

Esercizi sulla crittografia

Cifrario a sostituzione monoalfabetica

1. **[CifraCesare]** – Scrivere un'applicazione console che consenta di crittografare un messaggio testuale utilizzando il cifrario di Cesare. In particolare, il programma deve:
 - a) richiedere una stringa P_1 (inserita da tastiera) contenente un messaggio testuale;
 - b) generare una seconda stringa P_2 ottenuta rimuovendo da P_1 tutti i caratteri non appartenenti all'alfabeto del cifrario (si utilizzi l'alfabeto esteso a 26 caratteri) e convertendo i caratteri residui in maiuscolo;
 - c) determinare e visualizzare il testo cifrato applicando al messaggio P_2 l'algoritmo proposto.
2. **[DecifraCesare]** – Scrivere un'applicazione console che decifri una stringa cifrata con il cifrario di Cesare. In particolare, il programma deve:
 - a) richiedere l'inserimento di una stringa C effettuandone la validazione (controllare che ogni carattere di C appartenga all'alfabeto esteso)
 - b) determinare e visualizzare la stringa P ottenuta mediante applicazione dell'algoritmo di decifrazione.
3. **[CifraChiave]** – Scrivere un'applicazione console che codifichi una stringa testuale (composta solamente da caratteri dell'alfabeto esteso) utilizzando un cifrario a sostituzione monoalfabetica con chiave generica K , essendo K un numero intero inserito dall'utente.
4. **[DecifraChiave]** – Scrivere un'applicazione console che permetta di decifrare una stringa opportunamente validata mediante un cifrario a sostituzione monoalfabetica con chiave K , essendo K un numero intero inserito dall'utente.
5. **[CifraROT13]** – Scrivere un'applicazione console che consenta di cifrare o decifrare un messaggio testuale secondo la seguente regola: se il carattere è una lettera dell'alfabeto esteso, a esso è applicato l'algoritmo ROT13; in caso contrario il carattere rimane invariato.
6. **[CifraPizzini]** – Scrivere un'applicazione console che consenta di codificare un messaggio testuale (composto unicamente da caratteri dell'alfabeto italiano, è richiesta la validazione del messaggio) utilizzando l'algoritmo dei “Pizzini”. Si riporti in output un'unica sequenza di caratteri numerici priva di separatori.
7. **[DecifraPizzini]** – Scrivere un'applicazione console che consenta di decifrare una sequenza di caratteri numerici (non contenente spazi o altri separatori) generata dall'algoritmo dei “Pizzini”.
8. **[CifraPizziniFile]** – Scrivere una variante del programma **CifraPizzini** che consenta l'acquisizione dei dati iniziali e la memorizzazione del risultato utilizzando i file. I nomi dei file di input e output devono essere passati al programma mediante argomenti dalla linea di comando.
9. **[DecifraPizziniFile]** – Scrivere una variante del programma **DecifraPizzini** che consenta l'acquisizione dei dati iniziali e la memorizzazione del risultato utilizzando i file. I nomi dei file di input e output devono essere passati al programma mediante argomenti dalla linea di comando.