

A team

Bono Alessandro

Cerrato Mattia

Vinci Mattia

Glossario

Nomi	Definizione
albero delle ipotesi	struttura che mantiene il susseguirsi di assunzioni e scelte fatte durante il processo di analisi crittografica
analisi crittografica	processo in cui la spia/analista ricerca pattern/schemi nel testo crittografato con l'obiettivo di violare il messaggio, eventualmente con l'aiuto di altri strumenti
analisi delle frequenze	strumento con il quale si valuta quante volte un certo carattere ricorre nel messaggio o nella lingua in cui è stato scritto
analista	agente che effettua l'analisi crittografica e si dedica a violare i messaggi
assunzione	singola associazione lettera-lettera nella funzione crittografica
bozza	messaggio in stato di composizione da parte del mittente ma non ancora inviato e presente nella casella delle bozze
caselle	diverse caselle che contengono i diversi tipi di messaggi: inviati, ricevuti e bozze.
chiave	elemento segreto condiviso da due studenti (mittente e destinatario) prima di uno scambio di messaggi, necessaria alla cifratura e alla decifratura e vincolata al metodo scelto
cifratura di Cesare	un sistema di cifratura a sostituzione monoalfabetica in cui ogni lettera del testo originale viene sostituita con un'altra lettera dello stesso alfabeto, la quale si trova a distanza di un certo numero di posizioni dopo all'interno dell'alfabeto. tale distanza costituisce la chiave del sistema
cifratura Keyword	sistema di cifratura in cui la chiave è composta da una parola da cui viene calcolata la mappatura.
cifratura Pseudocasuale	sistema in cui la mappatura dei caratteri è scelta casualmente tramite un generatore di numeri casuali. La chiave è il seme iniziale del generatore.
composizione messaggio	scrittura del messaggio, che dovrà essere crittografato e spedito, compiuta dal mittente.
coordinatore	seleziona quali messaggi, tra quelli esistenti, dovranno diventare delle sfide
creatore	creatore del sistema di cifratura
decifrare	azione del destinatario che consiste nel riportare un messaggio cifrato alla sua forma in chiaro, essendo a conoscenza della chiave e del metodo di cifratura utilizzato dal mittente
destinatario	agente che riceve un messaggio cifrato e, conoscendo la chiave, ha la capacità di decifrarlo
difficoltà	diverse quantità di informazioni disponibili riguardo un dato messaggio oggetto di sfida
esercizi di analisi	serie di diverse analisi crittografiche guidate dal sistema
giocatore	partecipante alle sfide

informazioni sul messaggio	meta informazioni date a priori riguardanti ogni singolo messaggio (lingua, spaziatura, punteggiatura, mittente e destinatario)
intercettare	visualizzare e avere la possibilità di violare un messaggio scambiato fra altri due studenti comunicanti
invio messaggio	spedizione al destinatario del messaggio, in seguito alla cifratura dello stesso
ipotesi	insieme di assunzioni fatte su un testo da decifrare
lingua	lingua naturale in cui i messaggi sono stati composti
mappatura dei caratteri messaggi	permutazione dei caratteri che descrive la funzione crittografica scelta scambio di informazioni tra due utenti, che comprende un titolo e un testo che verrà cifrato all'invio secondo un sistema di cifratura concordato in precedenza. i messaggi sono salvati nelle relative caselle, distinguendo tra messaggi inviati, ricevuti e bozze.
mittente	l'agente che compone il messaggio e lo spedisce dopo aver concordato col destinatario il sistema di cifratura
negoziazione	momento di contatto tra mittente e destinatario in cui i due agenti si accordano sul metodo di cifratura e la chiave da utilizzare
partner	i due attori della negoziazione di un sistema di cifratura
partecipare (ad una sfida)	l'azione del giocatore che seleziona una delle sfide disponibili, sceglie una difficoltà a cui parteciparvi e tenta di decifrare il messaggio
proponente	lo studente che, dopo aver creato il sistema di cifratura, lo propone ad un altro studente per poterlo utilizzare nelle comunicazioni future
proposta	l'atto del creatore del sistema di cifratura di proporre tale sistema ad un altro studente con cui desidera interagire. può avere diversi stati: accepted, pending, declined, expired
punteggio	valore numerico utile a calcolare le classifiche di ogni sfida
risultato	l'insieme del punteggio e delle informazioni necessarie alla valutazione di una sfida, quali tempo impiegato e la mappatura inviata come soluzione
sessione	l'insieme delle informazioni mantenute nel sistema durante la violazione di un messaggio da parte di una spia, quali albero delle ipotesi
sfida	messaggio scelto dal coordinatore per essere decifrato in modo competitivo da parte dei giocatori, che possono parteciparvi e ottenere un punteggio
sistema di cifratura	insieme di funzione di crittografia e chiave utilizzata e concordata in precedenza da mittente e destinatario
soluzione	una mappatura che la Spia ha ritenuto essere quella adatta per decifrare un messaggio. Contiene almeno tutti i caratteri del messaggio cifrato
stato corrente	gli effetti delle ipotesi fatte sinora sul messaggio da violare
strumenti di supporto	insieme delle funzionalità di analisi crittografica offerte dal sistema (analisi frequenze, dizionario)
testo cifrato	testo risultante dall'applicazione della funzione di cifratura concordata da mittente e destinatario
testo in chiaro	il testo composto dal mittente prima della crittografia, quindi ancora in chiaro

undo	annullare l'ipotesi fatta al passo precedente dell'analisi crittografica eventualmente fornendo una motivazione del perché
utente	qualsiasi agente che opera nel sistema (mittente, destinatario e spia)
vincoli	restrizioni sulla tipologia di chiave da poter concordare o generare per il sistema di cifratura
violare	intercettare e decifrare un messaggio attraverso una serie di assunzioni sulla mappatura dei caratteri

Sinonimi

spia

parola chiave

insegnante

mossa

contrattazione

annullare,
scartare
utilizzatore,
agente