Il mestiere del crittografo

Massimiliano Sala, Univ. di Trento

Pisa, 31 Marzo 2017

Il crittografo di corte

Il crittografo antico

Nell'antichità e fino all'avvento dell'età moderna, il mestiere del crittografo è sempre stato appannaggio di una *elite* vicina al sovrano, tanto da essere spesso indicato come *"crittografo di corte".*

Una figura avvolta nel mistero e una strada percorribile da pochi iniziati.

Polibio

Polibio di Megalopoli (206-124 a.C.), noto storico greco, ci lascia nelle **Storie** una descrizione parziale di un codice che rappresenta ciascuna lettera dell'alfabeto greco tramite una coppia di numeri da uno a cinque (Hist. X.45.6).

Molti trattati antichi di crittografia sono andati persi (o nascosti)?

Leon Battista Alberti

Leon Battista Alberti (1404-1472) ha un'impostazione radicalmente diversa rispetto ai suoi predecessori. Pur lavorando per il Papato, scrive il

De Componendis Cifris

che è arrivato fino a noi è che viene considerato da molti la prima **importante** opera crittografica

Leon Battista Alberti

Lo storico americano David Kahn (quindi non di parte) enuncia due primati del **De Cifris** :

1. il primo trattato occidentale che parla di **crittoanalisi**,

2. l'invenzione della sostituzione **polialfabetica**.

De Componendis Cifris

Personalmente sono colpito dal **metodo espositivo** presente nel **De Cifris.**

Il libro è scritto per farsi capire e per essere usato in pratica.

Purtroppo, storicamente rimane secondario e i sistemi inventati da Alberti prenderanno il nome di sistemi di **de Vigenère** (un secolo posteriore).

Il crittografo militare

Fino all'800

Sebbene i generali abbiano **sempre** usato algoritmi cifranti per scambiarsi informazioni, è con la nascita degli **eserciti moderni**, che ci si rende conto dell'importanza di poter proteggere i messaggi da inviare a **numerosi** distaccamenti.

La **dimensione** dei nuovi eserciti e la loro **diffusione territoriale** rende superato l'uso di **pochi** esperti crittografi.

La crittografia viene studiata

Nell'800 vi è un'esplosione di **trattati sulla crittografia**, spesso di origine militare, e sempre più ufficiali delle forze armate sono iniziati alla misteriosa arte.

Addirittura vengono fondate delle **riviste** dedicate, come

La Cryptographie Militaire

dove Kerckhoffs pubblica i suoi famosi **principi**

Le macchine cifranti

Dopo la Prima Guerra Mondiale gli eserciti non possono più affidarsi a persone che manualmente cifrano e decifrano.
Si realizza una **demarcazione:**

1. chi **progetta** gli algoritmi e le macchine che li eseguono, che necessita di formazione scientifica e matematica
2. chi **opera** sulle macchine cifranti,
   a cui basta capire come usarle

Il crittografo oggi

Crittografia e Matematica

Dal discorso di apertura di Adrian A. Albert della

Conference of the American Mathematical Society - 1939

We shall see that cryptography is more than a subject permitting mathematical formulation for indeed it would not be an exaggeration to state that abstract cryptography is identical with abstract mathematics

Separazione dei ruoli dei crittografi

Ormai vi è una netta separazione tra i ruoli. Ne elenco alcuni:

1. progettista di nuovi algoritmi
2. l'implementatore di nuovi algoritmi
3. il crittoanalista
4. il certificatore
5. progettista di nuovi **protocolli** o **sistemi**
6. **.....**

Gli ambiti

Gli ambiti in cui le competenze crittografiche sono richieste:

1. il tradizionale ambito militare (diplomatico/governativo)
2. i pagamenti elettronici
3. le comunicazioni private su Internet
4. lo scambio di file su Internet (cloud)
5. IoT (Internet of Thing) -> automative
6. il riconoscimento di utenti/cittadini/persone
7. .....

Il crittografo in Italia

CryptoLabTN

I nostri laureati

Ogni anno, circa 15 ragazzi del curriculum

Coding Theory and Cryptography

del Dipartimento di Matematica dell'Università di Trento prendono la Laurea Magistrale con una tesi inerente alle tematiche del curriculum, spesso con stage in azienda.

La maggior parte di essi è assunta nei primi mesi dopo la Laurea (alcuni anche prima).

I nostri mestieri

Dal nostro osservatorio, tre sono i principali impieghi per un crittografo in Italia:

- programmatore di algoritmi crittografici (spesso su *mobile*)
- ideatore di sistemi informatici in cui la crittografia gioca un ruolo importante
- analista di sistemi informatici (con crittografia)

Programmatore di sistemi basati sulla crittografia

Un programmatore di algoritmi crittografici è spesso inserito in un team ideatore di sistemi informatici e sviluppa concretamente le sue idee, dialogando in maniera costruttiva con informatici e ingegneri.

Questa è forse la figura più richiesta in ambito aziendale.

Ideatore di sistemi

Un ideatore di sistemi informatici in cui la crittografia giochi un ruolo importante, collabora con altri specialisti (ad esempio informatici) allo scopo di ideare nuovi sistemi ad hoc per garantire la sicurezza o rispondere a nuove necessità nell'ambito della privacy.

Le aziende che sviluppano prodotti, ad esempio per il mondo bancario, sono sempre alla ricerca di queste figure.

Analista di sistemi

Un analista di sistemi si occupa di studiare la sicurezza dei sistemi crittografici garantita dalla crittografia sottostante.

Ad esempio considera qual è la complessità minima per rompere un cifrario.

Molte realtà, come le grandi banche, hanno bisogno di analisti di sistemi, prima di decidere quale software comprare.