ISTITUTO TECNICO COMMERCIALE STATALE
“ *Cav. Ing. ADRIANO OLIVETTI* ”
LECCE

La crittografia dall'antichità all'era digitale

Candidato:
Davide Quarta
Classe V A/Mercurio

"il n’exige pas le secret, et qu’il puisse sans inconvénient tomber entre les mains de l’ennemi"

Auguste Kerckhoffs LA CRYPTOGRAPHIE MILITAIRE JOURNAL DES SCIENCES MILITAIRES Janvier 1883.

ESAME DI STATO - A.S. 2006-2007

Indice generale

INTRODUZIONE

L'uomo sin dai tempi antichi ha cercato di proteggere i propri segreti; informazioni che possono spaziare dalla corrispondenza privata ai messaggi di importanza strategica. Per mantenere sicure queste informazioni viene usata, ormai in maniera sempre più diffusa, la crittografia.

L'origine etimologica della parola crittografia è greca, da *kryptós,* nascosto e *gráfein*, scrivere (scrittura nascosta).

L'esempio maggiormente citato è quello di Alice e Bob, queste due persone vogliono scambiarsi delle informazioni, di cui devono rimanere a conoscenza solo loro due. Notando che non esistono dei canali di comunicazione perfettamente sicuri attraverso cui scambiarsi le informazioni, decidono di utilizzare la crittografia per rendere il messaggio leggibile solo a loro due.

Una definizione completa di crittografia è difficile da formulare, poiché essa ha subito una profonda evoluzione nel corso del tempo.
In passato era un'insieme di metodi e tecniche utili per nascondere il messaggio, basandosi per lo più su metodi di sostituzione e trasposizione. La crittologia era quindi più un'arte che una scienza. Il passaggio alla crittografia moderna si è avuto con l'introduzione di metodi matematici, determinando un passaggio da arte a scienza. Di fatto, attualmente, la crittografia è lo studio dedito a trovare nuovi metodi basati sulla elevata difficoltà di risoluzione di alcuni problemi matematici (come la fattorizzazione di grandi numeri in fattori primi e la risoluzione di logaritmi discreti).
Al contrario, la crittanalisi cerca di compromettere i metodi crittografici, spesso con lo scopo di ottenere accesso alle informazioni protette. Anche questa ha subito una notevole evoluzione. La crittanalisi classica comprendeva una combinazione di statistica e altri strumenti matematici, ma soprattutto ingegno, fortuna e determinazione, mentre quella moderna consiste soprattutto nella ricerca di soluzioni ai problemi matematici utilizzati dalla crittografia. La crittologia è quanto risulta dalla unione di queste due discipline (da *kryptós e logos* cioè "*mondo nascosto*").

La "encryption" (parola che potrebbe essere italianizzata con il termine crittazione o cifratura) è il processo attraverso cui i dati vengono trasformati in maniera che non possano essere leggibili senza la chiave appropriata. La "decriptazione" (decrittazione) è il processo inverso, attraverso la giusta chiave i dati vengono ritrasformati nella forma originale.

Uno dei campi di applicazione più importanti è l'*autenticazione*. Così come uno viene identificato dalla propria firma la creazione di una firma digitale (digital signature) lega univocamente il possessore al documento emesso con la firma (recentemente riconosciuta con effetto giuridico anche in Italia). Questo meccanismo è largamente usato in moltissimi prodotti che sono già largamente usati per esempio le televisioni

pay per view, o in alcune forme di commercio elettronico.

Un altro metodo di nascondere informazioni è la steganografia che senza modificare sostanzialmente il messaggio lo nasconde all'interno di un altro. Per esempio nascondendo una lettera ad intervalli regolari in un testo di senso compiuto, il testo in chiaro è leggibile da chiunque ma solo chi sa dove cercare può ottenere il messaggio originale.

PRINCÌPI ED OBIETTIVI DELLA CRITTOGRAFIA

I più importanti princìpi su cui si basano i crittosistemi moderni sono quelli indicati da *Auguste Kerckhoffs* nel suo "*Cryptographie Militaire*" pubblicato nel 1883 su il "*Journal des sciences militaires*" e sono:

1. Il sistema deve essere materialmente se non teoricamente indecifrabile;
2. Non necessita della segretezza della implementazione, che può anche cadere in mani nemiche senza conseguenze. L'unica parte che deve essere per forza mantenuta segreta è quindi la chiave;
3. La chiave deve essere semplice da ricordare senza ricorrere a delle note scritte, ed è necessario che possa essere modificata o cambiata con semplicità da parte dei corrispondenti;
4. Il crittogramma deve essere trasmissibile attraverso il telegrafo;
5. L'apparato di cifratura deve essere portabile e non necessita del lavoro di più persone per essere utilizzato;
6. Il sistema deve essere semplice da utilizzare e da comprendere, e non deve richiedere la conoscenza di una lunga lista di regole da rispettare.

La crittografia ha anche degli obiettivi ben precisi e cerca di raggiungerli tutti quanti allo stesso modo sia teoricamente che praticamente:

1. La segretezza: per mantenere le informazioni accessibili soltanto a chi è autorizzato.
2. L'integrità dei dati: serve a garantire che i dati non vengano modificati, e che in caso lo fossero, si possa immediatamente capire che lo sono stati.
3. Autenticazione: serve ad identificare entità ed informazioni.
4. Non-ripudio: serve ad evitare che una entità possa negare di aver effettuato una azione.

Per garantire questi obiettivi non basta però da sola l'applicazione di algoritmi matematici e protocolli, c'è anche bisogno di un aiuto da parte della legge.

LA MATEMATICA E LA CRITTOGRAFIA

Le tecniche crittografiche moderne fanno largo uso di concetti, teorie, e teoremi matematici. Di particolare interesse sono il calcolo delle probabilità e statistica, la teoria dei gruppi, le aritmetiche finite, e la teoria dei numeri.

LE FUNZIONI

Un concetto fondamentale nella crittografia moderna è quello di funzione, strettamente legato al concetto di insieme.

Un insieme è un raggruppamento di oggetti distinti che vengono detti elementi dell'insieme; un dato insieme *X* contenente gli elementi a,b,c viene indicato con la notazione $X=\{a,b,c\}$.

Considerato un insieme di elementi x di X e un insieme di elementi y di Y, si dice che y è **funzione** di x quando è assegnata una legge *f*, di natura qualunque, che ad ogni elemento di *X* associa uno ed un solo elemento di *Y e* si rappresenta con la scrittura $f: X \to Y$.

L'insieme *X* è detto **dominio** della funzione o **insieme di definizione**, l'insieme dei valori di *Y* che hanno il corrispondente nel dominio si definisce **codominio.** Generalmente il codominio è un sottoinsieme di *Y;* nel caso in cui tutti gli elementi di *Y* sono corrispondenti di elementi dell'insieme *X,* il codominio coincide con *Y.*

Se $x \in X$, l'elemento $y \in Y$ corrispondente di x tramite la legge *f* è detto **immagine** di x e si indica con $y=f(x)$.
Se $y \in Y$ la **controimmagine** è un elemento $x \in X$ per il quale $f(x)=y$.

Possiamo aggiungere che una funzione è:

1. **suriettiva** se $f(X)=Y$, cioè se l'insieme delle immagini coincide con Y
2. **iniettiva** se ad elementi distinti di X corrispondono immagini distinte qualunque siano gli elementi scelti cioè $\forall x_1, x_2 \in X: \; x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$
3. **biiettiva** se è sia suriettiva che iniettiva. Pertanto una funzione $f: X \to Y$ è biiettiva se sussistono contemporaneamente le proprietà di iniettività e di suriettività, cioè: a elementi distinti di X corrispondono immagini distinte in Y, inoltre l'insieme immagine coincide con il codominio, $f(X)=Y$. Le corrispondenze biunivoche sono quindi le sole funzioni invertibili, in quanto è possibile stabilire una corrispondenza che ad ogni elemento di Y associa la sua controimmagine, tale funzione è detta funzione inversa di f e si indica con f^{-1} .
$$f^{-1}: Y \to X$$
$$y \to x / f(x)=y$$

In crittografia le biiezioni sono usate per criptare e le trasformazioni inverse sono usate per decrittare.

Ci sono dei particolari tipi di funzione dette one-way, che giocano un ruolo molto importante nella crittografia.
È il caso di una funzione *f* da un primo insieme *X* a un secondo insieme *Y* quando *f(x)* è *semplice* da calcolare per ogni $x \in X$ ma per la maggior parte degli elementi $y \in \mathrm{Im}(f)$ deve essere computazionalmente impossibile trovare una $x \in X$ in maniera che $f(x) = y$.

Esistono anche delle funzioni definite "trapdoor one-way", si tratta di funzioni one-way $f : X \to Y$ con una particolare proprietà: utilizzando alcune informazioni in più (trapdoor informations) diventa computazionalmente possibile trovare per una qualsiasi $y \in \mathrm{Im}(f)$ una $x \in X$ in modo che $f(x) = y$ (più semplicemente $x = f^{-1}(y)$).

Le funzioni one-way e trapdoor one-way rappresentano la base della crittografia asimmetrica.

Per esempio prendendo due numeri primi *p* e *q* ed il loro prodotto *n* quindi *n = p*q*, con $X = \{1,2,3,.....,n-1\}$ definiamo una funzione su X con $f(x) = r_x$ per ogni $x \in X$ dove r_x è il resto della divisione tra x^3 ed *n*. Computazionalmente, l calcolo di *f(x),* è relativamente semplice. Calcolare $x = f^{-1}(y)$, al contrario, è molto complesso. Questo corrisponde con la descrizione di algoritmo one-way, tuttavia, se sono conosciuti *p* e *q* esiste un algoritmo che permette di calcolare in maniera efficiente $x = f^{-1}(y)$.

LE PERMUTAZIONI

Le permutazioni sono usate spesso nella crittografia. Una permutazione *p* su *S* è una biiezione da *S* a se stesso ($p : S \to S$).

Dato $S = \{1,2,3,4,5\}$ una permutazione x $p : S \to S$ può essere scritta in due modi:
$p(1) = 5, p(2) = 1, p(3) = 4, p(4) = 2, p(5) = 3.$ oppure $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix}$
Visto che le funzioni biiettive possono essere invertite, è semplice trovare l'inversa di una permutazione $p^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix}$.

LE TRASFORMAZIONI INVOLUTORIE

Le trasformazioni involutorie sono delle funzioni che hanno la particolare proprietà di essere le proprie inverse. Dato un insieme finito *S* ed *f* una funzione di biiezione da da S a se stesso $f : S \to S$, la funzione *f* è chiamata *involuzione* se $f = f^{-1}$.

GRUPPI, TEORIA DEI NUMERI E ARITMETICHE FINITE

Un gruppo è una struttura algebrica astratta e può essere definito come una coppia *(G,*)*, dove *G* è un'insieme non vuoto e * è una operazione binaria su *G*.

$$* : GxG \to G$$
$$(a , b) \to a * b$$

per essere un gruppo, deve rispettare i seguenti assiomi:

1. * è *associativa*: $\forall a , b , c \in G \quad a * (b * c) = (a * b) * c$
2. esiste *e* in *G* tale che $e * a = a * e = a$; *e* è detto *elemento neutro* di G
3. per ogni *a* appartenente a *G* esiste *a'* in *G* tale che $a * a' = a' * a = e$, *a'* è detto *inverso di a in G*.

Se la operazione * è anche commutativa, cioè $a * b = b * a , \forall a , b \in G$, (G,*) è detto *gruppo abeliano* o *commutativo*.

La cardinalità dell'insieme G viene indicata con $|G|$ ed è chiamata *ordine* del gruppo, e rappresenta il numero di elementi dell'insieme base. Se è finita *G* è un gruppo *finito*, altrimenti è *infinito*.

L'ordine di un elemento di un gruppo viene definito in questo modo: dato un gruppo *G* ed un suo elemento *e*, si scrive *ord(e)*, il minimo numero intero *i* per il quale $e^i = I$ (dove *I* è l'elemento neutro di *G*).

È importante anche la nozione di sottogruppo. Sia *G* un gruppo, ed *H* un suo sottoinsieme, *H* è sottogruppo di *G* se sono verificate le seguenti condizioni:

1. $1 \in H$
2. $\forall h1 , h2 \in H , h1h2 \in H$
3. $\forall h \in H , h^{-1} \in H$

Per il teorema di Lagrange sia H un sottogruppo di G di ordine finito N, N è un multiplo dell'ordine n di H.

L'aritmetica ordinaria tratta di insiemi infiniti di numeri, nella realtà però sono spesso

presenti situazioni in cui gli insiemi di numeri sono finiti. L'orologio per esempio ha 24 ore, l'alfabeto è formato da 26 lettere etc...
Una aritmetica finita modulo *m* si basa su un insieme *{1,2,3,..,m-1};* che possono essere anche visti come il possibile resto di una divisione per m.
La somma e il prodotto vengono eseguite normalmente, il resto della divisione per m viene poi considerato come risultato.
Per la somma valgono le normali proprietà algebriche, per il prodotto il metodo è sempre lo stesso, ma può cadere la regola di annullamento del prodotto secondo cui un prodotto è nullo solo se lo è almeno uno dei due fattori:
modulo 16 : 8*4 = 32 , 32 mod 16 = 0;
questo può essere evitato se *m* è un numero primo in questo caso si ha un campo di Galois. Questo gruppo moltiplicativo ha come ordine la *funzione di Eulero* di N, *ΦN*.

L'*inverso* di un numero *x* in una aritmetica finita modulo *N* è il numero *y* per il quale *xy = 1 mod N*.
Un metodo di calcolo è fornito quando *x* ed *N* sono primi tra loro, dal teorema di Eulero-Fermat secondo cui: $x^{\Phi(N)} = 1 \ mod \ N$. È quindi semplice ottenere l'inverso: $y = x^{\Phi(n)-1} \ mod \ N$.

Questo metodo di calcolo è molto importante perché legato a un algoritmo efficiente per il calcolo della potenza in un'aritmetica finita. Il calcolo della *funzione di Eulero*, inoltre, per numeri elevati ha la stessa complessità della fattorizzazione. Se *N* è molto grande conviene quindi usare altri approcci, per esempio l'*algoritmo esteso di Euclide* per il calcolo del *MCD*. Le applicazioni sono evidenti, infatti questi metodi sono alla base del *cifrario RSA*.

Il calcolo della potenza può avvenire normalmente come avviene in una aritmetica finita, per poi ridurla a modulo n, $a^b \ mod \ n$. Se *b* è un numero grande il risultato sarà enorme. Per risolvere questo problema, si può moltiplicare *a* per *b* volte e ridurre il risultato a modulo n ogni volta. Per velocizzare il calcolo, si può elevare ripetutamente al quadrato senza superare l'esponente b, moltiplicando ogni volta a e riducendo modulo n.

Come nell'aritmetica ordinaria è possibile definire un'operazione inversa rispetto alla potenza cioè il logaritmo. Per definizione il logaritmo è l'esponente b che si deve dare alla base a per ottenere il valore x, il passaggio alla aritmetica modulare avviene attraverso la riduzione modulo N traducendosi in $b \log_a x \ mod \ N$. Tale logaritmo viene chiamato *logaritmo discreto*. Computazionalmente, il calcolo di quest'ultimo risulta molto complesso, e può avere molte soluzioni o nessuna.

Si ritiene che la complessità computazionale del logaritmo discreto sia dello stesso ordine di una fattorizzazione, nonostante manchi una dimostrazione. Per questo il logaritmo discreto è una possibile alternativa alla fattorizzazione e su di esso si basano alcuni algoritmi asimmetrici come ElGamal o alcuni cifrari relativi alle

Elliptic Curves (*curve ellittiche*).

LA FUNZIONE DI EULERO

La funzione di Eulero associa a un numero intero *n* il numero dei numeri interi primi con *n* e minori di *n* (compreso l'uno). La funzione di Eulero di un numero *n* si indica di solito con ***Φ(n).***

$\Phi(n) = n(1 - 1/n_1)(1 - 1/n_2)...(1 - 1/n_m)$

dove n_1, n_2 ... n_m sono i fattori primi distinti di *n*. Se *n* è primo allora ovviamente $\Phi(n) = n - 1$. Se *n* è il prodotto di due numeri primi p e q, è facile verificare che $\Phi(n) = (p - 1)(q - 1)$. Infatti $\Phi(n) = pq(1 - 1/p)(1 - 1/q)$ e svolgendo i prodotti $p(1 - 1/p)$ e $q(1 - 1/q)$ si ottiene la formula precedente.

IL TEOREMA DI FERMAT-EULERO

Dati due qualsiasi numeri m ed N primi tra di loro allora è:
$m^{\Phi(N)} = 1 \pmod N$ o $m^{\Phi(N)} - 1 = 0 \pmod N$

Se poi N è primo allora Φ(N) = N - 1, e si ritrova il piccolo teorema di Fermat che afferma che in un'aritmetica finita di ordine n con n primo $x^{(N-1)} = 1 \bmod N \; \forall \, x > 0, x < N$.
Questo può considerarsi una diretta conseguenza del teorema di Lagrange, infatti se m è primo con N appartiene al gruppo moltiplicativo Z_N che ha ordine $\Phi(N)$. Per il corollario del teorema di Lagrange l'ordine di m è quindi un divisore di $\Phi(N)$ e di conseguenza $m^{\mathrm{ord}(m)} = 1 \bmod N$ e a maggior ragione $m^{\Phi(N)} = 1 \bmod N$

Questo teorema può considerarsi una conseguenza del teorema di Lagrange.
Infatti se **m** è primo con **N** allora appartiene al gruppo moltiplicativo Z_N che ha ordine **Φ(N)**. Per il corollario del teorema di Lagrange l'ordine di m è allora un divisore di Φ(N) e quindi $m^{\mathrm{ord}(m)} = 1 \pmod N$ e a maggior ragione $m^{\Phi(N)} = 1 \pmod N$.

TERMINOLOGIA E CONCETTI DI BASE

Qui vengono presentati dei termini e concetti di base che vengono usati spesso nella crittografia, e sono quindi parte della base teorica di cui si deve tenere presente in uno studio della crittografia.

ASPETTO INSIEMISTICO

La *A* indica un insieme finito chiamato *alfabeto di definizione*. Molto spesso viene usato l'*alfabeto binario* $A=\{0,1\}$.
M indica un insieme chiamato *message space* e consiste in stringhe di simboli da un alfabeto di definizione. Un elemento di *M* è chiamato *plaintext* e rappresenta il messaggio in chiaro.
C è il cyphertext space, consiste in stringhe di simboli da un alfabeto di definizione, che potrebbe differire dall'alfabeto di definizione di *M*. Un elemento di *C* è chiamato crittogramma (*cyphertext*) e rappresenta il messaggio criptato.

ASPETTO ANALITICO

K indica un insieme chiamato *keyspace*, un elemento di *K* è chiamato *chiave* (*key*).
Ogni elemento $e\in K$ determina la biiezione da M a C, indicata da E_e .
E_e è chiamata *funzione* o *trasformazione* di *crittazione*. E_e deve essere una biiezione in modo che il processo possa essere invertito e si possa tornare a un plaintext unico per ogni cyphertext.
Per ogni $d\in K$, D_d indica un bigezione da C a M ($D_d: C\rightarrow M$). D_d è chiamata funzione o trasformazione di decrittazione.
L'applicazione della trasformazione E_e a un messaggio $m\in M$ viene definita *crittazione di m* (*encryption m* o *encryption of m*). L'applicazione della trasformazione D_d a un crittogramma viene definita decrittazione (*decryption c* o *decryption of c*).
Uno schema di crittazione consiste in un insieme $\{E_e: e\in K\}$ e il corrispondente $\{D_d: d\in K\}$ con la proprietà che per ogni $e\in K$ c'è una chiave unica $d\in K$ in maniera che $D_d=E_e^{-1}$ cioè $D_d(E_e(m))=m$ per ogni $m\in M$. Lo schema di crittazione viene indicato come *cifratura* (*cypher*).
Le chiavi *e* e *d* vengono chiamate *keypair* ed alcune volte indicate con *(e,d)* (*e* e *d* possono essere uguali).
Per costruire uno schema di cifratura bisogna scegliere *M*, *C* e *K*, ed un insieme di trasformazioni di cifratura $\{E_e: e\in K\}$ ed il corrispondente insieme di trasformazioni di decifrazione $\{D_d: d\in K\}$.

ASPETTO PRATICO

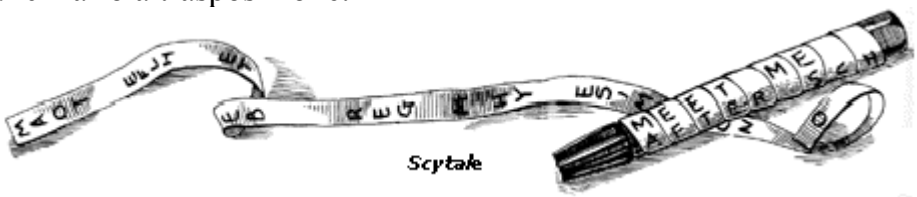
Una *entità* è qualcuno che invia, riceve o modifica le informazioni. Un *avversario* è una entità diversa da chi invia o riceve le informazioni, che tenta di compromettere la sicurezza del sistema, spesso giocando il ruolo di una delle entità legittime.
Un *canale* è il mezzo attraverso cui le informazioni vengono scambiate tra le entità. Un *canale sicuro* (*physically secure channel* o *secure channel*) è uno che non è fisicamente accessibile agli avversari. Un "*unsecured channel*" è un canale attraverso cui altre entità diverse da quelle legittime possono leggere o modificare le informazioni. Un "*secured channel*" è un canale attraverso cui gli avversari non possono leggere o modificare le informazioni.

Così come affermato da Kerckhoffs gli insiemi *M*,*C*,*K*, $\{E_e : e \in K\}$, $\{D_d : d \in K\}$, devono essere di pubblico dominio, l'unica parte che deve rimanere segreta è il keypair (e,d), mantenere segrete le caratteristiche del cypher può fornire una maggiore sicurezza, ma è sbagliato basare la sicurezza dell'intero sistema solo su questo, poiché mantenere segreta l'implementazione di un cypher, così come si è visto più volte nella storia, è molto difficile.

LA CRITTOGRAFIA CLASSICA

Il primo documento che sancisce la nascita della crittografia come intenzione di modificare un messaggio risale al 1900 a.C. sulle rive del Nilo, nella città di Menet Khufu. Nella camera principale della tomba di Khnumhotep II, lo scriba di questo nobile, sostituì alcuni dei geroglifici con altri meno utilizzati per lo più alla fine del documento dove venivano citati alcuni dei monumenti eretti per il faraone Amenemhet II. Molto probabilmente si trattò soltanto di un modo per dare una apparenza formale al documento. Rimane però il principio su cui si basa la crittografia, una sostituzione volontaria della scrittura.
Successivamente queste modifiche si fecero più frequenti, e le troviamo in formule funerarie, in un inno a Thoth, in un capitolo del libro dei morti ed altri a seguire, per conferire mistero, senso dell'arcano o un "potere magico" alle parole.
In Cina nonostante la situazione linguistica e culturale avanzata non ci fu nessuna forma di crittografia. In India, invece, la crittografia era già sviluppata e praticata in diverse forme: *l'Artha-Sastra* cioè i servizi di spionaggio, il *Latila-Vistara* che esalta Budda, vi erano scritture perpendicolari e disordinate, e nel *Kama-Sutra* tra le 64 arti (yoga) che la donna deve conoscere, la numero quarantacinque *mlecchita-vikalpa* è proprio la scrittura segreta.
In un periodo successivo, in Mesopotamia, Assiri e Babilonesi sostituiscono parti finali delle parole con forme stereotipate (*colofoni*), in particolare nella regione di Uruk (Iraq) nell'ultimo periodo della scrittura cuneiforme, alcuni scribi convertirono occasionalmente i loro nomi in numeri.
Continuiamo a trovare ancora molte altre testimonianze. Gli Yezidis, una popolazione di circa 25.000 abitanti che uso la crittografia per proteggere i testi sacri dai musulmani. I Tibetani, in questo caso la scrittura segreta era usata per la corrispondenza ufficiale. Gli Nsibidi, con una scrittura di tipo pittorico per esprimere concetti d'amore. In Thailandia, erano in uso diverse tecniche di cifratura, la sostituzione e la divisione delle lettere dell'alfabeto in gruppi. Alle Maldive due forme diverse di scrittura segreta. In Persia l'uso delle scritture segrete per documenti politici e fiscali (600 a.C.). Anche nella Bibbia troviamo tre diversi schemi: *Atbash* (***A**leph **t**aw **b**eth **sh**in*), l'alfabeto è rovesciato, "Babilonia" diventa "*SHESHACH*",

Albam l'alfabeto viene diviso a metà e *Atbah* in cui si stabilisce una relazione numerica.
Erodoto ci da la prima testimonianza dell'importanza della crittografia nella guerra. Due episodi sono di particolare interesse: nel primo è narrato di Isteo, un nobile persiano, che per far giungere informazioni segrete al tiranno di Mileto Aristagora, fece rasare un fidato corriere, per tatuargli il messaggio sulla testa, e mandarlo a destinazione a capelli ricresciuti, nel secondo invece si narra di Demerato che in esilio, avvisa gli spartani del progetto di invasione di Serse, re dei persiani, utilizzando delle tavolette di cera a strati sovrapposti, il primo con il messaggio inciso, e il secondo che copriva il messaggio facendo sembrare la tavoletta vuota.
Plutarco in "*Vite Parallele*" descrive la Scytale (scitala) spartana del 500 a.C. ed un metodo molto astuto con cui il re spartano Agide comunicava con i suoi generali: arrotolava una striscia di cuoio o di pergamena attorno a un cilindro di legno di uno specifico diametro, procedeva poi a scrivere longitudinalmente, l'unico modo per leggere il messaggio era di avere un bastoncino dello stesso diametro. È un ottimo esempio di cifrario a trasposizione.



Lo storico greco *Polibio* (~200-118AC), nel Libro X illustra il primo codice poligrafico, attribuendolo a Cleoxeno e Democleito. Si basa sull'utilizzo di una coppia di numeri compresa tra 1 e 5, utilizzando una matrice 5x5, in questo modo il messaggio poteva essere trasmesso tramite l'utilizzo di torce, riuscendo a inviare però una quantità maggiore di informazioni rispetto a quella che normalmente era possibile trasmettere tramite "telegrafi a torce".

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

IL CIFRARIO DI CESARE

Lo storico romano Svetonio, ci lascia testimonianza del "*cifrario di Cesare*" in "*De Bello Gallico*" e in "*De Vite Caesarum*".
Il funzionamento è molto semplice, ciascuna lettera viene sostituita da quella che la segue di *n* posizioni. *N* è quindi la chiave segreta di cifratura. Cesare solitamente

utilizzava il numero tre come chiave. Questo cifrario è detto *monoalfabetico*, perché sostituisce i caratteri singolarmente.

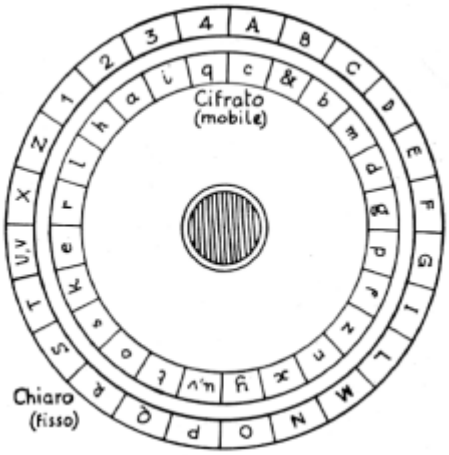
Il cifrario di Cesare può essere descritto matematicamente ricorrendo alla aritmetica modulare, e alle permutazioni, entrambe concetti già visti in precedenza.
Se consideriamo ogni lettera dell'alfabeto un numero, la operazione risultante sarà semplicemente una permutazione su un gruppo finito in cui ogni valore x viene addizionato e ridotto modulo 26 (quante sono le lettere dell'alfabeto e quindi la dimensione del gruppo), in questo modo si viene a creare una struttura circolare.

L'algoritmo può essere scritto in un qualsiasi linguaggio di programmazione in maniera molto semplice, per esempio in C.

```
//cifra il messaggio
void Cifra(char* messaggio, unsigned int spostamento )
{
	for(int i=0;i<strlen(messaggio);i++) //cifra tutti i caratteri del messaggio
		for(int cerca=0;cerca<26;cerca++) //cotrolla tutti i caratteri dell'alfabeto
			if(messaggio[i]==alfabeto[cerca]) //se il carattere è presente
							//nell'alfabeto lo cifra
			{
				int posizione = (cerca+spostamento)%26;
				messaggio[i]=alfabeto[posizione]; //cifra il carattere
				break; //se un carattere è stato cifrato non continuare
			}
}
//decifra il messaggio
void Decifra(char* messaggio, unsigned int spostamento)
{
	for(int i=0;i<strlen(messaggio);i++) //decifra tutti i caratteri del messaggio
		for(int cerca=0;cerca<26;cerca++) //cotrolla tutti i caratteri dell'alfabeto
			if(messaggio[i]==alfabeto[cerca]) //se il carattere è presente
							//nell'alfabeto lo decifra
			{
				int posizione = (cerca-spostamento);
				if(posizione < 0) posizione = 26+posizione; //se l'indice è
								//negativo parti dalla fine del buffer
				messaggio[i]=alfabeto[posizione]; //decifra il carattere
				break; //se un carattere è stato decifrato non continuare
			}
}
```

Il cifrario di cesare così come tutti i cifrari a sostituzione monoalfabetica è molto debole, ad ogni lettera, corrisponde infatti una lettera dell'alfabeto, ciò significa che ogni lettera crittata mantiene la stessa frequenza con cui è presente nel linguaggio originale. Ogni linguaggio ha una caratteristica distribuzione delle frequenze, e una ancora più particolare frequenza di bigrammi e trigrammi.
Per forzare un testo cifrato in questo modo si effettua una statistica della frequenza delle lettere del crittogramma, si fa un confronto con le frequenze di un particolare linguaggio e in seguito si fanno delle supposizioni, dopo alcune prove ed assunzioni è semplice ricostruire il messaggio.

I CIFRARI POLIALFABETICI



Dobbiamo un importante scritto in materia crittografica: il “De Componendis Cyfris ” (1466) a Leon Battista Alberti (Genova, 1404 – Roma, 1472), in questo scritto viene teorizzato il primo disco cifrante, ideato per l’utilizzo in Vaticano. Il dispositivo era formato da due ghiere concentriche, una esterna fissa, ed una interna mobile. Nella prima ghiera erano presenti tutte le lettere dell'alfabeto in ordine (tranne H, J, K, Q, W e Y, perchè essendo lettere a bassa frequenza avrebbero indebolito in maniera significativa il cifrario) ed i numeri 1 2 3 4; nella seconda ghiera vi erano le lettere minuscole in ordine casuale. La cifratura avveniva scegliendo una lettera, l'*indice di cifratura*, sulla ghiera esterna, facendole corrispondere la prima lettera dell'alfabeto della ghiera interna. L'Alberti ha proposto un metodo nuovo sostanzialmente differente dalla semplice sostituzione monoalfabetica, poichè era possibile cambiare durante il messaggio l'indice di cifratura, in modo da falsare l'analisi delle frequenze. Solo successivamente, l'idea avuta dall'Alberti, verrata utilizzata da Blaise de Vigenere (1523-1596) per inventare la "*cifratura di Vigenere*", in cui si usano tutti gli alfabeti cifranti possibili (26), variando l'alfabeto ad ogni lettera.

Successivamente nella storia troviamo i cifrari polialfabetici, un particolare metodo di cifratura di questo tipo è la cifratura playfair. Questa nasce nella lontana inghilterra del 1845 dalla mente di uno scenziato di nome Charles Wheatstone, allora, il Barone Playfair convinse il governo Inglese ad usarlo per scopi ufficiali e così il suo nome venne dato a questa cifratura. Questa cifratura si basa sulla codifica di blocchi attraverso la sostituzione di digrammi. Grazie a software adatti può essere forzato abbastanza in fretta, c'è però chi riesce anche a farlo solamente con carta e penna.
Per cifrare un testo dobbiamo prima sistemarlo in maniera apposita, cioè in blocchi di due lettere, e ogni digramma non deve essere composto dalla stessa lettera altrimenti verrà sostituita da X o Z, cambiando ovviamente in caso si ripeta più di due volte la lettera prima usiamo X poi Z e se non sono pari aggiungiamo una lettera a piacere. Adesso viene la nostra chiave, si prepara utilizzando un parola chiave e arrangiandola in modo che non si ripetano all'interno le lettere, e in seguito si aggiungono le lettere dell'alfabeto rimanenti in ordine alfabetico, la **I** e la **J** vengono considerate uguali quindi abbiamo 25 lettere arrangiate in un quadrato di 5 x 5. La cifratura avviene attraverso delle semplici regole: Se le lettere sono in una riga e in una colonna diversa, viene definita da esse una "sottomatrice":
Per forzare la cifratura dobbiamo lavorare in modo esattamente inverso a quello che abbiamo fatto in precedenza quindi verso sinistra. L'attacco migliore a questo tipo di cifratura è attraverso parole conosciute (plain text attack), cercando una

corrispondenza nel testo e cercando così di ottenere parte della chiave, man mano si cerca di dare un senso al testo fino ad ottenere la chiave originale. Altro attacco, meglio se combinato con questo, e valido soprattutto su testi cifrati abbastanza lunghi, è quello della frequenza dei trigrammi in cui si sfrutta la frequenza media con cui appare un trigramma in un determinato linguaggio.

LA CRITTOGRAFIA NEL PERIODO DELLE GRANDI GUERRE

I metodi di comunicazione utilizzati per scopi bellici a partire dalla I guerra mondiale ,telefono e radio, anche se permettevano uno scambio di informazioni pressoché immediato, erano molto semplici da intercettare. La Francia già dall'ottobre 1914, allo scoppio della guerra, disponevano di un ufficio cifra organizzato ed efficiente. Guidati dal col. Cartier e dal cap. Olivari erano in grado di decrittare i messaggi radio tedeschi. Il migliore crittanalista francese, Georges Painvin riuscì a decrittare la cifra campale germanica nel 1918. Anche gli Austriaci nello stesso anno erano già in grado di decrittare i messaggi russi. I russi erano totalmente impreparati, e non cifravano assolutamente i propri messaggi, durante la battaglia di Tannenberg (agosto 1914) persino gli ordini operativi venivano trasmessi in chiaro; ed i Tedeschi erano in grado di intercettare tutto. Anche dopo che i russi cominciarono a cifrare le comunicazioni radio, i tedeschi riuscirono comunque a decrittare i messaggi; ottennero anche qualche successo nei confronti dei francesi; il principale crittanalista tedesco fu il prof. Deubner. Sir Alfred Ewing, Capo dell'ufficio crittologico della Marina Britannica, organizzò la cosiddetta Room 40 dove si decrittavano i messaggi della marina militare tedesca. Il "telegramma Zimmermann" fu decifrato proprio dalla Room 40, in questo messaggio i Tedeschi offrivano un'alleanza ai Messicani promettendogli gli USA. Questo messaggio fu uno dei fattori che spinsero gli USA a entrare in guerra nel 1917. Negli USA, il reparto crittologico dei laboratori Riverbanks di Chicago, fu scelto come ufficio cifra federale. In questo reparto lavorava anche William Friedmann destinato a divenire il massimo crittologo e crittanalista USA. L'Italia fu colta del tutto impreparata, il cifrario militare tascabile in uso, era una variante del Vigenere, per il quale esisteva da tempo il metodo di decrittazione del Kasiski; inoltre non esisteva un ufficio cifra e i messaggi Austriaci intercettati non potevano essere decifrati. Fu inviato quindi nel luglio 1915 il cap. Sacco in Francia, per ottenere aiuto. Bisognava passare i messaggi ai francesi perché fossero decrittati, e questa collaborazione non fu soddisfacente: i crittanalisti francesi rifiutarono sempre di istruire gli Italiani sui loro metodi. Sacco riuscì ad ottenere di organizzare un ufficio cifra autonomo ("Se i Francesi sono riusciti in questa impresa, non vedo perché non dovremmo riuscirci anche noi"). Furono forzati il cifrario campale austriaco diplomatico, e quello navale e alcuni cifrari tedeschi in uso nei Balcani. La disfatta di Caporetto nel 1917 convinse il comando italiano ad abbandonare i vecchi cifrari, poiché venivano sistematicamente decifrati dagli austriaci, per utilizzare i nuovi metodi, non presi in considerazione fino ad allora perché troppo complicati. Anche se, a differenza di quelli di altri paesi, gli alti comandi italiani evitarono sempre di trasmettere per radio i messaggi più importanti.

Il cifrario di Vigenere, fu molto usato prima della Grande Guerra, ma una grossa debolezza, il cifrario è un insieme di cifrari di Cesare utilizzati a distanza fissa, la crittanalisi, per chiavi di piccole dimensioni, è quindi molto semplice; sono stati inventati degli algoritmi particolarmente efficienti, il metodo dei minimi quadrati e il metodo del Kasiski. Se la chiave avesse la stessa dimensione del testo (o della somma dei testi) da cifrare, sarebbe completamente diverso. Questo fu ideato da G.S.Vernam nel 1926 per il cifrario che porta il suo nome; una chiave casuale e lunga come il testo viene generata, e si procede poi a una cifratura identica a quella del cifrario di Vigenere. In questo caso però vengono combinati i singoli bit che codificano la lettera nei codici usati nelle telecomunicazioni (allora il codice Baudot, oggi il codice ASCII) con l'operazione logica XOR. In questo modo le proprietà statistiche del testo vengono distrutte e Claude Shannon, il padre della Teoria dell'Informazione, dimostrerà nel 1949 che l'unico cifrario realmente è proprio questo. Ovviamente si potrà usare la chiave una sola volta, rendendo il sistema quello che è comunemente chiamato “One Time Pads”. Se la chiave viene utilizzata più volte, genera infatti profondità, tornando ad essere più breve della somma dei messaggi, rendendo nuovamente possibile una crittanalisi. Una chiave lunga come il testo, può essere difficilmente scambiata, infatti va utilizzato un canale sicuro per lo scambio, che non è sempre disponibile. Data la notevole quantità di messaggi da scambiare, lo scambio delle chiavi per ognuno è materialmente impossibile, anche la generazione di una chiave molto lunga da usare man mano non è la soluzione adatta perché in ogni caso la chiave si esaurisce e bisogna scambiarla nuovamente. Una soluzione poteva essere di generare la chiave in maniera pseudo-casuale, e questa idea fece nascere diverse macchine cifranti, tra le quali la macchina Lorenz usata dai tedeschi nella II guerra mondiale. In questo modo però il cifrario non è più assolutamente sicuro perché la vera chiave diventava quindi la regola che generava la chiave. La macchina Lorenz fu forzata infatti dagli inglesi nel 1941.

Nella prima metà del XX secolo si cominciarono a diffondere macchine cifranti a rotori, sul modello del cilindro di Jefferson reinventato da Beziers. Una di queste, la più famosa, è “Enigma”. Fu inventata nel 1918 dal tedesco Arthur Scherbius e adottata dall'esercito e dalla marina tedesca fino alla seconda guerra mondiale. Enigma è una macchina simmetrica, la stessa lettera nella stessa posizione viene cifrata e decifrata con la lettera corrispondente, rendendo possibile cifrare e decifrare il messaggio con la stessa macchina, una comodità operativa che è però anche una debolezza crittografica. La macchina dispone all'interno di alcuni rotori

(3 nella prima versione) liberi di ruotare e collegati elettricamente. Premendo un tasto, un segnale elettrico passa da rotore a rotore fino al rotore finale detto "riflettore" e ritorna indietro illuminando una lettera che rappresenta il carattere cifrato. Non è possibile stampare, quindi bisogna copiare a mano il messaggio carattere per carattere. La chiave era la disposizione dei rotori, che veniva cambiata ogni 24 ore secondo una regola prefissata; la vera chiave segreta era quindi questa regola. Anche i collegamenti interni dei rotori sono segreti. E i rotori possono inoltre essere scambiati tra loro, dando luogo a n! possibili disposizioni (3! = 6), aumentando il numero di combinazioni iniziali possibili. Enigma sembrava inattaccabile, ma già nei primi anni '30 un gruppo di matematici polacchi guidato da Marian Rejewski riuscì a ricostruire la struttura dei rotori e a decrittarne i messaggi. A sua volta il servizio crittografico inglese (di cui faceva parte anche il matematico Alan Turing) riuscì a forzare l'Enigma già dai primi anni di guerra.

Nella II guerra mondiale la crittografia ha svolto un ruolo importantissimo. Questo aspetto della guerra è rimasto per moltissimo tempo, lasciando ancora oggi alcuni interrogativi.

La guerra segreta cominciò in realtà molto prima dello scoppio della guerra. Enigma fu presentata ad alcune mostre commerciali nel 1923, voluta dal governo tedesco per proteggere le proprie comunicazioni, venne immediatamente ritirata dal commercio. La facile portabilità, e la semplicità d'uso la resero lo strumento ideale per portare a compimento il Blitzkrieg. I tedeschi, nel 1928, inviarono per errore un esemplare della Enigma a Varsavia e fecero pressioni sulle autorità polacche per riavere il pacco, queste decisero di esaminarlo prima di rispedirlo due giorni dopo. Questo diede la possibilità di conoscere i meccanismi di funzionamento della macchina. Successivamente, i polacchi riuscirono ad ottenere anche il *codebook*, dove erano indicate le modalità con cui disporre i vari componenti nei vari giorni. Alcune modalità erano definite nel codebook, altre (come la lettera da cui partire per ogni rotore) venivano definite per ogni messaggio (*indicator system*): queste impostazioni dovevano essere casuali, ma per ovvi motivi organizzativi era difficile che lo fossero. Questa ripetizione costante, aiutava i crittoanalisti a decifrare i messaggi. I polacchi intercettarono e lessero i messaggi tedeschi dal 31 dicembre 1932. L'*indicator system* venne modificato nel 1938, ma l'invenzione da parte di Rejewski delle "bombe" permise di continuare il lavoro di decifratura. Queste bombe erano simili a Enigma, ma erano in grado di analizzare e trovare le impostazioni per ogni messaggio (sempre con la supervisione dei crittoanalisti).

Nel Dicembre del 1938 Enigma venne resa molto più sicura grazie all'introduzione di due ulteriori rotori tra i quali scegliere, e i polacchi non furono più in grado di decifrare i messaggi. Il 25 luglio 1939 i servizi polacchi consegnarono, in un incontro a Parigi, a francesci e inglesi i risultati ottenuti, e tutte le informazioni raccolte oltre a quelle sul lavoro di analisi e decifrazione.

Il 3 settembre 1939 la Germania dichiarò guerra all'Inghilterra e proprio in quei giorni il centro per la crittoanalisi inglese (British Government Code & Cypher School, GCCS) venne spostato da Londra a Bletchley Park: il governo inglese fu fermo nella decisione di investire molto; naturalmente non si conosce la cifra stanziata, ma è ormai più che provato che le speranze di Churchill risiedessero in gran parte nell'operato di decodifica dei messaggi tedeschi.
Si voleva anticipare il nemico per rendere inutile la superiorità militare. Circa 10'000 tra matematici, linguisti, geni degli scacchi e anche fanatici di cruciverba vennero arruolati e fatti vivere nei 58 acri di Bletchley Park sotto stretta sicurezza.
L'area era organizzata in maniera efficiente in edifici minori detti *Hut*. Tutti i messaggi intercettati venivano registrati, in modo che avendo più messaggi fosse più semplice ricostruire la chiave ogni volta. Negli ultimi mesi del 1939 pochissimi messaggi furono decifrati perché il lavoro era diventato troppo complesso.
Nel 1940 Alan Turing ultimò la cosiddetta *British Bombe* o *Turing Bombe*, che faceva uso della teoria probabilistica evitando un attacco di forza bruta che avrebbe richiesto tempi nell'ordine di migliaia di anni. Questo fu possibile supponendo che il messaggio iniziasse in un determinato modo, le comunicazioni erano infatti poco varie, soprattutto nei primi caratteri.
Nel 1940 vennero intercettate le comunicazioni di preparazione di un bombardamento su Conventry, ma la cittadina non fu fatta evacuare, agendo come se i messaggi non fossero mai stati decifrati. Il 14 novembre 1940 Coventry venne devastata dai bombardamenti della Luftwaffe, 6000 persone circa morirono e ci fu un numero imprecisato di feriti.
Per recuperare ulteriori informazioni su Enigma si cercò di fare irruzione negli U-boat tedeschi per recuperare la macchina cifrante e il relativo codebook, ma molte vite di militari furono perse (il tutto è stato riprodotto dal film U-571). Gli sforzi non furono però vani, nel 1941 fu nuovamente possibile decifrare le comunicazioni della marina. L'1 febbraio 1942 i tedeschi cominciarono ad utilizzare una versione a quattro rotori, e gli Inglesi dovettero ricominciare da capo.
Non potendo più conoscere la posizione degli U-boat molte navi alleate furono affondate, con pesanti ripercussioni sui rifornimenti.
Nel 1943, grazie alla creazione di macchine di decifrazione sempre più efficienti fu possibile decifrare nuovamente le comunicazioni della marina tedesca.

Molti successi sono dovuti in gran parte al lavoro svolto a Bletchley Park:
- si contribuì in maniera decisiva alla sconfitta degli U-boat nella Battaglia dell'Atlantico;
- si contribuì a rafforzare la difesa aerea (potendo di fatto prevedere le mosse del nemico) e l'offensiva aerea (capendo il momento migliore per attaccare);
- si contribuì a vincere le campagne del Mediterraneo e del Nord Africa (inclusa El Alamein);
- si contribuì al successo delle Operazioni Overlord e Double Cross e ad una più facile invasione della Francia;
- si contribuì a capire il potenziale e ad identificare le nuove armi tedesche (quelle

legate alla ricerca atomica, le armi V, i nuovi U-boat e jet);
- si contribuì a capire i reali effetti (economici e militari) degli attacchi alleati sulla Germania, ad esempio quelli mirati alle riserve di petrolio (fine del 1944);
- si contribuì inoltre a decifrare i messaggi giapponesi, fondamentali per capire la disposizione della difesa tedesca.

Per quanto riguarda lo sbarco in Normandia, il lavoro dell'Hut 8 fu fondamentale. I tedeschi prendevano in considerazione un possibile sbarco nei pressi di Calais e non in Normandia, questo fu molto importante per organizzare l'attacco.

Un evento che tutti conosciamo anche grazie all'omonimo film è l'attacco Giapponese a Pearl Harbour, probabilmente l'evento che permise la (seppure tragica) chiusura della guerra. Gli americani infatti, grazie a una macchina (*Magic*) erano in grado di decifrare i messaggi giapponesi cifrati con la macchina *Purple*, erano probabilmente a conoscenza dell'attacco in anticipo, ma si decise di non evacuare la zona, per mantenere segreto il fatto che le comunicazioni venivano decifrate, o probabilmente per dare una scossa alla opinione pubblica americana, per convincerla ad entrare in guerra. Molti lati della vicenda rimarranno oscuri, una cosa è certa, che i danni militari furono pressoché nulli, morirono invece 3000 civili americani.

L'Italia invece ebbe scarso successo, una macchina cifrante piuttosto sicura fu proposta da Sacco ma non fu mai utilizzata. Nel 1941 il servizio segreto italiano riuscì a trafugare dall'ambasciata americana a Roma il cifrario "Black". Per qualche tempo italiani e tedeschi riuscirono a decrittare i messaggi americani nel Nord Africa e molti dei successi di Rommel probabilmente furono dovuti a questo.
Nel 1942 gli alleati si resero conto della decifrazione sistematica dei propri messaggi, e abbandonarono il cifrario Black, per sostituirlo con la più sicura macchina M-138. E, stranamente, finirono anche i successi di Rommel in Africa.

Gli alleati hanno saputo dunque vincere la guerra segreta, forse sottovalutata dall'*Asse Roma-Berlino-Tokyo*, e questo ha aperto loro la strada verso la vittoria della Seconda Guerra Mondiale.

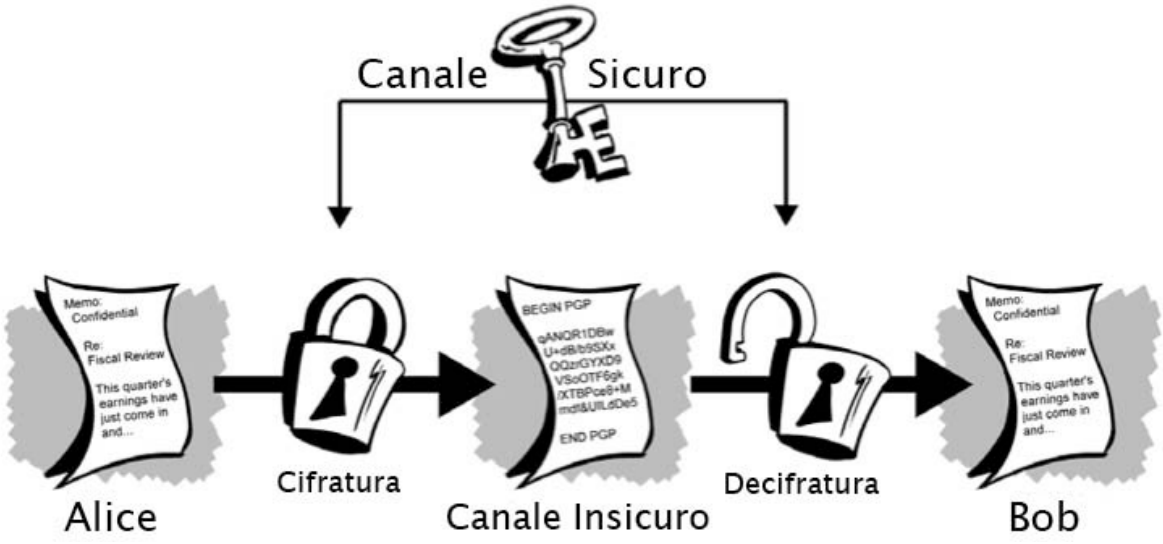
ACCENNO ALLA CRITTOGRAFIA MODERNA

La crittografia moderna, esce dai campi di battaglia, ed approda nella vita di tutti i giorni, è diventato uno strumento di massa, utilizzato per proteggere la privacy dei privati. Ormai molti degli utenti di internet per le loro comunicazioni pretendono autenticità, integrità e riservatezza. L'uso degli strumenti crittografici può garantirli almeno in parte, soprattutto se aiutati da una buona "*policy*" di sicurezza.

La crittografia moderna fa uso di problemi matematici particolarmente complessi la cui risoluzione risulta computazionalmente facile da eseguire, e teoricamente impossibile da forzare, questi vengono tradotti in algoritmi da eseguire sui calcolatori. Questi algoritmi possono essere divisi in alcune tipologie, una prima distinzione può essere fatta considerando che esistono algoritmi per cifrare completamente delle informazioni, per autenticarle, per garantire che le stesse non vengano modificate. Una seconda distinzione più specifica riguarda le tipologie di algoritmi, vengono suddivisi spesso in algoritmi a chiave simmetrica, algoritmi a chiave pubblica o asimmetrica, e algoritmi one-way di hashing.

GLI ALGORITMI SIMMETRICI

Gli algoritmi simmetrici sono tutti quegli algoritmi che usano una chiave sia per il processo di cifratura che per il processo di decifrazione, quindi gli elementi del keypair (e,d) sono uguali.
Questo sistema si basa sul presupposto di un utilizzo di due diversi canali di comunicazione, uno "*physically secure*" per lo scambio della chiave in modo da mantenerne la segretezza e uno "*secured*" attraverso cui scambiare le informazioni cifrate.



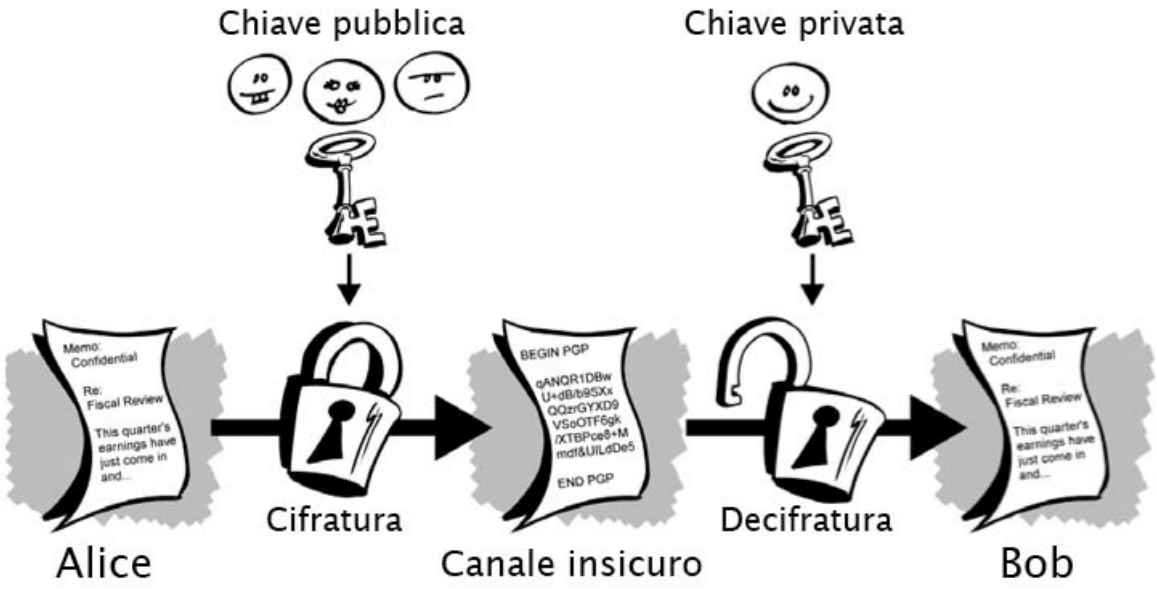
Un algoritmo simmetrico ancora largamente usato è il *DES* (Data Encryption Standard), un cifrario composto con 16 cifrature successive, presentato nel 1975 dalla IBM, è stato certificato dal NIST (National Institute of Standards and Technology), ogni 5 anni fino al 1993, divenendo già dal 1977 il sistema ufficiale del governo degli Stati Uniti d'America.

La sicurezza del sistema DES è stata infatti almeno teoricamente minata, la chiave corta (8+56 bit) potrebbe essere trovata con una crittoanalisi di tipo esaustivo, in cui si provano tutte le possibili soluzioni del sistema dato. 2^{56} (il numero di combinazioni possibili), infatti, è ormai un numero alla portata delle recenti tecnologie.

Sono state inventate anche tecniche quali la crittanalisi differenziale (ideata da Biham e Shamir) basato sull'analisi di 247 in chiaro scelti in maniera adeguata, e sul confronto dei risultati, e la crittanalisi lineare (ideata da Matsui), che utilizza 243 testi in chiaro noti.
In particolare quest'ultima ha avuto un primo successo, che venne però archiviato in quanto richiese 9735 stazioni di lavoro operanti per 50giorni e 12 ore, un tempo troppo lungo per una chiave che, come quella del DES, può essere cambiata spesso.

Recentemente in seguito ai vari tentativi di forzatura del DES, si è passati a un sistema 3DES (TripleDES) che utilizza tre livelli di cifratura.

GLI ALGORITMI ASIMMETRICI



Gli algoritmi asimmetrici fanno uso di un keypair (e,d) in cui le due chiavi sono differenti. Questo fornisce la possibilità di scambiare le chiavi anche su canali poco sicuri.

Facciamo un esempio: Alice e Bob devono comunicarsi delle informazioni top secret tramite un canale insicuro, e non hanno la possibilità di utilizzarne uno sicuro per scambiare la chiave, Bob sceglie una coppia di chiavi, la prima chiave è quella privata usata per decifrare la seconda chiave è pubblica usata per cifrare. Bob invia la sua chiave pubblica ad Alice, che cifra il messaggio lo invia a sua volta a Bob. Bob con la sua chiave privata è l'unico che è in grado di decifrarlo.

LA CIFRATURA RSA

RSA (dai nomi dei creatori Ron Rivest, Adi Shamir e Leonard Adleman) è un algoritmo particolarmente diffuso, basato sul problema matematico della fattorizzazione di grandi numeri.

Prendiamo un messaggio in chiaro *m* che deve essere cifrato ottenendo *c*. La scelta delle chiavi avviene selezionando casualmente due numeri primi molto grandi *p* e *q*.
Calcoliamo quindi $n = pq$ (n deve essere minore o al massimo uguale a m).
Dato che $\Phi(n)=\Phi(pq)=(p-1)(q-1)$ scegliamo un numero e primo con (p-1)(q-1) cioè Φ(n). n ed e formeranno la chiave pubblica.
Può quindi essere calcolata la chiave privata di decifrazione *d* in maniera che
$de+x\Phi(n)=1 \bmod n$
Per le proprietà dei gruppi moltiplicativi, essendo n un numero primo d ed x esisteranno sempre.
Per la cifratura si agisce quindi in questo modo: $c=m^e \bmod n$.
La decifrazione avviene nello stesso modo usando però la chiave d e il messaggio cifrato c: $m=c^d \bmod n$.

LA CONGETTURA DI RIEMANN

La congettura di Riemann, formulata dal matematico Gottinga Bernhard Riemann nel 1859, è uno sette "problemi del millennio". Per la risoluzione di questi, il Clay Mathematical Institute, offre un premio di un milione di dollari.
Lo studio della funzione ζ è molto importante per la teoria dei numeri. Secondo Riemann la parte reale di ogni radice non banale della funzione ζ(s) è pari a ½.
Questa congettura è legata però con la distribuzione dei numeri primi.
Eulero, scoprì che la funzione di zeta poteva essere riscritta come $\zeta(s)=\prod_{j=1}^{\infty} \frac{1}{(1-p_j^{-s})}$ tramite la produttoria con p che varia per tutti i numeri primi.

I numeri primi è ritenuto che siano distribuiti in maniera totalmente casuale, dimostrando questa congettura, potrebbe essere dimostrato il contrario, e cioè che i numeri primi seguano un certo "schema" di distribuzione nell'insieme dei numeri naturali. In questo modo sarebbe sicuramente verificare se un numero è primo in

maniera veloce ed efficace al 100%, infatti i metodi usati al momento hanno una buona probabilità di verificare se un numero è primo ma non sono le soluzioni perfette, in quanto rimane una minima percentuale per cui il numero trovato può non essere primo, anche se, le applicazioni reali non ne risentono.

Quello che si spera (o forse è più corretto dire che si teme) è che una dimostrazione della congettura di Riemann possa portare a un metodo per fattorizzare in modo veloce il prodotto di due numeri primi, facendo di fatto cadere la sicurezza del metodo di cifratura RSA.

Questo prospetta uno scenario disastroso, in quanto molte delle comunicazioni su internet sono basate proprio sul metodo RSA, un metodo veloce di fattorizzazione metterebbe a repentaglio la sicurezza di tali comunicazioni, si pensi per esempio a tutte le applicazioni di ecommerce, e più in generale a tutte le comunicazioni che avvengono attraverso internet che necessitano di sicurezza, anche tecniche di largo uso quali la firma digitale verrebbero messe a rischio.

LE FUNZIONI ONE-WAY E GLI HASH

Una funzione one-way di hashing trasforma un messaggio in una stringa di lunghezza relativamente limitata. Questa stringa rappresenta "un'impronta digitale" unica del messaggio e viene spesso definito valore di hash o checksum crittografico.
La stringa di output è detta anche *Digest* ed è univoca per ogni messaggio.
Nonostante tutto visto che i testi con dimensione finita maggiore dell'hash sono più degli hash possibili, ad almeno un hash corrisponderanno più testi possibili, questa corrispondenza viene chiamata *collisione*.
La qualità di un'algoritmo di hashing è data dalla difficoltà con cui si possano trovare queste collisioni.

LA CRITTOGRAFIA QUANTISTICA

Il futuro è rappresentato dalla *crittografia quantistica*, un approccio che utilizza particolari proprietà della *meccanica quantistica*.
Nella fase dello scambio infatti questa tecnologia permette una sicurezza nello scambio dando la possibilità di mantenere veloce lo stesso. Questo rende possibile un pratico utilizzo dei One Time Pads.

La crittografia quantistica, non permette alcun tipo di intercettazione o modifica, da parte di avversari, alla comunicazione. Per il principio di indeterminazione di Heisenberg non è possibile conoscere, simultaneamente e con precisione assoluta, alcune particolari coppie di caratteristiche di un oggetto quantistico, come ad esempio la posizione e la velocità di un elettrone. Se si cerca di misurarne esattamente la posizione, si perde la possibilità di verificare la velocità dell'elettrone. Se invece si misura con precisione assoluta la velocità, si perdono inevitabilmente informazioni sul luogo in cui l'elettrone si trova. I fotoni, anch'essi oggetti quantistici, sono quindi soggetti al principio di indeterminazione Heisenberg. Questa proprietà consente di capire se un sistema è stato osservato (misurato) da un intruso. Un intruso verrebbe immediatamente rilevato anche se questi provasse a spedire un nuovo messaggio al destinatario dopo aver intercettato il primo, fare una “copia perfetta” della comunicazione è impossibile (per il teorema di non-clonazione dimostrato nel 1982 da Wooters e Zurek e, indipendentemente da Dieks); la comunicazione sarebbe visibilmente corrotta e verrebbe così facilmente scartata.

ASPETTI GIURIDICI DELLA CRITTOGRAFIA

Una funzione meno nota ma allo stesso tempo importante è ricoperta da quello che è l'aspetto giuridico, non solo per quanto riguarda il mantenimento della privacy, ma soprattutto per l'utilizzo della firma digitale e il riconoscimento di valore giuridico ai documenti digitali.

Quello che veniva assolto nei documenti tradizionali dalla firma autografata, è svolto a livello informatico dalla firma digitale basata sulla crittografia a chiave pubblica. Questo è infatti il principale strumento in grado di assicurare l'integrità e l'autenticazione dei documenti informatici. Queste peculiarità lo rendono ideale per la creazione di un documento informatico valido e rilevante dal punto di vista legale esattamente come i documenti cartacei. Il documento informatico diviene atto giuridico a tutti gli effetti di legge grazie alla normativa italiana in materia di firma digitale, che è attualmente abbastanza completa ed organizzata.

[tratto da xxii]
“Il primo tassello di questo quadro normativo è rappresentato dall’Art. 15 della legge n. 59 del 15 marzo 1997 in materia di riforma e semplificazione amministrativa nella Pubblica Amministrazione. Questa legge, meglio nota come "Legge Bassanini", va inquadrata nell’ambito di una generale ristrutturazione della Pubblica Amministrazione per la quale svolge un ruolo fondamentale l'AIPA (Autorità per l’Informatica nella Pubblica Amministrazione), autorità indipendente istituita nel 1993 al fine di predisporre le norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche.

Nell’articolo citato viene sancito che "gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici e telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge". Si tratta di un’innovazione di portata eccezionale che introduce nel nostro ordinamento nuove forme di negozio (validità dei contratti stipulati per via telematica, trasmissione ed archivio di documenti in formato elettronico, firma digitale con piena validità legale).
I criteri e le modalità di applicazione del principio suddetto sono stati poi emanati attraverso il regolamento contenuto nel DPR 10 novembre 1997, n. 513. Tale regolamento ha stabilito quali sono gli scenari di riferimento giuridici, tecnologici ed organizzativi per ottenere quanto necessario ad un efficace utilizzo del documento informatico e della firma digitale. In particolare viene stabilito che il documento informatico soddisfa gli stessi requisiti dei documenti in formato scritto e viene sancito il principio che il documento informatico ha piena efficacia probatoria. I criteri di tale regolamento hanno portata molto ampia e sono validi sia nel settore pubblico che privato.

Un ulteriore provvedimento legislativo, il DPCM 8 febbraio 1999 recante :"Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici" ha regolato gli aspetti tecnici ed organizzativi di chi usufruisce ed opera con i documenti informatici e la firma digitale. In particolare vengono descritti gli algoritmi, le caratteristiche tecniche, gli standard in materia di generazione, conservazione e formato delle firme e dei certificati.

Con l'emanazione delle regole tecniche, l'Italia si è collocata al primo posto fra i Paesi dell'Unione Europea che hanno adottato nell'ordinamento giuridico interno il principio del pieno valore giuridico della firma digitale. Il fine ultimo di questo complesso sistema normativo è quello di rendere più efficace e meno costosa l'azione amministrativa, sia pubblica che privata, attraverso un impiego su vasta scala delle tecnologie dell'informazione.

Infine la pubblicazione della Circolare AIPA 26 luglio 1999, n.22 per l'iscrizione all'elenco pubblico dei certificatori costituisce il tassello conclusivo del processo legislativo descritto e che permette di rendere operativa la firma digitale. Tale circolare detta le norme per la formazione dell'Elenco Pubblico dei Certificatori, elenco tenuto dall'Autorità ed in cui vengono inserite, previa azione di verifica del soddisfacimento di opportuni requisiti, le società interessate ad esercitare l'attività di certificazione delle chiavi.

Il Certificatore a norma AIPA svolge l'attività di certificazione e può essere sia un soggetto pubblico che privato. In particolare deve poter garantire il rilascio del certificato digitale contenente la chiave pubblica, deve curare la pubblicazione dei certificati emessi e deve aggiornare appositi elenchi contenenti i certificati sospesi e revocati."

L'attuale quadro normativo è quindi in grado di fornire un discreto supporto per le attività che prevedano lo scambio di documenti elettronici con una valenza giuridica.
La firma digitale diviene quindi lo strumento da usare, e consente a privati, imprese e PA snellendo e velocizzando i processi amministrativi, dando una base adeguata per uno sviluppo sicuro, che permetta di sviluppare una linea operativa a cui possano adattarsi facilmente le imprese (private e pubbliche) per rendere migliore i servizi offerti.

CONCLUSIONE

Lo sviluppo tecnologico è ormai permeato nella vita di tutti i giorni.
Questa crescita tecnologica, deve essere supportata da strumenti per proteggere privacy e sicurezza e soprattutto da una opera di informazione rivolta agli utenti, spesso poco consapevoli dei pericoli celati dietro le attuali tecnologie, e incapaci di difendersi a causa di una scarsa informazione o di una errata informatizzazione per quanto riguarda lo scenario attuale e futuro delle comunicazioni.

Il mondo è entrato in una ottica di evoluzione ed integrazione tecnologica e, se da un lato le nuove tecnologie hanno ampliato enormemente lo spettro di possibilità, dall'altro hanno portato ad una informatizzazione della figura del criminale e del concetto di crimine: la tecnologia risulta un'arma a doppio taglio che può essere usata in diversi modi positivi ma che, in mano ad un malintenzionato, può risultare davvero pericolosa.

Per questo bisogna scegliere di creare dei percorsi di formazione verso le tecnologie di difesa della privacy e della sicurezza informatica, in modo da permettere uno sviluppo sicuro di internet e delle sue applicazioni.

BIBLIOGRAFIA

i. Cryptographie Militaire
http://www.petitcolas.net/fabien/kerckhoffs/index.html#english

ii. Handbook of Applied Cryptography
Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone
CRC Press
ISBN: 0-8493-8523-7
October 1996, 816 pagine
http://www.cacr.math.uwaterloo.ca/hac/

iii. A Brief History of Cryptography
http://www.cypher.com.au/crypto_history.htm

iv. Crittografia
http://sprite.csr.unibo.it/linuxday04/slide/crittografia.pdf

v. Ancient Egypt
http://library.thinkquest.org/28005/flashed/timemachine/courseofhistory/egypt.shtml

vi. Crittografia Classica
http://www.dia.unisa.it/professori/ads/corso-security/www/CORSO-0102/crittografia-classica.pdf

vii. HISTORIA DE LA CRIPTOLOGÍA – Antigüedad
http://serdis.dis.ulpgc.es/~ii-cript/PAGINA%20WEB%20CLASICA/CRIPTPLOGIA/HISTORIA%20DE%20CRIPTOLOGIA%20-%20ANTIGUA.htm

viii. RSA Laboratories FAQ, Frequently Asked Questions about Today's Cryptography
Author: RSA Laboratories
Title: RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1
Year: 2000
Publisher: RSA Security Inc.

ix. Cryptography faq
ftp://rtfm.mit.edu/pub/faqs/cryptography-faq/

x. Algoritmi di crittografia - comunicazione sicura
http://telemat.die.unifi.it/book/1999/crittografia/

xi. La funzione ζ e la congettura di Riemann
http://www.syllogismos.it/history/Zeta.pdf

xii. Crittografia: aspetti storici e matematici
http://www.infotech18.polito.it/Concorso/Pdf/Marco_Triverio.pdf

xiii. La crittografia da Atbash a RSA
http://www.liceofoscarini.it/studenti/crittografia/

xiv. Crittografia: una sfida e un'opportunità
http://www.regione.veneto.it/NR/rdonlyres/06015654-94BD-4DC0-BC98-E8E54D743BAF/0/RVE_Seminario13_2da.pdf

xv. Escrita escondida Criptografia
http://www.ajc.pt/cienciaj/n32/escrita.php

xvi.Storia di Bletchley Park
www.english-heritage.org.uk/bletchleypark

xvii.Permutazioni, disposizioni, combinazioni
http://utenti.quipo.it/base5/combinatoria/combinatorio.htm

xviii.Permutazioni
http://web.math.unifi.it/users/ottavian/geo1/permut.html

xix.Teoria dei gruppi
http://progettomatematica.dm.unibo.it/Gruppi/homepg.htm

xx. Algebra moderna e matematiche finite / R. Sprugnoli
Pisa, ETS, 1976
317 pgagine

xxi.Dizionario di matematica elementare,
Stella Baruk
Traduttore Gregori F., Curato da Speranza F., Grugnetti L.
Edizioni Zanichelli, 1998
652 pagine
ISBN 880809748X

xxii. Telecom Italia Open
http://www.firmasicura.it/legislazione.asp
http://www.firmasicura.it/faq.asp