UNIVERSITÀ DEGLI STUDI DI MILANO
FACOLTÀ DI SCIENZE MATEMATICHE,
FISICHE E NATURALI

Carlo Ferretti

EnigmaBreaker

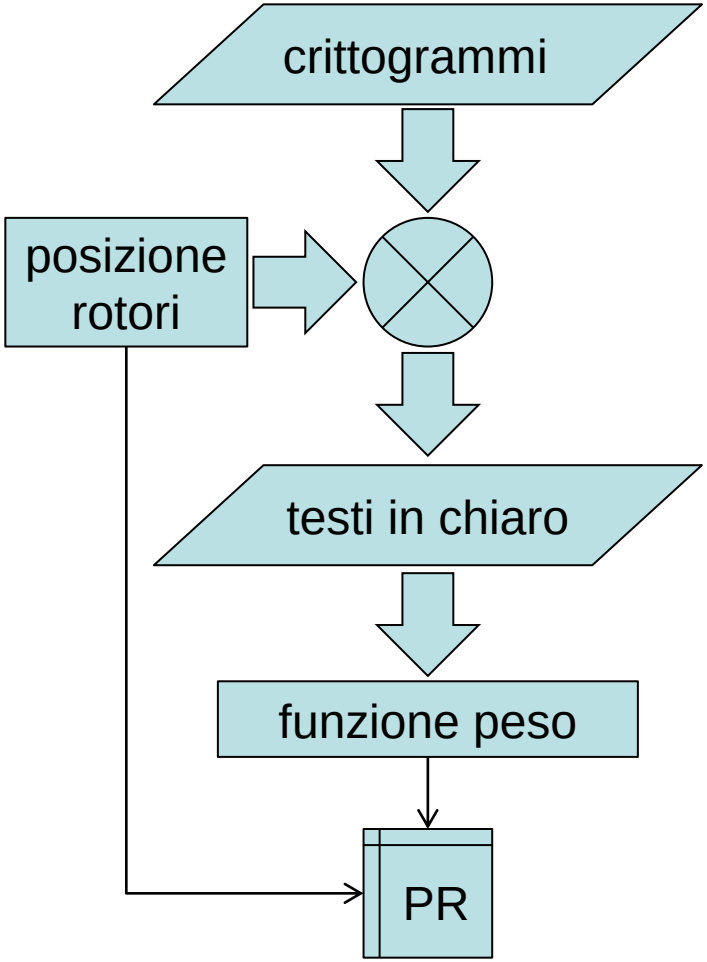
Attacco a forza bruta

Principio generale di funzionamento

Funzione peso

Attacco a forza bruta

Principio generale di funzionamento (1)



L'attacco opera su 2 o più crittogrammi

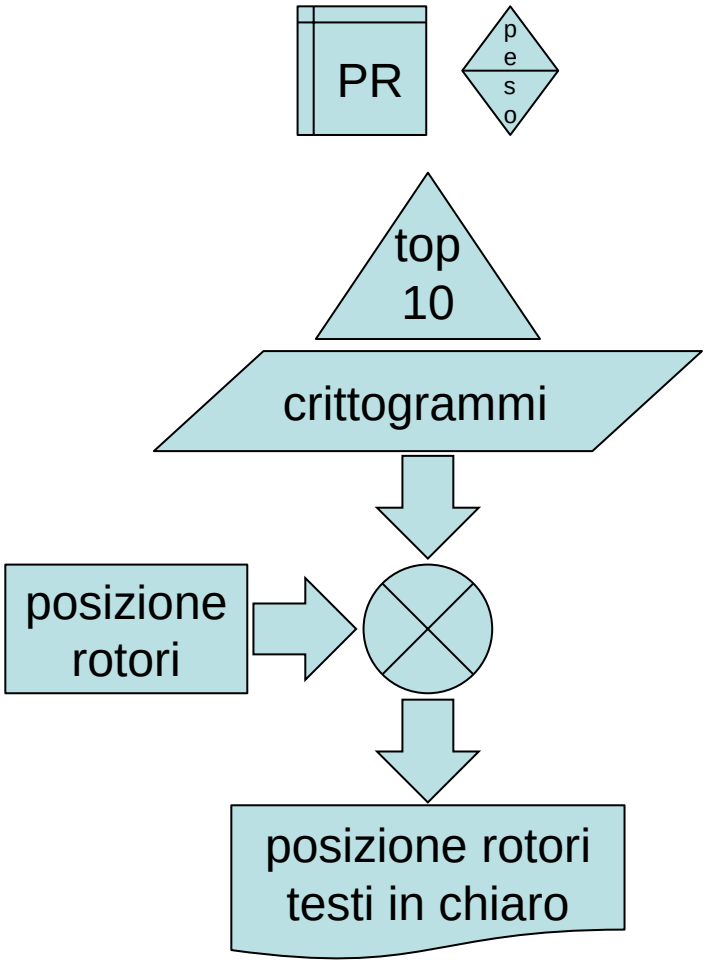
- Data una posizione dei rotori
- vengono generati i testi in chiaro
- che, insieme, sono processati da una funzione peso

- Posizione dei rotori e peso sono archiviati per la fase successiva

- L'operazione viene ripetuta per ciascuna delle 26^3 possibili posizioni dei rotori

Attacco a forza bruta

Principio generale di funzionamento (2)



- Le posizioni dei rotori sono ordinate in ordine decrescente in funzione del peso assegnato
- Si selezionano le 10 posizioni più significative
- Si rigenerano i testi in chiaro
- che vengono mostrati sullo schermo insieme alla posizione dei rotori che conduce ad essi

Attacco a forza bruta
Funzione peso

È importante scegliere una funzione peso adeguata

- Si ricerca la più lunga sottostringa comune ai testi in chiaro
- La lunghezza di tale sottostringa costituisce il peso assegnato alla posizione dei rotori con cui i testi in chiaro sono stati prodotti

Un esempio:

alan**turing****was**bornonehundredyearsago
atbletchleypark**turing**broketheenigma
turing**was**therealfatherofinformatics

turingwas (lunghezza 9) non è comune a tutti i testi in chiaro

turing (lunghezza 6) è la più lunga stringa comune a tutti

Il peso assegnato sarà quindi 6

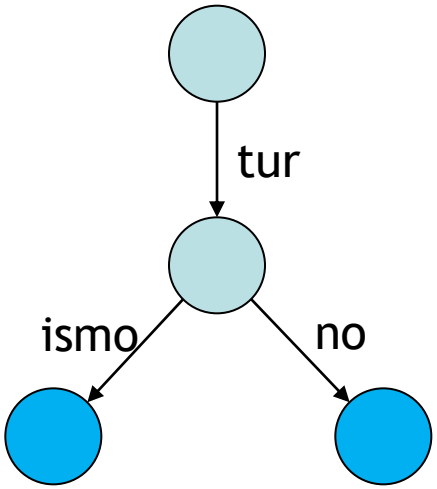
Ricerca sottostringa più lunga

Gli alberi PATRICIA

Antenato comune più basso

Estensione alle sottostringhe

Ricerca sottostringa più lunga
Gli alberi PATRICIA

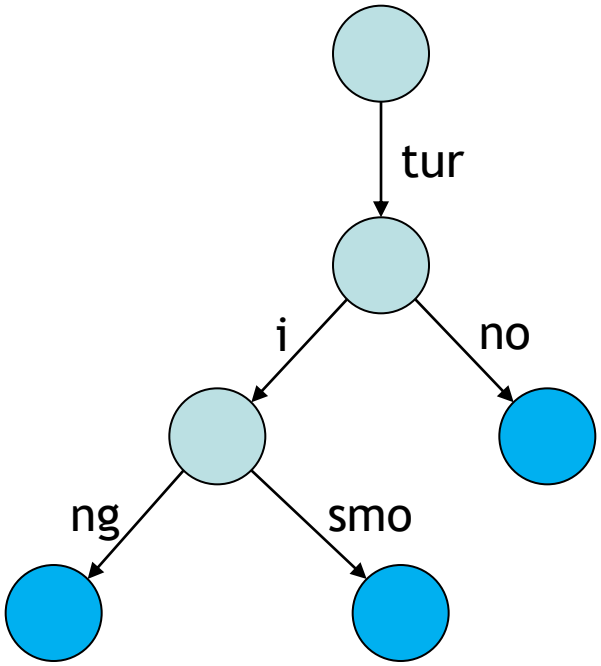


Practical **A**lgorithm **T**o **R**etrieve Information **C**oded **I**n **A**lphanumeric

- Albero di prefissi ottimizzato nello spazio
- Nell'albero PATRICIA raffigurato sono inserite due stringhe:
  - turno
  - turismo
- Un nodo azzurro indica la terminazione di una stringa
  - La colorazione è necessaria per riconoscere, in questo caso, che «tur» non è una stringa

Ricerca sottostringa più lunga

Gli alberi PATRICIA

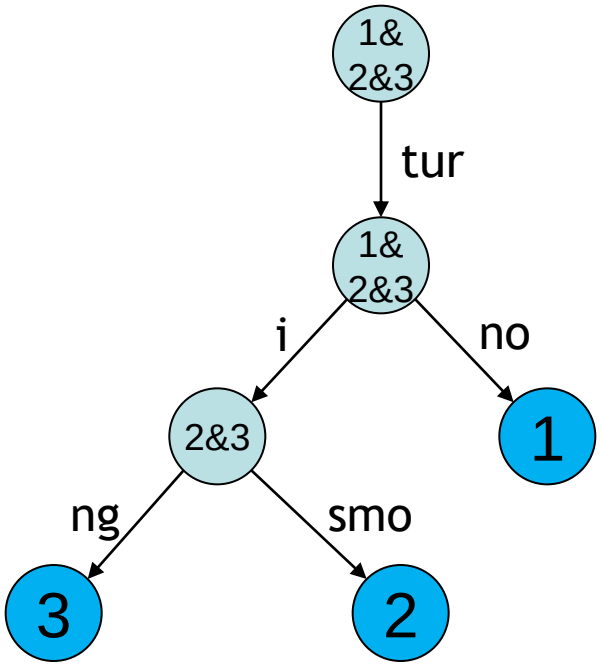


Practical **A**lgorithm **T**o **R**etrieve Information **C**oded **I**n **A**lphanumeric

- Da ciascun nodo dipartono solo stringhe senza alcun prefisso in comune con le altre
- Per inserire la stringa «turing» si procede pertanto a separare la sottostringa «ismo» in «i» e «smo» interponendovi un nuovo nodo, e legando a quest'ultimo la terminazione «ng»

Ricerca sottostringa più lunga

Antenato comune più basso



- Cercare il prefisso più lungo comune a tutte le stringhe equivale a cercare il nodo più lontano dalla radice al di sotto del quale terminino tutte le stringhe inserite nell'albero.
- È facile se, durante l'inserimento di una stringa, in tutti i nodi visitati si tiene traccia del numero della stessa.
- Un antenato comune a tutte le stringhe recherà le tracce di tutte le stringhe.

Ricerca sottostringa più lunga

Estensione alle sottostringhe

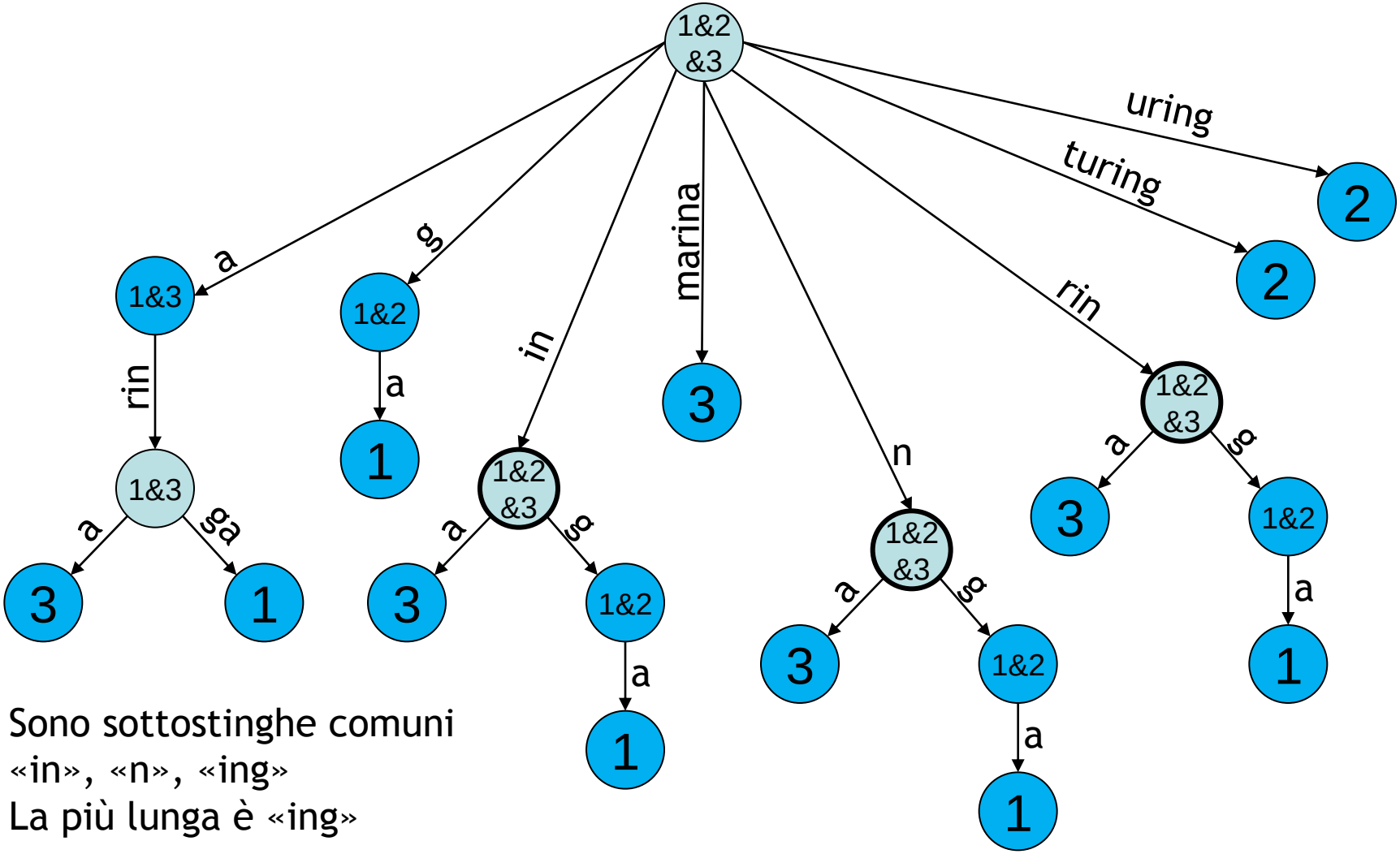
- Quanto fino ad ora esposto consente solamente di trovare il più lungo prefisso comune a tutte le stringhe inserite: un'operazione che non richiede una struttura simile per essere eseguita
- Per trovare la più lunga sottostringa comune, ciascuna stringa dovrà essere inserità più volte, togliendo ogni volta il primo carattere:

aringa	turing	marina
ringa	uring	arina
inga	ring	rina
nga	ing	ina
ga	ng	na
a	g	a

- Nella slide seguente è raffigurato l'albero PATRICIA completo costruito con le stringhe appena mostrate

Ricerca sottostringa più lunga

Estensione alle sottostringhe



Sono sottostinghe comuni
«in», «n», «ing»
La più lunga è «ing»

Conclusioni

L'importanza dell'ottimizzazione

Inapplicabilità alla vera Enigma

Conclusioni
L'importanza dell'ottimizzazione

- Per condurre efficacemente un attacco a forza bruta le operazioni che si ripetono più frequentemente devono essere ottimizzate il più possibile
- Quelle invece eseguite di rado possono essere non ottimizzate

UN ESEMPIO

- Nel caso esposto, l'uso di alberi PATRICIA in sostituzione dei comuni alberi di prefissi ha consentito di abbassare il tempo complessivo dell'attacco* da 40 minuti a soli 4 secondi
- Ottimizzare l'ordinamento finale che, nonostante l'uso di un ABR estremamente sbilanciato per la natura dei dati inseriti, impiega meno di mezzo secondo non porterebbe alcun reale giovamento

*Test condotti su una CPU Intel® Core™ i7-3610QM @ 2.30 GHz

Conclusioni

Inapplicabilità alla vera Enigma

- L’attacco appena esposto sarebbe stato inefficace contro la vera Enigma
- La macchina Enigmaduino, infatti, non implementa la plugboard
- La plugboard – la parte più semplice dell’intera macchina Enigma – è stata anche il più grande ostacolo alla sua decifrazione
- Il numero di possibili posizioni dei rotori ammonta ad appena 17576 – la presenza della plugboard introduce circa un milione di miliardi di ulteriori combinazioni

Riferimenti Bibliografici

In inglese

- Knuth, Donald (1997). *"6.3: Digital Searching"*. The Art of Computer Programming Volume 3: Sorting and Searching (2nd ed.). Addison-Wesley. p. 492.

- Morrison, Donald (1968). *PATRICIA – Practical Algorithm To Retrieve Information Coded In Alphanumeric*. Journal of the ACM, Volume 15 Issue 4. p. 514.

- Aho – Hopcroft - Hullman (1973). *On finding lowest common ancestor in trees*. STOC '73 Proceedings of the fifth annual ACM symposium on Theory of computing. p. 253.