Bruce Schneier
L'algoritmo di cifratura Solitaire

Versione 1,2 del 26/5/1999
Progettato da Bruce Schneier
Rappresentato da Neal Stephenson in Cryptonomicon

---

test vectors - Perl - Ada - C (#1) - C (#2) - C++ - C++ GUI - C# - Delphi (#1) - Delphi (#2) - Erlang - Forth (#1) - Forth (#2) - Java - Javascript - K - Palm OS - Pascal - Perl CGI - Python (#1) - Python (#2) - Ruby – TCL
Nota: solo l'implementazione in **Perl** è stata verificata dalla **Counterpane**.

La pagina originale in inglese è stata tradotta in tedesco da Nils Plaumann, in francese da Fernandes Gilbert ed in spagnolo da Jesús Avión.
Aggiornamento: Paul Crowley ha scoperto un errore nel generatore di numeri casuali. Il suo sito ospita pure implementazioni in **C** e **Perl** del Solitaire.

Nella novella **Cryptonomicon** di *Neal Stephenson*, il personaggio Enoch Root descrive un crittosistema, denominato in codice "**Pontifex**", ad un altro personaggio di nome Randy Waterhouse e successivamente rivela che l'algoritmo si basa sull'uso di un mazzo di carte da gioco. Questi due personaggi vanno avanti scambiandosi numerosi messaggi cifrati con questo sistema. Il sistema ha per nome "Solitaire" (nel romanzo, "Pontifex" è il nome in codice che ha la funzione di celare temporaneamente il fatto che si usa un mazzo di carte) ed io lo ho progettato per consentire ad agenti in servizio di comunicare in sicurezza senza ricorrere all'elettronica o a strumenti che li possano far incriminare. Un agente potrebbe non avere accesso ad un computer o potrebbe essere incriminato se trovato in possesso di strumenti per comunicazioni segrete. Ma un mazzo di carte… che arma è?
Solitaire basa la sua sicurezza sulla casualità derivante da un mazzo di carte mischiato. Manipolando questo mazzo, un corrispondente può creare una stringa di lettere "casuali" che può combinare col suo messaggio. Naturalmente, Solitaire può essere simulato al computer, ma esso è stato progettato per essere implementato manualmente.
Solitaire può sembrare di bassa tecnologia, ma la sua sicurezza è molto elevata. Ho progettato Solitaire in modo che esso sia sicuro anche contro gli avversari militari meglio finanziati con i computer più grandi ed i crittanalisti più intelligenti. Naturalmente, non posso garantire che qualcuno non scopra un attacco più intelligente contro Solitaire (osserva frequentemente questo sito per le novità), ma l'algoritmo è certamente migliore di qualunque altro di tipo carta e matita che io abbia mai visto.
Però non è veloce. Infatti può richiedere una serata per cifrare o decifrare un messaggio ragionevolmente lungo. Nel libro di David Kahn *Kahn on Codes* l'autore descrive un'autentica cifra carta e matita impiegata da una spia sovietica. Ma sia l'algoritmo sovietico che Solitaire necessitano della stessa quantità di tempo per cifrare un messaggio: quasi un'intera serata.

Cifrare un messaggio con Solitaire

Solitaire è una cifra a flusso con ritorno delle uscite (OFB). Talora viene denominato generatore di chiave (secondo la terminologia militare). L'idea alla sua base è che Solitaire genera un flusso, spesso denominato "flusso di chiavi" che contiene i numeri da 1 a 26. Per cifrare occorre generare una chiave composta da tanti numeri quante sono le lettere del messaggio chiaro. Poi questi numeri si sommano in modulo 26 alle lettere del testo chiaro, lettera per lettera, per generare il testo cifrato. Per decifrare occorre generare la

medesima chiave e sottrarla modulo 26 dal testo cifrato per recuperare il testo chiaro (non vi preoccupate, spiegherò tra breve il termine “modulo”).
Ad esempio, per cifrare il primo messaggio citato nel romanzo di Stephenson, “DO NOT USE PC”:

1. Dividere il messaggio da cifrare in gruppi di 5 lettere (non c’è nulla di magico in questo, i gruppi di 5 lettere sono una tradizione in crittografia). Utilizzare delle X per riempire l’ultimo gruppo se questi ha meno di 5 lettere. Perciò, la frase da cifrare “DO NOT USE PC” diventa:
   DONOT USEPC

2. Impiegare Solitaire per generare un flusso di dieci lettere (i dettagli sono esposti in seguito): Immaginiamo che esse siano:
   KDWUP ONOWT

3. Convertire le lettere del messaggio in cifre, A = 1, B = 2, ecc.
   4 15 14 15 20 21 19 5 16 3

4. Convertire allo stesso modo le lettere del flusso di chiavi:
   11 4 23 21 16 15 14 15 23 20

5. Sommare i numeri tra loro modulo 26 (ciò significa che se la somma supera 26, allora si sottrae 26 da essa). Ad esempio, 1 + 1 = 2, 26 + 1 = 27 e 27 – 26 = 1, perciò 26 + 1 = 1
   15 19 11 10 10 10 7 20 13 23

6. Convertire a ritroso i numeri in lettere.
   OSKJJ JGTMW
   Se ti trovi a tuo agio con quanto su esposto, puoi imparare a sommare a mente le lettere e quindi addizionare correttamente le lettere dei passi (1) e (2). È soltanto necessaria un po’ di pratica. È facile ricordare cha A + A = B; mentre ricordare che T + Q = K è più difficile.

Decifrare con Solitaire

L’idea di base è che chi riceve il messaggio cifrato deve produrre il medesimo flusso di lettere della cifratura e poi sottrarle al testo cifrato.

1. Prendere il messaggio cifrato e disporlo in gruppi di 5 lettere (dovrebbe già essere in questo formato alla sua ricezione).
   OSKJJ JGTMW

2. Ricorrere a Solitaire per generare il flusso di lettere chiave, in numero di 10. Se il destinatario utilizza la medesima chiave del mittente, allora il flusso sarà identico:
   KDWUP ONOWT

3. Convertire le lettere del messaggio cifrato in numeri, secondo la loro posizione nell’alfabeto:
   15 19 11 10 10 10 7 20 13 23

4. Convertire allo stesso modo le lettere del flusso:
   11 4 23 21 16 15 14 15 23 20

5. Sottrarre le cifre del flusso della chiave dai numeri del messaggio cifrato, modulo 26. Ad esempio: 22 – 1 = 21, 1 – 22 = 5 (è facile, se il primo numero è minore o uguale al secondo, si aggiunge 26 al primo numero prima di eseguire la sottrazione, così 1 – 22 modulo 26 diventa 27 – 22 = 5).
   4 15 14 15 20 21 19 5 16 3

6. Convertire i numeri in lettere:
   DONOT USEPC
   Come vedi, la decifrazione è identica alla cifratura, tranne che in questo caso si esegue una sottrazione.

Generazione delle lettere del flusso di chiavi

Questo è il cuore di Solitaire. Le descrizioni di cui sopra sulla cifratura e la decifrazione funzionano con ogni cifratura a flusso con ritorno delle uscite ed è così che funziona l'RC4. Il modo OFB del DES funziona parimenti. Questa sezione è specifica di Solitaire e spiega come questi genera le lettere del suo flusso di chiavi.

Solitaire genera il suo flusso ricorrendo ad un mazzo di carte. Puoi immaginare un mazzo di 54 carte (non dimenticare i due jolly) come una permutazione di 54 elementi. Si hanno quindi 54! combinazioni, cioè circa $2,3 \times 10^{71}$ sequenze possibili di carte. Ancora meglio: si hanno 52 carte in un mazzo (escludendo i jolly) e 26 lettere nell'alfabeto. Questo genere di coincidenza è troppo importante per ignorarlo.

Per poterlo utilizzare in Solitaire, il mazzo di carte deve avere 52 carte e due jolly. Questi ultimi devono essere diversi (come avviene comunemente, il mazzo in mio possesso ha due jolly differenti, il primo ha una stella piccola ed il secondo una stella più grossa). Chiamiamo A il primo jolly e B il secondo. Generalmente, c'è un elemento grafico identico sui due jolly, ma di dimensioni differenti. Il Jolly B sarà quello con l'elemento grafico maggiore, convenzione che si può ricordare con facilità. Se ti sembrasse più facile, puoi scrivere una grande A su uno dei due jolly, ma se la polizia segreta ti arrestasse, vorrebbe conoscerne il significato.

Per predisporre il mazzo, prendilo in mano, con le carte col recto verso di te. Devi disporre le carte nella sequenza che corrisponde alla chiave (della chiave ne parleremo più avanti, è una cosa differente dal flusso delle chiavi). Adesso sei pronto a generare una catena di lettere aleatorie.

Ecco come produrre un carattere. Questa è l'essenza di Solitaire:

1. Trova il jolly A. Spostalo verso il basso di una posizione (cioè scambialo con la carta che si trova dopo di esso). Se il jolly A è l'ultima carta, spostalla all'inizio del mazzo.

2. Trova il jolly B. Spostalo verso il basso di due posizioni. Se il jolly B è l'ultima carta del mazzo ponilo sotto la seconda carta del mazzo. Se invece il jolly B è la penultima carta allora ponilo sotto la prima carta del mazzo (immagina il mazzo di carte come un cerchio di carte).
   Non ti devi sbagliare sull'ordine di queste due tappe. Per pigrizia, potresti desiderare di spostare i jolly nel momento esatto in cui li incontri. Questo non è importante, a meno che essi non siano molto vicini l'uno all'altro.
   Se il mazzo di carte ha questa sequenza prima della tappa iniziale:
   A 7 2 B 9 4 1
   alla fine della seconda tappa diventa:
   7 A 2 9 4 B 1
   E se il mazzo è questo prima della tappa iniziale:
   3 A B 8 9 6

alla fine della seconda tappa diventa:
3 A 8 B 9 6
Se hai qualche dubbio, non dimenticare che il jolly A deve essere spostato prima del jolly B. E stai attento quando i jolly si trovano in fondo al mazzo. Se il jolly è l'ultima carta, immagina che sia la prima quando cominci a contare.

3. Spacca tre volte il mazzo. Scambia le carte che precedono il primo jolly con le carte al di sotto del secondo jolly. Se la successione del mazzo è la seguente:
   2 4 6 B 5 8 7 1 A 3 9
   allora dopo quest'operazione diventa:
   3 9 B 5 8 7 1 A 2 4 6
   Il primo jolly è quello che si incontra per primo procedendo dall'alto, l'altro è il secondo (sempre dall'alto). Ignora i termini jolly A e jolly B per questa tappa.
   Ricordati che i jolly e le carte tra essi comprese non si spostano: si spostano solo le carte alle estremità. È molto facile da fare manualmente. Se non ci sono carte sopra una delle tre sezioni (vuoi perché i jolly sono adiacenti, vuoi perché un jolly è la prima carta e l'altro è l'ultima) allora continua l'algoritmo senza spostare nulla con questa tappa. Se il mazzo è come questo:
   B 5 8 7 1 A 3 9
   dopo il taglio triplo diventa:
   3 9 B 5 8 7 1 A
   Un mazzo come questo:
   B 5 8 7 1 A
   non cambia in questa tappa.

4. Esegui un taglio contato. Osserva l'ultima carta. Convertila in un numero compreso tra 1 e 53 (utilizza l'ordine dei semi del Bridge: fiori, quadri, cuori e picche. Se la carta è di fiori, prendine il suo valore. Se la carta è di quadri, aggiungi 13 al suo valore, se la carta è di cuori, prendi il suo valore ed aggiungici 26 e se la carta è di picche prendi il suo valore aumentato di 39. Ogni jolly vale 53). Taglia dopo l'ultima carta contata e lascia l'ultima carta in fondo al mazzo. Se il mazzo è questo:
   7 … carte … 4 5… carte ... 8 9
   e la nona carta è 4, il taglio produce il risultato seguente:
   5 ... carte ... 8 7 ... carte ... 4 9
   Il motivo per cui l'ultima carta non viene spostata è di rendere reversibile questa tappa. Il modo corretto di contare è di passare ogni carta, una per volta, da una mano all'altra. Non utilizzare delle tavole o delle pile di carte.

5. Trova la carta d'uscita. Per questo scopo, guarda la prima carta del mazzo. Converti la carta in un numero da 1 a 53 come alla tappa (4). Conta dall'inizio del mazzo tante carte quante il numero ottenuto, contando, beninteso, anche la prima carta del mazzo. Quando raggiungi la carta in questione, dopo aver contato, annota il suo nome su un pezzo di carta: non togliere la carta dal mazzo (se la carta è un jolly, non annotare nulla sulla carta e ricomincia dalla tappa 1). Ecco la prima carta d'uscita. Nota bene che questa tappa non modifica lo stato del mazzo di carte.

6. Converti la carta così ottenuta in un numero. Come visto in precedenza, utilizzare l'ordine dei semi del Bridge per ordinarle. La sequenza, dal basso verso l'alto, è la seguente: fiori, quadri, cuori e picche. I fiori da A a K vanno da 1 a 13; i quadri da A a K vanno da 14 a 26, i cuori da A a K vanno da 1 a 13 e le picche da A a K vanno da 14 a

26 (noi abbiamo bisogno di andare soltanto da 1 a 26 e non da 1 a 52, perché vogliamo ottenere delle lettere).
Ecco come utilizzare Solitaire per cifrare un carattere. Puoi utilizzarlo per creare tante cifre di un flusso di chiavi quante sono necessarie; ti basta ripetere le sei tappe su esposte per ottenere i caratteri necessari in uscita. Non dimenticare che hai bisogno di una lettera di uscita per ogni lettera del messaggio da cifrare.
Sono a conoscenza che in base ai paesi ci sono delle differenze nei mazzi di carte. In generale, l'ordine dei semi non è molto importante, né il metodo che utilizzi per convertire le carte in lettere. Quello che importa è che il mittente ed il destinatario si accordino sulle medesime regole. Se i corrispondenti di ogni parte non sono coerenti, non è possibile comunicare.

Ottenere una chiave dal mazzo di carte

Prima di poter iniziare a produrre le tue carte d'uscita, devi ottenere una chiave dal mazzo di carte. Probabilmente è la tappa più importante dell'intera operazione ed è su questa tappa che si basa interamente la sicurezza del sistema. Solitaire è tanto sicuro quanto è sicura la chiave. Ciò significa che il modo più facile di violare Solitaire è quello di individuare con esattezza quale chiave è utilizzata nella comunicazione. Se non hai una buona chiave, niente di quanto segue potrà essere utile. Ecco qualche suggerimento per procedere allo scambio della chiave.

1. Mischia a caso un mazzo di carte. Poi, ordina il secondo esattamente allo stesso modo. Una chiave aleatoria è quella migliore. Ogni partita dispone di un mazzo completo. Poiché la maggioranza delle persone non sa mischiare correttamente un mazzo di carte, mischialo sei volte di seguito. Non commettere il minimo errore tra i due mazzi di carte. Inoltre, non dimenticare che la chiave rappresenta un pericolo per la sicurezza finché essa esiste: se la polizia ti arrestasse e trovasse il mazzo di carte, questa potrebbe copiarne l'ordine delle carte.

2. Utilizza l'ordine del Bridge. La descrizione del mazzo su un foglio di carta ti ritorna una chiave di circa 95 bit. Concorda con l'altra parte il modo di prendere il diagramma del Bridge e di convertirlo in un ordine di carte. Poi, accordati su come collocare i jolly nel mazzo di carte (ad esempio, porre il primo jolly dopo la prima carta citata nel testo scambiato ed il secondo jolly dopo la seconda carta citata.)

Fai attenzione: la polizia segreta può trovare il tuo ordine di Bridge e copiarlo. Ti puoi accordare su un modo particolare di utilizzare le colonne, ad esempio utilizzare la colonna del Bridge che corrisponde al numero del giorno in cui è stato cifrato il messaggio o qualcosa di simile. Puoi anche utilizzare parole chiave del sito Internet del *New York Times* ed utilizzare la colonna del Bridge del giorno di pubblicazione di un articolo di cui fornisci le parole chiave. Se le parole chiave vengono intercettate esse sembreranno una parola d'ordine. E scegli il tuo metodo per convertire le colonne del Bridge in ordine di carte; non dimenticare che la polizia segreta ha letto tutti i libri di Neal Stephenson…

3. Utilizza una frase chiave per ordinare il mazzo di carte. Questo metodo utilizza l'algoritmo Solitaire per creare un ordine iniziale del mazzo di carte. Sia il mittente che il destinatario devono conoscere la frase chiave (ad esempio: "CHIAVE SEGRETA"). Comincia con un mazzo di carte che abbia un ordine ben preciso; dalla carta più bassa alla più alta, secondo l'ordine dei semi del Bridge, seguite dal jolly a e poi da quello B. Esegui Solitaire su un mazzo di carte, ma invece di eseguire la tappa 5, fai un'altra conta in funzione della lettera della frase chiave (3 nel nostro esempio). In caso di altre

parole, esegui un'altra volta la tappa 4, utilizzando 3 come cifra di taglio invece del valore dell'ultima carta. Non dimenticare di collocare le carte dall'alto al di sopra dell'ultima carta del mazzo, come sopra.

Ripeti le 5 tappe dell'algoritmo Solitaire per ogni carattere della chiave. La seconda volta che utilizzi l'algoritmo ricorri alla seconda lettera della chiave, ecc. Utilizza le due ultime lettere per disporre i jolly. Se il penultimo carattere è una G (7), metti il jolly A dopo la carta numero 7. Se l'ultimo carattere è una T (20), colloca il jolly B dopo la carta numero 20.

Non dimenticare che ogni carattere ha una casualità di 1,5 bit. Per un messaggio, questo significa che hai bisogno di almeno 64 caratteri per rendere sicuro il sistema; ti raccomando 80 caratteri, per precauzione. Sono desolato, ma con una chiave più corta non hai sicurezza sufficiente.

Esempi dimostrativi

Ecco un esempio per addestrarti all'uso di Solitaire:

Esempio n° 1: comincia con un mazzo di carte senza chiave: fiori da A a K, quadri da A a K, Cuori da A a K e picche da A a K, con i due jolly A e B (puoi immaginare di andare da 1 a 52, a e B).
Ecco come generare le prime due uscite: Se il mazzo inizialmente è:
1 2 3 4 … 52 A B
dopo la prima tappa (spostamento del jolly A) è:
1 2 3 4 … 52 B A
dopo la seconda tappa (spostamento del jolly B) diventa:
1 B 2 3 4 … 52 A
dopo la terza tappa (taglio triplo) diventa:
B 2 3 4 … 52 A 1
dopo la quarta tappa (taglio contato):
2 3 4 … 52 A B 1
L'ultima carta è 1, ciò significa che noi dobbiamo tagliare una carta. Ricordati che 1 non deve essere spostato e il Jolly B va messo una carta prima della fine del mazzo, al di sopra di 1.
La quinta tappa non cambia il mazzo, ma produce una carta di uscita. La prima carta è un 2 e perciò contiamo due carte, fino a 4. La prima carta di uscita di Solitaire è dunque 4 (e, beninteso, non devi togliere questa carta dal mazzo. Lascia il 4 al suo posto e scrivi 4 da qualche parte).
Per produrre la seconda uscita di Solitaire, esegui nuovamente le cinque tappe precedenti.
Prima tappa:
2 3 4 … 49 50 51 52 B A 1
Seconda tappa:
2 3 4 … 49 50 51 52 A 1 B
Terza tappa:
A 1 2 3 4 … 49 50 51 52
Quarta tappa:
51 A 1 2 3 4 …49 50 52
L'ultima carta è 52, perciò contiamo 52 carte a partire da 51. Tagliamo la carta sola, la carta 51 va con il resto del mazzo. Non dimenticare: il 52 non si deve spostare.
La tappa 5 produce la carta di uscita. La prima carta è la carta 51. Contando verso il basso 51 carte arriviamo alla carta 49, che è la seconda carta di uscita. (Di nuovo, non togliere la carta 49 dal mazzo.)

Le prime 10 uscite sono:
4 49 10 (53) 24 8 51 44 6 4 33
Naturalmente la carta 53 viene saltata. L'ho indicata solo a scopo didattico.
Se il testo chiaro è:
AAAAA AAAAA
allora il testo cifrato è:
EXKYIZSGEH

Secondo esempio
Ricorrendo al metodo 3 per generare la chiave e se la chiave è "FOO", (ricorda che la tappa opzionale per generare la chiave non è utilizzata in questi esempi) i primi quindici numeri di uscita sono:
8 19 7 25 20 (53) 9 8 22 32 43 5 26 17 (53) 38 48
e se il testo chiaro è composto solo da A, otterremo il seguente testo cifrato:
ITHZUJIWGR FARMW

Terzo esempio
Utilizzando il terzo metodo e la chiave "CRYPTONOMICON", il messaggio "SOLITAIRE" è cifrato in:
KIRAK SFJAN

Non dimenticare che si devono utilizzare delle X per riempire l'ultimo gruppo di caratteri, al fine di ottenere un gruppo di 5 caratteri.
Certamente, puoi utilizzare una chiave più lunga. Gli esempi suesposti sono solo dimostrativi. Sul sito Internet vi sono altri esempi e puoi utilizzare lo script Perl per creare le tue chiavi personali.

Sicurezza reale e non sicurezza proveniente dal segreto
Solitaire è famoso per essere sicuro, anche se l'attaccante conosce il funzionamento dell'algoritmo. Ho assunto che "Cryptonomicon" sarà un best-seller e che dappertutto ci saranno delle copie del romanzo. Assumo anche che i servizi segreti studieranno l'algoritmo e lo sorveglieranno. L'unica cosa segreta è la chiave.

Ed è per questo che è tanto importante custodire la segretezza della chiave. Se hai un mazzo di carte nascosto in un luogo sicuro, devi pensare che il tuo nemico sa che utilizzi Solitaire. Se utilizzi una colonna del Bridge, posta in un cofanetto, potrai suscitare un certo sbalordimento. Se si sa che un gruppo utilizza Solitaire, le polizie ed i servizi segreti avranno a loro disposizione una base di dati di colonne di Bridge allo scopo di tentare di violare il messaggio. Solitaire resta forte anche se il nemico sa che l'utilizzi ed un semplice mazzo di carte non sarà più pericoloso di un software di cifratura trovato nel tuo computer; ma l'algoritmo è forte.

Note sull'utilizzo
1. La prima regola per una cifratura di flusso a ritorno di uscita è di non utilizzare mai, dico mai, la stessa chiave per due messaggi differenti. Ripeti con me: NON UTILIZZARE MAI UNA CHIAVE PIÙ D'UNA VOLTA. Se lo farai, comprometterai completamente la sicurezza del sistema. Ecco perché: se si dispone di due flussi, A + K e B + K che sono due flussi combinati ad una medesima chiave, è molto facile violare il messaggio. Fidati di me: tu non sarai mai capace di recuperare A e B a partire da A-B, ma un crittografo esperto sì. È importantissimo: non utilizzare mai una chiave più di una volta. Ad ogni messaggio la sua chiave, unica.

2. I tuoi messaggi siano corti. Questo algoritmo è stato progettato per messaggi corti: non più di un centinaio di caratteri. Ricorri ad abbreviazioni o al gergo. Non essere loquace. Se vuoi cifrare un romanzo di 100.000 parole ricorri ad un algoritmo informatico.

3. Come ogni cifratura OFB, questo sistema ha un grosso difetto: non tollera il minimo errore. Se cifri un messaggio e commetti involontariamente un errore in una delle operazioni, ogni lettera successiva diventerà indecifrabile. Tu stesso non potrai decifrare il messaggio, neppure con la sua chiave. E non saprai mai perché. Se cifri un messaggio, cifralo due volte di seguito. Se decifri, verifica il senso del messaggio man mano che decifri. E se utilizzi un mazzo aleatorio, conservane un mazzo come copia per questo motivo.

4. Solitaire è reversibile. Questo significa che se lasci in giro il mazzo di carte dopo che hai cifrato il tuo messaggio, la polizia segreta lo può trovare ed invertire l'algoritmo utilizzando il mazzo di carte. Questo processo può recuperare tutte le carte di uscita e decifrare il messaggio. È importante che tu mischi completamente 6 volte il mazzo di carte dopo che hai finito di cifrare un messaggio.

5. Per avere la massima sicurezza cerca di fare ogni cosa con le tue mani e la tua testa. Se la polizia segreta incomincia a sfasciare la tua porta, con serenità devi solo mischiare il mazzo di carte. (Non gettarlo in aria, saresti sorpreso nel constatare quanto ordine possa rimanere nel mazzo di carte.) Ricorda di mischiare la copia di riserva del mazzo, se ne hai una.

6. Stai attento ad utilizzare i fogli di calcolo, se devi scrivere qualcosa. Essi potranno ricavare da esso informazioni importanti.
   Probabilmente il fuoco è il modo migliore per distruggere i dati, pensa alla carta. La carta non gommata o quella delle sigarette è la migliore. Un collega ha fatto una prova con le carte Club Cabaret, esse bruciano completamente.
   Non è poi così difficile scrivere su una carta da sigaretta. Utilizzando una matita n° 2 a punta fine avrai un buon risultato. Una matita n° 3 è migliore, ma più difficile da trasportare. Le matite pongono una serie di problemi: la loro fine punta lascia delle impronte sulla superficie sottostante. Queste carte hanno il vantaggio di richiedere pochissimo spazio ed, al bisogno, possono essere deglutite.
   Sono anche molto sottili. Si possono piegare sei volte per ottenere una carta di un centimetro, per un millimetro di spessore. Una carta così può contenere tranquillamente 80 lettere in 8 righe, con blocchi di 5 lettere. Con un po' più di perizia vi si possono scrivere 120 caratteri.

7. Solitaire può funzionare sui computer. Solo una sua parte richiede un mazzo di carte, durante la cifratura. Il computer deve essere utilizzato tutte le volte che è possibile: è più veloce e non commette errori.

8. Molti mazzi di carte non possiedono jolly e se ne possiedi uno di questi, assicurati di poter giustificare la loro presenza.

9. La sicurezza di Solitaire non si basa sulla segretezza della metodica. Assumo che la polizia segreta sappia che tu lo utilizzi.

Analisi della sicurezza
Ci sono ancora molti altri argomenti; consulta regolarmente questa pagina.

Continuare l'apprendimento
Ti raccomando il mio libro, **Applied Cryptography** (John Wiley & Sons, 1996), poi, leggi **The Codebreakers** di David Kahn (Scribner, 1996). Esistono molti libri dedicati alla crittografia e qualche libro sulla crittografia manuale. È una materia divertente, buona fortuna.

---

test vectors - Perl - Ada - C (#1) - C (#2) - C++ - C++ GUI - C# - Delphi (#1) - Delphi (#2) - Erlang - Forth (#1) - Forth (#2) - Java - Javascript - K - Palm OS - Pascal - Perl CGI - Python (#1) - Python (#2) - Ruby – TCL
Nota: solo l'implementazione in **Perl** è stata verificata dalla **Counterpane**.