WordCrypt

Progetto di un cifratore simmetrico basato su dizionario.
 - Questo crypter si basa sulla codifica del testo mediante lo shuffle delle posizioni delle parole (id) all'interno di un dizionario: il messaggio cifrato consiste in una serie di numeri che daranno il messaggio originale solo fornendo la chiave corretta.
 - Se si tenta di decifare il messaggio usando una chiave errata, gli id ricavati puntano comunque a parole nel vocabolario e la frase ricostruita risulta distinguibile soltanto semanticamente da quella giusta, rendendo così molto difficile un tradizionale attacco a forza bruta.
 - Nell'archivio è presente l'eseguibile Java, due dizionari (italiano ed inglese) e la relazione completa sull'algoritmo, che contiene anche benchmark e un'analisi dello stato dell'arte dei sistemi di cifratura simmetrica.[Esame di Sicurezza Informatica] - (2005)>> DOWNLOAD <<autori: Ernesto, Giovanni, io