

CRITTOGRAFIA CLASSICA E QUANTISTICA
a.a. 2020/2021

CRITTOGRAFIA CLASSICA E QUANTISTICA

1201145 - DANIELE GIACHETTO



Indice

1	La segretezza nella comunicazione	2
1.1	Kryptós graphía	2
1.2	La legge di Kerckhoffs	2
2	Il passato della crittografia	2
2.1	La trasposizione	2
2.2	La sostituzione	3
2.2.1	La sostituzione monoalfabetica	3
3	L'inizio della crittografia moderna	3
3.1	La sostituzione polialfabetica	3
3.2	Il cifrario di Vigenère	3
3.3	Un sistema di cifratura perfetto	4
3.4	Enigma e codice Purple	4
4	Tempi moderni	4
4.1	Scambio di chiavi Diffie-Hellman	5
4.2	L'algoritmo RSA	5
4.3	Un nuovo orizzonte	5
5	Crittografia quantistica	5
5.1	Algoritmo di Shor	5
5.2	Introduzione ai qubit	6
5.3	Gli stati del qubit	6
5.4	Il protocollo BB84	6
5.5	Le sfide da superare	7
6	Fonti	8

1 La segretezza nella comunicazione

1.1 Kryptós graphía

La crittografia è la branca della scienza che tratta i metodi per rendere un messaggio inintelligibile per chiunque non sia in possesso di determinati strumenti.

Lo scopo di questo elaborato è quello di esporre la storia e l'evoluzione di questa disciplina, partendo dai suoi primi usi documentati fino ad arrivare al suo presente, in continuo e costante sviluppo.

1.2 La legge di Kerckhoffs

Nel 1883 il linguista olandese Auguste Kerckhoffs formalizzò in un articolo di una rivista militare delle regole alle quali deve sottostare un buon sistema crittografico. Le regole sono le seguenti:

- Un sistema crittografico deve essere materialmente, se non matematicamente, indecifrabile.
- Il sistema non deve esigere la segretezza, e deve poter cadere in mani estranee senza inconvenienti.
- Deve essere possibile scambiare e memorizzare la chiave senza bisogno di note scritte, ed essa deve poter essere cambiata o modificata a piacere degli utenti.
- Il sistema deve essere applicabile alla corrispondenza telegrafica.
- Il sistema dev'essere portatile ed il suo utilizzo o il suo funzionamento non devono richiedere l'impiego di un gran numero di persone.
- Infine, date le circostanze nelle quali verrà presumibilmente utilizzato, il sistema non deve richiedere la conoscenza di una lunga serie di regole né essere di difficile applicazione.

Mentre alcuni di questi principi risultano oggi superati, alcuni come il secondo risultano di estrema importanza.

2 Il passato della crittografia

2.1 La trasposizione

Uno dei primi esempi storicamente attestati di cifratura fu la scitola spartana, un bastone nel quale veniva avvolto un messaggio in chiaro e la sua trasposizione sul bastone diveniva il messaggio cifrato. Per trasposizione dunque si intende un metodo di cifratura che si basa dunque sulla traslazione, secondo un determinato schema, del messaggio originario.

Molti si dilettarono nella creazione di sistemi crittografici basati su questo concetto, uno degli esempi più noti è la *scacchiera di Polibio* pensata nel III secolo a.C. dalla quale il *cifrario di Playfair* realizzato nel 1854 prese forte ispirazione.

2.2 La sostituzione

I cifrari a sostituzioni sono tra le tecniche crittografiche classiche che hanno avuto più vita e successo. Uno dei primi e più famosi esempi si trova verso la fine della repubblica romana con il *cifrario di Cesare*, in esso ogni lettera corrispondeva alla lettera un numero 'k' di posizioni successive o precedenti alla lettera originaria.

2.2.1 La sostituzione monoalfabetica

Il *cifrario di Cesare* è un ottimo esempio di sostituzione monoalfabetica, ovvero un sistema che utilizza un solo alfabeto per il testo in chiaro ed una permutazione di esso per il testo cifrato.

Questo sistema ebbe un grande successo ma venne reso obsoleto dallo scienziato e teologo arabo Al-Kindi che sviluppò il metodo chiamato *analisi delle frequenze*.

L'*analisi delle frequenze* si basa sulla considerazione che, in qualsiasi lingua, le lettere si ripetono con frequenze ben definite all'interno di un testo sufficientemente lungo. Da questa considerazione è facile poter risalire al testo originale. Prendendo un esempio pratico, se si ha in un testo cifrato una lettera con maggior frequenza sappiamo che essa può essere la sostituzione della lettera 'e' oppure della lettera 'i'.

3 L'inizio della crittografia moderna

3.1 La sostituzione polialfabetica

Tra il 1460 ed il 1470 Leon Battista Alberti scrisse il *Trattato della cifra*, un testo da lui non divulgato per mantenere la segretezza delle nozioni scritte. In questo trattato spicca una sua geniale creazione, il *disco cifrante*. Questa macchina fu rivaleggiata solamente quattro secoli dopo da Thomas Jefferson con il suo *cilindro di Jefferson*. Queste macchine erano entrambe esempi di sostituzione polialfabetica, ovvero una sostituzione nella quale si fa uso di molteplici alfabeti per sostituire le lettere del messaggio, utilizzando un determinato ordine che costituisce la chiave.

3.2 Il cifrario di Vigenère

Il *cifrario di Vigenère* si può considerare una generalizzazione del *cifrario di Cesare*, invece di spostare dello stesso numero la lettera da cifrare, questa viene spostata di un numero di posti variabile ma ripetuto. Per portare un esempio di facile comprensione mentre con il primo cifrario con chiave 3 il testo 'SPQR' diventa 'VSTU' con

il secondo con chiave BD la prima lettera viene spostata di una posizione, la seconda di tre e così ripetuto fino a fine testo da cifrare, portando 'SPQR' a diventare 'TSRU'.

3.3 Un sistema di cifratura perfetto

In realtà anche il *cifrario di Vigenère* può essere sconfitto da una più profonda ed attenta analisi delle frequenze, questo per due grandi difetti della cifratura in questione: la ripetizione della chiave per tutta la lunghezza del testo e l'uso della stessa chiave per più testi.

Rimediando a questi difetti nasce il *blocco monouso*, inventato nel 1917-18 contemporaneamente da Gilbert Vernam e Joseph Mauborgne (il quale pose la condizione sulla casualità della generazione della chiave), l'unico sistema crittografico la cui sicurezza è comprovata da una dimostrazione matematica. Questo sistema risulta tanto sicuro quanto scomodo nell'utilizzo per comunicazioni quotidiane, le difficoltà insite nella distribuzione delle chiavi lo confina ad un utilizzo saltuario, riservato per messaggi estremamente importanti.

3.4 Enigma e codice Purple

Durante la seconda guerra mondiale servivano macchine cifranti capaci di garantire una forte sicurezza ed anche rapidità nella trasmissione dei messaggi. Da queste esigenze nascono le due macchine cifranti con cui gli alleati si confrontarono durante il conflitto: *Enigma* e *codice Purple*.

In Germania tra il 1910 e 1920 l'ingegnere tedesco Arthur Scherbius realizzò la *macchina Enigma*, una macchina elettromeccanica che ad ogni battito riceve un impulso elettrico che attraversa dei dischi cifranti (cifratura polialfabetica). A seconda della lettera premuta e della posizione del disco in quel momento viene stampata una lettera diversa, permettendo ad esempio di cifrare la lettera 'A' come 'S' alla sua prima battitura e come 'B' alla seconda. La controparte giapponese di *Enigma* era la macchina cifrante chiamata dagli americani *codice Purple*, una macchina ispirata da *Enigma* stessa.

Sia gli inglesi con *Enigma* che gli americani con *codice Purple* si avvalsero di opportune macchine in grado di ridurre i tempi di decifrazione: questa fu la prima volta che si vide un uso massiccio di macchine di decifrazione per poter decifrare messaggi cifrati effettuati da macchine cifranti.

4 Tempi moderni

Poco dopo la fine della seconda guerra mondiale avvenne ufficialmente il passaggio di testimone: crittografia e crittoanalisi, da appannaggio quasi esclusivo di linguisti ed appassionati di logica ed enigmistica, divennero una vera e propria scienza grazie all'ausilio della matematica.

4.1 Scambio di chiavi Diffie-Hellman

Per comunicare in segretezza è necessario produrre, registrare e distribuire le chiavi. Di questo si occuparono Martin Hellman e Bailey Whitfield 'Whit' Diffie in un articolo pubblicato nel 1976. L'idea teorica alla base è voler fare in modo che due soggetti diversi possano costruire la stessa identica chiave senza mai comunicarla esplicitamente, questo scopo venne raggiunto con l'utilizzo di una combinazione di algebra modulare con funzioni esponenziali.

4.2 L'algoritmo RSA

Fino all'algoritmo *Diffie-Hellman* il concetto principale alla base dei metodi crittografici era l'associazione di una chiave per ogni lucchetto (il lucchetto rappresenta cifratura e decifrazione). L'idea che invece permea la base dell'*algoritmo RSA* è la seguente: mettere pubblicamente a disposizione il lucchetto per cifrare il messaggio da mandare e tenere senza mai distribuire la chiave per decifrarlo.

Nel 1977 Ronald Rivest, Adi Shamir e Leonard Adleman pubblicarono una tecnica nota come *algoritmo RSA* che concretizza l'idea descritta in precedenza. Questa tecnica si basa sulla difficoltà di fattorizzare grandi numeri interi, questa proprietà rende quindi l'algoritmo *materialmente inviolabile* anche se non *matematicamente inviolabile*, andando dunque a soddisfare tutt'oggi i sei principi di Kerckhoffs (§ 1.2). Grazie a queste sue caratteristiche l'*algoritmo RSA* è di ampio utilizzo nella comunicazione moderna.

4.3 Un nuovo orizzonte

Se qualcuno riuscisse a fattorizzare velocemente i numeri potrebbe rendere l'*algoritmo RSA* completamente insicuro.

Il pericolo non è solamente teorico ma bensì completamente reale e vicino, in laboratori sparsi in tutto il mondo si sta lavorando a pieno ritmo sui computer quantistici che porterebbero a risolvere il problema della fattorizzazione dei numeri.

5 Crittografia quantistica

La crittografia quantistica consiste in un approccio alla crittografia che utilizza proprietà della meccanica quantistica. **Data la complessità dell'argomento esso verrà semplificato il più possibile per permettere una più facile fruizione dell'elaborato.**



5.1 Algoritmo di Shor



L'algoritmo di Shor è un algoritmo ideato da Peter Shor nel 1994 per risolvere il problema della fattorizzazione dei numeri interi in numeri primi. Questo algoritmo lavora in maniera molto efficiente su computer quantistici e comprometterebbe

completamente la sicurezza di algoritmi come *RSA*. Questa scoperta ha aumentato l'interesse verso la costruzione dei computer quantistici e contemporaneamente ha anche facilitato la ricerca su nuovi sistemi crittografici basati sui computer quantistici. Questi sistemi presero il nome di *Crittografia "Post-Quantum"*, ovvero sistemi che hanno lo scopo di creare algoritmi che rimarranno sicuri dopo l'avvento e la diffusione degli elaboratori quantistici.

5.2 Introduzione ai qubit

Il *qubit* - bit quantistico - è l'unità fondamentale di informazione di un computer quantistico. Mentre l'informazione contenuta in un bit classico corrisponde soltanto all'alternativa vero/falso, nei *qubit* essa può corrispondere ai due stati $|0\rangle$ e $|1\rangle$ ed inoltre allo stato di sovrapposizione.

5.3 Gli stati del qubit

Prendiamo una semplificazione degli stati traendo spunto dall'idea della *sfera di Bloch*. Pensiamo ad un cerchio con una freccia al suo interno. La freccia all'interno del cerchio andrà a rappresentare un 1 oppure uno 0 a seconda della misurazione a cui sarà soggetta:

- **Misurazione verticale:** con questa misurazione verrà associata alla posizione della freccia a 90° un valore ed a 270° il suo opposto.
- **Misurazione orizzontale:** con questa misurazione verrà associata alla posizione della freccia a 0° un valore ed a 180° il suo opposto.


Qualsiasi altra posizione diversa dalle due descritte per misurazione, obbligherà la funzione d'onda a collassare su una delle due posizioni. Per esprimere il concetto in maniera più semplice: se la freccia puntasse in qualsiasi altra direzione che non sia una delle due desiderate (a seconda del tipo di misurazione) essa nel momento della osservazione sarà costretta ad andare su una delle due direzioni desiderate.



5.4 Il protocollo BB84

Una delle proprietà fondamentali della crittografia quantistica è l'impossibilità di intercettare un messaggio senza che le due parti in comunicazione se ne accorgano. Il *BB84* è un protocollo quantistico di distribuzione delle chiavi che utilizza a pieno questa proprietà.

Il server crea una chiave composta da bit e procede a trasformarla in un insieme di *qubit* scegliendo un orientamento casuale ed inviando infine il tutto all'utente. L'utente una volta ricevuto il messaggio andrà a misurare indovinando casualmente l'orientamento usato dal server per i singoli *qubit* ed otterrà dunque una sequenza di bit. Il server e l'utente andranno a questo punto a comparare l'orientamento

utilizzato per le osservazioni dei singoli *qubit* ed entrambi elimineranno dalla chiave tutti i bit osservati in maniera diversa tra i due. 

5.5 Le sfide da superare

Le sfide che questo nuovo approccio alla crittografia deve superare sono diverse ma non insormontabili:

- Il protocollo *BB84* ma anche protocolli troppo complessi per essere trattati come *EN94* si basano sulla trasmissione senza errori dei *qubit*, in una loro applicazione reale ci sarà ovviamente una perdita di dati da dover gestire.
- L'infrastruttura attuale di internet non permette la comunicazione quantistica, essa è possibile unicamente in reti quantistiche che sono attualmente utilizzate solamente da ricercatori.
- Vi è ancora una forte presenza di attacchi classici che continuano a funzionare anche con l'uso di computer quantistici. Attacchi come *Man in the Middle* oppure *Denial of Service* continuano ad essere temibili avversari: il primo per l'impossibilità di scovare un intruso una volta che esso è riuscito a fingersi una delle due parti ed il secondo perché l'impossibilità di origliare senza che nessuno si accorga, permetterebbe all'intruso di far ricominciare continuamente la procedura descritta nel protocollo *BB84*.



6 Fonti



Bibliografia

- Eva Filoramo, Alberto Giovannini e Claudia Pasquero, *Alla scoperta della crittografia quantistica*, prima edizione settembre 2006.

Sitografia

- Wikipedia, *Crittografia*,
<https://it.wikipedia.org/wiki/Crittografia>
- Wikipedia, *Crittografia Quantistica*,
https://it.wikipedia.org/wiki/Crittografia_quantistica
<https://it.wikipedia.org/wiki/Qubit>
[https://it.wikipedia.org/wiki/Principio_di_sovrapposizione_\(meccanica_quantistica\)](https://it.wikipedia.org/wiki/Principio_di_sovrapposizione_(meccanica_quantistica))
https://en.wikipedia.org/wiki/Bloch_sphere
- Nikolina Ilic, *The Ekert Protocol*,
<https://www.ux1.eiu.edu/~nilic/Nina's-article.pdf>
- Anastasia Marchenkova, *Difference between quantum annealing and universal gate quantum computers*,
<https://medium.com/quantum-bits/what-s-the-difference-between-quantum-annealing-and-universal-gate-quantum-computers-c5e5099175a1>