ISIS V. CARDARELLI – LICEO SCIENTIFICO – TARQUINIA (VT)

Storia della Crittografia

Tesina d'Esame di Stato

Patrizio Tufarolo

Ci sono casi in cui un uomo deve rivelare metà del suo segreto per tener nascosto il resto.

Philip Dormer Stanhope, conte di Chesterfield

Indice

FONTI E REFERENZE TELEMATICHE:

Wikipedia (http://it.wikipedia.org)
La Sicurezza Informatica di Castiglioni Marco, Pozzetti Mirko, Trevisan Matteo (e-Book disponibile online gratuitamente)
Focus.it (http://www.focus.it), sito del noto mensile di attualità, scienza e sociologia italiano
Sicurezza Nazionale Americana (http://www.nsa.gov)

Introduzione

Un'impellente necessità dell'uomo sin dalla nascita della scrittura, è stata quella di trovare un modo per trasmettere i propri messaggi verso un destinatario definito senza essere intercettati da altri, nascondendoli in luoghi impensabili o sconosciuti a terzi.

Questo bisogno di trasmettere informazioni segrete si è manifestato in modi diversi nei vari periodi storici e nelle varie civiltà: la crittografia ha conosciuto un'incessante evoluzione per arrivare alla più complessa delle sue applicazioni, l'informatica.

Per entrare nel cuore dell'argomento è necessario partire dall'etimologia della parola *"crittografia"*. Essa, infatti, deriva dall'unione due parole greche: *kryptós* (nascosto) e *graphéin* (scrittura). Tratta perciò della "scrittura nascosta", cioè dell'offuscamento dei messaggi (*crittogrammi)* affinché risultino illeggibili da persone non autorizzate.

Lo studio dei sistemi crittografici prende così il nome di *crittologia*.

La steganografia

La **steganografia** è una delle prime tecniche utilizzate per comunicare segretamente. Anche questa parola ha origine greca: è data dall'unione di *steganos* (nascosto) e *graphéin*.
Consisteva, appunto, nel nascondere il messaggio da comunicare in un oggetto o in un posto, dove nessun altro fuorché il destinatario sarebbe mai andato a guardare.

A tal proposito lo storico **Erodoto**, ci racconta una tipica prassi dell'antica Persia: si era soliti rasare gli schiavi e scrivergli il messaggio sulla testa. Dopo essersi fatto ricrescere i capelli, lo schiavo si recava dal destinatario del messaggio e veniva rasato nuovamente.
Un simile metodo era applicato in Cina: il messaggio veniva scritto in sottili striscioline di seta, che venivano appallottolate e coperte di cera, quindi inghiottite dal messaggero.

Nel XVI secolo invece, grazie a **Giambattista della Porta**, si scoprì come comunicare tramite un uovo sodo: miscelando 30 grammi di albume con mezzo litro d'aceto, si otteneva un inchiostro che poteva essere usato per scrivere sul guscio poroso dell'uovo, che assorbiva il colore. Sbucciando l'uovo, il messaggio poteva essere riletto.

La steganografia moderna è invece basata sul metodo **LSB** (**l**east **s**ignificant **b**it, bit meno significativo), ed è strettamente legata all'informatica. La teoria che regola l'LSB è quella secondo la quale un'immagine ad alta definizione, così come un qualunque file multimediale (audio/video), se modificato nei suoi bit meno significativi, mantiene la propria integrità.
In questo modo un qualsiasi file multimediale può essere modificato, e solo chi conosce i bit modificati (che costituiscono la chiave di cifratura) può risalire al messaggio criptato.

La longevità di questi metodi di protezione delle informazioni ci dimostra l'effettiva sicurezza che essi sono in grado di garantire. Tuttavia i punti deboli sono molteplici: il messaggero può essere perquisito (nel caso persiano e in quello cinese) e il messaggio può essere scoperto, mentre per quanto riguarda la steganografia moderna, può essere fatto un attacco a distorsione. Basta diminuire la definizione del contenuto, e gli LSB vengono eliminati, con la conseguente perdita del contenuto cifrato.

Dalla steganografia alla crittografia

In parallelo allo sviluppo della Steganografia, si ha l'avvento della Crittografia.
Questa, non **mira a nascondere** il messaggio in sé, ma **il relativo significato**.

Perciò il testo è reso incomprensibile con un'alterazione mediante un procedimento concordato tra mittente e destinatario, in modo che solo chi conosca la chiave di cifratura possa essere in grado di ottenere il messaggio originale da una sequenza di simboli apparentemente casuale.

Troviamo forme di crittografia in India (nell'Artha-Sastra e nel Latila Vistara, due testi sacri; il primo di origine civile, l'altro religiosa, che testimoniano l'importanza di avere un codice cifrato per i servizi di spionaggio), in Mesopotamia (per opera dei Babilonesi e degli Assiri, che avevano la consuetudine di sostituire le parti finali delle parole con brevi suffissi stereotipati), in Iraq (dove, alla fine del periodo cuneiforme, troviamo l'usanza di sostituire i numeri alle lettere, per la prima volta).
Non troviamo forme di crittografia, invece, in Cina, dove le comunicazioni avvenivano perlopiù oralmente.

In ogni caso Steganografia e Crittografia non sono da ritenersi due ambiti separati: l'utilizzo dei due metodi di scrittura si incrocia continuamente nella storia. A prova di ciò si può considerare la tecnica del ***microdot***, molto in voga durante la Seconda Guerra Mondiale.
Gli agenti tedeschi erano in grado di ridurre intere pagine di testo scritto in piccole macchie del diametro inferiore al millimetro, che potevano essere nascoste in banali comunicazioni ordinarie.
Il primo *microdot* fu scoperto dagli agenti dell'FBI in una comunicazione proveniente dall'America Latina nel 1941, grazie ad una soffiata.

La crittografia nel mondo antico

La scitala lacedemonica

La scitala lacedemonica costituisce il più antico esempio di sistema crittografico.
Come testimoniato da Plutarco, essa era in uso a Sparta ai tempi di Licurgo (IX sec a.C.) e quasi sicuramente anche ai tempi di Lisandro (400 a.C.)

Fig. 1 - Scitala Lacedemonica

Consisteva in un bastone sul quale veniva avvolto ad elica un nastrino di cuoio. Su questo nastrino si scriveva per colonne parallele all'asse del bastone il messaggio segreto. Il nastro veniva poi tolto, e ciò che ne risultava era una sequenza casuale di lettere. Riavvolgendo il cuoio attorno a un altro bastone di uguale diametro (che costituisce la chiave di cifratura) si riotteneva il messaggio in chiaro.

Il disco di Enea

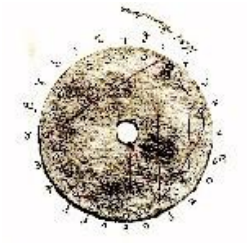


Fig. 2 - Disco di Enea

Si fa risalire al IV secolo il primo trattato di cifrari della Storia, redatto da Enea il Tattico (generale della lega arcadica). Nel ventunesimo capitolo di questo trattato vi è la descrizione di un disco, caratterizzato da 24 fori sulla zona esterna, ciascuno dei quali era contrassegnato con una lettera dell'alfabeto.
Partendo da un foro centrale, si faceva passare un filo nei fori delle lettere che componevano il messaggio. Così facendo, il destinatario doveva soltanto rimuovere il filo e leggere il messaggio al contrario.

Atbash, Albam, Atbah

Queste tre scritture segrete sono descritte in modo dettagliato nei testi sacri.
Nell'Antico Testamento ebraico troviamo esplicitati i principi di funzionamento dell'*Atbash*: questo metodo prevedeva l'inversione dell'alfabeto, facendo diventare la prima lettera l'ultima, la seconda la penultima, e così via.
L'*Albam* invece consisteva nel dividere l'alfabeto in due metà, e nel far corrispondere le lettere della prima metà a quelle della seconda metà.
L'*Atbah,* infine, presuppone una relazione di tipo matematico. A ogni lettera viene attribuito un numero, dopodiché le prime nove vengono sostituite con la loro lettera complementare rispetto a 10, le restanti con la lettera complementare rispetto a 28.

La crittografia di Polibio

Lo storico greco Polibio nelle "Storie" ci fornisce un interessante metodo di cifratura. Egli propone di cifrare ogni lettera con una coppia di numeri compresi tra 1 a 5, in conformità a una matrice 5x5 contenente le lettere dell'alfabeto.
Per la trasmissione del messaggio, introduce una novità a quanto già è stato descritto da Enea il tattico: propone di mandare un numero di messaggeri pari a quello dei caratteri, con un numero di torce pari all'indice di riga nella mano sinistra e un numero di torce pari all'indice di colonna nella mano destra. Così facendo crea, di fatto, un telegrafo ottico.

Il cifrario di Cesare e quello di Augusto

Un sistema ancora differente è quello utilizzato da Giulio Cesare. Come ci racconta Svetonio, Cesare utilizza un codice di cifratura molto semplice: era solito sostituire ogni lettera con quella che la segue nell'alfabeto. Augusto invece utilizza un testo chiave che viene sommato al testo da cifrare, mediante la somma delle distanze da inizio alfabeto. Così, solo chi possiede il testo chiave, può ricondurre il messaggio cifrato all'originale.

La crittografia medievale e pre-risorgimentale

Il disco di Alberti

Si attribuisce a Leon Battista Alberti l'invenzione di uno dei più complessi e innovativi cifrari meccanici. Si tratta di un disco composto di due cerchi concentrici di rame. Nel disco esterno sono riportate le lettere dell'alfabeto in chiaro, nel disco interno le lettere dell'alfabeto cifrante.

Fig. 3 - Disco di Alberti

Il disco esterno è composto di 24 caselle, contenenti le lettere dell'alfabeto maiuscole in ordine, escluse la J, la K, la W e la Y, che sono state sostituite dai numeri 1, 2, 3 e 4. Il disco interno riporta tutte le lettere in minuscolo in maniera disordinata (la u e la v sono collassate) e il simbolo wildcard &.

Per utilizzarlo bisogna scegliere una lettera maiuscola e farla corrispondere al simbolo wildcard. Tutte le altre lettere verranno poi associate. Le lettere corrispondenti a 1, 2, 3 e 4 non vengono usate.

Questo metodo non ottenne mai successo, anche perché fu tenuto segreto dallo stesso Alberti, e il suo trattato fu pubblicato postumo.

Il cifrario di Vigenère

Blaise de Vigenère pubblicò nel 1586 il suo Cifrario, una generalizzazione del già noto Cifrario di Cesare. Si tratta del più semplice dei cifrari polialfabetici, che godé di una grande reputazione in quanto ritenuto inattaccabile per secoli.

Invece di spostare la lettera da cifrare sempre dello stesso numero, Vigenère propose di spostarla di un numero di posti variabile ma ripetuto, in base a una parola chiave concordata tra mittente e destinatario. La chiave veniva scritta ripetutamente sotto il messaggio, e data la sua esigua lunghezza nei confronti del messaggio stesso doveva essere ripetuta per tutta la sua lunghezza, motivo per cui era anche detta "verme".

Si esegue così la somma circolare tra le lettere del messaggio da cifrare e quello della parola chiave.

```
Testo chiaro  - SEGRETO

Verme         -  VERMEVE

Testo cifrato - NIXDIOS
```

Così facendo si ottiene un cifrato con N alfabeti cifranti, complicando notevolmente l'operazione di crittoanalisi. Per cifrare più velocemente il messaggio, Vigenère suggerì di usare una matrice quadrata 26x26 contenente le lettere dell'alfabeto spostate di una posizione per ogni riga. La lettera da usare nel messaggio cifrato era così quella data dall'incrocio della lettera di partenza e di quella corrispondente nella chiave.

La crittografia moderna: il Rullo di Jefferson

Uno dei cifrari più importanti dell'età moderna è il **Rullo di Jefferson**, anch'esso meccanico. Prende il nome dal suo inventore (**Thomas Jefferson**), uno degli autori della Dichiarazione d'Indipendenza e presidente USA dal 1801 al 1804.

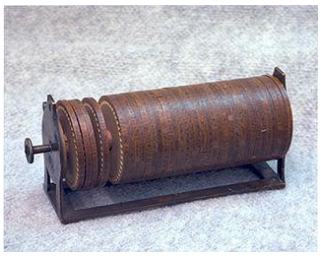


Fig. 4 - Rullo di Jefferson

Questo cifrario non fu mai usato da Jefferson, e rimase inutilizzato fino al 1922, divenne però fondamentale per gli americani durante tutto il periodo della Seconda Guerra Mondiale, fino al 1950.

Basato su un cilindro lungo circa 15cm e largo 4cm, è costituito da 36 dischi, imperniati su un asse, in grado di ruotare liberamente.

Su ognuno di questi sono riportate le 26 lettere dell'alfabeto, in ordini differenti.

L'ordine dei dischi costituisce un'ulteriore chiave: di volta in volta viene cambiato, ma solo conoscendo quello giusto il mittente e il destinatario possono comunicare.

Il messaggio viene perciò diviso in blocchi di 36 caratteri, per ogni blocco i dischi vengono ruotati in modo tale da far comparire i caratteri del blocco allineati. Poi si prende un'altra riga a caso, e si considerano i caratteri di questa riga.

Chi riceve il messaggio possiede un meccanismo identico a quello del mittente, sul quale deve riprodurre la sequenza cifrata, per poi andare ad analizzare le restanti righe in cerca di quella col messaggio di senso compiuto.

La crittografia nel Novecento

La "sicurezza perfetta": il cifrario di Vernam

Gilbert Vernam è stato un ingegnere statunitense dei laboratori della Bell Labs e della AT&T Inc. (American Telephone and Telegraph Incorporated), inventore di un cifrario One Time Pad noto come cifrario di Vernam.
Basato su una riedizione del Cifrario di Vigenère, esso **aveva lo scopo di proteggere le comunicazioni su un telegrafo di testi già codificati in binario.**
Per prima cosa costruì un dispositivo in grado di leggere contemporaneamente due nastri in input e di generare un unico nastro in output in cui ciascun foro fosse generato tramite un operatore XOR dei fori corrispondenti sui nastri in input.
In pratica se il testo in chiaro è

0 1 1 0

e la chiave

0 1 0 1

Il testo cifrato che ne risulterà sarà

0 0 1 1

L'operazione di decifratura avviene riapplicando l'operatore XOR tra la chiave e il testo cifrato.

Per parole complesse, ad ogni lettera viene perciò associato un numero, dopodiché viene sfruttata l'operazione di somma circolare.
Di conseguenza avremo per esempio che **A + D = 0 + 3 = 3 = D**, oppure **C + E = 2 + 4 = 5 = F**.
Per quanto riguarda la sicurezza, il metodo Vernam è l'unico a essere considerato, ad oggi, perfetto: il cifrario può essere considerato assolutamente indecifrabile.
Inoltre è di tipo One Time Pad:l'agente riceveva un taccuino che conteneva una chiave per pagina, da poter strappare una volta utilizzata).
Necessita di una chiave univoca della stessa lunghezza del messaggio originale, generata casualmente, i cui bit componenti non devono presentare nessuna relazione.
Di contro, però, è un sistema molto scomodo da applicare: le chiavi, ingombranti perché lunghe quanto il messaggio, devono essere generate in anticipo rispetto all'uso previsto, e devono essere conservate in un luogo assolutamente sicuro.
Per questa ragione venne usato in casi molto eccezionali: fu grazie ad esso se i **segreti della bomba atomica** transitarono da Occidente e Oriente, e che **Che Guevara** poté comunicare con Fidel Castro durante la missione in Bolivia (alla sua cattura gli fu trovato un foglio addosso con scritta una serie lunghissima di numeri).
Un altro inconveniente del cifrario di Vernam è che esso è modificabile: può essere contraffatto affinché il messaggio ricevuto risulti differente, o comunque rovinato, rispetto all'originale e il destinatario non ha alcun modo per verificarne l'integrità.
L'utilizzo di chiavi troppo grandi può essere evitato tramite delle varianti, le quali però aumentano le possibilità della crittoanalisi statistica di forzare il cifrario.

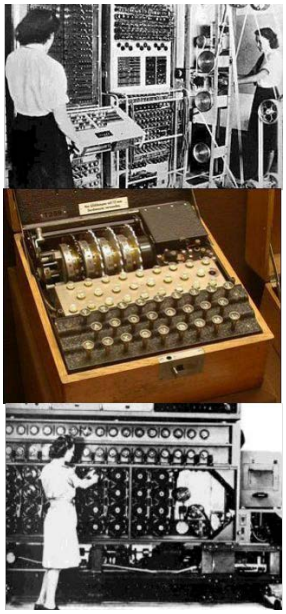
Operazione Colossus, la lotta contro Enigma.

Allo scoppio della Seconda Guerra Mondiale, le operazioni di decifrazione britanniche furono spostate da Londra a **Blechtley Park**.
Una delle figure più importanti che lavorò in questo dipartimento spionistico fu senza dubbio il matematico **Alan Turing**, il cui lavoro fu reso noto solo molti anni dopo, quando cadde il segreto militare sulle tecniche di crittoanalisi sviluppate durante la guerra.

Fig. 5 Enigma

La figura di Turing costituisce un baluardo per lo studio della calcolabilità logico-matematica, lo strumento da lui utilizzato è oggi noto come **Macchina di Turing**, un calcolatore in grado di leggere le informazioni da un nastro, eseguire un algoritmo e restituire un output su un altro nastro.

Le comunicazioni tedesche erano cifrate con una macchina chiamata ***Enigma***, uno dei più sofisticati cifrari a rotore (sostituiti poi dai più moderni e innovativi cifrari elettronici, che hanno letteralmente sconvolto il mondo della crittografia).
Enigma era però sprovvisto di una stampante, i risultati apparivano illuminati su un'apposita tastiera e dovevano essere trascritti su un foglio di carta: fu così che gli Inglesi entrarono in possesso di un "known plain text", "testo in chiaro noto", ribattezzato in seguito in *crib*. Ciò, unito alla reversibilità del processo, permise a Turing di scoprire l'algoritmo stesso e di costruire un meccanismo automatico di decrittazione: la **Bomba di Turing.**



Lo scopo del suo workgroup, formato da circa settemila persone tra militari, civili, matematici, giocatori d'azzardo, era quello di rompere Enigma: a questo fine, Turing si servì di ***Colossus***, una gigantesca macchina inventata da un esperto di centralini telefonici, che può essere considerata un predecessore dei successivi calcolatori elettromeccanici.
Grazie al Colossus, la "Bomba", Turing era in grado di trovare i codici nazisti in pochi minuti, per intercettare le comunicazioni italo-tedesche. In questo modo gli alleati poterono cambiare letteralmente il corso della guerra, prendendosi un grande vantaggio sulla stessa marina italiana sconfitta a capo Matapan nel 1941. Tutti gli esemplari di Colossus vennero smantellati alla fine della guerra.

Dal canto loro gli Americani, nel tentativo di ottenere comunicazioni vocali "sicure", avevano sperimentato il linguaggio degli indiani Choctaws, che già era di per se criptato. Dopo la guerra questo tipo di comunicazione venne ulteriormente perfezionato, tramite l'uso del linguaggio Navajos.
Questo tipo di comunicazioni, chiamati comunemente NAC (Native American Codetalkers) non è mai stato infranto.

La crittografia dalla Guerra Fredda ai giorni nostri

Cifrari a sostituzione

I cifrari a sostituzione sono quei cifrari in cui ogni simbolo del testo viene trasformato in un simbolo dell'alfabeto cifrato. I segni di punteggiatura vengono rimossi.
Si dividono in due categorie:

1. **Cifrari monoalfabetici** (come quello di Cesare), in cui ogni carattere viene sostituito con un altro per tutta la fase di cifratura. Se alla parola C A S A corrisponde il codice cifrato P I N I, alla A corrisponderà sempre la I, alla S corrisponderà sempre la N e così via.
   I cifrari affini sono particolari cifrari monoalfabetici la cui chiave di cifratura è regolata tramite una legge matematica: il numero d'ordine del simbolo viene moltiplicato per un numero a piacere, poi viene spostato (shifting) di un altro numero di caratteri a piacere.
2. **Cifrari polialfabetici**, più complessi, spesso basati su sistemi meccanici. A ogni carattere vengono assegnate diverse lettere dell'alfabeto.

Gli algoritmi DES e RSA

Basato sull'algoritmo **Lucifer**, sviluppato da IBM nei primi anni 70, il **DES** fu ideato dai dipendenti dell'**NBS** (**N**ational **B**ureau of **S**tandard), l'odierno **NIST** (**N**ational **I**nstitute of **S**tandard and **T**echnology), con lo scopo di proteggere i dati riservati non categorizzati come "segreti di stato".
Così nel 1974 abbiamo l'ingresso del **DEA** (**D**ata **E**ncryption **A**lgorithm) rinominato in seguito in **DES** (**D**ata **E**ncryption **S**tandard). Venne adottato dal governo USA nel 1977, come standard crittografico federale.

Il DES è l'archetipo della **cifratura a blocchi**, un algoritmo che prende in ingresso una stringa di lunghezza fissa di testo in chiaro e la trasforma con una serie di operazioni complesse in un'altra stringa di testo cifrato della stessa lunghezza. Nel caso del DES la dimensione del blocco è di 64 bit. Il DES usa inoltre una chiave per modificare la trasformazione in modo che l'operazione di decifratura possa essere compiuta solo conoscendo la chiave stessa. La chiave è lunga 64 bit ma solo 56 di questi sono effettivamente utilizzati dall'algoritmo. Otto bit sono utilizzati solo per il controllo di parità e poi scartati, per questo la lunghezza della chiave effettiva è riportata come di 56 bit.

L'**RSA** è un algoritmo di codifica che prevede l'utilizzo di una chiave pubblica e di una chiave privata, ideato da tre matematici: Ron **R**ivest, Adi **S**hamir e Leonard **A**dleman, nel 1977.
Il procedimento che regola questo algoritmo sfrutta le proprietà dei numeri primi.
La chiave pubblica è ottenuta dal prodotto di due fattori primi molto grandi, ottenendo un risultato molto difficile da fattorizzare ed è univoca. La chiave privata invece viene fornita a chi deve decifrare il messaggio.
L'algoritmo RSA è applicato in larga scala alle odierne tecnologie informatiche: basti pensare alla cifratura WPA (Wi-Fi Protected Access) per la protezione delle reti Wi-Fi attive in ognuna delle nostre case, oppure alle reti private virtuali (VPN, Virtual Private Network) con autenticazione per mezzo di certificati, o ancora alle firme digitali, al software PGP (Pretty Good Privacy) molto in voga su Internet.

Il ruolo della pseudo-casualità

Introducendo l'elemento logico-matematico all'interno del processo criptico, è stato possibile per l'uomo creare nuovi sistemi crittografici, che hanno conosciuto l'apice della loro macchinosità grazie all'elemento pseudo-casuale.
I numeri pseudocasuali sono perciò quei numeri generati da un calcolatore tramite un algoritmo

deterministico con approssimativamente le stesse proprietà statistiche di una sequenza di numeri generati casualmente.
Quando c'è necessità di utilizzare numeri casuali bisogna invece utilizzare un generatore hardware di numeri casuali.

I generatori di numeri pseudocasuali possono essere classificati in vari gruppi, a seconda dell'algoritmo utilizzato. In linea di massima essi generano numeri interi distribuiti uniformemente tra 0 e un valore massimo stabilito, oppure valori reali compresi tra 0 e 1, come nel caso delle macchinette calcolatrici tascabili.
In crittografia vengono utilizzati due algoritmi principali per la generazione di numeri pseudocasuali:

- **Fortuna**

  E' costituito da tre parti principali:

  1) Un file di seed (seme) che contiene un certo quantitativo di dati casuali usati per inizializzare il generatore.
  2) Il generatore stesso che, partendo dal file di seed, produce una quantità indefinita di dati pseudo-casuali.
  3) Un accumulatore di entropia, che cattura dati casuali da varie fonti in input (mouse, tastiera, touchscreen…), e li usa per rinnovare il seed. L'entropia viene utilizzata per prevenire gli attacchi di tipo injection sul generatore.

  Fortuna è uno degli algoritmi più comuni: viene utilizzato, ad esempio per generare i certificati SSL SHA256, quelli che sono utilizzati per impedire l'intercettazione del traffico web.
  Senza SSL chiunque sarebbe in grado di analizzare tutto il traffico che passa per una rete, spiando anche illecitamente l'attività degli altri utenti di quella rete o nodo.

- **Blum Blum Shub**

  E' stato proposto nel 1986 da Lenore Blum, Manuel Blum e Michael Shub, e tiene conto delle proprietà dei numeri primi.
  Per questo motivo non è ritenuto adatto alle simulazioni, ma solamente alla crittografia, a causa della sua lentezza. Rimane comunque un algoritmo molto sicuro, data la difficolta di fattorizzazione di numeri primi molto grandi.

La crittoanalisi

La crittoanalisi è la scienza volta a debellare le protezioni offerte dalla crittografia.
La crittoanalisi statistica mira a studiare la frequenza con cui si ripetono alcuni costrutti in una determinata lingua. Questa caratteristica, infatti, può essere sfruttata per decrittare interi testi o documenti di significato ignoto: analizzando un testo in italiano, ad esempio, si può notare come ricorra la presenza degli articoli e delle preposizioni. Associando statisticamente dei simboli frequenti nel testo crittografato ad articoli e preposizioni, si può pian piano ricostruire il testo originale.
Ovviamente nel caso di cifrari polialfabetici, la situazione si complica rispetto a testi crittografati, ad esempio, col metodo cesariano.

La crittoanalisi lineare è basata sul confronto di due elementi: il "plain text" (testo in chiaro) e il "cyphered

text" (testo cifrato). Questo tipo di attacco ha come scopo quello di trovare l'algoritmo di cifratura per riapplicarlo, ad esempio, su un'altra fonte che si suppone cifrata allo stesso modo.

La crittoanalisi differenziale mira a studiare le differenze tra due testi in chiaro cifrati con la stessa chiave. Questo metodo ha portato gli studiosi Bahim e Shamir alla forzatura dell'algoritmo DES precedentemente trattato.

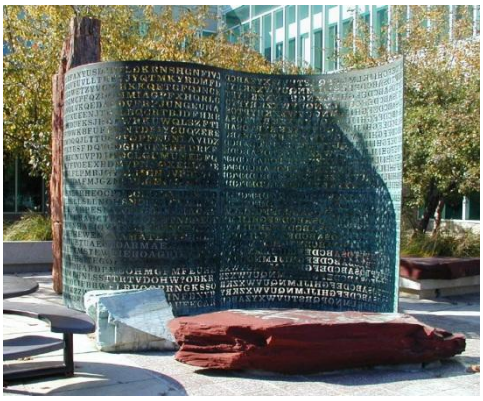
Attacco a forza bruta

L'attacco a forza bruta (brute-force) è uno dei più moderni e diffusi metodi di crittoanalisi, possibile solo grazie al recente avvento dei computer.
Consiste nella ricerca esaustiva della chiave di cifratura (password), e può procedere in due modalità:

1. **Attacco a dizionario** – Il software cerca la chiave di cifratura in un dizionario di parole di senso compiuto fornito in input.
2. **Attacco a combinazione** – Il software tenta di risalire alla chiave di cifratura provando tutte le combinazioni possibili, seguendo un ordine prestabilito.

Ovviamente questo tipo di attacco presenta non pochi svantaggi tra cui la necessità di un'elevata capacità di calcolo, e la disponibilità di tempo.
Per scoprire tramite forza bruta una chiave DES ad esempio occorrerebbe far lavorare circa 700.000 computer contemporaneamente per 24 ore.

La Crittografia nell'Arte: Kryptos



Nell'ormai lontano 1990 l'artista Jim Sanborn realizzò Kryptos, una scultura che abbellisce il cortile del quartier generale della CIA di Langley (Virginia). Su questa scultura è inciso un messaggio in codice di 865 caratteri in un algoritmo ancora indecifrabile sviluppato dallo stesso Sanborn: nessuno degli esperti di cifratura dell'intelligence americana è riuscito a decifrare l'iscrizione per intero.
Il codice che nasconde il messaggio di Kryptos è frutto della collaborazione tra l'artista e Ed Scheidt, un ex-responsabile dei laboratori crittografici della CIA.

L'opera è fatta di granito rosso, ardesia rossa e verde, quarzo bianco, legno pietrificato, magnetite e rame, ed è divisa in quattro sezioni, ognuna delle quali è codificata con una precisa chiave.
Il tema sembra essere quello dell'"intelligence gathering" (letteralmente: riunire l'intelligenza), la forma è quella di una S, il che evoca del testo scorrevole sullo schermo di un computer.
Il cifrario utilizzato nella prima metà è costituito da un banale cifrario a sostituzione, mentre nella seconda metà sarebbe presente un cifrario di Vigenère, ma le omissioni e gli errori di scrittura inseriti volutamente dall'ideatore dell'opera complicano il lavoro di qualsiasi critto analista e di qualsiasi software di decriptazione.
Si tratta di un enigma nell'enigma: come dichiarato da Sanborn stesso solo dopo che tutta la scultura sarà stata decifrata, sarà possibile accedere all'enigma vero e proprio.

Diversi crittanalisti si sono cimentati nella traduzione: il primo ad aver annunciato pubblicamente di essere

riuscito a tradurre le prime tre sezioni è stato James Gillogly, un esperto informatico sud californiano.
Sia la CIA (tramite David Stein, che avrebbe svolto il lavoro con carta e penna) che l'NSA, sarebbero riuscite a decifrare le prime tre parti, ma sembra che per la quarta non ci sia niente da fare.

Aneddoti e curiosità

PRIMA GUERRA MONDIALE

- Sin dall'ottobre 1914 i crittanalisti francesi erano in grado di decrittare i messaggi radio tedeschi, mentre quelli austriaci erano perfettamente in grado di intercettare le comunicazioni dei Russi, che non si preoccupavano neppure di cifrarle (Battaglia di Tannenberg, Agosto 1914).
  Solo dopo la Rivoluzione, iniziarono a crittare i messaggi. I tedeschi impiegarono pochissimo tempo a decrittarli.
- Il capo dell'ufficio crittologico della marina britannica, Sir Alfred Ewing, aveva istituito la cosiddetta Room 40, dove si decrittavano i radiomessaggi della marina tedesca.
- Negli USA per molto tempo è esistito un unico reparto crittologico: quello dei laboratori Riverbanks di Chicago.
- La situazione dell'Italia era, come al solito, molto arretrata rispetto agli altri Paesi. Nella prima fase della Guerra si appoggiarono all'ufficio cifra francese, la cui collaborazione era stata garantita da Jules Cambon nel Patto di Londra.
  All'inizio del 1916 l'Italia aveva la possibilità di intercettare, ma non di decrittare i messaggi.
  Grazie a Luigi Sacco nacque un Ufficio Crittografico autonomo, che portò alla decrittazione di alcuni cifrari austriaci e tedeschi.
  Ciò consentì di fronteggiare l'offensiva austriaca sul Piave (1918).
  I cifrari Italiani erano comunque molto deboli, venivano facilmente decrittati dagli austriaci e vennero definitivamente abbandonati dopo la disfatta di Caporetto nel 1917.

SECONDA GUERRA MONDIALE

- Un primo tentativo di forzatura della macchina Enigma fu da parte dell'ufficio cifra polacco, ma solo gli Inglesi con Turing poterono portare a compimento l'opera decifrando, grazie agli scienziati impiegati nel progetto ULTRA, anche i messaggi cifrati con la macchina di Lorenz.
- Durante lo sbarco in Normandia Eisenhower e Montgomery erano in grado di leggere tutti i messaggi degli alti comandi tedeschi.
- Sul fronte del Pacifico, gli americani avevano realizzato Magic (1940), una macchina in grado di decrittare i messaggi giapponesi cifrati con la macchina Purple. A tal proposito due episodi:
  - Battaglia delle Midway (furono intercettati i piani dell'ammiraglio Yammamoto in procinto di attaccare a sorpresa le isole Midway. Inoltre fu decrittato un messaggio concernente un viaggio di Yammamoto, e il suo aereo venne abbattuto.)
  - Alcune fonti incerte affermano che gli americani sapevano in anticipo dell'attacco a Pearl Harbour, ma decisero di non impedirlo. Altre fonti asseriscono che gli alleati sapessero di un probabile attacco, ma non ne conoscevano la località.
- In Italia la macchina del generale Sacco era andata distrutta per motivi ignoti. Un successo di natura spionistica, più che crittoanalitica, si ebbe nel 1941: i Servizi Segreti italiani trafugarono all'ambasciata Americana di Roma il cifrario Black.