Cifrario di Cesare, encryption

Il cifrario di Cesare costituisce uno tra i più antichi algoritmi crittografici conosciuti. Esso si basa sull'utilizzo dell'aritmetica modulare e ogni carattere x viene criptato secondo la seguente relazione

$$\mathcal{C}(x) = (x + s) \ mod \ a, \tag{1}$$

Dove $\mathcal{C}$ è la funzione di cifratura, a il numero di lettere che compongono l'alfabeto considerato ($a = 21$, da 0 a 20 se consideriamo l'alfabeto italiano) e s indica il numero di spostamenti verso destra che devono essere compiuti per effettuare la sostituzione di un carattere.

Supponiamo ad esempio di lavorare con l'alfabeto italiano, quindi $a = 21$, e di volere trovare $\mathcal{C}(x)$ dove $x =' b'$, sapendo che $s = 3$. Avremo dunque che $\mathcal{C}(x) =' e'$. Implementare la procedura di cifratura di Cesare considerando l'alfabeto italiano, in modo da poter cifrare una qualunque stringa di caratteri appartenenti a tale alfabeto. L'implementazione dell'esercizio richiesto deve essere accompagnata da relazione che comprenda una breve introduzione al tipo di tecnica utilizzata e la spiegazione del codice.