Crittografia e traduzione del lineare B

Materiale didattico

N.B.: i due fascicoli Crittografia 1 e Crittografia 2, i due simulatori Enigma, l'ambiente di programmazione Blockly dedicato alla crittografia, sono disponibili sul sito http://researchinaction.it/ e di solito sono aggiornati ogni volta che ci son cambiamenti, immagini e testi di questo materiale sono di pubblico dominio o ne possediamo i diritti.

Le due presentazioni e la cartella con i font di caratteri non sono sul sito sostanzialmente perché può essere che non possediamo i diritti di diffusione di testi, immagini o altro materiale (e quindi sarebbero da considerare … a uso interno*).*

- *Crittografia 1, L'arte di svelare segreti* (RiA – Research in Action, http://researchinaction.it/materials/13-Crittografia-1.pdf), definizione e convenzioni, codice di Cesare, cifratura per sostituzione e con frase chiave, analisi delle frequenze, metodo di Vigenére. Come consueto per i fascicoli di *RiA*, si tratta di un laboratorio, guidato *passo passo*, con relative soluzioni: l'idea è quella di realizzare uno strumento che possa essere usato dagli studenti con un minimo intervento dell'insegnante.
- *Crittografia 2, Carta e penna non bastano!* (RiA – Research in Action, http://researchinaction.it/materials/14-Crittografia-2.pdf), Enigma, costruzione di un simulatore della macchina Enigma, il problema della trasmissione della chiave, algoritmo RSA: la chiave pubblica. Come consueto per i fascicoli di *RiA*, si tratta di un laboratorio …
- Un ambiente di programmazione a blocchi dedicato (RiA – research in Action, http://researchinaction.it/myblockly/criptography.html) in via di completamento ma già funzionante con procedure e funzioni per i metodi di cifratura presentati nei due fascicoli *Crittografia 1* e *Crittografia 2*.
- *Cifratura con frase chiave – un esempio di criptoanalisi*, un esempio descritto passo passo (è una presentazione sia in formato *PowerPoint* che PDF) di analisi delle frequenze applicata a un testo cifrato con il metodo della frase chiave.
- *La traduzione del lineare B*, la storia della traduzione del Lineare B, una lingua preellenica o minoica, ponendo l'accento in modo particolare sul lavoro di Evans e Chadwick (che richiama le tecniche di criptoanalisi viste in precedenza). Una presentazione per chiudere il laboratorio che *racconta* la storia dei progressi nella traduzione di questa lingua minoica (per leggere correttamente la presentazione in formato *PowerPoint* è necessario installare il font *aegean.ttf*, vedi più avanti).
- Un simulatore Enigma, da costruire con carta e forbici, funzionante seguendo esattamente gli stessi principi della macchina originale (RiA – Research in Action, versione mini, alfabeto di sole sei lettere: http://researchinaction.it/materials/enigmasimulator-mini.pdf; versione completa, alfabeto di 26 lettere: http://researchinaction.it/materials/enigmasimulator-all.pdf; istruzioni ed esempi di utilizzo: http://researchinaction.it/materials/enigmasimulator.pdf – già presenti in *Crittografia 2, …*).
- *Font* per i caratteri del lineare B e lineare A *(Aegean.ttf)*: sono necessari per visualizzare correttamente la presentazione nel formato PowerPoint *La traduzione del lineare B*! Sono contenuti nella cartella compressa *Aegean*, comprensivi di descrizioni e tabella dei codici ma per usarli è sufficiente un *doppio click* sul file *aegean.ttf* e, successivamente, premere il pulsante *Installa*.

Risorse *online*

- Un simulatore che funziona su Windows: http://users.telenet.be/d.rijmenants/en/enigmasim.htm (dallo stesso sito è possibile scaricare anche un'applicazione per creare il *manuale* delle configurazioni – *codebook*), il manuale è sempre su questo sito. Molto bella, facile da installare e da usare! Salva anche le impostazioni.
- Un simulatore Enigma è disponibile anche per Android (*Enigma Simulator* di Franklin Heath Ltd. Su Google Play)

Schema di una serie di laboratori

0. Prerequisiti (i concetti relativi a questi prerequisiti possono essere affrontati in orario curricolare, prima del laboratorio, nel corso dell'anno, oppure forniti e discussi *ad hoc* nel corso del laboratorio):
    a. Calcolo combinatorio (fattoriale di un numero, cenni sul binomio di Newton, disposizioni, combinazioni e permutazioni semplici)[1]
    b. Aritmetica modulare[2]
    c. Statistica (cenni sulle percentuali e sull'uso delle tabelle)[3]
1. Introduzione alla crittografia
    a. Definizioni (testo e alfabeto in chiaro e cifrato, chiave, convenzioni) – *Crittografia 1*
2. Codici per sostituzione – *Crittografia 1*
    a. Codice di Cesare: si può decifrare con la *forza bruta* – *Crittografia 1*
    b. Codice per sostituzione: la *forza bruta* non basta più, decifrare usando la frequenza delle lettere. Criptoanalisi: forzare un testo usando l'analisi delle frequenze – qui si possono usare le slide della presentazione *Cifratura con frase chiave - un esempio di criptoanalisi*.
        i. Costruiamo piccole applicazioni con *Blockly*[4] (usando procedure e funzioni già presenti) per contare le lettere di un testo.
        ii. Integrazione con matematica: quante sono le possibilità (cenni di calcolo combinatorio).
    c. Alfabeti utopici (cenni storici sugli alfabeti usati da Mary Stuart, Chaucher, Leon Battista Alberti), la *Divina Proportione* di Luca Pacioli. Integrazione con *disegno*. Integrazione con *inglese*?
3. Cifratura con frase chiave
    a. Cifratura e decifratura
        i. Costruiamo piccole applicazioni con *Blockly* (usando procedure e funzioni già presenti) per cifrare e decifrare rapidamente e per controllare la cifratura eseguita manualmente.
    b. Criptoanalisi: forzare un testo usando l'analisi delle frequenze, ricostruzione della frase chiave. *Blockly*. Se non fatto in precedenza, qui si possono usare le slide della presentazione *Cifratura con frase chiave - un esempio di criptoanalisi*.
4. Il problema delle chiavi di cifratura
    a. Enigma: meccanizzazione di cifratura e decifratura, schema della macchina, *simulatore Enigma* *(Singh, S. – Codici & segreti, La storia affascinate dei messaggi cifrati dall'antico Egitto a internet, cap. 4 Far breccia in Enigma, pag 162 – 2014, RCS Media Group)*
        i. Integrazione con matematica: calcolo delle possibili configurazioni (della macchina e del simulatore mini).
        ii. *Crib*: provare a ricostruire la configurazione del simulatore mini conoscendo l'inizio del testo in chiaro, è fattibile? Migliora la situazione se si usa *Blockly*?
    b. Algoritmo RSA: come funzione, un esempio semplificato
        i. Integrazione con matematica: aritmetica modulare
5. La traduzione del *lineare B* *(Singh, S. – Codici & segreti, La storia affascinate dei messaggi cifrati dall'antico Egitto a internet, Il mistero del lineare B, pag 242 – 2014, RCS Media Group)* – qui si possono usare le slide della presentazione *La traduzione del lineare B*.
    a. Civiltà micenee, il palazzo di Cnosso, la scoperta delle tavolette. Integrazione con *geo-storia* (eventualmente in compresenza)

---

[1] Il calcolo combinatorio è usato soprattutto nel paragrafo *2.2 Qualche conticino* di *Crittografia 2* e *2.4 Forzare Enigma* dello stesso fascicolo. Volendo è possibile evitare di usarlo *saltando* questi due paragrafi, non si pregiudica la comprensione del funzionamento della macchina Enigma (anche se non risulta evidente la complessità delle operazioni di decifrazione).

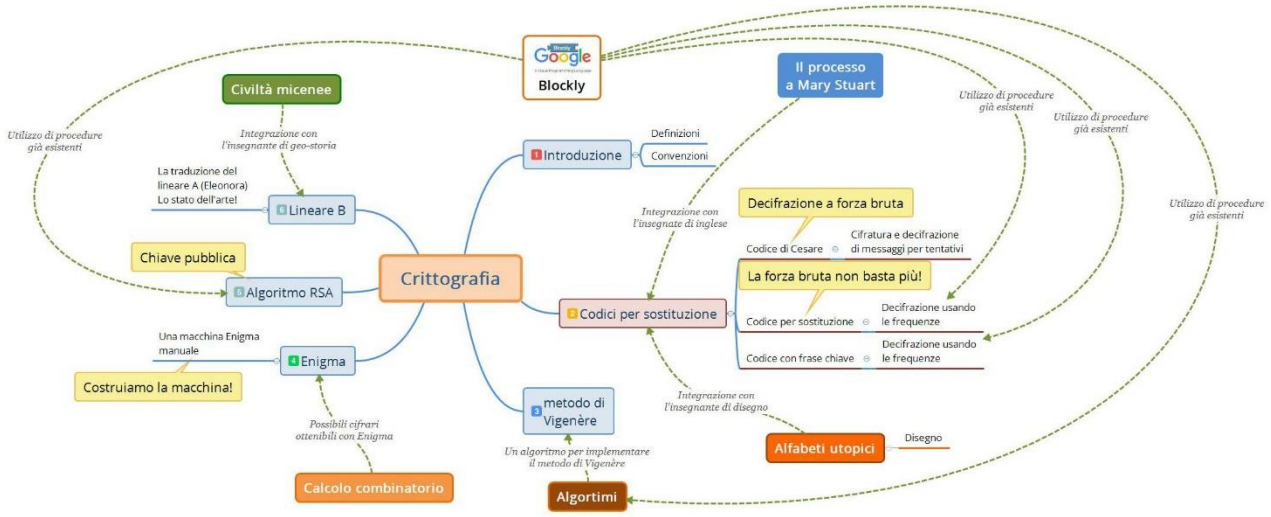
[2] L'aritmetica modulare è usata sin da subito (paragrafo *2.2 Precisazioni* del fascicolo *Crittografia 1*, nello stesso paragrafo ci sono alcuni cenni sull'operatore modulo), è essenziale per la piena comprensione delle procedure.

[3] L'uso delle percentuali è usato nella criptoanalisi di un testo cifrato (paragrafo 3.2 La criptoanalisi del fascicolo Crittografia 1), sono sufficienti alcuni cenni e la capacità di calcolare una percentuale e di comprenderne il significato

[4] L'idea alla base dell'uso di Blockly è quella di introdurre, per piccoli passi, il *coding* nel percorso. In questa fase si chiede di *montare* pochi blocchi (da due a sei) che permettano di richiamare le funzioni già presenti, sviluppate appositamente e disponibili su *Research in Action*.

b. Come è stato tradotto il *lineare B*
c. Come si lavora oggi alla traduzione del lineare A: cenni di *machine learning* (intervento di un esperto esterno)

Mappa delle attività



Riferimenti storici

- 480 a.C.: Demarato avverte gli elleni dei preparativi per l'invasione di Serse *(Singh, S. – Codici & segreti, La storia affascinate dei messaggi cifrati dall'antico Egitto a internet, pag 19 – 2014, RCS Media Group)*
- 1467: il disco cifrante di Leon Battista Alberti (cifratura per sostituzione parzialmente meccanizzata)
- 1586: Mary Stuart, i suoi messaggi decifrati da Thomas Phelippes *(Singh, S. – Codici & segreti, La storia affascinate dei messaggi cifrati dall'antico Egitto a internet, pag 17 – 2014, RCS Media Group)*. Vedi anche *(Singh, S. – Codici & segreti, La storia affascinate dei messaggi cifrati dall'antico Egitto a internet, pag 49 e ss. La congiura di Babbington – 2014, RCS Media Group)*
- 1942: Le forze armate statunitensi sperimentano l'utilizzo di marconisti navajo per aggiungere la difficoltà della lingua a quella della decifrazione *(Singh, S. – Codici & segreti, La storia affascinate dei messaggi cifrati dall'antico Egitto a internet, La barriera della lingua pag 214 e ss. La congiura di Babbington – 2014, RCS Media Group)*

La scitale spartana

La *scitale* era un'asta o meglio, un parallelepipedo che ha per base un poligono regolare. Si avvolgeva attorno all'asta una striscia di pelle e si scriveva il messaggio; per decifrarlo era sufficiente avvolgere la strisciolina su una *scitale* dello stesso diametro e con la stessa base (Singh, S. – *Codici & segreti, …*, pag 24 – *2014, RCS Media Group).*

Il codice di Cesare

Primo impiego documentato di crittografia in campo militare *(Singh, S. – Codici & segreti, La storia affascinate dei messaggi cifrati dall'antico Egitto a internet, pag 26 – 2014, RCS Media Group)*. La cifratura per sostituzione, come nel caso del codice di Cesare, può essere decifrata con la *forza bruta*, semplicemente provando tutte le possibili sostituzioni.

Ci sono esempi storici di sostituzione con insiemi di simboli qualsiasi ma la sostanza non cambia *(Singh, S. – Codici & segreti, La storia affascinate dei messaggi cifrati dall'antico Egitto a internet, pag 44 – 2014, RCS Media Group)*. Qui si può inserire il docente di disegno con gli alfabeti utopici.

Le chiffre indéchiffrable

Sostituzione con più alfabeti cifranti in sequenza, Leon Battista Alberti suggeriva di usarne 25 *(Singh, S. – Codici & segreti, La storia affascinate dei messaggi cifrati dall'antico Egitto a internet, pag 63 e ss. – 2014, RCS Media Group).* La decifrazione di questo codice è descritta in *Singh, S. – Codici & segreti, La storia affascinate dei messaggi cifrati dall'antico Egitto a internet, pag 133 Il santo Graal della crittografia – 2014, RCS Media Group)*.