanto, tutti i valori desiderati dalla pagina. Il trick funziona anche adesso, e credo che Mino lo utilizzi ancora oggi con sua soddisfazione.

Fortunatamente, come dicevamo, oggi l'ambiente si è evoluto in maniera articolata; basta pensare alle tecniche, del tutto trasparenti all'utente, del trasferimento "secure" dei dati su Internet per capire a quale livello di sofisticazione siano giunte oggi le tecniche di lock-encrypt dei dati. Oggi la maggior parte dei pacchetti di posta elettronica, possiede un suo motore interno di cifratura che rende il trasferimento di notizie riservate veramente sicuro.

Ma ritorniamo a noi; il problema di oggi è semplice, abbiamo il nostro PC in ufficio o allo studio, con le nostre cose (per l'amor di Dio, nessun segreto, solo che non ci va che altri mettano il naso nei nostri file) e desideriamo che nessuno ci possa mettere mano; NYEO, come è chiamato dagli addetti ai lavori Your Eyes Only, fa al caso vostro.



Gli splashscreen di NYEO, con le caratteristiche generali del pacchetto e la personalizzazione del messaggio di benvenuto.



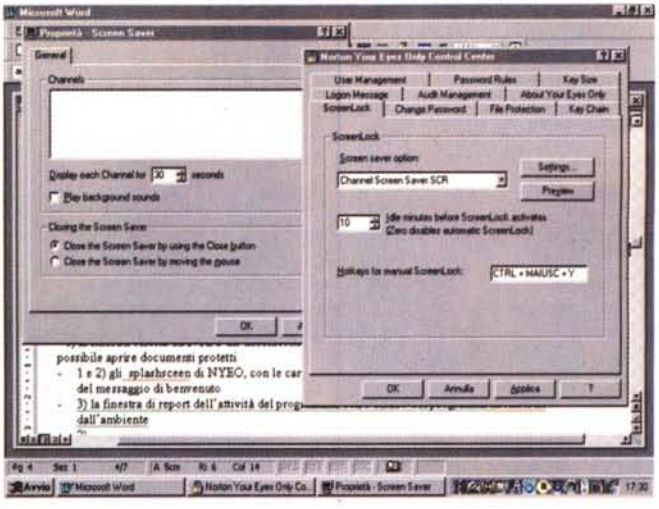
La finestra di report dell'attività del programma, con l'elenco dei programmi monitorati dall'ambiente.

Prova

NYEO, il pacchetto

NYEO fornisce due servizi di base relativi alla sicurezza; controlla l'accesso alla macchina e ai file in essa contenuti, e cifra i file. Si compone di due differenti utility, BootLock e SmartLock. Il primo è un vero e proprio programma di controllo d'accesso, con numerose facce e tecniche d'utilizzo, ed è disegnato per prevenire accessi non autorizzati a sistemi W95, accessi eseguiti sia in maniera standard che attraverso tecniche alternative (ad esempio, lanciando il sistema da un dischetto). La salvaguardia del sistema e dei file è garantita anche su sistemi sotto Windows NT.

SmartLock è un ambiente di cifratura "on the fly", vale a dire sensibile alle operazioni dell'utente; la cifratura avviene automaticamente se si parte da un'applicazione, e il file viene successivamente di nuovo crittato quando l'applicazione viene chiusa. Inoltre NYEO offre un metodo di cifratura manuale, per esigenze particolari, come quella di "chiudere" un file e successivamente depositarlo su una memoria di massa di un network o su un disco removibile per una successiva lettura.



Il setup dello screen saver che, una volta lanciato, può essere istruito a non disabilitarsi se non dopo l'inserimento della password.

Una breve storia dei metodi crittografici

scritta in maniera da far impallidire d'invidia Corrado Giustozzi

Caro Corrado,

ricordo che una volta, sulle pagine di MC, caso voleva (ed era un puro caso, c'è da crederci) che, quasi ogni mese, in rubriche diverse trattassimo spesso gli stessi argomenti. La cosa mi è tornata alla mente sfogliando le pagine dei vecchi numeri, per la rubrica "Altri tempi". E nei numeri intorno al 60, me ne sono ricordato solo ora, abbiamo trattato l'argomento crittografia, tu in Intelligiochi e chi scrive in MCAlgoritmi.

Ne è passata di coca nelle bottiglie (perdonami, l'acqua non mi piace per nulla, né quando vado al mare né versata nei bicchieri; e poi sono rigorosamente astemio) e dopo una quindicina d'anni, complice NYEO, eccomi a riparlare di cifratura. Ricordo che allora mi rivolsi alla libreria "Anglo American Book" in Via della Vite a Roma, che mi fornì una preziosa consulenza bibliografica e copie di documenti rari e di materiale declassificato; oggi basta fare un giretto su WWW per procurarsi tanto di quel materiale da scriverci un libro. Per stavolta mi limito a scriverci un riquadro, che serve a due cose: evitare che l'articolo divenga un mattone, e permettermi di salutare un amico con cui, una volta, frequentemente lanciavamo allusioni e frecciate sulle pagine della rivista.

Si definisce cifratura, il metodo in base al quale un messaggio può essere interpretato solo da certe parti o persone, in quanto il suo testo è stato sottoposto a manipolazioni tali da renderne incomprensibile il significato. Le tecniche di crittografia (dal greco kriptao, nascondo) vanno, ovviamente, di pari passo con quelle di decrittazione, essendo le une inutili senza le altre.

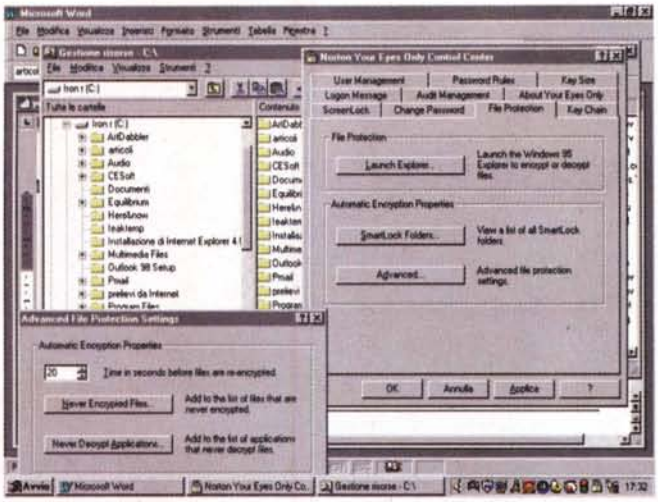
L'esigenza di cifratura dei messaggi è sempre stata sentita, nella storia dell'umanità, e menti anche famose non hanno disdegnato di cimentarsi con tali tecniche, in un senso e nell'altro (generalmente la scoperta di un metodo di decrittazione impiega molte più risorse ed energie del contrario). Sebbene il codice Cesare abbia assunto notorietà estrema come il primo metodo codificato, occorre precisare che già i greci, ai tempi di Lisandro, usavano più o meno correntemente la scitala lacedaemonica (pare inventata almeno quattrocento anni prima), che si basava sull'uso di un bastone su cui era avvolta a spirale, lungo l'asse e in direzione della lunghezza, una striscilina di pelle o stoffa. Su questa si scriveva poi il messaggio, nel senso della lunghezza del bastone, in modo che ogni lettera capitasse su una spira dell'elica. Dopo lo svolgimento il messaggio si presentava come una serie senza senso di lettere e, per la lettura, occorreva avere un bastone dello stesso diametro di quello di partenza, che funzionava, si può dire, da chiave d'interpretazione.

Enea il Tattico, generale della lega arcadica, sviluppò, nella prima metà del quarto secolo a.C. un disco cifrante, da lui stesso descritto in un suo trattato di arte militare. Si tratta di un disco di legno che ha, sul suo bordo, ventiquattro fori, ognuno corrispondente a una lettera. La chiave sta nella disposizione confusa delle lettere lungo il bordo (disposizione che fa parte di un anello esterno di riferimento, in possesso dei due corrispondenti); un filo, in funzione del messaggio, viene fatto passare attraverso i corrispondenti fori; all'arrivo esso è svolto e il messaggio letto al rovescio.

Polibio, nato a Megalopoli intorno al 200 a.C. inventò, per la Lega Achea, un sistema di cifratura che doveva servire per la trasmissione di messaggi a vista, per mezzo di torce o di bandierine. Le venticinque lettere greche venivano trascritte, nell'ordine, in un quadrato di 5x5 lati, e la stringa del messaggio trasposta in una serie numerica, ovviamente di lunghezza doppia dell'originale, in funzione dei numeri di riga e colonna; sebbene sia facilmente violabile in base all'analisi statistica delle frequenze, il codice è importante perché introduce il concetto di conversione in numero, la riduzione del numero dei simboli e la riduzione del simbolo in due parti. Su questi tipi di scacchiere si baserà il lavoro di molti studiosi successivi.

Il medioevo non è privo di esempi validi di tecniche di cifratura; in questo periodo furono molto diffuse le nomenclature, vale a dire le tecniche di indicare una parola (e più spesso un nome proprio) con un simbolo, un segno immaginario, e così via. L'antipapa Clemente VII adottò una nomenclatura (elenco di parole chiave) elaborata da Gabriele Levinde, ma è solo verso la metà del 1400 che si notano i primi veri tentativi di superare il problema dell'analisi statistica delle frequenze nel messaggio; il problema fu risolto con l'introduzione dei cosiddetti "gruppi cifranti", sequenze di lettere che ne indicavano un'altra e che non erano mai gli stessi nello stesso messaggio. La sicurezza di una comunicazione era ovviamente legata all'abbondanza di tali gruppi e, sebbene il sistema fosse abbastanza resistente agli attacchi, cadde inspiegabilmente in declino, tanto che fu applicato solo in maniera distratta per tutto il Settecento e i primi dell'Ottocento (pare che il disastro russo e la sconfitta di Lipsia di Napoleone siano dovuti alla scarsa impenetrabilità dei messaggi assegnati ai portaordini intercettati dal nemico).

Intorno al 1459 Leon Battista Alberti inventa un ingegnoso sistema basato sull'uso di una coppia di dischi cifranti; non si sa bene perché, il volume in cui tale tecnica è descritta, il "Trattato della Cifra", non fu mai pubblicato se non circa un secolo dopo, e non gli fu mai prestata soverchia attenzione. Come dicevamo, questa efficace tecnica si basa sull'uso di due anelli concentrici di cui l'interno contiene venti lettere maiuscole dell'alfabeto latino e quattro cifre, quello esterno le ventiquattro minuscole; le prime sono in ordine alfabetico, le seconde sono alla rinfusa. Il principio si basa sul fatto che un unico messaggio è cifrato con diverse chiavi successive, in modo da evitare l'analisi statistica. Ad esempio, fissata una lettera maiuscola come indice, si sceglie sul disco interno la minuscola su cui basare la cifratura e si fanno



Un esempio della ricerca e della selezione dei file da cifrare e proteggere; questa operazione può avvenire sia singolarmente sia, come in questo caso, servendosi dell'Explorer di Windows.

Il package può essere installato sotto W95 e NT, su sistemi con almeno un 486/33 MHz con 16 MB di memoria (per funzionare sotto NT è necessario disporre di un Pentium, dell'NT Workstation 4.x, service Pack release 3). In ambedue i casi sono necessari circa 10 MB di spazio su disco. Al momento della installazione si può scegliere di inserire il BootLock, sistema che previene accessi non autorizzati a una macchina allo startup, e viene richiesto se si desidera poter gestire il sistema da un Emergency Unlock Disk. Questa seconda opzione non è intuitiva ma la si comprende quando si immagina di avere NYEO sulla macchina principale e si desidera gestire successivamente un documento su un'altra (ad esempio un laptop) senza dover montare tutto il programma. Ovviamente il dischetto servirà anche in caso di problema del programma principale. Durante la creazione di questo disco, infatti, viene non solo installata un'utility di decifrazione, ma anche il database delle chiavi di accesso ai vari file.

L'installazione avviene attraverso anche la scelta di un nome utente e di una password, ed è inutile raccontare qui quello che sulle pagine della nostra rivi-

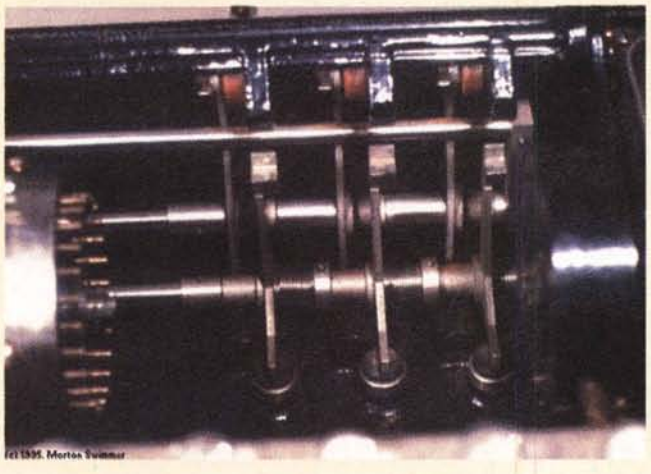
coincidere le due lettere. Una parte del messaggio viene così codificata secondo le corrispondenze. Se si decide, nel corso della cifratura, di cambiare chiave, si esegue di nuovo l'operazione, si porterà la nuova lettera chiave a coincidere con l'indice e si continuerà. Poiché le lettere maiuscole rappresentano un indubbio punto di riferimento per l'addetto alla decifratura, lo stesso Alberti consigliava di usare uno dei quattro numeri come riferimento del cambio d'ordinamento.

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

C	A	R	L	O
S	B	D	E	F
G	H	IJ	K	M
N	P	Q	T	U
V	W	X	Y	Z

Alcuni esempi di tabelle di codifica con differenti tecniche di cifratura, nell'ordine il codice di Polibio, una tabella di Playfair e una matrice di Vigenère; visibili anche alcuni particolari di una Enigma, intera e smontata. Il codice prodotto da questa macchina fu inaccessibile fino alla cattura di una unità da parte di Jan Fleming (già, il padre di James Bond); il sistema di decodifica fu scoperto poco dopo, ma i tedeschi non ammisero mai questa perdita, e sostennero sempre che l'unità era affondata in mare con tutto l'equipaggio, portando con sé l'esemplare.

Uno studio attentissimo di Enigma, con una gran quantità di foto dei particolari anche minimi, può essere trovato al sito http://www.math.arizona.edu/~dsl, da dove sono state ricavate le immagini e la maggior parte delle notizie del riquadro. E se proprio desiderate risentire il profumo dei bunker segreti del fronte occidentale, collegatevi al sito http://www.adelheid.demon.co.uk/enigma.html, dal quale potrete scaricare una versione software della vostra enigma...tica macchina (l'autore, onore al merito, è tal Peter G. Strangman , Peter@adelheid.demon.co.uk) e scambiare messaggi, più o meno impenetrabili, con tutto il mondo.



E' della metà del 1500 la pubblicazione del "De furtivis literarum noti" di Giovan Battista della Porta, codifica basata sull'uso di tavole di conversione e di alfabeti fissi; interessante è, di questa tecnica, l'uso del "verme letterario", parola usata per produrre il periodo di cifratura. Della Porta usò undici alfabeti arbitrari, e sebbene la tecnica fosse efficace, il numero ridotto di questi alfabeti ne era un po' il tallone d'Achille. Una variazione a tale tecnica, in ogni modo, non si fece aspettare. Un altro Giovan Battista, stavolta Bellaso, pubblicò, qualche anno dopo, un libretto in cui introduceva i suoi cifrari polialfabetici, basati sull'idea che gli alfabeti arbitrari destinati alla cifratura non erano fissi, ma prodotti da una parola, frase o motto convenuti (noti solo al mittente e al destinatario). La tecnica era buona ma il numero di alfabeti generato, ancora ridotto, non portava ancora a un miglioramento effettivo.

A dimostrazione che la fortuna certe volte è proprio cieca, citeremo come un codice piuttosto debole abbia avuto fortuna per tanto tempo; Blaise de Vigenère presentò nel 1586 un trattato nel quale proponeva una tecnica di cifratura semplice e pratica, che offriva una certa sicurezza e alcune difficoltà alla violazione. Si tratta, forse, dell'ultimo e più illustre esempio di codice a sostituzione polialfabetica, ed ha avuto una lunga e immeritata fama, usato come è stato da diversi eserciti anche dopo che fu pubblicato un metodo di decrittazione che lo rendeva perfettamente inutile.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

La scelta di un algoritmo di cifratura

NYEO offre all'utente diversi metodi di cifratura, basati su algoritmi crittografici a chiave simmetrica standard e ben conosciuti. Gli algoritmi descritti successivamente, disponibili nelle opzioni del pacchetto, sono differenti per sicurezza, resistenza alla decrittazione e velocità delle operazioni di cifratura e decifratura. NYEO offre diversi protocolli di cifratura, tra cui:

- RC4 e RC5: questi due algoritmi sono stati sviluppati dalla RSA e usano una chiave a 128 bit. RC4 è più veloce di RC5, ma talvolta meno sicuro
- DES BCB; adottato come standard dal governo degli Stati Uniti nel 1977, si basa su una chiave a 56 bit ed è discretamente efficace
- Triplo DES; un'implementazione più recente del precedente, che ne raddoppia, per una serie di motivi, la sicurezza. Si basa sul vecchio algoritmo del DES a 56 bit, applicato tre volte con tre differenti chiavi
- CBC blowfish; è un algoritmo sviluppato da Bruce Schneier, autore del famoso trattato Applied Cryptography; molto veloce, è notevolmente sicuro e usa una chiave a 128 bit ed è particolarmente adatto per macchine a 32 bit
- RC4 e DES internazionali; un efficiente algoritmo con chiave a 40 bit, approvato dal Governo USA per l'esportazione al di fuori degli USA e del Canada. E' la versione standard da usare per utenti internazionali che adottano NYEO

sta, Corrado ha, certamente in maniera più esauriente e chiara, raccomandato circa la scelta e la tenuta di questi parametri. Ovviamente l'Emergency Unlock Disk va costantemente aggiornato, altrimenti non sarebbe in grado di decifrare documenti trattati dopo la sua creazione.

Usando NYEO

Usare Norton Your Eyes Only è cosa agevole e pratica, dato che, dopo un minimo di organizzazione iniziale, il funzionamento del pacchetto è pressoché trasparente. Al primo lancio, se si è scelto di inserire anche il BootLock si apre una finestrina che chiede l'inserimento dell'User Name e della Password (poiché BootLock parte prima del sistema operativo occorre, essendo disabilitato il mouse, usare il Tab per passare da

Il metodo di Vigenère ha il vantaggio di essere estremamente semplice e si può considerare l'evoluzione più avanzata del codice di Cesare. Esso si basa sull'uso di un "verme", una parola riservata che viene ripetuta, senza spazi, tante volte fino alla corrispondenza con la lunghezza del messaggio stesso. Intendiamoci con un esempio.

Si voglia cifrare il messaggio "Leggete MCMicrocomputer"; stabiliremo come chiave la parola "rivista", i passi da eseguire li vedete di seguito

testo in chiaro:	LEGGETEMCMICROCOMPUTER
verme:	RIVISTARIVISTARIVISTAR
testo cifrato:	CMBOWMEDKHQUKOTWHXMMEI

Il testo finale cifrato si otterrà shiftando, sull'alfabeto, verso destra, ogni lettera del messaggio in chiaro dell'ordinale della lettera corrispondente al verme. Così la L diventa C, E diviene M alla prima occorrenza, ma W alla seconda e la terza volta resta E. Due righe di C o di BASIC, o magari anche una routine in Excel, e potremo scriverci la nostra utility di cifratura e decifrazione. Vigenère offriva anche una tavola per la conversione immediata che poteva essere usata per la cifratura e la decifratura.

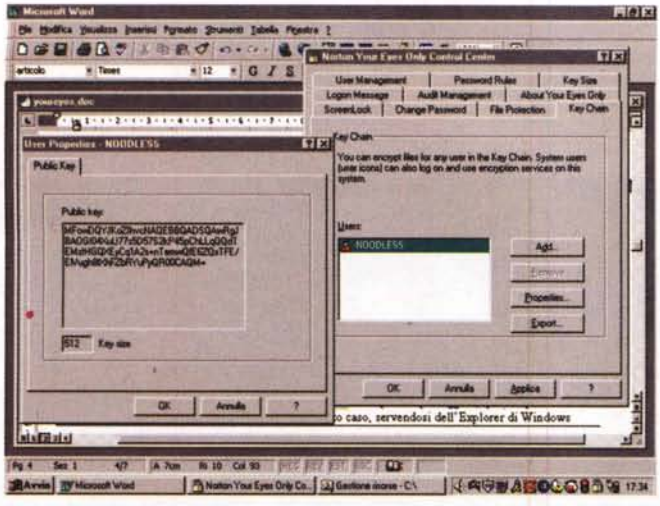
La macchina di Jefferson, dovuta proprio al presidente che redasse la Dichiarazione d'Indipendenza proclamata a Filadelfia, è il primo esempio di macchina cifrante, per così dire. Il principio su cui si basa ha dato poi origine a macchine più potenti e complesse, tra cui anche la famosissima Enigma tedesca. E' pratica e facile da usare, sebbene abbia avuto alterna fortuna fin dalla sua nascita (ai suoi tempi era praticamente inattaccabile, ma il fatto di essere meccanica le precluse sempre il favore delle alte sfere militari); il principio e la sicurezza di funzionamento erano tanto efficaci che fu riscoperta nel '22 dall'esercito americano, che la mantenne in servizio fin dopo la seconda guerra mondiale.

Il principio di funzionamento è tanto semplice da lasciare perplessi sull'effettiva efficacia del metodo. L'apparecchio è rappresentato da un tamburo su cui girano trentasei dischi coassiali, ognuno con impressi sul bordo i caratteri dell'alfabeto in maniera del tutto casuale e diversa l'uno dall'altro. La chiave è numerica, dall'uno al venticinque; si compone la frase, in un traguardo, su una qualsiasi riga e si ruota la fila di dischi di un numero pari al valore della chiave; la frase che si leggerà nel traguardo sarà il messaggio cifrato. La vera complicazione sta nel fatto che l'ordine dei dischi sul tamburo può essere variato come si crede; poiché la caduta di una serie di dischi in mano al nemico poteva compromettere la sicurezza della messaggistica, le forniture militari prevedevano un numero di dischi elevato (oltre duecento) ognuno con permutazioni dell'alfabeto differenti; il vero segreto da mantenere stava quindi solo nei dischetti da utilizzare e nell'ordine con cui venivano inseriti nel tamburo (la combinazione di questi con la chiave di rotazione rendeva inaccessibile il sistema stesso).

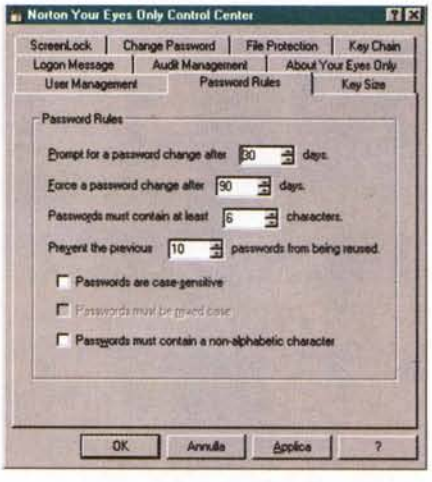
Due parole, infine sul Playfair Chipher e sulla più recente cifra campale germanica. Il primo fu inventato da sir Wheatstone intorno al 1845, ma si deve a Playfair se fu portato a conoscenza delle alte sfere militari durante una cena offerta da Sir Granville a Lord Palmerston, ministro degli esteri di Sua Maestà. Fu utilizzato per la prima volta nella sanguinosa guerra contro i Boeri. Il cifrario si basa su una tavola quadrata di venticinque lettere ed è il primo metodo di cifratura a bigrammi. La parola chiave viene scritta nelle prime caselle (eliminando le doppie) e le restanti lettere dell'alfabeto vengo scritte di conseguenza, saltando quelle che già sono scritte in precedenza. Il testo da cifrare viene scomposto in bigrammi e le lettere si cercano nel quadrato in base a regole diverse a seconda di come, in questo quadrato, sono posizionate. La cifratura è abbastanza rapida, ma presenta un difetto; la parola chiave è presente sempre all'inizio del quadrato, le lettere meno frequenti lo sono verso l'ultimo, e, alla fine del quadrato, ci sono lettere messe sempre in ordine alfabetico. In particolari casi questo consente di risalire rapidamente al messaggio e alla parola radice.

La Cifra Campale germanica è un metodo usato fin dall'inizio della 1ª guerra mondiale dall'esercito tedesco. Anch'esso si basa su una scacchiera a venticinque posti, che usa, come simboli delle coordinate, segnali Morse difficilmente confondibili tra loro. La matrice viene costruita allo stesso modo del metodo Playfair, e alle lettere del messaggio in chiaro vengono sostituiti bigrammi cifrati, formati dalla coppia di lettere che ne rappresentano le coordinate. Questi bigrammi vengono inseriti in una seconda matrice, anch'essa dotata di una chiave alfabetica e di una numerica, da cui si ricavano bigrammi poi combinati assieme per ottenere la cifratura finale. Il sistema della doppia cifratura rende il metodo difficile da demolire, tant'è che è considerato, ancora oggi, uno dei efficienti, anche se, ovviamente, la disponibilità di computer permette di analizzare in tempi brevi un enorme numero di combinazioni diverse, con conseguente notevole riduzione dei tempi di scoperta delle chiavi.

Di Enigma, la macchina di cifratura leggendaria dell'esercito tedesco della seconda guerra mondiale, Corrado ha fin troppo parlato su queste pagine perché io possa in qualche modo illudermi di aggiungere qualcosa di nuovo. E oltre non credo di dover andare; questo riquadro non ha alcuna pretesa di trattazione di alcun genere, è solo qualche riga su un argomento che certo non finirà qui. E non ci azzardiamo neppure ad andare oltre le date della seconda guerra mondiale; la disponibilità di computer sempre più potenti, capaci di opporre tecniche euristiche e forza bruta alle più sofisticate modalità di cifratura, ha dato una spinta all'acceleratore incredibile; basti pensare che il DES e l'RSA, sistemi di codifica ritenuti inattaccabili (il primo frutto delle ricerche svolte in seno all'IBM), oggi cominciano a vacillare, come ha dimostrato Hellman della Stanford University



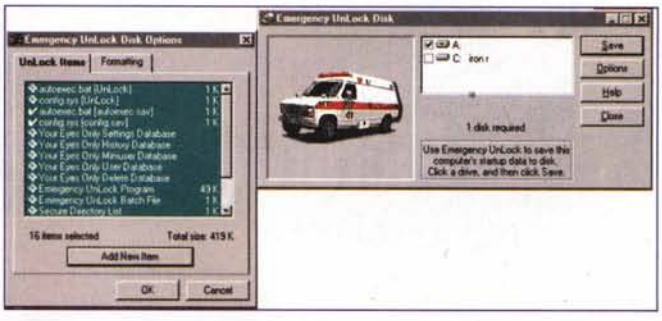
Un esempio di cifratura a chiave pubblica di un file, con la sequenza chiave mostrata sulla sinistra.



Un esempio della gestione delle password; il programma obbliga l'utente al cambio dopo un certo periodo ed evita che, per pigrizia, si usino sempre le stesse.

campo a campo). La prima cosa da fare è passare attraverso il NYEO Control Center, che contiene una serie di setup per la gestione dell'ambiente e del materiale che, attraverso di esso, passerà. La sofisticazione del sistema appare subito elevata, se si pensa che è possibile bloccare addirittura lo schermo; in questo modo la macchina diverrà insensibile a qualunque intervento, e continuerà a mostrare un salvaschermo se non si inserirà la password giusta. Questa potrà essere cambiata in ogni momento (anzi, è raccomandato che questo avvenga spesso) e il manuale dà anche una serie di consigli per una scelta oculata della stessa. La scelta dei file da cifrare può essere automatica (si sceglie una o più cartelle di default, e tutto quel che in esse c'è verrà cifrato automaticamente) o manuale, e si può indicare alla macchina di cancellare in maniera "sicura" i file dal disco quando questi vengono infilati nel cestino (in gergo più preciso vengono azzerati i cluster che contengono i dati del file). BootLock protegge efficacemente la macchina dall'accesso attraverso altre periferiche cifrando anche parte del sistema operativo, ed è questo il motivo per cui la creazione e il continuo aggiornamento del dischetto di emergenza è la fase più importante e critica dell'ambiente. L'Emergency Unlock disk può risolvere davvero una situazione che potrebbe rivelarsi disastrosa, ma attenzione, la perdita della password può rappresentare davvero un disastro.

Tanto per intenderci, se state lavorando sulla versione personal, avete perso la password, e siete stati tanto pigri da non esservi preparato e aggiornato per tempo il disco d'emergenza, siete in un bell'impiccio; l'unica prospettiva è quella che vi rassegniate a perdere i vostri file cifrati. Neppure Symantec vi può dare una mano. Un po' più rosea è la situazione se state lavorando con una versione condivisa in quanto queste versioni prevedono sempre un supervisore che potrà aiutarvi, avendo lui libero accesso a ogni file del sistema, attraverso il suo ambiente di amministratore. Ma, sempre per i sistemi condivisi, c'è un'altra soluzione; il sistema possiede quella che comunemente viene detta i gergo la one-time password, un'opzione che fornisce una password utilizzabile una volta sola. La one time password è comunque uno di quei sistemi che si definiscono in gergo "a uomo morto", vale a dire che può essere abilitata solo in presenza di due utenti, tipicamente l'amministratore della sicurezza e l'utente finale. In ogni caso il sistema tiene sempre aggiornato un registro dei login, tentati o giunti ad effetto, con i relativi risultati.



La creazione di un disco di emergenza; inutile piangere quando il latte sarà versato, il recupero potrebbe divenire impossibile.

Qualunque sia la modalità di lavoro NYEO cifra solamente file di dati; i file con suffisso .EXE o .DLL sono ignorati automaticamente dal pacchetto, a meno di non indicare specificamente al programma di cifrarli (ma perché poi?). I file sono decifrati automaticamente quando sono lanciati da desktop o quando un'applicazione li chiama; anche questa opzione può essere disabilitata dall'utente. In ogni caso tutti i file cifrati sono elencati nell'albero completo della loro locazione sul disco. Ogni file, cifrato con un certo algoritmo, può essere convertito ad un altro senza che per questo debba essere decifrato.

E per finire, qualche parola sulla gerarchia delle utenze in caso di sistemi condivisi. Esiste, in questo caso, il classico Utente Primario (altrove chiamato Amministratore o SuperUtente), mentre i secondari godono dei privilegi che il precedente decide di assegnare loro. Le possibilità di accesso di un utente sono stabilite e riassunte in un elenco dei diritti dell'ospite, e queste possono anche essere definite non per un network, ma per un singolo PC cui hanno accesso diversi utenti. Un utente secondario può essere, per così dire, mobile, vale a dire che un utente guest può portare con sé una chiave d'accesso che gli consente di accedere a diversi PC, anche fisicamente separati. Le password d'accesso sono verificate dal sistema, nel senso che l'ambiente è fatto in modo da avvisare l'utente di cambiare la password dopo un certo numero di giorni (da 1 a 255; 30 è il default) o di obbligarlo, al logon, a farlo se gli inviti precedenti non hanno avuto successo.

Conclusioni.

Norton Your Eyes Only , giunto alla quarta release, è uno dei pacchetti di protezione di dati su una macchina più efficienti e pratici da usare. Esso è praticamente trasparente per l'utente normale, cui è chiesto solo di custodire e, con una certa frequenza, di cambiare la password. Il resto, salvo a voler cercare setup particolari, o nel caso di esigenze di ambiente specifiche, può essere all'inizio ignorato dall'user medio, che ha la necessità solo di evitare che qualcuno, per caso o per volontà, vada a dare una occhiata alle nostre cose; e questo anche se si tratta di chi pensa di bypassare la cosa, lanciando il sistema da dischetto.

MC