CryptoHelper: Versione finale

CryptoHelper

Progetto SvilAppSW 2013-14

Descrizione del progetto

Si vuole mettere a punto un sistema di supporto allo studio del metodo di cifratura noto come *cifratura monoalfabetica*, in cui si cifrano dei messaggi scritti in un dato alfabeto A sostituendo ogni carattere di A con un altro appartenente allo stesso alfabeto.
Il software verrà utilizzato in un centro di addestramento all'analisi crittografica come strumento didattico per allenare i crittoanalisti.
In prima approssimazione possiamo assumere che A sia l'alfabeto di 26 lettere della lingua inglese.
Il sistema dovrà permettere:

- lo scambio "legittimo" di messaggi fra un mittente e un destinatario che hanno precedentemente stabilito una chiave da condividere per tutte le loro interazioni.
- la possibilità di improvvisarsi "spie", quindi intercettare un messaggio cifrato scambiato fra altri due partner, e provare a decifrarlo senza conoscerne la chiave, grazie a funzionalità di supporto all'analisi crittografica (che è il vero scopo didattico dell'applicazione).

Si richiede che lo scambio di messaggi sia gestito tramite database.

Le funzionalità centrali di questa applicazione dovranno dunque essere le seguenti:

- generare una cifratura monoalfabetica a partire da una chiave K (per i dettagli sulle metodologie elencate si veda l'allegato tecnico)
  - con il sistema di Cesare
  - in modo pseudocasuale
  - a partire da una vera e propria parola chiave sullo stesso alfabeto
- cifrare/decifrare messaggi essendo in possesso della chiave di cifratura K (quindi legalmente). A questo scopo dovrà essere possibile per l'utente scegliere come trattare i caratteri speciali (punteggiatura, lettere accentate, etc) e gli spazi (l'opzione più comune è quella di eliminare entrambi, ma a scopo di esercitazione dovrebbe essere possibile lasciare entrambi o solo gli spazi)
- supportare un analista nel decifrare un messaggio senza essere in possesso della chiave; in particolare
  - mostrare la decifratura (anche incompleta) che si ottiene dato un certo insieme di ipotesi sulla mappatura dei caratteri
  - mantenere un albero delle ipotesi permettendo di aggiungere/rimuovere ipotesi

- conoscendo la lingua in cui il messaggio originale è scritto, supportare l'analisi delle frequenze (per dettagli si veda l'allegato tecnico), in particolare:
  - fornire analisi di frequenza (almeno di caratteri singoli e di coppie) sul testo cifrato
  - fornire le frequenze (almeno di caratteri singoli e coppie) relative alla lingua del messaggio originale, e permettere di confrontarle con quelle del testo cifrato

Si richiede poi di progettare un meccanismo a "sfide" per inserire un elemento ludico nell'applicazione. Il messaggio cifrato andrà a costituire una "sfida" per le spie. Si può pensare che le sfide abbiano diversi livelli di difficoltà a seconda di quali informazioni sul messaggio sono note (la lingua in cui è scritto, la spaziatura delle parole, il posizionamento della punteggiatura, chi sono il mittente e il destinatario...)
E' da valutare quando e come un messaggio cifrato diventi una sfida e come ne venga stabilita la difficoltà (es.: tutti i messaggi sono sfide ed è la spia a scegliere la difficoltà alla quale vuole giocare; oppure: è il mittente a decidere se e come il suo messaggio diventa una sfida; oppure ancora: c'è un "coordinatore" che vede tutti gli scambi e sceglie quali trasformare in sfide e con che difficoltà, ecc....)
Inoltre è da valutare anche come possa funzionare un meccanismo a punteggi che porti gli utenti a sfidarsi (quindi a fare più esercizi di analisi).

In generale, la persistenza dei dati dovrà essere gestita tramite database condiviso, previa autenticazione da parte dell'utilizzatore, in modo che l'utente possa accedere al proprio lavoro da elaboratori diversi.
Inoltre, il sistema dovrà essere realizzato tramite un'applicazione standalone in linguaggio Java, in modo da garantire la massima portabilità su macchine con sistemi operativi differenti.