Per a poder dur a terme les operacions criptogràfiques calia definir un alfabet amb una equivalencia numérica per a fer el desplaçament de carácter indicat per la clau. La especificació de la pràctica no deia quin alfabet de caràcters haviem d’utilitzar així que nosaltres vam decidir utilizar les lletres majúscules dels caràcters en ASCII (American Standard Code for Information Interchange). D’aquesta manera utilitzàvem l’equivalencia numérica entre caràcters i nombres donada per aquesta codificació (taula 1).

El conjunt de lletres majúscules eren els caràcters del 65 fins al 90, tots dos inclosos. Aquest rang de caràcters representa el conjunt de les majúscules present en anglès, pel que val a dir que la ‘ç’ i la ‘ñ’ així com les seves majúscules no es troben incloses en aquest conjunt. La resta de caràcters que no estan presents en aquest conjunt s’ignoren. Com el seu tractament no canvia, qualsevol cosa que no sigui una lletra en el rang anterior será per anosaltres un carácter especial.

Primer de tot es llegeix tot un fitxer com un sol String i es retorna. Prèviament li hem aplicat el mètode upperCase() de la classe String, que serveix per a transformar totes les minúscules en majúscules. Això ho fem per a que tot el que es potencialment informació (lletres) es trobi en el rang d’encriptació.

L’alfabet de caràcters d’encriptació s’utilitza com si fos circular, és a dir, si al aplicar l’algoritme d’encriptació o desencriptació obtenim un caràcters que se surten de l’alfabet, passarem aquest nombre per a recomençar a comptar per l’altre costat. Per exemple, si tenim el caràcter ‘X’ i la clau del missatge ens indica que hem de sumar 4 al caràcter, obtindríem el símbol ‘\’, però com el que ens interessa és obtener un caràcter, tractem l’alfabet de manera circular, de manera que busquem el nombre de caràcters que ens hem sortit de l’alfabet (en aquest cas ens sortim de dos caràcters), i ho sumem com si vinguéssim de la posició 0 de l’alfabet, de manera que obtenim el caràcter ‘B’. De manera anàloga succeeix a la hora de desfer la encriptació, però en lloc de sortir-nos per la part del final de l’alfabet, ens sortiríem del principi, pel que les operacions serien les inverses.

Després d’això, segons esculli l’usuari es duu a terme l’encriptació o la desencriptació,

L’algoritme d’encriptació consisteix en el recorregut d’un vector de caràcters que conté el missatge. A cada iteració es fa un casting a int per a obtenir el nombre ASCII del caràcter en la posició determinada i es mira que es trobi en el rang de caràcters que formen el conjunt d’encriptació. Si es troba en aquest rang es desencua el valor de la clau i es torna a reencuar. Aquest valor es suma al nombre ASCII del caràcter i es fan les operacions necessàries si es surt de l’alfabet. A mesura que es va recorrent l’array es va actualitzant cada carácter que pertanyi al conjunt d’encriptació per la seva versió encriptada. Després s’actualitza l’array de caràcters.

L’algoritme de desencriptació funciona de la manera anàloga a l’algoritme d’encriptació, però aquest cop desfent el canvi.