Introduzione alla crittografia

A. Ferrari

Terminologia

- Steganografia: occultamento del messaggio
- Crittografia: occultamento del significato del messaggio
- Messaggio in chiaro: testo da crittare
- Chiave: informazione usata come parametro in un algoritmo crittografico
- Crittoanalisi: scienza dell'interpretazione del messaggio di cui si ignora la chiave

Steganografia

- Il termine steganografia è composto dalle parole greche στεγανός (nascosto) e γραφία (scrittura) e individua una tecnica risalente all'antica Grecia che si prefigge di nascondere la comunicazione tra due interlocutori.
- La steganografia si pone come obiettivo di mantenere nascosta l'esistenza di dati.
- Un esempio: LSB (least significant bit, bit meno significativo) è la tipologia di steganografia più diffusa. Si basa sulla teoria secondo la quale l'aspetto di un'immagine digitale ad alta definizione non cambia se i colori vengono modificati in modo impercettibile.
- Ogni pixel è rappresentato da un colore differente, cambiando il bit meno significativo di ogni pixel, il singolo colore non risulterà variato e il contenuto dell'immagine sarà preservato.
- L'insieme dei bit meno significativi di ogni pixel rappresenta il messaggio che si vuole mantenere nascosto.

Wikipedia

Crittografia

- La parola crittografia deriva dall'unione di due parole greche: κρυπτός (kryptós) che significa "nascosto", e γραφία (graphía) che significa "scrittura".
- La crittografia tratta dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile a persone non autorizzate a leggerlo.
- Un tale messaggio si chiama comunemente crittogramma.
- Lo studio della crittografia e della crittanalisi si chiama comunemente crittologia.

Wikipedia

Chiave

- In crittografia una chiave è un'informazione usata come parametro in un algoritmo crittografico.
- Le chiavi sono utilizzate in molte applicazioni crittografiche e sono l'unico dato che è davvero necessario tenere segreto.
- La dimensione della chiave, generalmente misurata in bit, dipende dal particolare algoritmo usato.
- Esiste un metodo per stimare la lunghezza minima della chiave da utilizzare e si basa sulla simulazione di un attacco di forza bruta: una chiave di n bit avrà 2^n chiavi distinte e non conoscendo quale chiave sia stata usata bisognerà provarle tutte fino ad individuare la chiave giusta.

Wikipedia

Crittoanalisi

- Per crittoanalisi (dal greco kryptós, "nascosto", e analýein, "scomporre") si intende lo studio dei metodi per ottenere il significato di informazioni cifrate senza avere accesso all'informazione segreta che è di solito richiesta per effettuare l'operazione.
- Tipicamente si tratta di trovare una chiave segreta. La crittoanalisi è la "controparte" della crittografia, vale a dire lo studio delle tecniche per occultare un messaggio, ed assieme formano la crittologia, la scienza delle scritture nascoste.

Wikipedia

Storia della crittografia

Crittografia classica
(dall'antichità al 1975)

- Metodi antichi
  - la scitala spartana,
  - la scacchiera di Polibio,
  - il codice atbash
  - il codice di Cesare.
- Rinascimento
  - Blaise Vigenère
- XX secolo
  - la macchina Enigma (usata dai tedeschi durante la Seconda Guerra Mondiale),
  - il DES (Data Encryption Standard)

Crittografia Moderna

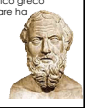
- La crittografia moderna nasce nel 1975 con un articolo di Diffie & Hellman nel quale si proponeva un **nuovo protocollo per lo scambio delle chiavi**, che è e rimane il vero tallone d'Achille della crittografia classica.
- Un aspetto fondamentale è la possibilità dell'applicazione alla trasmissione sicura di dati fra entità che non hanno concordato preventivamente le chiavi, e che non necessariamente si fidano l'una dell'altra.
- Esempi:
  - RSA

Un esempio di steganografia

Per il timore di ciascuna di queste cose [Aristagora] meditava una rivolta. Accadde anche che gli arrivasse da Susa, da parte di Istieo, un uomo con la testa tatuata che gli annunciava di ribellarsi al re. Infatti Istieo, volendo segnalare ad Aristagora di ribellarsi, non aveva d'altra parte nessun modo sicuro per farlo, dal momento che le strade erano sorvegliate e quindi, avendo rasato il capo del più fedele dei servi, vi incise dei segni, e attese che gli ricrescessero i capelli; e non appena gli furono cresciuti lo mandava a Mileto, ordinandogli soltanto, una volta giunto a Mileto, di dire ad Aristagora di guardare sul suo capo dopo avergli rasato i capelli. E i segni indicavano, come ho detto prima, rivolta.

Erodoto, Storie

Erodoto (greco: Ἡ ρόδ ο τ ος, Herodotos; Alicarnasso, 484 a.C. – Thurii, 425 a.C.) è stato uno storico greco antico, famoso per aver descritto paesi e persone da lui conosciute in numerosi viaggi. In particolare ha scritto a riguardo dell'invasione persiana in Grecia nell'opera Storie (Ἱστορίαι, Istoriai)..



Crittografia Classica

(dall'antichità al 1975)

500-600 a.c.
cifrario ATBASH

- L'atbash è un semplice cifrario a sostituzione monoalfabetica in cui la prima lettera dell'alfabeto è sostituita con l'ultima, la seconda con la penultima, e così via, "invertendo" l'ordine alfabetico delle lettere.
- Testo in chiaro:
  - `ABCDEFGHIJKLMNOPQRSTUVWXYZ`
  - Testo cifrato:
  - `ZYXWVUTSRQPONMLKJIHGFEDCBA`
  - Un esempio:
  - `PIANO LAUREE SCIENTIFICHE`
  - `KRZML OZFIVV HXRVMGRURXSV`

400 a.c. Scitala spartana

- Una scitala (dal greco $\sigma\kappa\upsilon\tau\acute{\alpha}\lambda\eta$ = bastone) era una piccola bacchetta utilizzata dagli Spartani per trasmettere messaggi segreti.
- Il messaggio veniva scritto su di una striscia di pelle arrotolata attorno alla scitala, come se fosse stata una superficie continua.
- Una volta srotolata e tolta dalla scitala la striscia di pelle, era impossibile capire il messaggio.
- La decifrazione era invece possibile se si aveva una bacchetta identica alla scitala del mittente: vi si arrotolava nuovamente la striscia di pelle ricostruendo la primitiva posizione.
- Si tratta del più antico metodo di crittografia per trasposizione conosciuto.

150 a.c. Scacchiera di Polibio

- La scacchiera originale è costituita da una griglia composta da 25 caselle ordinate in 5 righe ed altrettante colonne.
- Le lettere dell'alfabeto vengono inserite da sinistra a destra e dall'alto in basso.
- Le righe e le colonne sono numerate: tali numeri sono gli indici o "coordinate" delle lettere costituenti il messaggio in chiaro.
- Esempio
  - PIANO LAUREE SCIENTIFICHE
  - FGDFAAFDFFDXAAGFFXAVAVGAAFDFAVFDGDDFAXDFAFDDAV

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

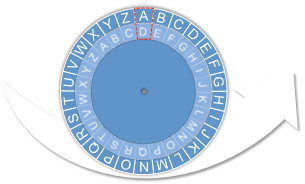
Substitution matrix

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

50-60 a.c.
Il metodo di Cesare

- Il cifrario di Cesare è un cifrario a sostituzione monoalfabetica in cui ogni lettera del testo in chiaro è sostituita nel testo cifrato dalla lettera che si trova un certo numero di posizioni successive nell'alfabeto.
- Questi tipi di cifrari sono detti anche cifrari a sostituzione o cifrari a scorrimento a causa del loro modo di operare: la sostituzione avviene lettera per lettera, scorrendo il testo dall'inizio alla fine.
- In particolare, Cesare utilizzava uno spostamento di 3 posizioni (la chiave era dunque 3).
- Un esempio:
  - PIANO LAUREE SCIENTIFICHE
  - SLDQR ODXUHH VFLHQWLLFKH

Cifrari a scorrimento



Debolezze
del metodo di Cesare

- Il metodo di Cesare ha due principali debolezze:
  - è sensibile all'**analisi di frequenza**
  - sono possibili solo **poche chiavi** diverse (n – 1) se n è il numero di caratteri dell'alfabeto.
- Chi intercetta un messaggio cifrato con il metodo di Cesare può limitarsi a provare successivamente tutte le possibili chiavi di cifratura e trovare il testo in chiaro in un tempo ragionevolmente breve (attacco a **forza bruta**).

Brute force

- Il metodo "forza bruta" (ricerca esaustiva della soluzione) è un algoritmo di risoluzione di un problema che consiste nel verificare tutte le soluzioni teoricamente possibili fino a che si trova quella effettivamente corretta.
- Il suo principale fattore positivo è che consente teoricamente sempre di trovare la soluzione corretta, ma per contro è sempre la soluzione più lenta o dispendiosa.
- Fu il metodo utilizzato dal controspionaggio polacco e poi inglese per decifrare i messaggi tedeschi della macchina Enigma. Per ottenere il risultato infatti, essi utilizzarono la famosa Bomba, una speciale macchina calcolatrice in grado di sottoporre il messaggio cifrato ad un attacco di forza bruta, fino a trovare la soluzione. La macchina venne poi perfezionata dagli inglesi, grazie al contributo del grande matematico Alan Turing.

1586 Il cifrario di Vigenère

- E' il più semplice dei cifrari polialfabetici.
- Pubblicato nel 1586, il cifrario di Blaise de Vigenère fu **ritenuto per secoli inattaccabile**.
- Si può considerare una generalizzazione del cifrario di Cesare: invece di spostare sempre dello stesso numero di posti la lettera da cifrare, questa viene spostata di un numero di posti variabile ma ripetuto, determinato in base ad una parola chiave da scrivere ripetutamente sotto il messaggio, carattere per carattere.
- Un esempio:
  - PIANO LAUREE SCIENTIFICHE
  - ITIS
  - XBIFW EIMZXM KKBMFBBNAKAM

Confronto Vigenère - Cesare

- Il metodo di Vigenère rendere impossibile l'analisi di frequenza perché le lettere più frequenti saranno codificate con lettere diverse da colonna a colonna, con il risultato di rendere quasi uguali le frequenze relative delle lettere del testo cifrato.
- Il metodo di Vigenère sembra essere molto più robusto di quello di Cesare perché il crittanalista ha due problemi:
  - determinare la lunghezza k della chiave
  - e poi la chiave stessa.
- Se l'alfabeto ha n caratteri, vi sono n^k possibili chiavi di cifratura, mentre sono solo n!/(n − k)! se vogliamo che i caratteri siano tutti diversi fra loro.
- Anche da questo punto di vista il metodo di Vigenère è migliore di quello di Cesare.

Cryptographia ad usum Delphini – A.Zaccagnini

Debolezza del metodo di Vigenère

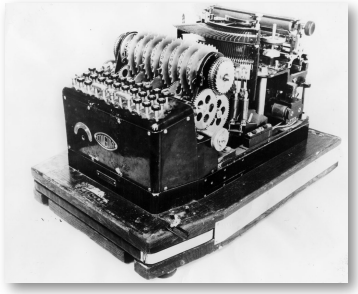
- Questo metodo è stato considerato sicuro per alcuni secoli, finche un'analisi statistica più raffinata, di Kasinski, mostrò che è possibile "indovinare" la lunghezza k della chiave di cifratura, riducendo il problema della decifratura a k problemi di decifratura del metodo di Cesare.
- L'analisi si basa sul fatto che in ogni lingua vi sono alcune combinazioni di due lettere piuttosto frequenti: se due istanze di questa coppia di lettere compaiono nel testo in chiaro ad una distanza che è un multiplo della lunghezza della chiave, saranno cifrate allo stesso modo, perché vanno a finire nelle stesse colonne.

Cryptographia ad usum Delphini – A. Zaccagnini

La macchina Enigma

- Macchina elettromeccanica tedesca ENIGMA usata nella seconda guerra mondiale.
- Composta da ruote con i caratteri incisi sul bordo, e con contatti elettrici in corrispondenza delle lettere in entrambi i lati.
- Il testo in chiaro, digitato su una tastiera, veniva riprodotto utilizzando i caratteri della prima ruota, la quale a sua volta costruiva un nuovo alfabeto utilizzando i caratteri della seconda, e poi della terza, e così via ... Tutte le ruote, e potevano essere parecchie, venivano "scalate", in modo che la sostituzione delle lettere fosse ogni volta diversa.
- La chiave consisteva nel settaggio iniziale delle ruote, che potevano essere posizionate in una quantità di posizioni diverse tanto alta quante più erano le ruote utilizzate.
- Questo meccanismo è facile da costruire via software e abbastanza sicuro, può tuttavia essere infranto. Fu brillantemente attaccato dal matematico polacco Marin Rejewsky che con il suo lavoro permise di decifrare numerosi messaggi militari tedeschi, un fattore che probabilmente contribuì alla vittoria finale degli alleati.

Enigma

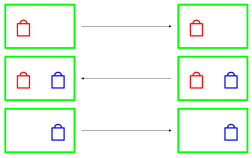


1976 DES

- Il Data Encryption Standard (DES) è un algoritmo di cifratura scelto come standard per il governo degli Stati Uniti d'America nel 1976 e in seguito diventato di utilizzo internazionale.
- Si basa su un algoritmo a chiave **simmetrica** con chiave a 56 bit.
- DES è considerato insicuro per moltissime applicazioni. La sua insicurezza deriva dalla chiave utilizzata per cifrare i messaggi, che è di soli 56 bit.
- Nel gennaio del 1999 si dimostrò pubblicamente la possibilità di individuare una chiave di crittazione in 22 ore e 15 minuti.
- L'algoritmo è ritenuto sicuro reiterandolo 3 volte nel Triple DES.
- DES è stato sostituito dall'Advanced Encryption Standard (AES) un nuovo algoritmo che elimina molti dei problemi del DES.

Il protocollo del doppio lucchetto

- A mette il suo messaggio per B in una scatola, che chiude con un lucchetto e invia a B.
- B mette il suo lucchetto alla scatola e la rispedisce ad A.
- A toglie il suo lucchetto e rispedisce la scatola a B.
- B toglie il suo lucchetto e legge il messaggio.
- La scatola non viaggia mai senza lucchetto
- Ne A ne B ha dovuto inviare all'altro la chiave del proprio lucchetto.
- E' possibile comunicare con sicurezza senza dover effettuare un preventivo scambio delle chiavi ! ! !



Crittografia Moderna

1975 …

1975 Diffie-Hellman-Merkle

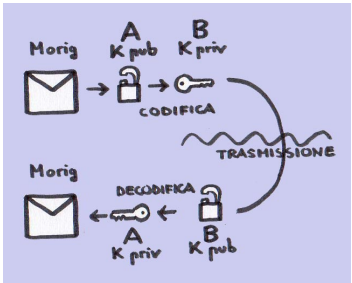
- Tutti i sistemi di cifratura classici sono detti a chiave segreta ed utilizzano la stessa chiave sia per cifrare che per decifrare.
- Questo costituisce un problema non indifferente se pensiamo all'utilizzo della crittografia per la comunicazione a distanza, infatti le due parti devono riuscire in qualche modo a scambiarsi la chiave con la certezza che nessuno ne venga a conoscenza.
- La soluzione a questo tipo di problema fu proposta nel 1975 da Whitfield Diffie e Martin Hellman, col tributo di Ralph C. Merkle, che ebbero un'intuizione che rivoluzionò il mondo della crittografia.

Crittografia a chiave pubblica

- Diffie ed Hellman pensarono ad un sistema **asimmetrico**, basato su l'uso di due chiavi generate in modo che sia impossibile ricavarne una dall'altra.
- Le due chiavi vengono chiamate **pubblica** e **privata**: la prima serve per cifrare e la seconda per decifrare.
- Una persona che deve comunicare con un'altra persona cifra il messaggio con la chiave pubblica del destinatario, che una volta ricevuto il messaggio lo decifra con la chiave segreta personale.
- Ogni persona possiede una coppia di chiavi, quella pubblica può essere distribuita e resa di pubblico dominio perché consente solo di cifrare il messaggio, mentre quella privata deve essere conosciuta solo da una persona.
- Il problema è quello di trovare il modo di implementare matematicamente questo sistema, riuscire cioè a creare due chiavi per cui **non sia possibile dedurre quella privata conoscendo quella pubblica**.

Il meccanismo in azione

Sicurezza del mittente e del destinatario



1977 RSA

- L'algoritmo a **chiave asimmetrica** è stato pubblicamente descritto nel 1977 da Ron **Rivest**, Adi **Shamir** e Leonard **Adleman** al **M**assachusetts **I**nstitute of **T**echnology. La sigla RSA deriva dalle iniziali dei cognomi dei tre creatori.
- L'algoritmo è basato su particolari proprietà formali dei numeri primi con alcune centinaia di cifre.
- Non è sicuro da un punto di vista matematico teorico, in quanto esiste la possibilità che tramite la conoscenza della chiave pubblica si possa decrittare un messaggio, ma l'enorme mole di calcoli e l'enorme dispendio in termini di tempo necessario per trovare la soluzione, fa di questo algoritmo un sistema di affidabilità pressoché assoluta.
- Una variante del sistema RSA è utilizzato nel pacchetto di crittografia Pretty Good Privacy (PGP).
- L'algoritmo RSA costituisce la base dei sistemi crittografici su cui si fondano i sistemi di sicurezza informatici utilizzati sulla rete Internet per autentificare gli utenti.

RSA Funzionamento (semplificato)

- A deve spedire un messaggio segreto a B.
- B sceglie due numeri primi molto grandi (per esempio da 300 cifre) e li moltiplica con il suo computer (impiegando meno di un secondo).
- B invia il numero che ha ottenuto ad A. *Chiunque può vedere questo numero.*
- A usa questo numero per cifrare il messaggio
- A manda il messaggio cifrato a B, *chiunque può vederlo ma non decifrarlo*
- B riceve il messaggio e utilizzando i due fattori primi che solo lui conosce lo decifra.
- A e B hanno impiegato pochi secondi a cifrare e decifrare, ma chiunque avesse intercettato le loro comunicazioni impiegherebbe troppo tempo per scoprire i due fattori primi, con cui si può decifrare il messaggio.
- In realtà A e B si scambieranno con questo sistema una chiave segreta (che non occupa molto spazio), che poi useranno per comunicare tra loro usando un sistema a crittografia simmetrica, più semplice e veloce.

Sicurezza di RSA

- Per quanto riguarda l'algoritmo RSA l'attacco a forza bruta (ovvero ottenere i due numeri primi usati per creare la chiave pubblica), è una procedura lentissima.
- L'attacco più veloce è durato 5 mesi utilizzando 80 processori da 2,2GHz
- Questi dati consentono di dire che l'algoritmo è sufficientemente sicuro.

Sicurezza

nel mondo internet

1994 - SSL (Secure Socket Layer)

- Transport Layer Security (TLS) e il suo predecessore Secure Sockets Layer (SSL) sono dei protocolli crittografici che permettono una comunicazione sicura e una integrità dei dati su reti TCP/IP come, ad esempio, internet.
- TLS e SSL cifrano la comunicazione dalla sorgente alla destinazione (end-to-end) sul livello di trasporto.
- Diverse versioni del protocollo sono ampiamente utilizzate in applicazioni come i browser, l'E-mail, messaggistica istantanea e VOIP.
- TLS è un protocollo standard IETF che è sviluppato sulla base del precedente protocollo SSL da Netscape

1999 - WEP (Wired Equivalent Privacy)

- Il Wired Equivalent Privacy è parte dello standard IEEE 802.11 (ratificato nel 1999) e in particolare è quella parte dello standard che specifica il protocollo utilizzato per rendere sicure le trasmissioni radio delle reti Wi-Fi.
- WEP è stato progettato per fornire una sicurezza comparabile a quelle delle normali LAN basate su cavo.
- WEP adesso viene considerato un sottoinsieme del più sicuro standard Wi-Fi Protected Access (WPA) rilasciato nel 2003 e facente parte dell'IEEE 802.11i.
- Il WEP viene ritenuto il minimo indispensabile per impedire a un utente casuale di accedere alla rete locale.

2003 - WPA (Wi-fi Protected Access)

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

CrypTool

- CrypTool è un software libero e open source di e-learning per Microsoft Windows che illustra i concetti fondamentali della crittografia in via pratica.
- Scritto in C++, è disponibile in inglese, in tedesco, in spagnolo e in polacco.
- La versione scritta in Java, che prende il nome di JCrypTool, è disponibile da agosto 2007.
- http://www.cryptool.de/index.php/en