LA STORIA

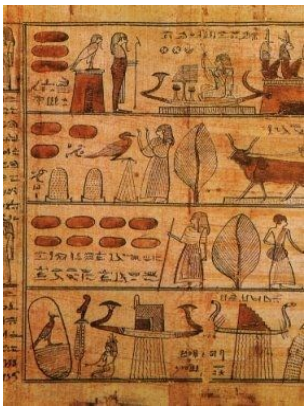
1- Cronologia storica della Crittografia

3500 a.C. - I Sumeri

La scrittura cuneiforme sumera rappresenta il più antico linguaggio scritto nella storia dell'umanità e non è stata decifrata prima del XIX secolo d.C.. Questo tipo di scrittura si basava sull'utilizzo di segni e incisioni impresse nell'argilla ancora umida. La prima forma di questo linguaggio ci giunge dalla popolazione Uruk che utilizzava i pittogrammi, disegni impressi su argilla o pietra da cui poi si sarebbe sviluppata la scrittura cuneiforme. Ogni pittogramma rappresentava un oggetto. Si passò in seguito agli ideogrammi che erano in grado di esprimere anche un concetto e ai fonogrammi.

1900 a.C. - Gli Egizi

Gli antichi Egizi utilizzavano più di 2000 caratteri geroglifici. Con essi si poteva rappresentare un oggetto comune nell'antico Egitto, un'idea associata ad un oggetto oppure il suono dell'oggetto stesso. Furono proprio gli Egizi ad usare per la prima volta la crittografia per proteggere delle informazioni. In particolare sappiamo che uno scriba per proteggere un documento da sguardi indiscreti utilizzò geroglifici non convenzionali.



1500 a.C. - Mesopotamia

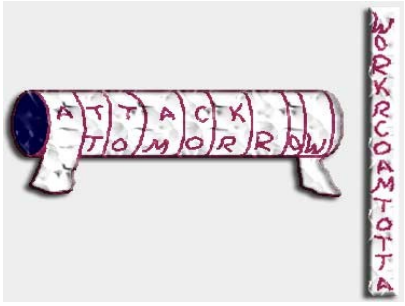
In Mesopotamia si sviluppò il linguaggio cuneiforme. I pittogrammi, o i disegni rappresentanti cose reali, furono la base per lo sviluppo della scrittura cuneiforme. Nell'immagine puoi vedere ciò che resta di una piccola tavoletta mesopotamica trovata sulle rive del Tigri che conteneva una formula cifrata per produrre una patina di terracotta. I segni cuneiformi sono stati usati negli ultimi gruppi sillabici per tentare di nascondere i segreti della formula.

500 -600 a.C. - Cifrario ATBASH

Gli scribi Ebrei che scrissero il libro di Geremia usarono un cifrario a sostituzione semplice noto come ATBASH. Si crede che molti nomi di persone e posti siano stati deliberatamente occultati nella Bibbia ebraica utilizzando questo cifrario.

486 a.C. - Scitala spartana

La scitala spartana veniva utilizzata per proteggere le informazioni strategiche durante le guerre. Plutarco racconta, nella Vita di Lisandro, un aneddoto significativo: nel 404 a.C. lo spartano Lisandro venne raggiunto al suo accampamento da un corriere il quale era riuscito a sopravvivere (insieme a pochi altri) all'attraversamento del territorio persiano. Il corriere aveva con sè un nastro che consegnò a Lisandro il quale lo avvolse attorno ad un cilindretto di legno. In questo modo lo spartano venne a conoscenza del fatto che il persiano Farnabazo intendeva attaccarlo. Organizzata la difesa, l'attacco venne respinto.



150 a.C. - Scacchiera di Polibio

Nonostante la procedura di codifica e decodifica fosse abbastanza elementare, con la scacchiera ideata da Polibio (storico greco del mondo mediterraneo), si potevano facilmente trasmettere a distanza messaggi in codice utilizzando delle torce dato che i messaggi venivano convertiti in sequenze di numeri.

	1	*2*	*3*	*4*	*5*	*6*
1	α	β	γ	δ	ε	ζ
2	η	θ	ι	κ	λ	μ
3	ν	ξ	ο	π	ρ	σ
4	τ	υ	φ	χ	ψ	ω

50-60 a.C. - Cifrario di Cesare

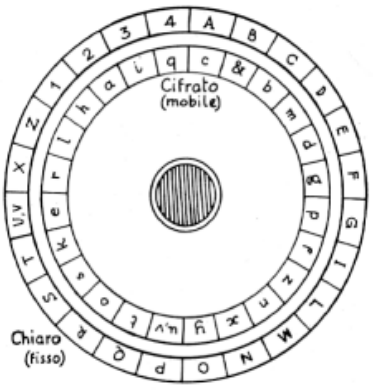
Il cifrario ideato da Cesare è la prima forma di crittografia monoalfabetica (detta anche a sostituzione) che veniva utilizzata soprattutto per proteggere le comunicazioni militari e quelle con Augusto. Svetonio ci dà testimonianza di questo (traduzione da Vita di Cesare):
"Restano quelle [le lettere] a Cicerone, così come quelle ai familiari sugli affari domestici, nelle quali, se doveva fare delle comunicazioni segrete, le scriveva in codice, cioè con l'ordine delle lettere così disposto che nessuna parola potesse essere ricostruita: se qualcuno avesse voluto capire il senso e decifrare, avrebbe dovuto cambiare la quarta lettera degli elementi, cioè D per A e così via per le rimanenti."

1450-1520 - Manoscritto Voynich

Il manoscritto Voynich (prende il nome da colui che lo ha trovato) è "il più misterioso libro della Terra". E' scritto in un corsivo fluente e fa uso di un alfabeto mai visto in precedenza. Ancora oggi, nessuno conosce il significato che si cela dietro questo documento lungo circa 200 pagine. Tuttavia le tante immagini al suo interno farebbero pensare ad una "enciclopedia naturale del Rinascimento". Le ultime indagini comunque, ci dicono che probabilmente il manoscritto Voynich "altro non sarebbe che lo strumento di una truffa ai danni di Rodolfo II, imperatore del Sacro Romano Impero e grande collezionista di testi esoterici e mirabilia, al quale sarebbe stato venduto per una cifra esorbitante, spacciandolo per un’opera di Ruggero Bacone."

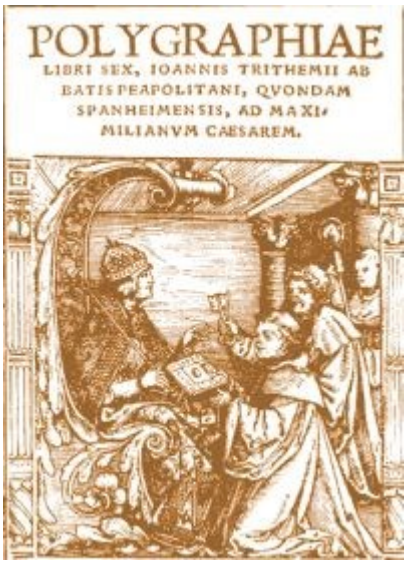
1466 - Leon Battista Alberti

Leon Battista Alberti ha inventato il disco cifrante e la chiave crittografica. Il disco cifrante era polialfabetico, perciò un nuovo alfabeto poteva essere creato ogni volta facendo ruotare opportunamente il disco. Questo, fino al XVI secolo, era l'unico metodo conosciuto per utilizzare un cifrario polialfabetico e Leon Battista Alberti credeva non ci fosse possibilità di "rompere" il sistema. Naturalmente si sbagliava...



1508 - Giovanni Tritemio

La data fa riferimento all'anno in cui fu terminata la stesura di quello che sarà il primo libro stampato sul tema della crttografia: Polygraphiae Libri Sex ("Sei libri sulla Poligrafia"). La pubblicazione, tuttavia, risale a qualche anno dopo la morte di Tritemio (avvenuta nel 1516). Il testo raccoglie gli avvenimenti più significativi nello studio della crittografia a partire dagli antichi Egizi fino all'era cristiana. L'autore mette in evidenza le particolari abilità dei Franchi, principalmente di Carlo Magno, nel comprendere l'utilizzo dei sistemi crittografici ed esorta l'imperatore Massimiliano (a cui il libro è dedicato) a prendere esempio dal sovrano franco.

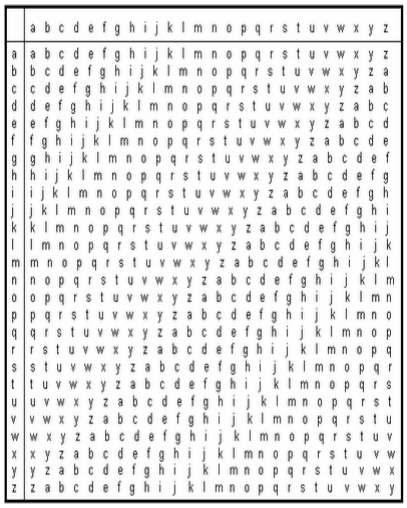


1553 - Cifrario di Bellaso

Il titolo del libro pubblicato a Venezia in quell'anno è: "La Cifra del Sig. Giovan Battista Bellaso [...]", dedicato al poligrafo Girolamo Ruscelli. Il testo descrive un utilizzo più efficace della tabula recta introducendo un frase chiave ("verme") che viene ripetuta tante volte fino ad arrivare alla lunghezza del testo in chiaro. In questo modo l'alfabeto varia continuamente grazie proprio a questa chiave. Questo sistema risulta essere più debole di quello di Leon Battista Alberti.

1586 - Codice di Vigenère

Questo cifrario polialfabetico in realtà riprende il concetto introdotto da Bellaso per la cifratura utilizzando più alfabeti, ma risulta addirittura più debole anche se per anni è stato considerato sicurissimo.



	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
a	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
c	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
d	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
e	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
f	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
g	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
h	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
i	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
j	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
k	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
l	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
m	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
n	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
o	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
p	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
r	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
s	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
t	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
u	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
v	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
w	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
x	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

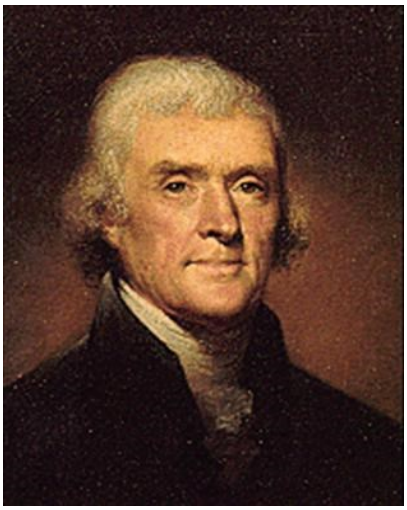
1586 - Maria Stuarda di Scozia

Maria Stuarda di Scozia fu decapitata per aver complottato contro la Regina Elisabetta utilizzando cifrari a sostituziione monoalfabetica. La condanna a morte avvenne sulla base di prove ottenute da masseggi cifrati che furono decodificati da Tomas Phelippes, nonostante al loro interno ci fossero soltanto zeri o parole in codice.

1626 - "La Gran Cifra"

Considerata una delle più sicure cifrature monoalfabetiche, la "Grande Chiffre" veniva utilizzata per proteggere le comunicazioni riservate del re Luigi XIV. Fu ideata dai Antonie e Bonaventure Rossignol (padre e figlio) i quali grazie alla scoperta di questo sistema furono accolti a corte ed ebbero incarichi di rilievo sotto la dominazione del Re Sole.

1795 - Il disco di Jefferson



Questo sistema fu ideato da Thomas Jefferson (presidente degli Stati Uniti dal 1801 al 1804), ma, nonostante le buone caratteristiche di sicurezza, non divenne molto famoso. Fu il comandante Etienne Bazaries a creare una seconda versone del "cifrario a ruota" che prese il nome di Cilindro di Bazaries. Questa volta il sistema ebbe successo tant'è che fu utilizzato dall'esercito degli Stati Uniti dal 1923 al 1942 come implementazione nella macchina cifrante M-94.

1799 - Esperimenti sulla luce

Thomas Young condusse nel 1799 un esperimento in cui fece passare della luce attraverso due sottili fessure aspettandosi di vedere due strisce luminose proiettate su uno schermo posto di fronte alle fessure ad una cera distanza. Accadde invece che la luce una volta attraversate le due fessure, si allargava a ventaglio formando sullo schermo una trama a strisce di luce/oscurità.

La spiegazione di questo fenomeno arrivò alla mente di Young qualche tempo dopo osservando delle anatre in uno stagno. Esse nuotando una dietro l'altra, producevano una scia di piccole onde che ovviamente interferivano in qualche modo tra di loro. Se due picchi d'onda arrivavano in un punto simultaneamente, il risultato era un picco ancora più grande, mentre due depressioni (tra un'onda e l'altra) simultanee producevano un depressione ancora più profonda. Perciò, Young suppose che la luce fosse in realtà qualche genere d'onda e le strisce sul suo schermo erano il risultato di una interazione tra i raggi di luce. Le anatre diedero allo studioso inglese una più profonda conoscenza della natura della luce e lo spinsero a pubblicare il suo capolavoro "La teoria ondulatoria della luce".

Più di un secolo dopo i fisici furono in grado di ripetere l'esperimento di Young con un singolo fotone e rimasero perplessi nell'osservare nuovamente una trama a strisce di luce/oscurità sullo schermo. Era impossibile spiegare come un singolo fotone potesse interagire con se stesso usando le leggi della fisica classica e perciò nacque la "Teoria Quantistica" su cui oggi si basa Crittografia Quantistica.

1822 - Cifrario Beale

Si tratta di tre messaggi lasciati da Thomas J. Beale ad un amico, composti da sequenze di numeri che un volta decifrati dovrebbero condurre ad un tesoro nascosto negli Stati Uniti. Fino ad oggi solo il secondo messaggio è stato decifrato basandosi sul testo della Dichiarazione d'Indipendenza Statunitense e sembra indicare che il valore del tesoro si aggiri intorno a 20 milioni di dollari! Tuttavia si teme che organi governativi come l'NSA (che dispone di mezzi potentissimi per la decifrazione dei codici) abbia già scoperto e recuperato il bottino. C'è anche chi pensa che, dato tutto il tempo trascorso a cercare una risposta senza ottenere risultati, il cifrario sia quindi una bufala. Lo studio di questo crittogramma, comunque, non si è fermato.

1835 - Codice morse

Il codice fu creato da Alfred Vail in collaborazione con Samuel Morse durante lo sviluppo della telegrafia: il codice Morse rappresenta lettere, numeri e punteggiatura sottoforma di segnali codici inviati ad intermittenza. Si tratta quindi di una prima forma di comunicazione digitale. Nel 1863 fu creata la forma europea del codice Morse.

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: ––··	

1854 - Cifrario Playfair

Sebbene il nome del barone Playfair sia collegato a quello del cifrario meglio conosciuto, l'amico del barone, lo scienziato Charles Wheatstone (in foto), è in realtà colui che ha progettato il sistema. Tuttavia, poichè dopo la pubblicazione del cifrario nel 1854 il barone sollecitò il governo britannico affinchè esso venisse adottatto per uso ufficiale, questo metodo crittografico prese il nome del barone Playfair e non quello di Wheatstone.

1883 - Principi di Kerckhoffs

Auguste Kerckhoffs è conosciuto per aver pubblicato nel 1883 due saggi nel "Journal of Military Science". Questi articoli esaminavano lo stato dell'arte nella crittografia militare e includevano consigli e linee guida, oltre ai 6 famosi principi per la progettazione di un algoritmo crittografico. Di questi 6, il più famoso è il secondo: "Non c'è segretezza nell'algoritmo; La segretezza sta tutta nella chiave." Questo principio è noto anche come Legge di Kerckhoffs.

Per completezza ecco qui i 6 principi tradotti dal francese:

1) Il sistema deve essere praticamente, se non matematicamente, indecifrabile;

2) Non deve essere un requisito la segretezza del sistema che, anche cadendo in mani nemiche non presenterà alcun inconveniente;

3) La chiave del sistema deve essere comunicabile e memorizzabile senza l'utilizzo di ulteriori note scritte, e modificabile a piacimento dagli interlocutori;

4) Il sistema deve essere applicabile alla corrispondenza telegrafica;

5) Il sistema deve essere portabile e il suo utilizzo e le sue funzioni non devono richiedere la partecipazione di più persone;

6) Infine è necessario, date le circostanze che dirigono l'applicazione, che il sistema sia facile da usare, senza richiedere né sforzo mentale, né la conoscenza di lunghe serie di regole da osservare.

1918 - Cifrario ADFGVX

Fu usato dall'esercito tedesco durante la Prima Guerra Mondiale. Inventato dal colonnello Fritz Nebel, venne pubblicato nel Marzo 1918. Inizialmente si chiamava ADFGX e permetteva di codificare solamente 25 lettere (la i e la j erano codificate allo stesso modo). In seguito si aggiunse la lettera V al nome e quindi al sistema per avere 36 caratteri codificabili (tutto l'alfabeto più i numeri caratteri da 0 a 9).

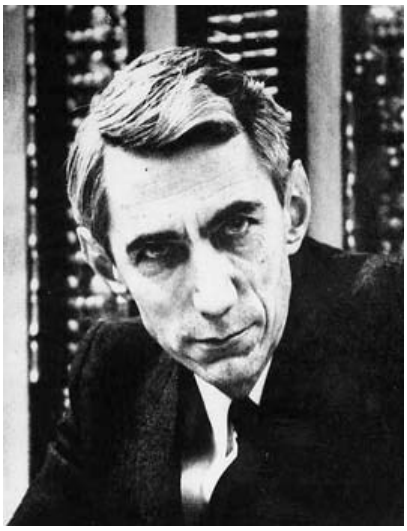
	A	D	F	G	V	X
A	S	U	B	J	E	C
D	T	A	D	F	G	H
F	I	K	L	M	N	O
G	P	Q	R	V	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

1937-1945 - Navajo "Code Talkers"

Ai "Parla codice Navajo" è stata attribuita la salvezza di innumerevoli vite e la riduzione della durata della guerra.
Il loro compito principale era di parlare e trasmettere informazioni riguardo tattiche, movimenti delle truppe, ordini e altre informazioni di vitale importanza attraverso il telegrafo o la radio utilizzando il dialetto nativo.
Un notevole vantaggio di questo sistema era la velocità, infatti rispetto alla comunicazione in codice Morse che spesso richiedeva ore per essere completata, i Navajo potevano trasmettere messaggi in pochi minuti.
Inoltre, ai tempi della Seconda Guerra Mondiale la lingua nativa dei Navajo era compresa da meno di 30 persone nel mondo native di altri luoghi ed era per la sua complessità, molto difficile da decifrare.

1949 - Claude Shannon

L'età moderna della crittografia cominciò quando Shannon entrò nel campo. In particolare viene ricordato per un suo famoso testo: "Teoria della comunicazione nei sistemi di segretezza". In questo libro la crittografia viene innalzata al livello di una vera e propria scienza. Inoltre, viene dimostrato che l'unico metodo per ottenere una cifratura perfetta, è quello di usare una chiave della stessa lunghezza del messaggio da codificare. Un sistema che viene detto One-Time-Pad (conosciuto anche come Cifra di Vernam). Questo sistema è, appunto, alla base della crittografia moderna.



1959 - Nasce il circuito integrato

Quando fu introdotto nel 1959, il circuito integrato consisteva almeno di due dispositivi semiconduttori interconnessi; perlopiù transistor e resistori. Molti studiosi credono che la rivoluzione digitale apportata da questi dispositivi rappresenti uno degli eventi più significativi nella storia del genere umano.

1970 - "Soldi Quantistici"

Le radici della Crittografia Quantistica si trovano alla fine degli anni 60', quando Stephen Wiesner, laureato alla Columbia University, provò a rendere pubblica la sua idea sui "Soldi Quantistici" che dovrebbero essere impossibili da contraffare. Un'idea talmente rivoluzionaria che all'epoca quasi nessuno ne intuì il grande potenziale, infatti Wiesner non ottenne alcun supporto per la ricerca e per la diffusione di questa teoria. Nella sua mente, ogni banconota dovrebbe contenere 20 "light trap", ossia piccoli dispositivi atti a catturare un fotone ciascuno, ed in più un numero di serie univoco per ogni banconota. I light trap dovrebbero essere riempiti con 20 fotoni polarizzati in modo casuale che possono essere solo letti e ripristinati dalla banca che conosce, a partire dal numero di serie, l'esatta sequenza di filtri polarizzati da utilizzare.

1971 - Cifrario Lucifer

Fu sviluppato da Horst Feistel e dai suoi colleghi all'IBM. E' un cifrario a blocchi utilizzato nel sue prime versioni già dal 1970 per la protezione dei dati elettronici bancari. E' il diretto precursore del famoso DES (Data Encryption Standard).

1973 - Bell-LaPadula

David Bell e Len LaPadula crearono il Modello di Riservatezza Bell-LaPadula in risposta alla preoccupazione del Dipartimento della Difesa Statunitense per la sicurezza dei sistemi di condivisione dati tra mainframe. Il modello descrive una serie di regole per il controllo degli accessi ad informazioni classificate, ma si concentra anche sulla riservatezza dei dati.

1973 - Horst Feistel

Horst Feistel è stato uno dei primi ricercatori non militari nel campo della crittografia e può essere considerato il padre dei moderni cifrari a blocchi. Nel 1973 egli pubblicò un articolo dal titolo "La Crittografia e la Privacy dei Computer" sul magazine "Scientific American"; in questo articolo cercò di coprire i più importanti aspetti della cifratura ad opera di macchine ed introdusse quella che oggi è conosciuta come "Rete di Feistel", alla base del DES.

1975 - Algoritmi Hash

Tipicamente, gli algoritmi Hash sono usati per fornire una impronta digitale del contenuto di un file in modo da assicurare che quel file non sia stato modificato da un intruso o da un virus. La loro funzione principale è, quindi, garantire l'integrità dei dati.

1975 - Diffie-Hellman-Merkle

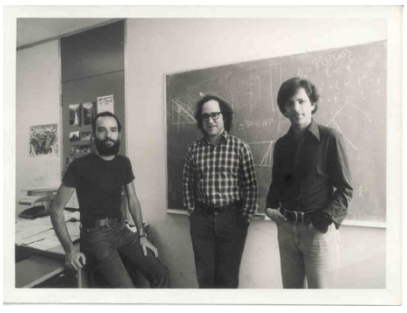
La Crittografia a Chiave Pubblica nasce grazie all'opera di Whitfield Diffie, Martin Hellman e al contributo di Ralph C. Merkle (nella foto da sinistra a destra: Merkle, Hellman, Diffie) che nel 1976 progettarono un sistema di comunicazione sicuro anche se i dati venivano trasmessi su un canale insicuro. Il protocollo fu pubblicato nel documento titolato "Nuove direzioni nella Crittografia" e fu un successo perchè era stato risolto (almeno teoricamente) il problema della distribuzione delle chiavi.

1976 - Des (Data Encryption Standard)

Nel 1972, dopo aver concluso uno studio sulle esigenze di sicurezza per i computer del Governo degli Stati Uniti, l'NBS (National Bureau of Standards, oggi noto come NIST [National Institute of Standards and Technology]) riconobbe che era necessario creare uno standard di crittografia per proteggere le informazioni sensibili del governo. Nel 1974, l'IBM propose uno standard di protezione basato sul cifrario Lucifer progettato qualche anno prima da Horst Feistel. Il DES divenne uno standard nel Novembre del 1976 e fu reso pubblico il 15 Gennaio 1977 col nome di FIPS PUB 46.

1977 - RSA

L'algoritmo è stato pubblicamente descritto nel 1977 da Ron Rivest, Adi Shamir e Leonard Adleman al Massachusetts Institute of Technology. La sigla RSA deriva dalle iniziali dei cognomi dei tre creatori.



1982 - Teoria dei computer quantistici

Il fisico Richard Feynman fu il primo ad introdurre il concetto di un computer che dovrebbe sfruttare l'effetto quantistico, infatti nel 1982 egli sviluppò un modello teorico proprio di questo computer detto, "computer quantistico". Alla base di questo modello c'è il concetto di sovrapposizione degli stati che Erwin Schrödinger spiega con il famoso Paradosso del Gatto:

"Immaginate un gatto in una scatola. Ci sono due possibili stati per il gatto: vivo o morto. All'inizio sappiamo che esso è vivo quindi non c'è alcuna sovrapposizione di stato; se però poniamo all'intero della scatola una fiala di cianuro e chiudiamo la scatola stessa, non sapremo se il gatto è ancora vivo o no. Quindi l'animale è in sovrapposizione di stato. Quando apriamo la scatola costringiamo il gatto a lasciare lo stato di sovrapposizione ed esso deve essere o vivo o morto. Questo concetto è valido anche per piccole particelle come i fotoni."

Library of Congress (AP photo)

Torniamo al computer quantistico. Un registro a 8 bit tradizionale utilizzato nel computer normali rappresenta sempre uno stato ben conosciuto, che è un valore da 0 a 255. Nel computer quantistico, invece, il registro produce una sovrapposizione di tutti i 256 stati e può quindi svolgere calcoli con tutti i 256 stati possibili allo stesso tempo.

1984 - Crittografia Quantistica

Lo studio di Stephen Wiesner sui cosiddetti "Soldi Quantistici" non venne compreso dalla maggior parte degli studiosi, a parte uno: Charles Bennett che, ai tempi della pubblicazione di Wiesner era ancora uno studente universitario. Tuttavia, aveva capito l'enorme potenziale derivante da un utilizzo di questo sistema nella Crittografia. I suoi studi continuarono per molti anni e cominciarono a concretizzarsi nei primi anni 80' quando entrò in contatto con uno scienziato dell'Università di Montreal: Gilles Brassard. La ricerca su un nuovo protocollo di comunicazione sicura utilizzando la crittografia quantistica andò avanti per un pò di tempo, ma c'era una debolezza nel sistema che stava portando i due ricercatori ad abbandonare l'intero studio. La svolta arrivò nel 1984, quando Bennett e Brassard inventarono un nuovo protocollo (il BB84) conversando in una atmosfera molto informale: l'idea arrivò durante una conversazione alla stazione.

1991 - PGP (Pretty Good Privacy)

PGP viene pubblicato nel 1991 da Philip Zimmermann. In origine fu creato in risposta al Disegno di Legge 266 del Senato degli Stati Uniti con il quale si intendeva costringere i produttori di sistemi di comunicazione protetti a fornire una backdoor utile al governo Statunitense per leggere queste comunicazioni. Alla fine, il Disegno di Legge venne respinto.

1991 - MD5

Versione 5 dei Message Digest creati da Ron Rivest. L'MD5 è stato introdotto poichè il suo predecessore MD4 si è rivelato insicuro. L'algoritmo hash viene utilizzato in svariati ambiti nel campo dell'informatica anche se le sue debolezze sono molteplici e sempre più gravi.

1994 - SSL (Secure Socket Layer)

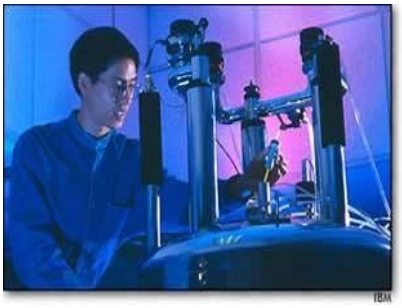
La prima versione del protocollo è stata rilasciata nel 1994 da Netscape Communication Corporation, anche se in realtà non fu mai usata a favore della versione 2.0 introdotta in Navigator 1.0. L'utilizzo principale del protocollo SSL è in ambito e-commerce, infatti tramite esso si possono proteggere da eventuali intrusioni le transazioni online.

1994 - RC4 pubblicato su Internet

Si tratta di un generatore di numeri pseudo-casuali creato originariamente nel 1987 da Ron Rivest. La data riportata (1994) si riferisce alla pubblicazione su Internet di una presunta copia del codice sorgente dell'algoritmo ad opera di uno sconosciuto. Le applicazioni di RC4 sono innumerevoli anche se esso non è immune da alcuni tipi di attacchi.

1998 - Informatica Quantistica

Il primo computer quantistico fu costruito nel 1998 presso l'Università della California e consisteva di due QBit (Bit Quantici). Negli anni la ricerca è cresciuta e così nel 2001 l'IBM è riuscita a costruire un computer a 7 QBit in grado di eseguire l'algoritmo di Shor fattorizzando il numero 15 in 3 e 5.



1999 - WEP (Wired Equivalent Privacy)

Lo standard IEEE 802.11 (ratificato nel 1999) definisce un meccanismo per la riservatezza dei dati conosciuto come Wired Equivalent Privacy (WEP), il quale si pone l'obiettivo di raggiungere un livello di sicurezza pari a quello delle reti cablate. Questo sistema viene ritenuto, a causa della facilità con cui può essere forzato, il minimo indispensabile per impedire a un utente casuale di accedere alla rete locale.

2001 - AES (Advanced Encryption Standard)

L'AES è il risultato di 3 anni di lunghe richieste pubbliche da parte del NIST (National Institute of Standards and Technology) di proposte per un nuovo standard di crittografia. Nel 1999, di tutte gli algoritmi proposti (più di 15), solo 5 furono selezionati per la finale: Rijndael, Mars, RC6, Serpent e Twofish. Alla fine del processo di standardizzazione, Rijndael, un cifrario sviluppato dai due crittanalisti belgi Joan Daemen and Vincent Rijmen (in foto), venne annunciato come il vincitore, divenendo divenne il successore del DES.

2003 - WPA (Wi-fi Protected Access)

Wi-Fi Protected Access (WPA) è un protocollo per la sicurezza delle reti senza filo Wi-Fi creato nel 2003 per tamponare i problemi di scarsa sicurezza del precedente protocollo di sicurezza, il WEP. Studi sul WEP avevano individuato delle falle nella sicurezza talmente gravi da renderlo quasi inutile. Il WPA implementa parte del protocollo IEEE 802.11i e rappresenta un passaggio intermedio per il raggiungimento della piena sicurezza. Questa verrà raggiunta quando i dispositivi implementeranno completamente lo standard IEEE 802.11i.

TEORIA

Contenuti

Cenni sulle Funzioni

Insiemi

Un insieme è costituito da oggetti distinti detti elementi dell'insieme. Per esempio un insieme X potrebbe contenere gli elementi a,b,c e questo viene indicato così:
X = {a,b,c}.

Funzioni

Una funzione (o trasformazione) è definita da due insiemi X e Y e una regola f che assegna ad ogni elemento in X esattamente un elemento in Y.

Dominio e codominio

L'insieme X si chiama dominio della funzione, mentre Y è detto codominio.

Immagine e Preimmagine

Se x è un elemento di X (in simboli x Є X) l'immagine di x è l'elemento in Y che la regola f associa ad x; l'immagine y di x è indicata con: $y = f(x)$. La notazione standard per una funzione f da un insieme X a un insieme Y è $f: X \to Y$. Se y Є Y, allora una preimmagine di y è un elemento x Є X per cui $f(x) = y$. L'insieme di tutti gli elementi in Y che hanno almeno una preimmagine è detto immagine di f, in simboli $\mathrm{Im}(f)$.

Funzione iniettiva

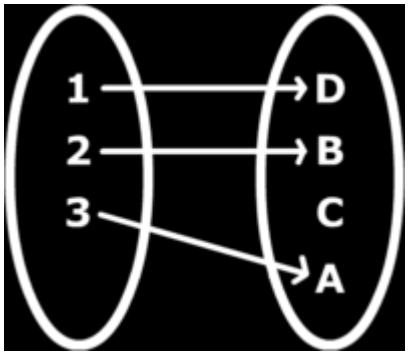
Una funzione si dice iniettiva (o ingettiva) se elementi distinti del dominio hanno un' immagine distinta, o equivalentemente se ogni elemento del codominio corrisponde al più ad un elemento del dominio.

Funzione suriettiva

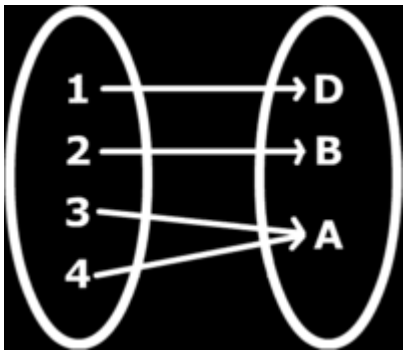
Una funzione si dice suriettiva (o surgettiva, o una suriezione) quando l'immagine della funzione coincide con il codominio, ovvero quando ogni elemento y del codominio è immagine di almeno un punto del dominio.

Funzione biiettiva

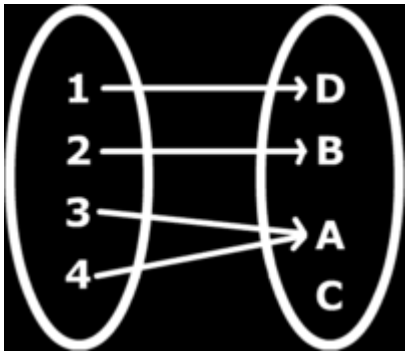
In matematica, una corrispondenza biunivoca tra due insiemi X e Y è una relazione binaria tra X e Y, tale che ad ogni elemento di X corrisponda uno ed un solo elemento di Y, e viceversa ad ogni elemento di Y corrisponda uno ed un solo elemento di X.
Lo stesso concetto può anche essere espresso usando le funzioni: una funzione $f: X \to Y$ è una biiettiva, bigettiva o biunivoca se per ogni elemento y di Y vi è uno e un solo elemento x di X tale che $f(x) = y$. Una tale funzione è detta anche biiezione o bigezione.
La funzione $f: X \to Y$ se e solo se è invertibile.



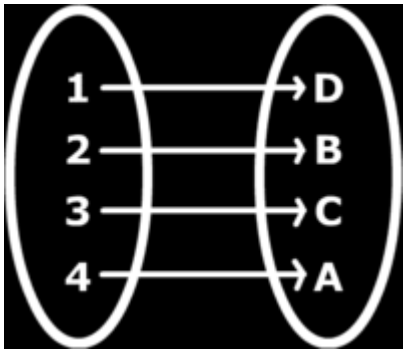
Esempio di funzione iniettiva ma non suriettiva.



Esempio di funzione suriettiva ma non iniettiva.



Esempio di funzione non iniettiva e non suriettiva.



Esempio di funzione biiettiva.

Funzione inversa
Se f è una bigezione da X a Y allora si può definire una bigezione g da Y a X come segue: per ogni y Є Y si definisce g(y) = x dove x Є X e f(x) = y. Questa funzione g ottenuta da f è chiamata funzione inversa di f ed è indicata con: g = f^{-1}.

In Crittografia le biiezioni sono utilizzate come strumento per codificare i messaggi e le trasformazioni inverse sono usate per decifrare.

Funzioni One-Way (ad un solo senso)
Ci sono alcuni tipi di funzioni che giocano un ruolo fondamentale nella Crittografia.

Una funzione f: X → Y è chiamata funzione one-way se f(x) è facilmente computabile per ogni x Є X, ma per "sostanzialmente tutti" gli elementi di y Є Im(f) è "computazionalmente irrealizzabile" trovare un qualsiasi

x Є X tale che $f(x) = y$.
Nota: la frase "per sostanzialmente tutti gli elementi di
y Є Im(f)" si riferisce al fatto che ci sono alcuni valori di y Є Y per cui è facile trovare un x Є X tale che
$f(x) = y$.

Funzioni one-way trapdoor (ad un solo senso con botola)
Una funzione one-way trapdoor può essere una funzione one-way $f: X \rightarrow Y$ con la proprietà aggiuntiva che date alcune informazioni supplementari (chiamate informazioni botola) diventa possibile trovare per un dato y Є Im(f) un x Є X tale che $f(x) = y$.
Questo tipo di funzioni sono alla base della Crittografia a Chiave Pubblica.

Permutazioni
Le permutazioni sono funzioni che vengono spesso utilizzate in vari concetti teorici della Crittografia.

Sia S un insieme finito di elementi. Una permutazione p su S è una bigezione da S a se stesso
($p: S \rightarrow S$).

Esempio. Sia S = {1,2,3,4,5}. Una permutazione $p: S \rightarrow S$ è definita come:

p(1) = 3; p(2)= 5; p(3)= 4; p(4)= 2; p(5)= 1.

Una permutazione può essere descritta in vari modi. Un altro modo diverso da quello di cui sopra è l'array:

$$p = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 3\ 5\ 4\ 2\ 1 \end{pmatrix}$$

dove la riga di sopra è il dominio e la riga in basso è l'immagine sotto la mappatura p. Naturalmente, esistono altre rappresentazioni.
Dato che le permutazioni sono biiezioni, esse possiedono inversi. Se una permutazione è scritta sotto forma di array, la sua inversa è facilmente ottenuta scambiando le righe nell'array e riordinando gli elementi nella nuova riga in alto se desiderato (la riga in basso dovrà essere riordinata in corrispondenza con quella in alto). Nell'esempio l'inverso di p è p^{-1}:

$$p^{-1} = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 3\ 5\ 4\ 2\ 1 \end{pmatrix}$$

Involuzioni
Le involuzioni sono un altro tipo di funzioni che hanno la proprietà di essere i loro stessi inversi.

Sia S un insieme finito di elementi e sia f una bigezione da S in S (f: S → S). La funzione f è detta involuzione se $f = f^{-1}$. Equivalentemente si potrebbe dire che si ha una involuzione se $f(f(x)) = x$ per ogni x ∈ S.
Top

Terminologia

Crittografia
Il termine Crittografia deriva dalle parole greche "kryptòs" (nascosto) e "gràphein" (scrittura) da cui deriva il significato di "scrittura nascosta".
Per cui, volendo dare una breve definizione, diremo che la Crittografia è la scienza che si occupa di proteggere il contenuto di messaggi da coloro che non sono autorizzati a conoscerlo.
Secondo l'RFC 2828, la parola Crittografia si riferisce alla "scienza matematica che si occupa di trasformare i dati rendendo il loro significato inintellegibile (ossia nascondendo il contenuto semantico), prevenendo alterazioni dello stesso significato o un utilizzo non autorizzato. Se la trasformazione è reversibile, la Crittografia si occupa anche di riportare i dati cifrati in forma intellegibile."
Conseguentemente, la Crittografia fa riferimento al processo di protezione dei dati in senso molto ampio al fine di fornire confidenzialità agli stessi.
La Crittografia costituisce insieme alla Crittanalisi, la scienza che va sotto il nome di Crittologia.

Partecipanti ad una Comunicazione
- Una entità o parte è qualcuno o qualcosa che invia, riceve o manipola informazioni. Esempi di entità sono le persone, i terminali di computer, ecc...;

- Un mittente in una comunicazione con due partecipanti è un'entità la quale è il legittimo trasmettitore di informazioni;

- Un destinatario in una comunicazione con due partecipanti è un'entità che rappresenta il ricevente dell'informazione trasmessa;

- Un avversario in una comunicazione con due partecipanti è un'entità che non è nè mittente, nè destinatario e la quale cerca di abbattere il servizio di sicurezza dell'informazione presente tra mittente e destinatario. In campo crittografico il termine avversario è sinonimo di intruso, nemico, attaccante.

Canali
- Un canale è un mezzo per trasmettere informazioni da un'entità ad un'altra;

- Un canale fisicamente sicuro o canale sicuro è un particolare canale che non può essere in alcun modo acceduto dall'avversario;

- Un canale insicuro è un tipo di canale a cui possono accedere anche i partecipanti a cui il messaggio non è rivolto;

- Un canale reso sicuro (secured channel) è un canale a cui un avversario non è in grado di accedere.

Messaggi e Codifica
Considereremo l'insieme A finito che prende il nome di alfabeto di definizione. Per esempio, A = {0,1}, l'alfabeto binario è un alfabeto di definizione molto usato. Si noti che qualsiasi alfabeto può essere codificato in termini di alfabeto binario. Per esempio, dato che ci sono 32 stringhe binarie di lunghezza cinque, ad ogni lettera dell'alfabeto può essere associata un'unica stringa binaria di lunghezza cinque.

La lettera M denota l'insieme chiamato spazio dei messaggi. L'insieme M consiste di stringhe (presumibilmente non vuote) composte da concatenazioni di simboli appartenenti all'alfabeto di definizione. Un elemento di M è chiamato testo in chiaro (o messaggio in chiaro o ancora plaintext). Quindi un elemento di M altro non è che un messaggio leggibile da chiunque. Esso può essere un testo, un flusso di bit, una immagine, un flusso video, ecc...Il testo in chiaro, che debba essere trasmesso oppure memorizzato, è in ogni caso l'informazione da codificare.

La lettera C indica l'insieme chiamato spazio dei messaggi cifrati. C consiste di stringhe (presumibilmente non vuote) composte da concatenazioni di simboli appartenenti a un insieme di definizione diverso dall'insieme A per M.
Un elemento di M è chiamato messaggio cifrato o ciphertext.

K indica un insieme chiamato spazio delle chiavi. Un elemento di K è una chiave.

Ogni elemento e Є K determina una ed una sola biiezione da M a C indicata con Ee. Ee è chiamata funzione di codifica o trasformazione di codifica. Si noti che Ee deve essere una funzione biunivoca per essere invertibile e quindi per poter recuperare il testo in chiaro a partire da quello cifrato.

Per ogni d Є K, Dd indica una biiezione da C a M
(Dd : C → M). Dd è chiamata funzione di decodifica o trasformazione di decodifica.

Il processo di applicazione della trasformazione Ee ad un messaggio m Є M viene detto cifratura o codifica di m.

Il processo di applicazione della trasformazione Dd ad un messaggio c Є C viene detto decifratura o decodifica di c.

Uno schema di cifratura è formato da un insieme
{Ee : e Є K} di funzioni di codifica ed un corrispondente insieme {Dd : d Є K} di funzioni di decodifica con la proprietà che per ogni e Є K esiste un'unica chiave d Є K tale che $Dd = Ee^{-1}$. Questo equivale ad affermare che Dd(Ee(m)) = m per ogni m Є M. Spesso uno schema di cifratura è chiamato cifrario.

Le chiavi e ed d di uno schema di cifratura sono dette coppia di chiavi (key pair) ed è usuale indicarle con la scrittura (e,d). Si noti che e e d potrebbero essere uguali.

La costruzione di un cifrario richiede che venga scelto un insieme M, un insieme C, lo spazio delle chiavi K, un insieme di funzioni di codifica {Ee : e Є K} e un corrispondente insieme di funzioni di decodifica
{Dd : d Є K}.

Ottenere confidenzialità
Uno schema di cifratura dovrebbe essere usato nel seguente modo al fine di ottenere confidenzialità: due entità Alice e Bob per prima cosa scelgono segretamente o si scambiano segretamente la coppia di chiavi (e,d). In un momento successivo, se Alice vuole inviare un messaggio m Є M a Bob, calcola c = Ee(m) e lo trasmette a Bob. Ricevendo c, Bob calcolerà Dd(c) = m ottenendo il messaggio m originale.

A questo punto ci si potrebbe interrogare sull'effettiva necessità delle chiavi (perché non scegliere semplicemente una funzione di codifica e la corrispondente funzione di decodifica?). Avere trasformazioni molto simili tra loro ma caratterizzate da una chiave, significa che se una particolare trasformazione di codifica/decodifica viene rivelata, non è necessario riprogettare da capo lo schema; basta semplicemente cambiare la chiave. E' infatti pratica comune nella Crittografia il cambiamento frequente della chiave (funzioni di codifica/decodifica).

Facendo un confronto con qualcosa di fisico, potremmo pensare ad un comune lucchetto a combinazione numerica. La sua struttura è disponibile a chiunque ne acquisti uno e ne studi il funzionamento. Tuttavia, la combinazione numerica è scelta dal proprietario. Se il proprietario sospetta che qualcuno sia venuto a conoscere la combinazione, potrà facilmente cambiare combinazione senza comprare un lucchetto nuovo.

Autenticazione, Integrità e Non ripudio
Oltre a garantire la confidenzialità, la Crittografia ha spesso il compito di fornire:

- Autenticazione. Dovrebbe essere possibile per il ricevente accertare l'origine del messaggio; un intruso non dovrebbe essere in grado di spacciarsi per qualcun altro.
- Integrità. Dovrebbe essere possibile per il ricevente verificare se durante la trasmissione il messaggio sia stato modificato o meno; un intruso non dovrebbe essere in grado di sostituire un messaggio legittimo con uno falso.
- Non ripudio. Serve per fornire la prova incontestabile di una avvenuta spedizione o di una avvenuta ricezione di messaggi.

Sicurezza
Una fondamentale premessa nella Crittografia è che gli insiemi M, C, K, {Ee : e Є K}, {Dd : d Є K} siano di pubblico dominio e non segreti. Quando due entità vogliono comunicare tra loro in sicurezza usando un cifrario, l'unica cosa che deve rimanere segreta è la coppia di chiavi (e,d) che stanno usando e che devono aver precedentemente selezionato. Si potrebbe ottenere sicurezza aggiuntiva mantenendo segrete le classi di funzioni codifica/decodifica, ma la sicurezza dell'intero schema non dovrebbe essere bastata su questo fattore. La storia, infatti ha mostrato che realizzare la segretezza delle funzioni di codifica/decodifica è molto difficile e poco pratico.

Protocolli Crittografici
Introduzione
L'obiettivo della Crittografia, in definitiva, è quello di risolvere problemi, anzi una particolare categoria di problemi: quelli in cui sono coinvolti segretezza, autenticazione, integrità e gente disonesta. Si potrebbero imparare tutte le tecniche e gli algoritmi crittografici, ma essi rimangono una questione accademica finché non risolvono un problema. Ecco perché introduco alcuni concetti sui protocolli.

Generalità
Un protocollo è una serie di passi, che coinvolgono due o più parti (partecipanti), progettato per portare a termine un lavoro. Questa definizione è importante. Una "serie di passi" significa che il protocollo ha una sequenza che va dall'inizio alla fine. Ogni passo (operazione) deve essere eseguito in successione e nessun passo può essere eseguito prima che quello precedente non sia stato completato.
"Che coinvolgono due o più parti" sta a significare che almeno due entità sono richieste perché un protocollo si possa dire tale; una entità da sola non costituisce un protocollo. Una persona può eseguire una serie di operazioni per portare a termine un lavoro (es. preparare una torta), ma questo non rappresenta un protocollo (qualcun altro deve mangiare la torta per rendere plausibile il protocollo).
Infine, "progettato per portare a termine un lavoro" ci lascia intendere che il protocollo deve necessariamente realizzare qualcosa. Un oggetto che assomigli ad un protocollo ma che non compia alcun compito sarebbe uno spreco di tempo.

Altre caratteristiche
I protocolli posseggono altre caratteristiche che qui elenco:
- ogni entità coinvolta nel protocollo deve sapere in anticipo come esso agisce e tutti i passi da seguire;
- ogni entità coinvolta nel protocollo deve accettarne le regole;
- il protocollo deve essere non ambiguo; ogni passo deve essere ben definito e non deve esistere la possibilità di fraintendimenti;
- Il protocollo deve essere completo; deve esistere una operazione specifica per ogni possibile situazione.

Protocollo crittografico
Un protocollo crittografico è un protocollo che fa uso di crittografia. In esso è quindi coinvolto qualche tipo di algoritmo di crittografia; tuttavia, l'obiettivo di un protocollo crittografico va oltre la semplice segretezza. Le parti coinvolte in un protocollo potrebbero voler condividere parte dei loro segreti per calcolare un valore, generare congiuntamente una sequenza casuale, convincersi a vicenda della loro identità, o firmare simultaneamente un contratto. In definitiva, la crittografia all'interno dei protocolli è utilizzata per prevenire o segnalare intrusioni.

Obiettivo dei Protocolli
Nella vita di tutti i giorni esistono protocolli informali per quasi tutto: ordinare merce via telefono, giocare a poker, votare per le elezioni. Nessuno in realtà pensa molto a come funzionano questi protocolli; essi si sono evoluti nel tempo, ognuno sa come usarli e il servizio offerto funziona abbastanza bene.

Negli ultimi tempi, le interazioni umane avvengono sempre più attraverso reti di computer piuttosto che faccia a faccia. I computer necessitano di protocolli formali per fare le stesse cose che normalmente le persone fanno senza pensare. Una persona che va a votare in un altro stato diverso da quello di origine dove ha sempre votato, molto probabilmente si troverà in una cabina per il voto abbastanza differente da quella che conosce; tuttavia potrà facilmente adattarsi alla nuova situazione. I computer non sono affatto così flessibili.

Molti protocolli faccia a faccia si affidano alla presenza fisica delle persone per garantire giustizia e sicurezza. Nel mondo delle reti di computer questo fattore viene meno e diventa necessario fare alcune considerazioni:
è ingenuo pensare che la gente connessa alla rete sia onesta; è anche ingenuo pensare che coloro i quali

gestiscono le reti di computer siano persone oneste; è perfino ingenuo credere che i progettisti delle reti di computer siano onesti. Forse molti di loro lo saranno, ma i pochi disonesti che ci sono possono creare grossissimi danni. A questo proposito i protocolli tornano utili: la formalizzazione dei protocolli permette di esaminare il modo in cui la gente disonesta li sovverte. A questo punto si possono sviluppare nuovi protocolli immuni a quella sovversione.

TECNICHE

Contenuti

---> **Crittografia a chiave simmetrica**

---> Introduzione
---> Un primo sguardo ai cifrari a blocchi
---> Cifrari a sostituzione semplice
---> Cifrari a sostituzione polialfabetica
---> Cifrari a trasposizione
---> Composizione di cifrari
---> Un primo sguardo ai cifrari a flusso
---> Lo spazio delle chiavi

-> **Firme digitali**

-> **Autenticazione ed identificazione**

---> Identificazione
---> Autenticazione origine dati

-> **Crittografia a chiave pubblica**

---> Metodo di codifica
---> La necessità di autenticazione
---> Firme digitali dalla codifica reversibile

-> **Chiave simmetrica vs. Chiave pubblica**

---> Vantaggi della Crittografia a chiave simmetrica
---> Svantaggi della Crittografia a chiave simmetrica
---> Vantaggi della Crittografia a chiave pubblica
---> Svantaggi della Crittografia a chiave pubblica
---> Tiriamo le somme

-> **Funzioni Hash**

-> Numeri e sequenze pseudocasuali