

CRITTOGRAFIA: IL PRESENTE

Introduzione

Da sempre per la protezione dei messaggi si utilizza il metodo della crittografia, che consiste nella trasformazione del messaggio originario in una forma *reversibile* ma *inintelligibile* a tutti tranne che al destinatario. Si è visto come nel passato la sicurezza si basava sul fatto che la regola di trasformazione era nota solo al mittente ed al destinatario, sia nel caso di sostituzione sia nel caso di trasposizione.

Oggi, il metodo di trasformazione si basa su un algoritmo eseguito da uno o più calcolatori, che trasforma il messaggio. L'algoritmo di crittografia è costituito da una regola di trasformazione che viene fatta dipendere da una chiave. Ciò significa che lo stesso messaggio codificato con due chiavi diverse, utilizzando in ogni modo lo stesso algoritmo, produce sempre due risultati diversi e, inoltre, il messaggio criptato può essere decriptato solo applicando la chiave giusta. Quindi, la sicurezza è basata sulla segretezza della chiave e non dell'algoritmo, come enunciato da Kerckhoffs nel 1883 (principio di Kerckhoffs). In pratica il metodo è tanto più sicuro quanto più difficile è trovare la chiave necessaria per decriptarlo, supponendo di conoscere l'algoritmo utilizzato, almeno un messaggio criptato e anche la tipologia del contenuto.

Con l'avvento dei computer si è avuto un salto di qualità nel settore crittografico; inoltre, utilizzando una codifica binaria, è possibile cifrare informazioni di qualunque tipo non solo testuali, ed è più difficile l'applicazione di una crittoanalisi statistica, perché si spezzano le correlazioni intra-simbolo (i bit della codifica di un simbolo) e intersimbolo (parole e frasi).

Per ottenere il messaggio cifrato, si esegue semplicemente l'EXOR (è la somma binaria senza riporto) tra i bit corrispondenti del messaggio da cifrare e della chiave. Per decifrare è necessario rifare l'EXOR tra la chiave ed il messaggio cifrato.

Per anni si è pensato di creare algoritmi relativamente semplici con chiavi molto lunghe per aumentare la complessità di decodifica da parte di "estranei". Adesso, l'orientamento è opposto data la potenza di calcolo di cui si può disporre per fare un "brute force", quindi si pensa a

CRITTOGRAFIA: IL PRESENTE

complicare gli algoritmi da decifrare, in modo che chi volesse forzarli, anche avendo parecchio materiale per l'analisi, non riuscirebbe a farlo.

Ricordiamo che oggi la crittografia serve in tanti campi importantissimi, come l'autenticazione, la riservatezza delle informazioni, il commercio elettronico, etc. Bisogna capire che il metodo di crittografia è noto a tutti, e non è possibile modificarlo ogni volta che si ha il sospetto che qualcuno sia riuscito a infrangerlo. E' più semplice e logico modificare le chiavi. Per questo si dice che i metodi si basano sulle chiavi di codifica e decodifica.

Si parlerà di crittografia classica a chiave simmetrica o segreta quando la chiave è la stessa sia per la codifica sia per la decodifica. Invece, quando le due chiavi sono diverse e tra loro complementari, una pubblica e una privata, si parla di crittografia a chiave asimmetrica o pubblica. La chiave pubblica è conosciuta da tutti e serve a cifrare i messaggi, mentre quella privata è del destinatario dei messaggi che, solo lui, può decifrarli.

Alcune volte si usano tecniche ibride simmetrica - asimmetrica perché il metodo asimmetrico è molto lento se bisogna trasmettere molti dati. Tra i programmi più utilizzati vi è il famoso PGP (Pretty Good Privacy), creato da Philip Zimmerman e del tutto freeware che realizza la crittografia a chiave pubblica permettendo lo scambio di documenti garantendo segretezza, autenticità ed integrità dei dati su un canale considerato insicuro.

Crittografia a chiave simmetrica

Come detto, è il caso in cui si usa una stessa chiave K per la codifica e la decodifica. In questo caso indichiamo con C e D rispettivamente gli algoritmi di cifratura e di decifratura. L'algoritmo C è funzione della chiave K e del messaggio in chiaro M e fornisce il messaggio criptato M_C . Al contrario, l'algoritmo D è funzione della chiave K e del messaggio criptato M_C , e ritorna il messaggio in chiaro.

CRITTOGRAFIA: IL PRESENTE

In definitiva, il messaggio criptato può essere inviato su un canale insicuro, mentre la chiave K deve essere trasmessa attraverso un canale sicuro (un corriere fidato, un incontro personale, un altro sistema di cifratura già attivo, ma allora che serve un altro sistema di cifratura, etc.). E' questo uno dei punti deboli del sistema. Un altro punto è che, ai fini della sicurezza, è necessario che venga generata e scambiata una chiave segreta per ogni coppia di interlocutori; immaginatevi il proliferarsi del numero di chiavi. Un altro problema deriva dal fatto che periodicamente è sempre conveniente rinnovare le chiavi con conseguente problema di sicurezza dovuto al loro scambio.

Si è già detto come la sicurezza si basi sulla segretezza della chiave e sulla pratica impossibilità di ricavarla dal messaggio criptato anche conoscendo l'algoritmo utilizzato. Per esempio, supponiamo che la chiave venga generata con un calcolatore a 256 bit (32 byte) e applichiamo in modo esaustivo tutte le chiavi possibili con l'algoritmo D su un messaggio criptato. Assumiamo di conoscere il messaggio in chiaro; nel caso peggiore, il risultato positivo potrebbe arrivare con l'ultima chiave provata. Se usiamo un calcolatore che prova una chiave ogni un nanosecondo, sarebbero necessari nel caso peggiore: $T = 2^{256} / 10^9 \text{ s} \approx 10^{77} / 10^9 \approx 10^{68} \text{ s}$, che corrispondono a circa $3 * 10^{60}$ anni.

Tra i più importanti algoritmi a chiave simmetrica si notano: DES, Triplo - DES, IDEA, SAFER, RC2, RC4, RC5, AES.

DES (Data Encryption Standard)

Il DES è un cifrario composto¹ che prevede 16 cifrature successive (trasposizioni e sostituzioni di bit). E' stato presentato dall'IBM nel 1975 ed accettato come standard federale per gli USA dal

¹ Un semplice accorgimento per aumentare la sicurezza di un cifrario è quello di cifrare più volte il messaggio, generalmente con metodi alternativi. Si parla, in questo caso, di sovracifratura. Uno dei metodi più diffusi è quello di far seguire ad una cifratura monoalfabetica o polialfabetica, una trasposizione in modo da distruggere le informazioni su bigrammi e trigrammi, che sono una caratteristica statistica delle lingue. Così è molto più difficile "aprire" un cifrario. Bisogna, però, rendersi conto che cifrare più volte un messaggio non ne aumenta necessariamente la sicurezza. La composizione di due codici monoalfabetici rimane sempre un codice monoalfabetico.

CRITTOGRAFIA: IL PRESENTE

1977. E' un codice che è stato certificato per la sua affidabilità dal N.I.S.T. (National Institute of Standards and Technology), ogni 5 anni solo fino al 1993. Infatti, in seguito ai numerosi tentativi di forzatura, il NIST ha dichiarato che non avrebbe più certificato il DES.

Il DES è un algoritmo che lavora con una chiave di 64 bit, di cui 56 generati casualmente (vera lunghezza della chiave) ed 8 calcolati come bit di parità² per ciascun gruppo di 7 bit dei 56 generati. Il numero di chiavi possibili è pari a $2^{56} \approx 7,2 * 10^{16}$, e tale numero che sembrava impressionante nel 1977 è diventato più critico con l'avvento dei supercomputer o cluster negli anni '90.

Molto in sintesi, l'algoritmo segue i seguenti passi. Inizialmente il messaggio viene scomposto in blocchi di 64 bit, con un riempimento dell'ultimo blocco se non completo con degli zero. Poi, ogni blocco subisce la seguente sequenza di trasformazioni:

- Si permutano i 64 bit dei blocchi del messaggio secondo una mappa prefissata (IP);
- Detti S e D rispettivamente i 32 bit della prima metà (sinistra) e della seconda metà (destra) del blocco, si esegue 16 volte di seguito la seguente coppia di operazioni, dalla quale si ottiene come risultato una nuova combinazione di 64 bit S' e D':

$$S' = D$$

$$D' = S \text{ (EXOR) } f(D,K)$$

dove K è un blocco di 48 bit prelevati, secondo una mappa prefissata, diversa da ogni ciclo di ripetizione, dai 64 bit della chiave; $f(D,K)$ è una funzione di trasformazione non descritta per semplicità che opera su un blocco di 32 bit ed uno di 48 bit, producendo un blocco di 32 bit;

- Si permutano i 64 bit ottenuti con la mappa inversa delle permutazioni iniziale (IP)⁻¹.

Le caratteristiche di simmetria dell'algoritmo fanno sì che l'algoritmo di decifratura è identico a quello di cifratura salvo l'applicazione in ordine inverso della sequenza di blocchi K ricavata dalla chiave.

² Vedi Capitolo sui Codici correttori.

CRITTOGRAFIA: IL PRESENTE

Nel gennaio del 1998 la RSA Laboratories, per violare il DES, lanciò il “DES challenge II” coordinato e risolto da distributed.net in soli 39 giorni. Tale record non resistette a lungo. Infatti, la EFF (Electronic Frontier Foundation’s) costruì una macchina, chiamata DES cracker machine, per distruggere il DES, e scrisse un libro nel maggio 1998 dove spiegava tutto il procedimento nei minimi particolari. La macchina costò 210.000 \$ (80.000 per lo sviluppo ed il resto per il materiale); il software è stato scritto in due settimane da volontari. Tutto ciò per mostrare come il DES non fosse assolutamente sicuro e che con un super computer dedicato era possibile distruggerlo in breve tempo. Tale macchina, il 17/07/1998, forzò un DES in soli 56 ore di lavoro. Una inezia.

Non solo, ma sei mesi dopo, il 19/01/1999, distributed.net lavorando con un network mondiale in Internet di 100.000 PC e con il DES cracker della EFF, vinse l’RSA Data Security’s DES challenge III con il tempo record di 22 ore e 15 minuti.

Dal novembre 1998 il DES non è più l’algoritmo standard federale americano. E’ stato sostituito dal Triplo – DES.

Triplo - DES

Il testo in chiaro viene cifrato 3 volte. Esiste una vasta gamma di modi per fare ciò:

- DES-EEE3. Consiste nel cifrare un testo chiaro usando il DES con tre chiavi distinte;
- DES-EDE3. Il testo in chiaro viene cifrato con una chiave DES. Poi, si eseguirà una nuova cifratura, operando come se il crittogramma fosse il testo in chiaro. Si ripete la stessa operazione per tre volte con tre chiavi diverse;
- DES-EEE2 e DES-EDE2. La procedura è la stessa dei metodi precedenti, ma il primo ed il terzo passaggio usano la stessa chiave.

Attacchi al Triplo – DES a due chiavi sono stati proposti in tempi successivi da Merkle e Hellmann e poi da Van Oorschot e Wiener, ma i requisiti che bisogna avere li rendono tuttora inespugnabili. In realtà, l’utilizzo di una doppia o tripla cifratura non comporta necessariamente una sicurezza a prova di forzatura.

CRITTOGRAFIA: IL PRESENTE**IDEA (International Data Encryption Algorithm)**

Questo algoritmo è stato creato nel 1991 da Xuejia Lai e James L. Massey; come il DES, è un codice cifrato a blocchi di 64 bit però con chiave a 128 bit. Anche IDEA è un algoritmo che usa calcoli semplici basati su operazioni modulari, scambi e concatenamenti, ma a differenza del DES che usa solo l'operazione XOR, l'IDEA usa tre operazioni: XOR, addizione modulo 2^{16} e moltiplicazione modulo $2^{16}+1$. Le sottochiavi usate nel procedimento sono tutte diverse e a 16 bit. E' generalmente considerato sicuro ed immune dalla crittoanalisi differenziale e da quella lineare.

SAFER (Secure And Fast Encryption Routine)

E' un cifratore a blocco sviluppato da Massey nel 1993 per la Cylink Corporation. Usa una dimensione di blocco di 64 bit.

RC2

RC2 sta per Ron's Code o Rivest's Cipher. E' un cifrario a blocco di 64 bit sviluppato da Rivest per la RSA Data Security. Usa una lunghezza di chiave variabile, diventando più o meno sicuro del DES variandone la misura. E' circa 2 o 3 volte più veloce del DES.

RC4

E' un cifratore a flusso sviluppato da Rivest per la RSA Data Security. E' un algoritmo a lunghezza di chiave variabile.

RC5

E' un cifrario a blocco veloce di 64 bit sviluppato da Rivest per la RSA Data Security. E' un algoritmo parametrico, infatti ha una dimensione di blocco variabile, una lunghezza di chiave variabile, ed un numero di cicli variabile. La dimensione del blocco può essere di 32, 64 o 128

CRITTOGRAFIA: IL PRESENTE

bit. La dimensione della chiave può andare da 0 a 2048 bit. Infine, il numero di cicli va 0 a 255. Tale variabilità procura una flessibilità a livello sicurezza ed a livello efficienza.

Esistono tre fasi nel cifrario RC5: espansione della chiave, codifica e decodifica. La prima fase prevede l'espansione della chiave per ottenere una tabella delle chiavi di dimensione dipendente dal numero di cicli. Tale tabella è usata sia per la codifica che per la decodifica. La fase di codifica consiste nelle tre operazioni di addizione, XOR e rotazione.

La sicurezza del cifrario RC5 è dovuta all'utilizzo delle rotazioni e dall'insieme di operazioni differenti. In particolare, tali rotazioni aiutano a difendersi dalla crittanalisi lineare e differenziale.

AES (Advanced Encryption Standard)

Questo algoritmo è stato creato nel 2000 ed usa chiavi lunghe fino a 256 bit.

Crittografia a chiave pubblica o asimmetrica

Con questo tipo di crittografia si risolve brillantemente i problemi della crittografia a chiave segreta. Il concetto di crittografia asimmetrica è stato introdotto nel 1976 da Whitfield Diffie e Martin Hellman, e si basa sul concetto fondamentale che un messaggio codificato mediante una chiave pubblica può essere decodificato **solo** dalla corrispondente chiave privata che è unica ed associata strettamente a quella pubblica. Le due chiavi vengono di norma generate da un potenziale destinatario, che può trasmettere la chiave pubblica tranquillamente anche su un canale non sicuro, addirittura può metterla su un sito Internet. In questo modo solo colui che ha la chiave privata può decrittare un messaggio codificato con la corrispondente chiave pubblica.

Ma conoscere la chiave pubblica non permette di ottenere anche quella privata?

CRITTOGRAFIA: IL PRESENTE

No. Basti pensare che, impiegando 1024 bit, per ottenere la unica chiave segreta da quella pubblica occorrerebbe una potenza di calcolo pari ad una rete di milioni di computer al lavoro per 1000 anni.

Quindi, una volta decifrato il messaggio con la propria chiave pubblica, può essere decifrato solo con la corrispondente chiave privata; nemmeno chi effettua la cifratura se non ha la chiave privata può ritornare al messaggio in chiaro.

Siccome, l'unica chiave importante è quella privata perché è l'unica che può decodificare certi messaggi, ogni utente deve conservare attentamente solo quella. Questo elimina il problema della proliferazione delle chiavi che affliggeva il metodo delle chiavi simmetriche. Comunque, è sempre buona norma rinnovare periodicamente la coppia delle chiavi.

Algoritmo di Diffie - Hellman

Nel 1976 Diffie ed Hellman hanno proposto un metodo particolare per generare e trasmettere su un canale insicuro una chiave segreta, da utilizzare successivamente con un algoritmo più veloce a chiave simmetrica. L'importanza di tale algoritmo, deriva dal fatto che, successivamente, è stato usato come base per lo sviluppo degli algoritmi a chiavi asimmetriche.

Supponendo di avere due interlocutori **Bob** e **Alice** i passi che devono seguire sono i seguenti:

1. Bob e Alice scelgono pubblicamente un numero naturale molto grande m ed un altro M appartenente all'intervallo chiuso $I = [0, m-1]$;
2. Bob sceglie in modo del tutto casuale e privato un altro valore A nell'intervallo I ; poi calcola, utilizzando le tecniche dell'aritmetica modulare, il valore $x = M^A \pmod{m}$ e lo invia ad Alice;
3. Alice sceglie in modo del tutto casuale e privato un altro valore B nell'intervallo I ; poi calcola, utilizzando le tecniche dell'aritmetica modulare, il valore $y = M^B \pmod{m}$ e lo invia a Bob;

CRITTOGRAFIA: IL PRESENTE

4. A questo punto entrambi gli interlocutori possono calcolare la stessa chiave privatamente, Bob nella forma $K_x = y^A \pmod{m}$, e Alice nella forma $K_y = x^B \pmod{m}$.

Si può verificare facilmente che la chiave generata separatamente sia la stessa:

$$K_x = y^A \pmod{m} = (M^B \pmod{m})^A \pmod{m} = (M^B)^A \pmod{m}$$

$$K_y = x^B \pmod{m} = (M^A \pmod{m})^B \pmod{m} = (M^A)^B \pmod{m} = (M^B)^A \pmod{m} = K_x.$$

Attraverso il canale insicuro sono transitati solo m , M , x e y ma non A e B , necessari per il calcolo della chiave. La sicurezza si basa sulla elevata difficoltà computazionale di ricavare gli esponenti A e B .

Vediamo un esempio con numeri piccoli per semplificare un po' i calcoli: $m = 100$, $M = 6$. Bob sceglie privatamente $A = 3$, ed Alice $B = 4$.

$$\text{Bob calcola } x = 6^3 \pmod{100} = 216 \pmod{100} = \mathbf{16};$$

$$\text{Alice calcola } y = 6^4 \pmod{100} = 1296 \pmod{100} = \mathbf{96}.$$

$$K_x = 96^3 \pmod{100} = 884736 \pmod{100} = \mathbf{36}$$

$$K_y = 16^4 \pmod{100} = 65536 \pmod{100} = \mathbf{36}$$

Algoritmo RSA

Nel 1978, due anni dopo l'algoritmo di Diffie – Hellman, è stato proposto il più noto e utilizzato algoritmo a chiavi asimmetriche: RSA, dal nome degli inventori Ronald L. Rivest, Adi Shamir e Leonard Adleman. L'algoritmo RSA si basa sul fatto che, sebbene sia semplice, sotto il profilo computazionale, trovare due numeri primi con un centinaio di cifre decimali, è viceversa un problema intrattabile³ la scomposizione del prodotto dei suddetti numeri primi.

³ Un problema si dice intrattabile quando gli algoritmi richiedono un tempo di calcolo che cresce rapidamente. Ovviamente viene utilizzata l'aritmetica modulare.

CRITTOGRAFIA: IL PRESENTE

La potenza di tale algoritmo si basa sull'estrema difficoltà di ricreare la chiave segreta dalla chiave pubblica basandosi su funzioni unidirezionali e quindi invertibili, e tali che la funzione diretta sia banale ma quella inversa sia molto difficile.

I passi da seguire per ottenere le due chiavi pubblica e privata sono i seguenti: Alice

- deve scegliere a caso un centinaio di basi e verificare col Test di Fermat se i due numeri dispari, scelti sempre a caso, h e g , con almeno un centinaio di cifre decimali, sono quasi certamente primi;
- deve calcolare il prodotto $m = h \cdot g$, e la funzione di Eulero: $\phi(m) = \phi(h \cdot g) = (h - 1) \cdot (g - 1)$;
- deve scegliere un numero $E_k < m$ e primo con $\phi(m)$, ciò vuol dire che E_k non ha fattori in comune, escluso l'1, con il numero $(h - 1) \cdot (g - 1)$;
- deve dare forma esplicita alla funzione: $C = P^{E_k} \pmod{m}$, che è poi la chiave pubblica posseduta da Bob ed utilizzata per criptare i messaggi diretti ad Alice;
- deve determinare D_k in modo che $D_k \cdot E_k \pmod{\phi(m)} = 1$;
- deve dare forma esplicita alla funzione inversa $P = C^{D_k} \pmod{m}$, che è la chiave privata e sarà usata da Alice per decriptare.

Pertanto, la funzione C ovvero la coppia dei numeri (E_k, m) è la chiave pubblica, mentre la coppia di numeri (D_k, m) , ossia la funzione P , è la chiave privata.

Se un criptanalista, a partire dalla funzione C nota e pubblica tenta di calcolare la funzione inversa P , dovrà prima calcolare D_k . Per piccoli numeri non ci sono problemi, mentre per numeri con un centinaio di cifre diventa un problema intrattabile. Infatti deve fattorizzare un numero m a 200 cifre. Solo in questo modo potrà calcolare $\phi(m) = (h - 1) \cdot (g - 1)$ e quindi D_k . Se tenta, a partire da un numero limitato di valori della variabile dipendente C , per estrapolazione di calcolare i valori ignoti rimanenti, per riuscire a risalire alla funzione inversa P , non lo può fare, perché la funzione C è ad andamento disordinato. Per poter invertire la funzione è necessario

CRITTOGRAFIA: IL PRESENTE

conoscere tutti i valori della funzione C , cosa praticamente impossibile dato che m ha almeno 200 cifre.

Infatti, ad un modulo m corrispondono m resti. Se ad esempio m è un numero a cinque cifre, i possibili resti sono un numero compreso tra 10000 e 99999. Ad un modulo m a 200 cifre corrispondono un numero di resti compreso tra 10^{199} e $10^{200}-1$.

Essendo tale protezione eccessiva si preferisce dar luogo al frazionamento del numero P , dato che le funzioni modulari esponenziali agiscono su numeri naturali, in una successione di blocchi di numeri P_1, P_2, \dots con lo stesso numero di cifre inferiore nettamente alle 200 di m . In realtà anche ad un blocco con 10 cifre corrispondono un numero di resti compreso tra 1 miliardo e 10 miliardi meno 1.

La cifratura diventa più lenta se la chiave è più grande. Se aumenta il numero di bit della chiave ci vogliono molto più tempo e denaro per cercare di craccarla. Comunque solo chiavi a 2048 bit si possono ritenere sicure per qualche anno ad ogni livello.

Per velocizzare il problema si utilizza un sistema ibrido con RSA e DES. Con il DES Bob produce una chiave casuale che verrà criptata con RSA e che servirà per criptare il messaggio in modo simmetrico. Spedisce, poi, sia il messaggio sia la chiave DES criptata ad Alice che con la sua chiave segreta decifrerà prima la chiave che poi impiegherà per decodificare il messaggio.

Questo viene fatto normalmente perché il DES è da due volte (software) a 5 volte (hardware) più veloce dell'RSA.

Esempio

Vengono scelti due numeri interi primi tra loro piccoli ma sufficienti per capire l'algoritmo RSA anche se non garantiscono assolutamente una effettiva sicurezza. Vediamo i vari passaggi matematici:

1. Alice sceglie come numeri primi $h = 47$ e $g = 61$ e calcola il prodotto $m = h \cdot g = 2867$ e la funzione di Eulero: $\phi(2867) = (h - 1) \cdot (g - 1) = 46 \cdot 60 = 2760$.
2. Decompone $2760 = 23 \cdot 5 \cdot 3 \cdot 2^3$ e sceglie $E_k = 1183$ (non ha fattori in comune con 2760).

CRITTOGRAFIA: IL PRESENTE

3. La chiave pubblica diventa: $C = P^{1183} \pmod{2867}$ e viene fornita a Bob per criptare i messaggi.
4. Trova D_k con l'algoritmo $\frac{\phi(m) \cdot Q + 1}{E_k} = \frac{2760 \cdot Q + 1}{1183} = D_k = 7$, con $Q = 3$ (solo tre iterazioni). Nella realtà con numeri molto più grandi questo diventa un problema intrattabile.
5. La chiave privata diventa $P = C^7 \pmod{2876}$, che rimane ad Alice e che le serve per decriptare i messaggi di Bob.

Ma quanto vale P ? Dipende dal messaggio che si vuole spedire. Si suppone che Bob vuole spedire segretamente ad Alice il seguente messaggio: Sono uscito.

Bob deve convertire la sua frase in un numero P mediante una qualsiasi tabella che deve essere conosciuta anche da Alice per la decriptazione. Si può usare la tabella ASCII oppure una tabella appositamente creata:

a	01	A	27	spazio bianco	53
b	02	B	28	etc.....	
c	03	C	29		
d	04	D	30		
e	05	E	31		
f	06	F	32		
g	07	G	33		
h	08	H	34		
i	09	I	35		
j	10	J	36		
k	11	K	37		
l	12	L	38		
m	13	M	39		
n	14	N	40		
o	15	O	41		
p	16	P	42		
q	17	Q	43		
r	18	R	44		
s	19	S	45		
t	20	T	46		
u	21	U	47		
v	22	V	48		
w	23	W	49		

CRITTOGRAFIA: IL PRESENTE

x	24	X	50
y	25	Y	51
z	26	Z	52

La versione numerica del messaggio diventa: **P = 4414131452201802081914.**

Adesso Bob effettua il frazionamento del numero P in una successione P_i di blocchi numerici tutti della stessa dimensione in cifre, ad esempio 3 cifre ottenendo:

$$P_1 = 441 \quad P_2 = 413 \quad P_3 = 145 \quad P_4 = 220 \quad P_5 = 180 \quad P_6 = 208 \quad P_7 = 191 \quad P_8 = 452.$$

Si noti lo spazio bianco (numero 52) in fondo al numero P in modo che anche l'ultimo blocco contenga 3 cifre.

Bob determina 8 blocchi cifrati C_i che trasmette ad Alice:

$$C_1 = P_1^{E_k} \pmod{m} = 441^{1183} \pmod{2867} = 2515.^4$$

Si lascia agli studenti il compito di calcolare gli altri sette blocchi cifrati.

Il compito di Alice è inverso e solo lei può riuscirci perché solo lei possiede D_k . Se qualche blocco ha meno di tre cifre, Alice aggiunge degli 0 a sinistra; poi, accorpa i vari blocchi P_i per ottenere P. Infine, grazie alla tabella precedentemente vista ed accordata fra loro riesce ad ottenere la frase di partenza.

Algoritmo di ElGamal (1985)

E' un algoritmo che si basa sul problema di logaritmo discreto. Vale sia come sistema di codifica sia come firma. L'algoritmo di cifratura è molto simile a quello di Diffie/Hellman. L'algoritmo consiste nella scelta di un numero primo p ed un numero intero g, la potenza modulo p del quale genera un grande numero di valori come in Diffie/Hellman. Alice ha una chiave privata a ed una chiave pubblica y, dove $y = g^a \pmod{p}$. Supponiamo che Bob desideri spedire un messaggio m ad Alice. Bob inizialmente genera casualmente un numero k minore di p. Poi, egli calcola y_1 e y_2 in questo modo: $y_1 = g^k \pmod{p}$ e $y_2 = m \oplus y^k$, e li spedisce ad Alice.

⁴ Vedi secondo paragrafo del capitolo sull'Aritmetica modulare.

CRITTOGRAFIA: IL PRESENTE

Alice, dopo aver ricevuto un messaggio cifrato, calcola il messaggio in chiaro m con questa formula: $m = (y_1^a \bmod p) \oplus y_2$.

L'algoritmo di firma è simile ma non uguale all'algoritmo di codifica.

Lo studio sugli algoritmi mostra che tale cifrario è equivalente come grado di sicurezza all'algoritmo RSA a parità di lunghezza della chiave. Lo svantaggio principale è che è più lento di RSA.

Curve ellittiche

Le curve ellittiche sono costrutti matematici della teoria dei numeri che recentemente ha trovato numerose applicazioni nel campo della crittografia. Una curva ellittica può essere definita in tutti i campi (reale, complesso, etc.), ma nella crittografia vengono usate curve ellittiche definite nel campo finito. Una curva ellittica consiste di elementi (x,y) che soddisfano la seguente equazione: $y^2 = x^3 + a \cdot x + b$ insieme ad un singolo elemento O chiamato "punto all'infinito", che può essere visualizzato come il punto più alto e più basso di ogni linea verticale. La somma di due punti su una curva ellittica è definita dalla seguente semplice regola: $p_1 + p_2 = -p_3$, vedi figura.

L'operazione di somma in una curva ellittica è la controparte della moltiplicazione modulare nei sistemi a chiave pubblica, e la somma multipla è la controparte dell'esponentiale modulare.

I criptosistemi basati sulle curve ellittiche sono simili ai cifrari a chiave pubblica come RSA e ElGamal, dove le moltiplicazioni modulari vengono sostituite dalle operazioni di somma della curva ellittica. Le curve usate sono normalmente della forma: $y^2 = x^3 + a \cdot x + b \pmod{p}$, dove p è un numero primo.

Il metodo delle curve ellittiche è basato, come RSA, sulla difficoltà della fattorizzazione, pertanto ha un grado di sicurezza molto elevato.

CRITTOGRAFIA: IL PRESENTE

Cifrari Knapsack

Il sistema Merkle-Hellman Knapsack è un cifrario a chiave pubblica nato nel 1978. E' comunemente chiamato cifrario Knapsack. E' basato su un problema di somme combinatorie. Il problema richiede di selezionare un numero di oggetti con un dato peso da un insieme molto grande in modo che la somma dei pesi è uguale ad un peso prefissato. Questo è un problema difficile da risolvere in generale, ma alcuni casi del problema sono facilmente risolvibili e servono come "trabocchetto" del sistema. Shamir infranse il sistema a singola iterazione già nel 1978. Anche il sistema con più iterazioni fu rotto abbastanza velocemente.

Anche il cifrario Chor-Rivest Knapsack pubblicato per la prima volta nel 1984 e, poi, successivamente rivisto nel 1988, fu rotto ma dopo molto tempo.

LUC

Il LUC è un cifrario a chiave pubblica sviluppato da un gruppo di ricercatori in Australia e Nuova Zelanda. E' analogo ai cifrari RSA, ElGamal e Diffie-Hellman e si chiamano rispettivamente LUCRSA, LUCELG e LUCDIF. Il sistema in generale si basa sulla seguente relazione iterativa lineare del secondo ordine: $T_n = P \cdot T_{n-1} - Q \cdot T_{n-2}$, con P e Q numeri primi.

Un recente scritto di Bleichenbacher *et al.* Ha mostrato come questo sistema non ha poi tutti i vantaggi di sicurezza declamati dall'autore.

La firma digitale

La crittografia a chiavi asimmetriche risolve le limitazioni che presentavano i metodi a chiave simmetrica (proliferazione delle chiavi e necessità di invio sicuro). In più si hanno altri problemi che possiamo riassumere:

CRITTOGRAFIA: IL PRESENTE

- Garanzia di integrità del messaggio inviato. E' fondamentale che il messaggio che giunge a destinazione sia perfettamente uguale all'originale.
- Autenticazione dell'invio. Il mittente deve farsi riconoscere come autore del messaggio.
- Impossibilità del ripudio. Il mittente non può negare di aver trasmesso un certo messaggio per sua volontà in un certo istante.
- Identificazione del destinatario. Il mittente deve essere sicuro dell'associazione chiave pubblica/destinatario.

I primi due punti vengono risolti con la tecnica della firma digitale e tutti e quattro i punti sono legati al ruolo della cosiddetta Autorità di Certificazione.

La firma digitale è semplicemente il messaggio cifrato con la chiave privata del mittente. In questo modo il destinatario può verificare, decriptando la firma con la chiave pubblica del mittente e rilevando l'eguaglianza tra il messaggio effettivo e quello contenuto nella firma, sia l'identità del mittente sia l'associazione tra firma e messaggio. Ovviamente, non avendo senso lo spreco di tempo per cifrare un intero messaggio ai soli fini di firma, si cifra solo un riassunto del messaggio mediante un metodo legato al cifrario RSA. In realtà sono stati proposti altri metodi che qui non vengono menzionati.

La firma può essere anche spedita separatamente al messaggio sia in chiaro che in forma sicura criptando il messaggio e la firma con la chiave pubblica del destinatario.

Impronta hash

Il riassunto del messaggio è detto impronta del messaggio ed è un'informazione di lunghezza prefissata di 128 o 160 bit. L'impronta viene usualmente calcolata applicando al messaggio una funzione H non reversibile detta funzione hash: $I = H(M)$.

Ad esempio, supponiamo di avere un messaggio M lungo L byte, una funzione hash esegue il seguente calcolo: $I = \left(\sum_i m_i \right) \bmod 2^k$, con $i = 1..L$ e con m_i l' i -esimo byte del messaggio.

CRITTOGRAFIA: IL PRESENTE

Vengono sommati gli L byte e della somma si prendono i k bit meno significativi; in questo caso l'impronta, di k bit, è di lunghezza fissa contro la lunghezza arbitraria del messaggio di partenza.

La non reversibilità della funzione hash garantisce l'impossibilità di ottenere il messaggio completo dall'impronta che, pertanto, può essere tranquillamente trasmessa in chiaro.

Deve essere anche estremamente bassa, praticamente trascurabile, la probabilità che due messaggi diversi con la stessa lunghezza generino la stessa impronta. Questo fatto garantisce che l'impronta hash sia univoca come l'impronta di un individuo. La bontà di un algoritmo di hashing sta nella difficoltà crittoanalitica di trovare un messaggio diverso dall'originale ma che produce la stessa impronta. Alcuni algoritmi di hashing sono in tal senso già stati violati.

Sono stati proposti molti algoritmi che realizzano funzioni hash diverse (i primi tre in ambito RSA):

- MD2 (Message Digest 2) produce un'impronta a 128 bit, con il messaggio diviso in blocchi da 16 byte. E' già stato violato.
- MD4 con impronta da 128 bit con blocchi da 512 bit e più veloce del precedente. Esegue il riempimento dell'ultimo blocco non completato con un valore di 64 bit che rappresenta la lunghezza del messaggio, cosa che rende l'algoritmo più sicuro. E' stato violato.
- MD5 è più sicuro del precedente ma più lento ed è basato su operazioni logiche e di OR esclusivo.
- SHA-1 (Secure Hash Algorithm) è utilizzato nel protocollo S/MIME, deriva da MD4 e genera un'impronta di 160 bit.
- RIPE-MD è derivato da MD4 e SHA-1 ed ha varie versioni con impronte da 128, 160, 256 e 320 bit).

Integrità ed autenticazione

Quando Bob invia ad Alice sia il messaggio che la firma digitale, che ricordiamo è l'impronta codificata con la chiave privata di Bob, in chiaro o criptati, Alice può verificare l'integrità

CRITTOGRAFIA: IL PRESENTE

dell'invio. Infatti, Alice può decifrare l'impronta I del messaggio M applicando la chiave pubblica di Bob sulla firma digitale, calcolare essa stessa l'impronta I del messaggio M con lo stesso algoritmo hash applicato da Bob e confrontare le due impronte per verificare che siano uguali. In caso affermativo, Alice è certa dell'originalità del messaggio ricevuto e della sua integrità.

Inoltre, avendo Alice usato la chiave pubblica di Bob, l'uguaglianza delle due impronte garantisce che il messaggio è stato spedito da Bob in quanto lo ha sottoscritto con la sua chiave privata.

Assunto che la chiave privata deve essere gelosamente conservata dal legittimo possessore che in qualunque momento può decidere di cambiarla insieme a quella pubblica corrispondente, rimangono aperte le questioni relative alla fidejussione delle chiavi pubbliche e al non ripudio che vengono affrontate mediante l'istituzione delle autorità di certificazione.

Le Autorità di Certificazione

Se Bob non può ricevere direttamente da Alice la sua chiave pubblica, deve cercare di ottenerla da Carol che fa da garante. Sta qui la fondamentale differenza tra firma autografa e firma elettronica: la prima è riconducibile all'identità di chi l'ha prodotta, mentre la seconda non possiede questa proprietà. Per superare questo problema il garante deve sottoscrivere la chiave pubblica di Alice con la propria firma sempre supponendo che Bob abbia ottenuto in modo fidato la chiave pubblica di Carol. Altrimenti bisogna coinvolgere un altro garante e così via, fino ad arrivare ad un garante fidato di cui si dispone della chiave pubblica. Per questo motivo sono state istituite le Autorità di Certificazione (AC).

Queste autorità hanno il compito di verificare l'identità degli utenti che registrano la propria chiave pubblica, di generare documenti elettronici (Certificati) che contengono la chiave pubblica sottoscritta dalla AC, di mantenere aggiornate le liste degli utenti registrati e la lista dei certificati revocati.

CRITTOGRAFIA: IL PRESENTE

In Italia è la stessa autorità che registra dopo opportuna verifica l'utente e che mantiene il database delle chiavi e dei certificati. All'estero è possibile che le autorità siano due .

La registrazione di un utente avviene attraverso i seguenti passi:

1. l'utente fornisce, ai fine della sua identificazione, la documentazione richiesta dalla AC;
2. la AC attribuisce all'utente "validato" un identificatore univoco per facilitare le successive operazioni di ricerca;
3. la AC inserisce l'utente nel database degli utenti registrati;
4. la AC fornisce all'utente, tramite un canale sicuro, ad esempio tramite un algoritmo di cifratura simmetrica, la chiave che l'utente userà per la richiesta di certificazione delle sue chiavi pubbliche.

Ogni volta che l'utente genera con un proprio software una coppia di chiavi pubblica e privata, si dovranno seguire i seguenti passi per ottenerne la certificazione:

1. l'utente invia in forma 'autenticata' la chiave pubblica generata, sottoscritta dalla firma ottenuta con la corrispondente chiave privata (questo dà garanzia che l'utente possieda effettivamente la chiave privata, ma anche difende l'utente da possibili modifiche della chiave pubblica presso la AC), effettuando l'invio cifrato con la chiave fornita dalla AC;
2. la AC genera il certificato che include: i dati dell'utente, compreso il suo identificativo, la sua chiave pubblica, la sua firma, la firma di autenticazione della AC, altre informazioni relative all'uso del certificato ed il suo periodo di validità;
3. il certificato viene inviato all'utente;
4. l'inclusione del nuovo certificato nelle liste della AC per un accesso di prelievo pubblico.

La firma della AC deve essere fidata. Per questo motivo anche le AC hanno un certificato pubblico che può essere autofirmato o firmato da una AC di livello superiore. Nel primo caso, il certificato deve essere stato ottenuto attraverso un canale sicuro. Infatti, è prassi comune inserire nei browser i certificati pubblici delle principali AC mondiali. Per l'Italia il ruolo è svolto dall'AIPA (Autorità per l'Informatica nella Pubblica Amministrazione).

CRITTOGRAFIA: IL PRESENTE

Il periodo di validità del certificato garantisce, ai fini della sicurezza, che una coppia di chiavi scada dopo un certo tempo dalla sua generazione. In questo caso il certificato viene revocato e l'utente deve generare una nuova coppia di chiavi. Anche l'utente, se non più sicuro delle proprie chiavi per vari motivi, può chiedere alla AC la revoca del proprio certificato anche se non ancora scaduto.

Per far sapere a tutti che un certificato è stato revocato, la AC mantiene una lista di certificati revocati. E' responsabilità del mittente verificare se la chiave pubblica da usare è ancora valida. Resta comunque valido un certificato che al momento della firma fosse valido ma successivamente revocato.

La garanzia di non ripudio da parte del mittente di un messaggio, non è ottenibile con la sola sottoscrizione del documento da parte del mittente perché manca la qualificazione temporale in forma fidata che può essere ovviamente fornita da un'altra autorità. Per questo motivo, le AC svolgono anche un servizio di marcatura temporale, che consiste nei seguenti passi:

1. l'utente invia al servizio l'impronta del documento da marcare, senza provare, come visto precedentemente, problemi di sicurezza;
2. la marcatura dell'impronta consiste nell'aggiungere ad essa, da parte del servizio, data ed ora;
3. l'impronta marcata viene cifrata con una chiave privata del servizio; il mittente ed il destinatario del messaggio possono ricavare l'impronta e la marcatura temporale decifrando con una chiave pubblica del servizio;
4. l'impronta marcata viene inviata all'utente che la allega al messaggio.

Una volta inviati, in chiaro o criptati, il messaggio, la firma del mittente e la corrispondente marcatura temporale, il mittente non potrà in alcun modo ripudiare tale invio.

Normalmente la AC usa chiavi diverse per la autenticazione e per la marcatura temporale.

CRITTOGRAFIA: IL PRESENTE

Normativa italiana

L'Italia è stato uno dei primi paesi a dotarsi di un complesso normativo per la regolamentazione della firma digitale, addirittura prima dello sviluppo dell'e-commerce con lo scopo di semplificare le procedure burocratiche con la pubblica amministrazione. In questo caso, purtroppo siamo stati molto precipitosi in quanto le normative europee alle quali dobbiamo attenerci sono decisamente meno restrittive. Lascio allo studente la possibilità di approfondire la questione, che per altro esula dal nostro corso.

Protocolli di trasmissione sicuri

Il dialogo tra applicazioni in internet richiede l'utilizzo di protocolli stratificati, nei quali ogni strato usa le funzioni degli strati sottostanti e fornisce funzioni a quelli soprastanti. Se due applicazioni vogliono comunicare, possono farlo se si conoscono gli indirizzi IP attraverso una specifica porta.

I protocolli non nascono con un grado di sicurezza adeguato, pertanto per permettere alle applicazioni di comunicare in modo sicuro, si può agire ai vari livelli sia IP sia TCP sia addirittura a livello delle applicazioni. Un interessante esempio a livello TCP è SSL (Secure Socket Layer) e la sua versione internet standardizzata TLS (Transport Layer Security). La variante di protocollo HTTP è chiamata HTTPS. Altre volte la sicurezza è dentro le applicazioni come nel caso di PGP e dei protocolli SET (Secure Electronic Transaction) e S/MIME (Secure Multipurpose Mail Extension).

SSL è un protocollo creato da Netscape per ottenere uno scambio di informazioni sicure attraverso internet. Esso garantisce:

- Riservatezza. Dopo la fase di contrattazione iniziale (handshake) i dati vengono trasmessi cifrati con algoritmi simmetrici (3DES, IDEA);

CRITTOGRAFIA: IL PRESENTE

- Autenticazione. L'identità dei soggetti è autenticata con l'uso di certificati e di algoritmi asimmetrici (RSA, DH);
- Integrità. Sono previsti dei controlli di integrità dei dati via via che vengono trasmessi, controlli basati su MAC (Message Authentication Code) ottenuto con funzioni hash sicure (SHA, MD5).

La specifica S/MIME è nata nel 1995 ad opera della RSA Data Security ed è finalizzata alla sicurezza della posta elettronica relativamente ai servizi di trasmissione, memorizzazione, autenticazione e trasferimento (forwarding). Successivamente nel 1999 è stata rivista per standardizzarla. Può essere integrata nei programmi di posta e può garantire che il messaggio resti in forma cifrata anche se scaricato dal server e memorizzato sull'hard disk locale. Prevede anche la possibilità della firma digitale del messaggio.

Telepay Light

E' una soluzione tecnologica proposta da SSB (Società per i servizi Bancari) fin dal 1977 per i pagamenti elettronici sicuri con carta di credito. Nel processo di pagamento sono coinvolti:

- L'acquirente ossia il possessore della carta di credito;
- L'emettitore della carta che è l'istituto bancario che emette la carta di credito e che garantisce il pagamento dalla transazione in accordo con le regole del circuito a cui aderisce;
- Il venditore che mette a disposizione la merce del negozio virtuale;
- La banca d'appoggio che è l'istituto con il quale è convenzionato il venditore e che provvede alla ricezione, verifica ed effettuazione degli ordini di pagamento con carte di credito;
- La banca convenzionante Telepay che è l'istituto finanziario collegato a SSB e che accetta l'adesione del venditore al servizio Telepay.

Le fasi tipiche di una transazione con Telepay si possono riassumere in

CRITTOGRAFIA: IL PRESENTE

- l'acquirente accede al negozio virtuale e riempie il carrello della merce da comprare, totalizzando la cifra da versare;
- l'acquirente verifica gli estremi dell'ordine e lo conferma;
- il browser dell'acquirente viene ridirezionato dalla pagina del venditore verso una apposita pagina, protetta da SSL, del webserver SSB: questa pagina include alcuni dati riassuntivi dell'ordine, spediti in questa fase dal server del venditore, e deve essere riempita dall'acquirente con i dati della carta di credito;
- se l'acquirente conferma i dati impostati, SSB li elabora, e se si opera in modalità di autorizzazione on-line, effettua la richiesta di autorizzazione al circuito della carta e ne dà l'esito all'acquirente; invia, inoltre, l'esito dell'operazione anche al server di questo ultimo, in modo protetto dalla chiave fornita in fase di adesione;
- se la risposta è positiva, il browser dell'acquirente viene ridirezionato, con un bottone di conferma, al sito del venditore per la conclusione della transazione; se negativa ritorna alla sezione del carrello.

Molte banche utilizzano ancora oggi questo tipo di servizio.

SET

Formalizzato nel 1997, il protocollo SET è dovuto alla collaborazione di varie aziende del settore con l'obiettivo di rendere sicuri al massimo i pagamenti in rete con carte di credito. Gli obiettivi che il protocollo si prefigge sono:

- Riservatezza, ottenuta con cifratura simmetrica dei dati sensibili ed in particolare del numero di carta di credito;
- Integrità, ottenuta mediante firma digitale;
- Autenticazione dell'acquirente. La firma ed il certificato garantiscono il venditore dell'identità dell'acquirente e della validità della carta di credito in suo possesso;

CRITTOGRAFIA: IL PRESENTE

- Autenticazione del venditore. La firma ed il certificato garantiscono l'acquirente dell'identità del venditore.

Oltre agli attori visti per il Telepay Light, è coinvolto il Servizio di Pagamento che è un dispositivo HW/SW che elabora le istruzioni di pagamento inviate dall'acquirente.

Si prevede che ogni partecipante disponga di due coppie di chiavi pubblica e privata, una riservata per firmare i dati (chiavi di firma) e l'altra a proteggere lo scambio delle chiavi per gli algoritmi simmetrici di cifratura (chiavi di scambio), cui corrispondono i relativi certificati.

Un pagamento si svolge attraverso la fase di richiesta di acquisto e la fase di autorizzazione di pagamento, gestite dai vari software utilizzati dagli attori in gioco.

La fase della richiesta di acquisto corrisponde a:

1. l'acquirente invia al venditore l'informazione relativa al tipo di carta che desidera utilizzare;
2. in risposta, il venditore invia all'acquirente un identificatore univoco assegnato alla transazione (TI), il proprio certificato per le chiavi di firma e quello del Servizio di Pagamento per le chiavi di scambio, entrambi corrispondenti al tipo di carta comunicato;
3. dopo aver verificato i certificati ricevuti, l'acquirente crea gli estremi d'ordine (OI) e gli ordini di pagamento (PI) contenente i dati della carta di credito. Le impronte di OI e PI vengono concatenate e si ricava un'altra impronta che viene cifrata con la chiave privata dell'acquirente. Viene quindi generata una chiave simmetrica casuale che viene usata per cifrare PI, l'impronta di OI e la firma complessiva prima calcolata. PI firmati e cifrati, e chiave simmetrica vengono cifrati con la chiave pubblica del servizio di Pagamento. L'acquirente invia al venditore questa ultima informazione cifrata insieme agli OI, all'impronta di PI, alla sua firma complessiva ed al suo certificato di firma;

CRITTOGRAFIA: IL PRESENTE

4. il venditore, verificato il certificato dell'acquirente, verifica l'integrità del messaggio calcolando tutte le impronte necessarie e le confronta con quelle a lui giunte. Se il confronto dà esito positivo, il messaggio è integro. Allora, il venditore elabora gli OI e, dopo, invia all'acquirente un messaggio firmato e cifrato con la propria chiave privata di firma a conferma dell'avvenuta ricezione della richiesta di acquisto;
5. l'acquirente, verificata l'integrità del messaggio di conferma ricevuto, verificandone la firma, lo salva opportunamente.

La fase della autorizzazione di pagamento corrisponde a:

1. al punto 4 dalla fase precedente il venditore provvede anche a generare e firmare una richiesta di autorizzazione che include l'ammontare della transazione ed il suo TI. La richiesta viene cifrata con una chiave simmetrica casuale a sua volta cifrata con la chiave pubblica di scambio del Servizio di Pagamento. La richiesta, insieme ai PI cifrati ricevuti dall'acquirente, viene inviata al Servizio di Pagamento con i certificati del venditore e di firma dell'acquirente;
2. quando il Servizio di Pagamento riceve il messaggio effettua tutti i passi necessari al contrario per verificare l'integrità dei dati. Se il confronto dà esito positivo, invia una richiesta di autorizzazione all'Emittitore della carta specificandone i dati. Ricevuta la risposta, il Servizio di Pagamento genera e firma un messaggio di risposta che comprende il suo certificato di firma e la risposta dell'emittitore della carta. Tale messaggio viene cifrato con la chiave pubblica di scambio del venditore. Il messaggio cifrato e la chiave simmetrica cifrata vengono inviati al venditore;
3. il venditore decifra chiave e messaggio; controlla la validità del certificato di firma del Servizio di Pagamento e, se tutto va bene, salva la risposta ricevuta e consegna la merce richiesta.

Si nota immediatamente il salto di qualità in relazione alla privacy che si ottiene utilizzando il protocollo SET, ma si nota anche la sua complessità che né limita l'uso e la diffusione privilegiando sistemi meno sicuri.

CRITTOGRAFIA: IL PRESENTE**E-cash**

Sono state ideate altre forme di pagamento elettronico, basate sul concetto di moneta virtuale, alternative all'uso della carta di credito che possono risolvere il problema che nasce quando la consistenza economica della transazione è paragonabile al costo finanziario della stessa (piccoli acquisti). Si ha in questo caso una carta "pre-pagata" dalla quale si può prelevare fino ad esaurimento del valore della carta. La carta può, ovviamente, essere ricaricata. Un esempio è quello di E-cash della Digicash.

Alice, tramite un versamento tradizionale (bonifico, assegno, etc...) effettuato a favore di Digicash, in cambio di moneta reale, richiede della moneta elettronica (E-cash). La moneta reale ricevuta viene depositata in una Banca on-line. Digicash provvede ad effettuare la trasmissione via internet ad Alice, di quanto richiesto, autenticando con la propria chiave privata e segregando con la chiave pubblica di Alice E-cash, e trasmettendo i riferimenti identificativi di questa ultima alla Banca on-line.

Alice decripta ciò che le arriva per verificare se l'E-cash crittata che ha ricevuto è effettivamente diretta a lei, utilizzando la sua chiave privata, ma soprattutto va a vedere se è autentica, usando la chiave pubblica di Digicash. Se è tutto a posto Alice può scambiare E-cash.

Decide, poi, di fare un acquisto on-line nel negozio di Bob e pagare via internet. Allora, Alice prende dal suo computer la versione di E-cash e prima di spedirla a Bob la critta anche con la chiave pubblica di Bob.

A sua volta, Bob decripta il messaggio che gli è arrivato, per verificare se è effettivamente rivolto a lui, utilizzando la sua chiave privata, e soprattutto se è valido, utilizzando la chiave pubblica di Digicash.

Se è tutto a posto, prima di spedire la merce ad Alice, Bob fa verificare alla Banca on-line se l'E-cash che ha ricevuto non sia già stata spesa in precedenti acquisti di Alice, e se ha intenzione di trasformarla in moneta reale. Infatti, il limite di E-cash è che può essere spesa solo una volta.

Bob, allora, prende dal suo computer la versione di E-cash crittata con la chiave privata di Digicash e, prima di spedirla alla banca, la critta con la chiave pubblica della banca stessa.

CRITTOGRAFIA: IL PRESENTE

La banca decripta il messaggio per vedere se è diretto a lei, se è autentico e se la E-cash non sia già stata spesa. Se è tutto a posto, Bob può spedire la merce ad Alice e la Banca, o trasforma l'E-cash in moneta reale sul conto di Bob o chiede a Digicash di trasferire nuova E-cash sul computer di Bob.