

Cryptotext (ver. 1.0)

Guida dell'utente

Cryptotext è un software di codifica e decodifica di testo tramite la scelta di uno dei tre algoritmi implementati:

- Codifica/decodifica semplice
- Codifica/decodifica con chiave di cifratura
- Codifica/decodifica con chiave di cifratura e XOR bit a bit

All'apertura del programma verrà visualizzata una schermata di questo tipo:

```
Benvenuto al codificatore, decodificatore di messaggi.  
Seleziona dal menu' sottostante cosa desideri fare:  
  
1) Codifica un messaggio  
2) Decodifica un messaggio  
3) Codifica un messaggio con chiave di cifratura  
4) Decodifica un messaggio con chiave di cifratura  
5) Codifica un messaggio con chiave di cifratura e XOR bit a bit  
6) Decodifica un messaggio con chiave di cifratura e XOR bit a bit  
7) Genera chiave di cifratura  
8) Aiuto  
9) Esci dal programma
```

Da questo menù è possibile scegliere il tipo di codifica e generare la chiave di cifratura.

Codifica di un messaggio

Selezionando la codifica di un messaggio verrete ricondotti al seguente sottomenù:

```
Preferisci inserire il messaggio manualmente o caricarlo da un file?  
  
1) Scrivi il messaggio manualmente      2) Carica da file      3) Torna al menu' principale
```

Cryptotext permette di inserire manualmente il messaggio da codificare oppure caricarlo da un file. Nel caso in cui si scegliesse il caricamento del file è possibile utilizzare il file .txt allegato oppure un file personale, sempre in formato .txt denominato "Input". In questo file la sintassi del testo deve essere del seguente tipo: "3 esempio frase cryptotext", dove il numero indica quante parole devono essere codificate seguito dalle parole stesse.

Andando a scegliere, invece, il primo caso, ovvero l' inserimento manuale del testo, verrà richiesto quante parole si vogliono codificare. Inserite il numero di parole e premete invio, successivamente inserite le parole normalmente (divise da spazi) e non appena finito premete invio. A fine procedura, il programma restituirà il testo codificato:

```
La frase codificata e':  
suryd iudvh fu|swrwh{w
```

Questo tipo di codifica utilizza l' algoritmo del cifrario di Cesare (link wikipedia per approfondire: https://it.wikipedia.org/wiki/Cifrario_di_Cesare).

Decodifica di un messaggio

Selezionando la decodifica di un messaggio è possibile decodificare il testo codificato utilizzando il metodo precedentemente visto. Il sottomenù è identico al precedente, bisogna specificare se inserire il testo manualmente oppure caricarlo da un file. Inserendo il testo manualmente chiederà quante parole si vogliono decodificare, in seguito bisogna inserire le parole. A fine procedura, il programma restituirà il testo decodificato:

```
La frase decodificata e':  
prova frase cryptotext
```

Codifica di un messaggio con chiave di cifratura

A differenza della codifica vista precedentemente, questo tipo di codifica utilizza una chiave di cifratura per cifrare il testo. È possibile utilizzare una chiave generata con lo stesso programma oppure una password a nostro piacimento. L' algoritmo eseguirà una somma carattere per carattere (in ASCII) tra la chiave e il testo da codificare. Il programma chiederà, prima dell' inserimento del testo, di inserire la chiave per la codifica:

```
Inserisci la chiave per la codifica
```

A fine procedura, il programma restituirà il testo codificato:

```
La frase codificata e':  
ááÂÁº ûáç¼ ôá↳|| ¼½p
```

Decodifica di un messaggio con chiave di cifratura

Selezionando questo tipo di decodifica è possibile decodificare un testo codificato utilizzando la codifica con chiave di cifratura. Per poter visualizzare correttamente il testo, infatti, bisogna inserire la stessa chiave di cifratura inserita per la codifica e che verrà richiesta prima dell' inserimento del testo codificato. A fine procedura, il programma restituirà il testo decodificato.

Codifica/decodifica di un messaggio in esadecimale con chiave di cifratura numerica e XOR bit a bit

Questo tipo di codifica utilizza l'operazione di XOR tra ogni singolo carattere da codificare ed i caratteri di una chiave di cifratura. L'utente inserirà la parola o la frase da codificare/decodificare ed una chiave. È possibile utilizzare una chiave generata con lo stesso programma oppure una password a nostro piacimento. La parola o frase codificata verrà riportata in esadecimale; in fase di decodifica si potrà scegliere se visualizzare la parola o frase decodificata in esadecimale o in caratteri ASCII.

Genera chiave di cifratura

Tramite questa scelta è possibile generare randomicamente una chiave di lunghezza 24 caratteri da utilizzare per la codifica di un messaggio con chiave di cifratura e la codifica XOR bit a bit. Questa chiave serve per la successiva decodifica quindi è necessario salvarla in un posto sicuro o inviarla tramite canale sicuro al destinatario del messaggio.

Aiuto

Questa sezione serve per poter ottenere chiarimenti immediati, direttamente dentro il programma, su come utilizzare il software:

```
Su quale sezione vorresti dei chiarimenti?  
1) Codifica di un messaggio  
2) Decodifica di un messaggio  
3) Codifica di un messaggio con chiave di cifratura  
4) Decodifica di un messaggio con chiave di cifratura  
5) Codifica di un messaggio con chiave di cifratura e XOR bit a bit  
6) Decodifica di un messaggio con chiave di cifratura e XOR bit a bit  
7) Genera chiave di cifratura  
8) Torna al menu' principale
```