A team
Bono Alessandro
Cerrato Mattia
Vinci Mattia

Glossario

Nomi	Definizione	Sinonimi
albero delle ipotesi	struttura che mantiene il susseguirsi di assunzioni e scelte fatte durante il processo di analisi crittografica	
alfabeto	insieme di simboli che compongono l'alfabeto inglese (26 lettere) che il messaggio può contenere	
analisi crittografica	processo in cui si cercano pattern/schemi nel testo crittografato con l'obiettivo di decifrare il messaggio	
analisi delle frequenze	processo con il quale si valuta quante volte un certo pattern (uno o più caratteri) ricorre nel messaggio	
analista	agente che effettua l'analisi crittografica	spia
applicazione standalone	programma indipendente e completo (non necessita componenti esterni)	
area di lavoro	insieme di messaggi già scambiati, in corso di decodifica e già decodificati	
autenticazione	processo utile ad assegnare a ogni utente la sua area di lavoro	login
caratteri singoli	simboli dell'alfabeto	
caratteri speciali	punteggiatura e spazi	
chiave	elemento segreto condiviso da due agenti (mittente e destinatario) durante uno scambio di messaggi, necessario alla cifratura e dipendente dal metodo scelto	
cifratura monoalfabetica	sistema crittografico basato su permutazioni di simboli dell'alfabeto	
composizione messaggio	scrittura del messaggio, che dovrà essere crittografato e spedito, compiuta dal mittente.	
database	base di dati condivisa con memorizzate le aree private degli utenti	
decifrare	obiettivo dell'analisi crittografica: invertire la funzione di cifratura, riportando il messaggio alla forma originale	
destinatario	agente che riceve un messaggio cifrato e, conoscendo la chiave, ha la capacità di decifrarlo	
esercizi di analisi	serie di diverse analisi crittografiche guidate dal sistema	

funzionalità di supporto	insieme delle funzionalità di analisi crittografica offerte dal sistema (analisi frequenze, feedback dopo ogni assunzione fatta)	
informazioni sul messaggio	meta informazioni date a priori riguardanti ogni singolo messaggio (lingua, spaziatura, punteggiatura, mittente e destinatario)	
insieme di ipotesi	ipotesi presenti nell'albero delle ipotesi	
interazioni	insieme di scambi di messaggi	
intercettare	visualizzare e avere la possibilità di decifrare un messaggio scambiato fra altri due agenti comunicanti	
invio messaggio	spedizione al destinatario del messaggio cifrato	
ipotesi	singola assunzione di associazione lettera-lettera nella funzione crittografica	
lingua	lingua naturale in cui i messaggi sono stati composti. in questo caso, la lingua inglese	
livelli di difficoltà	diverse quantità di informazioni conosciute a priori dalla spia	
mappatura dei caratteri	permutazione dei caratteri che descrive la funzione crittografica scelta	
messaggi	insieme di stringhe sull'alfabeto in linguaggio naturale; possono contenere spazi e simboli di punteggiatura	
messaggio originale	il messaggio composto dal mittente prima della crittografia, quindi ancora in chiaro	
mittente	l'agente che compone il messaggio e lo spedisce dopo aver concordato col destinatario il metodo di crittografia	
negoziazione	momento di contatto tra mittente e destinatario in cui i due agenti si accordano sul metodo di cifratura e la chiave da utilizzare	
parola chiave	elemento conosciuto solo dal mittente e dal destinatario che permette di cifrare/decifrare il messaggio	
persistenza dei dati	possibilità da parte degli utenti di interrompere la propria sessione e recuperare la propria area di lavoro	
portabilità	proprietà dell'applicazione finale di poter essere eseguita su diversi sistemi operativi	
pseudocasuale	particolare sistema di cifratura	
scopo didattico	obiettivo finale dell'applicazione prodotta	
sessione di lavoro	insieme delle operazioni compiute e lasso di tempo trascorso tra l'entrata e l'uscita dall'area di lavoro	

sessione di crittografia	processo di decifratura di un singolo messaggio, da poter interrompere e riprendere a piacimento	
sistema di cifratura	funzione di crittografia utilizzata e concordata in precedenza da mittente e destinatario	
sistema di Cesare	un particolare sistema di cifratura	
testo cifrato	messaggio risultante dall'applicazione della funzione di cifratura concordata da mittente e destinatario	
utente	qualsiasi agente che opera nel sistema (mittente, destinatario e spia)	utilizzatore, agente
violare	intercettare e decifrare un messaggio	