LA CRITTOGRAFIA.

Sempre più spesso ci si rende conto che molte persone sottovalutano l'importanza delle informazioni contenute all'interno dei propri computer. Tutti tendono a proteggere in qualche modo i propri beni materiali, dimenticandosi che all'interno del nostro computer possono essere memorizzate informazioni ancora più preziose, o comunque riservate, che nella maggior parte dei casi sono accessibili da chiunque abbia accesso al PC. Ad esempio, solitamente, i gioielli si mettono in cassaforte, oppure si nascondono in un remoto angolo di un cassetto dove si presume che un ipotetico ladro avrebbe più difficoltà a trovarli; in modo analogo i file e le informazioni contenute nel nostro PC possono essere protette ricorrendo ad una tecnica chiamata crittografia. Detta in maniera molto semplice, la crittografia è in grado di rendere i propri file illeggibili attraverso una operazione di cifratura che, utilizzando una chiave da noi scelta, fa sì che per poter leggere un file cifrato sia indispensabile effettuare l'operazione inversa (decifratura), la quale però potrà essere eseguita solamente da chi conosce la chiave utilizzata. In tal modo il contenuto del file viene occultato, ed anche se intercettato da terzi, non potrà essere letto a meno che questi non siano a conoscenza del sistema di cifratura utilizzato.

1. CHE COS'E' LA CRITTOGRAFIA?

La crittografia (dal greco kryptos = nascosto, e graphein = scrivere) è la scienza che si occupa dello studio delle scritture "segrete"; è nata come branca della matematica e dell'informatica grazie all'utilizzo di tecniche di teoria dei numeri e di teoria dell'informazione; per scrittura segreta si intende una modalità di scrittura non leggibile da chiunque ma solo da chi è in possesso di una informazione segreta, indicata con il termine chiave (key).
La crittografia può infine essere definita come "l'insieme delle tecniche che consentono di realizzare la cifratura di un testo e la decifrazione di un crittogramma" (cfr.dizionario Garzanti).

2.1 ORIGINI STORICHE

La crittografia è una scienza antichissima utilizzata sin dai tempi più remoti per nascondere messaggi tra regnanti, imperatori, nobili: la scitala lacedemonica e il cifrario di Cesare ne sono alcuni esempi. Tuttavia il periodo d'oro della crittografia è relativo alla seconda guerra mondiale, durante la quale tutte le comunicazioni militari tedesche venivano cifrate con una macchina cifrante chiamata Enigma, ideata dall'ingegnere tedesco Arthur Scherbius. All'apparenza Enigma somigliava a una macchina da scrivere un po' particolare: una tastiera sormontata da un pannello di lettere luminose; ma il suo cuore era costituito da una serie di rotori e di spinotti elettrici che potevano essere regolati su decine di milioni di combinazioni di partenza differenti: ad ogni combinazione corrispondeva un codice di cifratura diverso. L'operatore mittente regolava la macchina, iniziava a battere sulla tastiera il messaggio in chiaro e ogni volta che premeva un tasto la corrispondente lettera cifrata si illuminava: per esempio, la parola "casa" poteva diventare "uyhj" (ma con una regolazione iniziale differente "casa" avrebbe potuto diventare "fwqp"). Per riottenere il messaggio in chiaro, l'operatore ricevente doveva regolare rotori e spinotti sull'identica posizione iniziale della macchina trasmittente, digitare sulla sua tastiera il messaggio cifrato e leggere sul pannello il testo originale: "uyhj" ritornava magicamente "casa", ma solo se la regolazione iniziale era quella giusta, altrimenti si ottenevano solo lettere senza senso.
A differenza degli esempi fin ora citati, nella crittografia moderna si ricorre a sistemi più complessi. Le tecniche utilizzate sono di natura matematica, basate principalmente su applicazioni di teoria dei

numeri, mediante le quali si costruiscono cifrari molto affidabili e sicuri poiché basati su teoremi ed applicazioni numeriche assolutamente dimostrabili.

2.2 CHE COS'E' UN CIFRARIO?

Un cifrario è un sistema di qualsiasi tipo, composto da un algoritmo, in grado di trasformare un testo in chiaro (messaggio) in un testo inintellegibile (testo cifrato o crittogramma). Per poter utilizzare un cifrario è necessario definire due operazioni: la cifratura del messaggio e la decifrazione del crittogramma. Definendo con Msg "l'insieme di tutti i messaggi" e con Critto "l'insieme di tutti i crittogrammi", le operazioni di cifratura e decifrazione possono essere definite come:

- **Cifratura**: operazione con cui si trasforma un generico messaggio in chiaro *m* in un crittogramma *c* applicando una funzione C: Msg → Critto.
- **Decifrazione**: operazione che permette di ricavare il messaggio in chiaro *m* a partire dal crittogramma *c* applicando una funzione D: Critto → Msg.

Il cifrario di Cesare è uno dei più antichi esempi di algoritmi crittografici di cui si abbia traccia storica. È un cifrario a sostituzione monoalfabetica in cui ogni lettera del testo in chiaro è sostituita nel testo cifrato dalla lettera che si trova ad un certo numero di posizioni dopo nell'alfabeto. Questi tipi di cifrari sono detti anche cifrari a sostituzione o cifrari a scorrimento a causa del loro modo di operare: la sostituzione avviene lettera per lettera, scorrendo il testo dall'inizio alla fine. In particolare, Cesare utilizzava uno spostamento di 3 posizioni (la chiave era dunque 3), secondo il seguente schema:

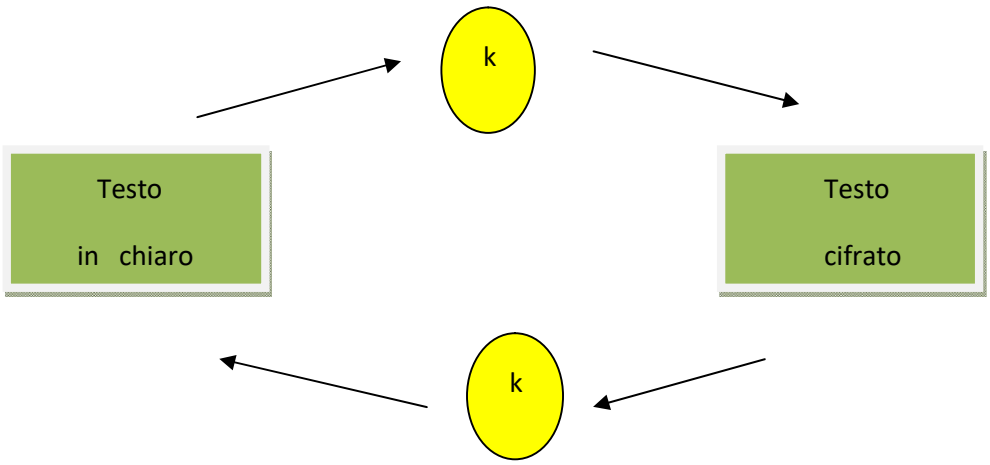
Testo in chiaro	a	b	c	D	e	f	g	h	i	J	k	l	m	N	o	p	q	r	s	t	u	V	w	x	y	z
Testo cifrato	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Per cifrare un messaggio, basta prendere ogni lettera del testo in chiaro e sostituirla con la corrispondente lettera della riga testo cifrato. Per decifrare, viceversa. Ecco un semplice esempio:

Testo in chiaro	attaccare gli irriducibili galli alla ora sesta
Testo crittato	DZZDFFDUH LON NUUNGAFNENON LDOON DOOD RUD VHVZD

3. LA CRITTOGRAFIA SIMMETRICA

Si parla di crittografia simmetrica quando ciascuna coppia di corrispondenti condivide una stessa chiave k, che ha la funzione sia di cifrare il messaggio che di decifrarlo.
La robustezza del cifrario dipende, di conseguenza, solo dalla segretezza della chiave k.



3.1 IL PRINCIPIO DI KERCKHOFFS

Risulterà strano, ma, uno dei principi fondamentali della crittografia, utilizzato ancora nei moderni sistemi crittografici, è stato individuato nel lontano 1883 dal linguista franco-olandese August Kerckhoffs e reso noto col suo celebre articolo "*La cryptographie militaire*" apparso nel *Journal des sciences militaires.*

Il principio di Kerckhoffs afferma che : "*La sicurezza di un sistema crittografico è basata esclusivamente sulla conoscenza della chiave; in pratica si presuppone noto a priori l'algoritmo di cifratura e decifrazione*." Questo significa che se la sicurezza/segretezza delle mie informazioni è affidata solo ed esclusivamente al metodo, allora essa non è tutelata, in quanto basterà comprendere il metodo, e quelle informazioni non saranno più segrete. E' la chiave a dover essere segreta, la quale è esterna al messaggio.

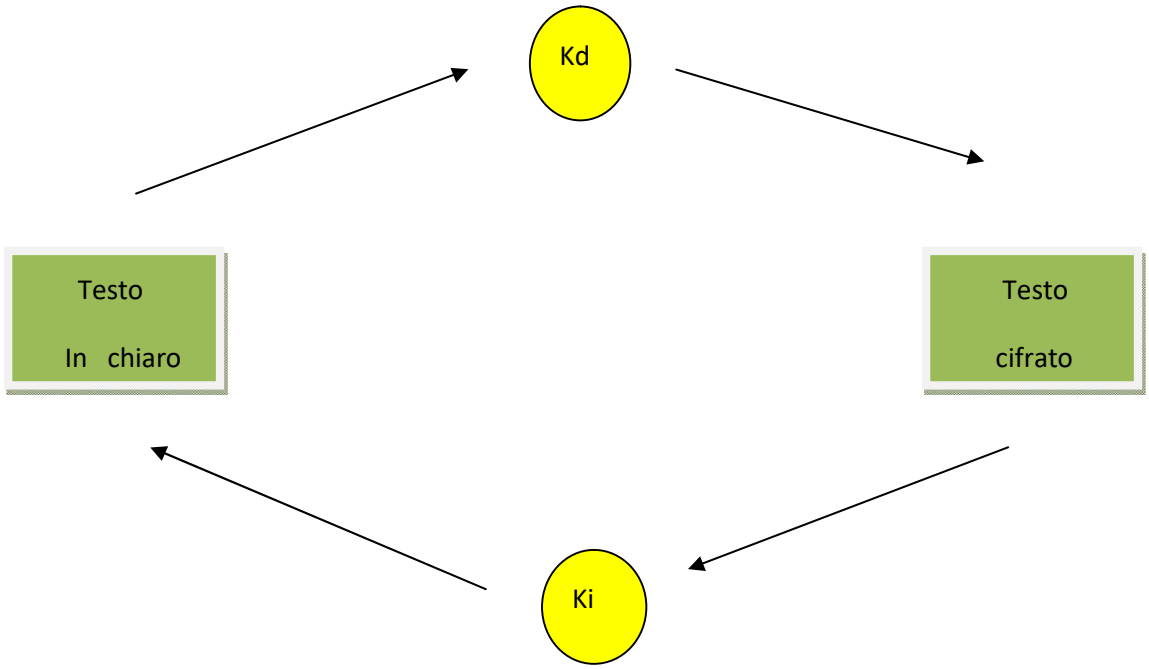
3.2 IL PROBLEMA DELLA TRASMISSIONE DELLA CHIAVE

E' opportuno, a questo punto, chiarire un punto di fondamentale importanza. Come faccio a trasmettere la chiave segreta che viene utilizzata in un cifrario simmetrico? Devo utilizzare una "canale sicuro" di comunicazione.

Ma tale "canale sicuro" esiste nella realtà?
Non esiste un canale sicuro!

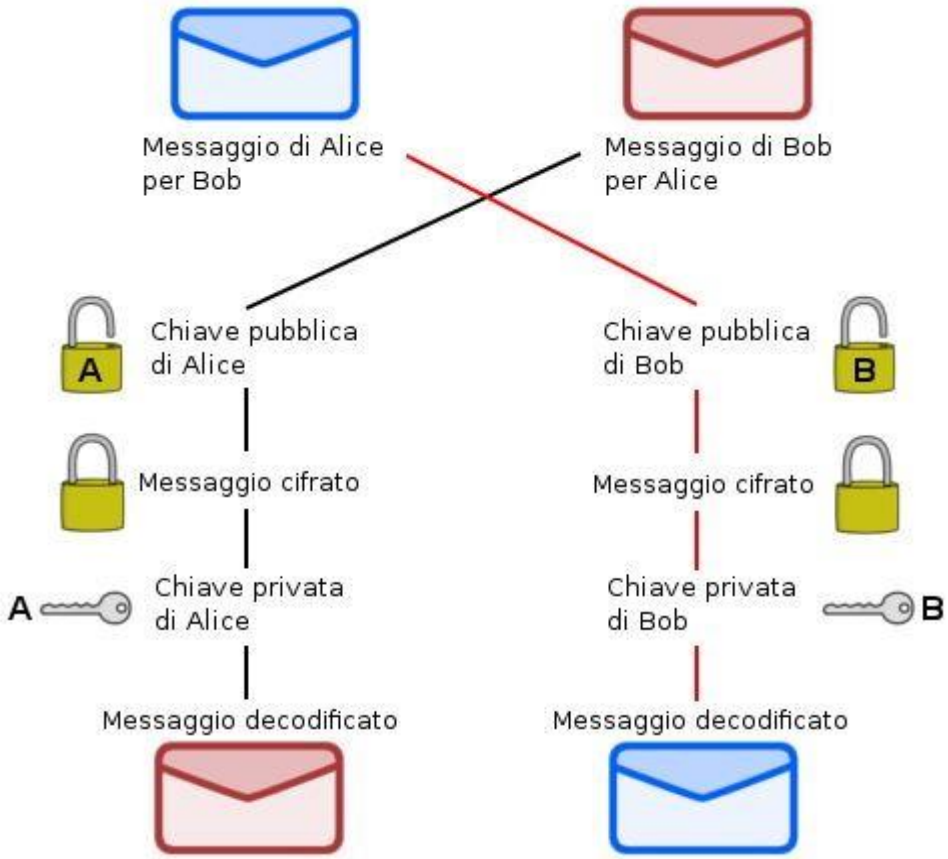
4. LA CRITTOGRAFIA A CHIAVE PUBBLICA O ASIMMETRICA

Per ovviare ai problemi inevitabilmente connessi alla crittografia simmetrica, nasce la crittografia a chiave pubblica, o asimmetrica.
La crittografia a chiave pubblica utilizza una coppia di chiavi per le operazioni di cifratura (encryption) e decifrazione (decryption).
Una chiave, detta pubblica, (public key) viene utilizzata per le operazioni di encryption.
L'altra chiave, detta privata (private key), viene utilizzata per le operazioni di decryption.
Le due chiavi sono legate da una relazione algebrica, ma conoscendo la chiave pubblica non è in alcun modo possibile risalire a quella privata in tempi computazionali ragionevoli (diverse decine di anni di calcolo con la migliore tecnologia attuale).
A differenza dei cifrari simmetrici, non è più presente il problema della trasmissione delle chiavi. Sono intrinsecamente sicuri poiché utilizzano tecniche di tipo matematico basate sulla teoria dei numeri, sulla teoria delle curve ellittiche, etc.



Kd= chiave pubblica, o diretta
Ki= chiave privata, o indiretta

Quindi, riassumendo, la chiave privata è personale e segreta, e viene utilizzata per decodificare un documento che è stato precedentemente cifrato. La chiave pubblica, invece, deve essere distribuita e, quindi, deve essere nota in quanto serve a cifrare un documento destinato esclusivamente alla persona che possiede la relativa chiave privata.



L'idea base della crittografia con coppia di chiavi diviene più chiara se si usa un'analogia postale, in cui il mittente è Alice ed il destinatario Bob, i lucchetti fanno le veci delle chiavi pubbliche e le chiavi recitano la parte delle chiavi private:

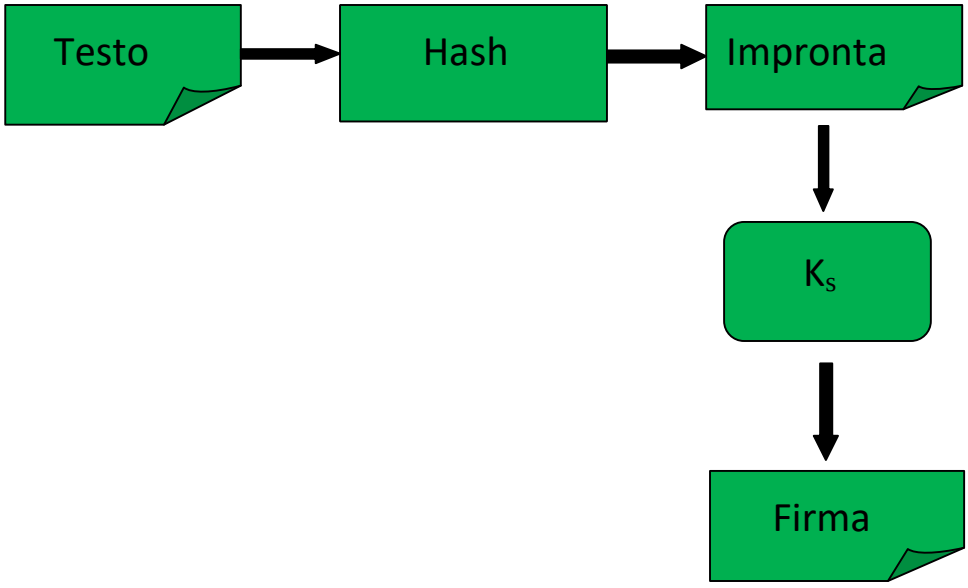
1. Alice chiede a Bob di spedirle il suo lucchetto, già aperto. La chiave dello stesso verrà però gelosamente conservata da Bob.
2. Alice riceve il lucchetto e, con esso, chiude il pacco e lo spedisce a Bob.
3. Bob riceve il pacco e può aprirlo con la chiave di cui è l'unico proprietario.

Se adesso Bob volesse mandare un altro pacco ad Alice, dovrebbe farlo chiudendolo con il lucchetto di Alice (che lei dovrebbe aver preventivamente dato a Bob) che solo lei potrebbe aprire. Si può notare come per mettere in sicurezza il contenuto dei pacchi ci sia bisogno del lucchetto del destinatario, mentre per aprirli viene usata esclusivamente la propria chiave segreta, rendendo l'intero processo di cifratura/decifratura asimmetrico (una chiave per cifrare ed una differente per decifrare). Chiunque intercettasse il lucchetto (aperto) o il messaggio chiuso con il lucchetto non potrebbe leggerne il contenuto poiché non ha la chiave. Uno dei vantaggi della crittografia asimmetrica sta nel fatto che le chiavi pubbliche possono essere scambiate anche utilizzando un mezzo insicuro, come Internet. Nella crittografia simmetrica invece, che basa la sicurezza del sistema sulla segretezza della chiave di codifica utilizzata, si rende necessario utilizzare un canale sicuro per la trasmissione della chiave, poiché l'intercettazione della stessa, da parte di terzi, vanificherebbe la sicurezza del sistema stesso.

5. AUTENTICAZIONE DEI DOCUMENTI: COS'E' LA FIRMA DIGITALE?

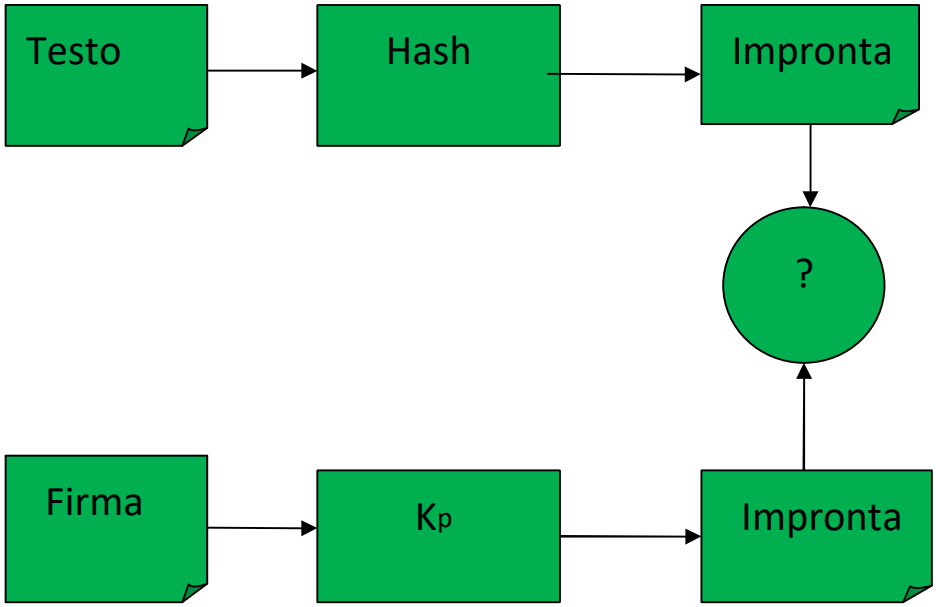
La crittografia asimmetrica presenta altri possibili impieghi, oltre quelli esaminati in precedenza. Molto importante è stato, infatti, il suo utilizzo per verificare l'autenticazione del mittente di un messaggio e l'integrità dello stesso lasciandolo in chiaro (senza necessariamente cifrarlo) . In tal senso viene utilizzata la firma digitale.
Esaminiamo, ora, nel dettaglio, la procedura attraverso la quale è possibile associare la firma.

Si utilizza un cifrario a chiave pubblica e si cifra un documento, anche un file, con la propria chiave segreta. Chiunque può verificare la paternità del documento utilizzando la chiave pubblica dell'utente firmatario.
Esiste, però, un problema che deve essere preso in considerazione: per autenticare un documento di grandi dimensioni, con un algoritmo a chiave pubblica, occorre molto tempo. E' possibile, in tali situazioni, autenticare solo un "riassunto" del documento, tramite l'utilizzo di una funzione hash sicura.
Una funzione hash è una funzione non invertibile che trasforma un testo di lunghezza arbitraria in una stringa di lunghezza fissa.
Tale stringa è chiamata in diversi modi: impronta digitale, valore hash o hash, message digest…
Possiamo applicare una funzione hash ad un qualsiasi oggetto digitale: ad un testo ma anche ad un qualsiasi file, come ad esempio uno script di un sistema web oppure una foto.
Esaminiamo più nel dettaglio attraverso un esempio.
Un utente, Alice, deve firmare un testo utilizzando la propria chiave privata. Per far ciò viene creato un "riassunto", un'impronta del messaggio, attraverso la funzione hash. Tale impronta viene firmata da Alice con la sua chiave privata. In tal modo Alice associa la sua firma al documento.
L'impronta, generata per mezzo di un algoritmo di hash, è tale che varia sensibilmente al minimo variare del messaggio. Infatti ad ogni stringa di bite originaria (il testo che intendo firmare) deve corrispondere uno ed un solo hash. Anche considerando due messaggi M ed M', differenti solo per un carattere, le loro funzioni hash H(M) e H(M') saranno diverse.
Per la proprietà della non invertibilità, non è possibile risalire dal valore di hash al testo di partenza.



5.1 COME PUO' ESSERE VERIFICATA LA FIRMA DIGITALE, E L'AUTENTICITA' DEL DOCUMENTO?

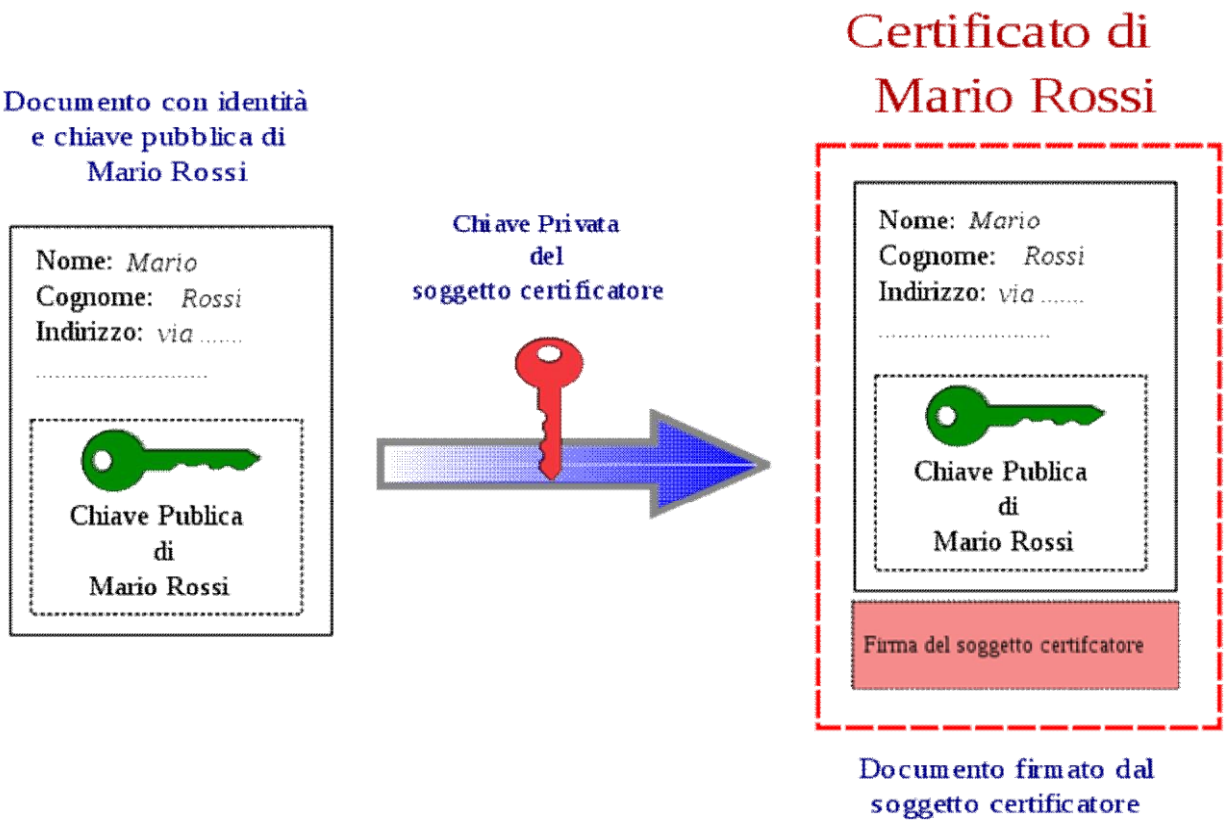
Chiunque può verificare l'autenticità di un documento: per farlo,basta decifrare la firma del documento con la chiave pubblica del mittente, ottenendo l'impronta digitale del documento. L'impronta così ottenuta verrà, poi, messa in comparazione con quella ricevuta assieme al messaggio. Se le due impronte risultano identiche il messaggio è integro, ovvero non ha subito modificazioni da parte di terzi da quando è stato firmato dall'autore (ad esempio mediante attacchi del tipo man in the middle).



Associare la firma digitale è molto importante. Essa, infatti,assicura il "non ripudio": il firmatario di un documento trasmesso non può, pertanto, negare di averlo inviato, né può il ricevente negare di averlo ricevuto. Detta in altre parole, significa che l'informazione non può essere disconosciuta, come nel caso di una firma "convenzionale", su un documento cartaceo, in presenza di testimoni.

6. IL PROCESSO DI CERTIFICAZIONE (AUTORITA' DI CERTIFICAZIONE)

Esistono dei garanti di certificazione, delle entità super partes, le Certification Authority, che attestano la validità delle chiavi, garantendo l'identità del titolare. Queste entità gestiscono l'elenco delle chiavi pubbliche.
Le Certification Authority sono abilitate al rilascio di un certificato digitale. Esso è un documento elettronico che attesta, con una firma digitale, l'associazione tra una chiave pubblica e l'identità di un soggetto (una persona, una società, un computer, etc …).



Esistono due modelli di certificazione:

- modello formale, standardizzato, avente valore legale in italia (ISO X 509);
- modello molto utilizzato su internet, anche se in italia non ha valore legale (PGP).

Lo scopo del certificato digitale è quello di garantire che una chiave pubblica sia associata alla vera identità del soggetto che la rivendica come propria.
Nello schema tipico di un'infrastruttura a chiave pubblica, (PKI), quindi, la firma apposta sarà quella di una autorità di certificazione (CA). Nella rete di fiducia ("web of trust"), invece, la firma è quella o dell'utente stesso (un'auto-certificazione) oppure di altri utenti ("endorsements").
In entrambi i casi, la firma certifica che la chiave pubblica appartiene al soggetto descritto dalle informazioni presenti sul certificato (nome, cognome, indirizzo abitazione, indirizzo IP, etc.)

6.1 PRINCIPIO E UTILIZZO

I certificati sono utili per la crittografia a chiave pubblica quando usata su larga scala.
Infatti, scambiare la chiave pubblica, in modo sicuro, tra gli utenti, diventa impraticabile, se non impossibile, quando il numero di utenti comincia a crescere. I certificati digitali sono una soluzione per superare questa difficoltà.
In principio se Mario Rossi voleva inviare/ricevere un messaggio segreto, doveva solo divulgare la sua chiave pubblica. Ogni persona che la possedeva poteva inviargli e/o ricevere da lui messaggi sicuri; tuttavia qualsiasi individuo poteva divulgare una differente chiave pubblica (di cui conosceva la relativa chiave privata) e dichiarare che essa era la chiave pubblica di Mario Rossi.
Per ovviare a questo problema, Mario Rossi inserisce la sua chiave pubblica in un certificato firmato da una terza parte fidata ("trusted third party"): tutti quelli che riconoscono questa terza parte devono

semplicemente controllarne la firma per decidere se la chiave pubblica appartiene veramente a Mario Rossi.
In una PKI, la terza parte fidata sarà un'autorità di certificazione. Nel web of trust, invece, la terza parte può essere un utente qualsiasi e sarà compito di chi vuole comunicare con Mario Rossi decidere se questa terza parte è abbastanza fidata.
Chiariamo il concetto con un esempio:
Alice e Bob vogliono scambiarsi messaggi firmati e crittografati; a tale scopo entrambi creano la loro coppia di chiavi e le pubblicano su un keyserver. Quindi, Alice scrive un messaggio per Bob, lo firma con la propria chiave privata e lo cifra con la chiave pubblica di Bob; il messaggio viene inviato.
In ricezione Bob decifra il messaggio con la propria chiave privata e verifica la firma di Alice con la chiave pubblica intestata a lei. Bob a questo punto sa due cose:

1. il messaggio era diretto a lui, perché è riuscito a decifrarlo con la propria chiave privata;
2. il messaggio è stato firmato con la chiave privata di Alice, perché Bob è riuscito a decifrare il messaggio proprio utilizzando la chiave pubblica di Alice.

Nel contempo Bob, però, non ha alcuna garanzia che la chiave sia realmente di proprietà di Alice. Continuando l'esempio, supponiamo che una terza persona, Matt, riesca ad intercettare la comunicazione in cui Bob ottiene la chiave di Alice, e riesca a sostituirla con la sua chiave pubblica in cui si spaccia per Alice. Bob non ha alcun modo per scoprire l'inganno.
E' proprio per risolvere situazioni di questo tipo che nascono le Certification Authority che si fanno carico di verificare e garantire la corrispondenza fra la chiave e il proprietario. Quando un utente richiede un certificato, la CA verifica la sua identità, quindi crea un documento digitale, firmato con la chiave privata della CA, e pubblicato. Nell'esempio precedente supponiamo che Alice e Bob si facciano firmare le loro chiavi da una CA che, entrambi, ritengono attendibile. In questo caso l'attacco di Matt non è più possibile, in quanto non è in grado di riprodurre la firma della CA. Descriviamo ora, a grandi linee, i compiti di una CA standard. Il procedimento illustrato è una linea guida che può variare caso per caso.
I compiti delle Certification Authority sono:

- identificazione certa di chi richiede la certificazione della chiave pubblica;
- rilascio e pubblicazione del certificato (firmato con la propria chiave privata);
- manutenzione del registro delle chiavi pubbliche;
- revoca o sospensione dei certificati in caso di istanza dell'interessato o in caso di abusi, falsificazioni, ecc. e nel contempo aggiornamento della lista pubblica dei certificati sospesi o revocati (certificate revocation list);
- risposta (per via telematica) alle domande di trasmissione dei certificati.

7. PRETTY GOOD PRIVACY (PGP)

Il PGP, Pretty Good Privacy,è un programma creato da Phil Zimmermann, per la crittografia delle email sicuro, relativamente "semplice" da usare ed assolutamente gratuito. Più precisamente permette di firmare una e-mail lasciando il testo in chiaro, oppure cifrarla senza firmarla, o fare tutte e due le cose insieme. Nelle intenzioni di Zimmermann, PGP doveva servire a tutelare le comunicazioni e la sicurezza individuale degli oppositori politici (leader sindacali, esponenti dei movimenti per i diritti civili, etc.) nei paesi dove il rispetto dei diritti umani non era "particolarmente sviluppato". In realtà, PGP si è progressivamente affermato, anche grazie ai suoi continui miglioramenti, come lo "standard de facto" della crittografia delle email in Internet.

PGP usa sia la crittografia asimmetrica (detta anche a chiave pubblica) sia quella simmetrica, e fino ad un certo punto una infrastruttura a chiave pubblica (PKI). PGP usa la crittografia a chiave asimmetrica, nella quale il destinatario del messaggio ha generato precedentemente una coppia di chiavi collegate fra loro; una chiave pubblica ed una privata. La chiave pubblica del destinatario serve al mittente per cifrare una chiave comune (detta anche chiave segreta o convenzionale) per un algoritmo di crittografia simmetrica; questa chiave viene quindi usata per cifrare il testo in chiaro del messaggio. Molte chiavi pubbliche di utenti PGP sono a disposizione di tutti dai numerosi key server (server delle chiavi) PGP sparsi per il mondo, che operano come mirror reciproci.
L'unico metodo possibile per decifrare il messaggio in assenza della chiave privata è quello dell'attacco a forza bruta: dovremmo far provare al nostro computer tutte le chiavi possibili ma anche uno dei più moderni computer impiegherebbe centinaia di anni per trovare una chiave a 1024 bit, immaginiamo dunque quanto impiegherebbe per trovare una chiave a 2048 o 4096 bit. Nonostante ciò il PGP non è un sistema assolutamente sicuro; nessun sistema di crittografia è sicuro e mai potrà esserlo. La sicurezza fornita dal PGP è assolutamente relativa per quanto molto vicina a quella assoluta: essa dipende da una serie di fattori tra cui quello umano. E' perfettamente inutile speculare su milioni di anni di calcolo per spezzare una chiave se poi la propria chiave segreta e la propria frase di accesso rimangono a disposizione di chiunque sulla propria scrivania o sulla propria agenda.

Conclusioni

Al fine di non violare le norme del codice penale e del codice deontologico, lo psicologo (clinico, giuridico, penitenziario) può utilizzare le nuove conoscenze informatiche per non incorrere in sanzioni.
La crittografia rappresenta un valido strumento per non incorrere in tali sanzioni.
Lo psicologo, a causa della natura della sua professione, è costantemente a contatto con dati sensibili, che secondo la legislazione italiana, sono quei dati personali idonei a rivelare:

- le convinzioni religiose, filosofiche o di altro genere,
- le opinioni politiche,
- l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale,
- lo stato di salute e la vita sessuale.

È anche importante non sottovalutare quelle che possono essere le conseguenze psicologiche per il paziente, qualora, tali informazioni venissero intercettate da terzi. Proteggere i dati sensibili dei propri pazienti significa tutelare non solo la privacy, ma anche lo stato psico-fisico degli stessi, al cui dovere lo psicologo non può far deroghe.
Concludendo, si raccomanda agli psicologi di non sottovalutare l’importanza dei dati raccolti e memorizzati sul pc, inviati e ricevuti per mezzo di Internet.