

Functions

void getinputc

Inputs: inputstring,
integer sizelimit

Flowchart below for this fn

Gets an inputstring(max size sizelimit) from user, cleans it (removes newlines and turns all lowercase to uppercase) and stores cleaned string back to inputstring

void keyinput

Inputs: inputstring,
integer matrix[[3]

Fills up int array matrix [3][3] with the contents of an inputstring. Function does this by assigning all 27 chars of the alphabet with a unique integral equivalent. (A=0, B=1, ' '=26). Afterwards, assigns all 9 characters of inputstring to matrix.

int checknum

Inputs: inputstring,
integer sizelimit

checks each character of inputstring to make sure that it only contains letters of the alphabet (A to Z, a to z, ' '). Returns value 0 if special char detected. Value 1 if all chars valid.

flowchart for fn below

int checkfordetmatrix

Inputs: integer matrix[[3]

Gets the determinant of the matrix[3][3] by using given formula. If determinant is 0 or has a common factor w/ 27, fn returns value 0. Else, fn returns the value of determinant.

flowchart for fn below

void encrypt

Inputs: inputstring, int
keymatrix[[3], int
sizelimit

Gets an inputstring from user, performs getinputc and checknum, then checks if inputstring is a multiple of 3. If not, adds extra spaces to the end of string. Afterwards, places three characters of inputstring into a temporary chararray[3][1] at a time. Function then performs matrix multiplication to chararray and keymatrix[3][3] to get 3 characters for the encrypted message. Prints the 3 resultant characters. Repeats until end of inputstring reached.

Flowchart below for this fn

Decryption function is the same as encrypt , though adds a few extra separate functions to make it work: (aka program uses "encrypt" with below functions to decrypt)

int modularmultinverse

Inputs: int determinant

Gets an int determinant (from previous function checkfordetmatrix) and applies given formula to find x in $ax(\bmod n)=1$. Returns the value of x (this is the modmultinverse).

flowcharts below for these 2 fns

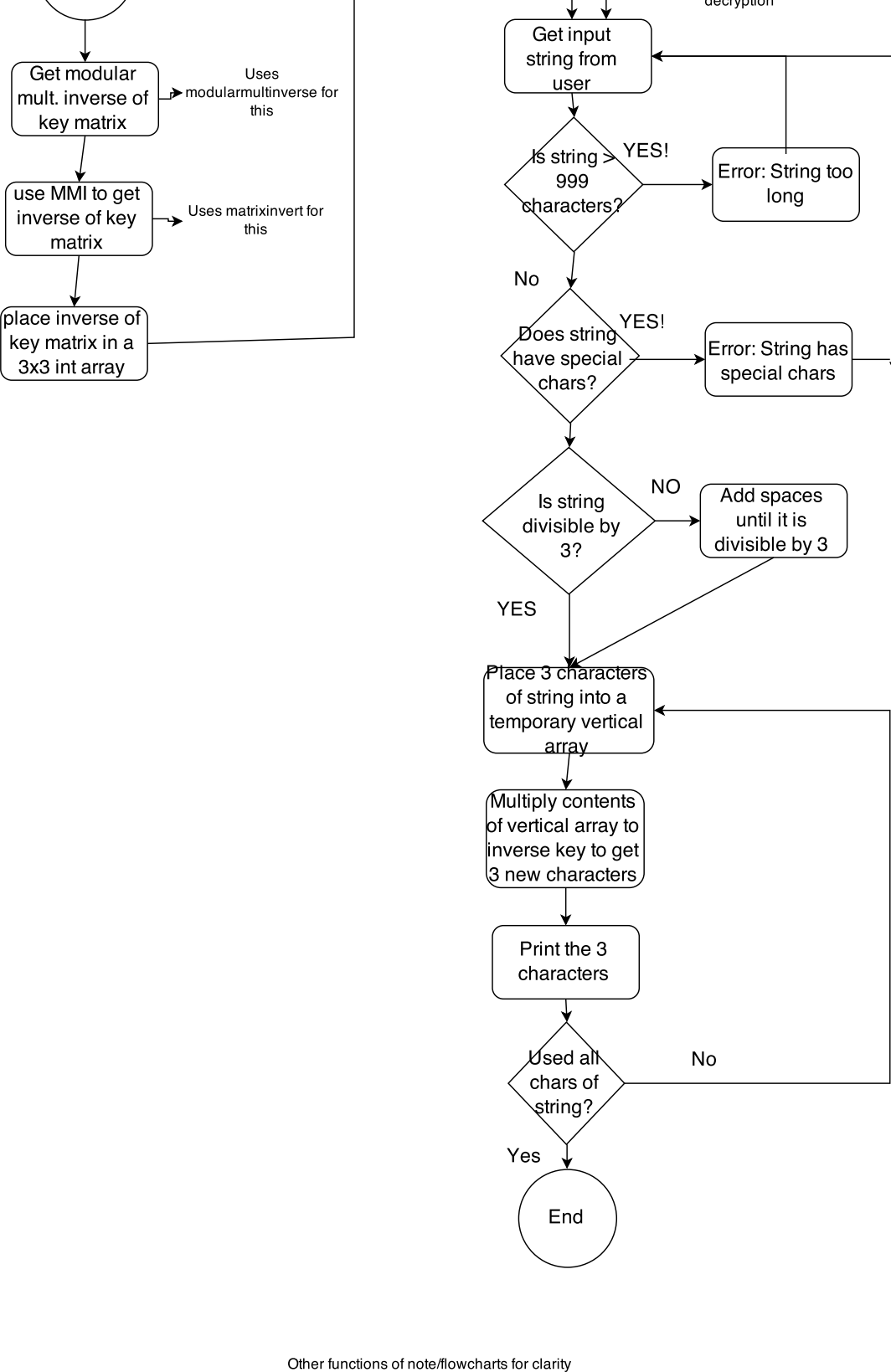
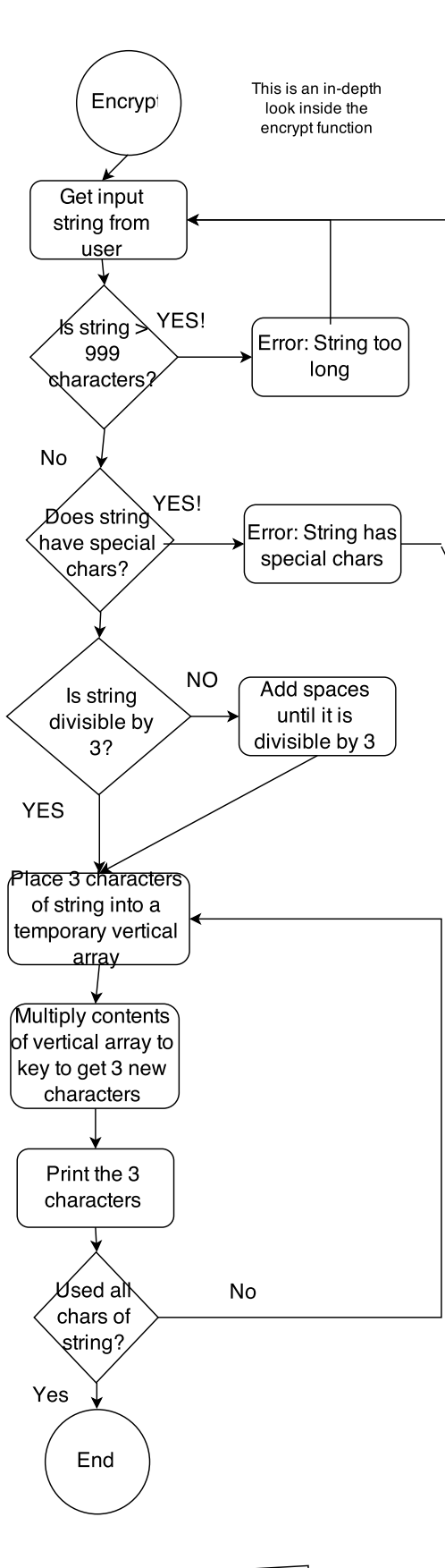
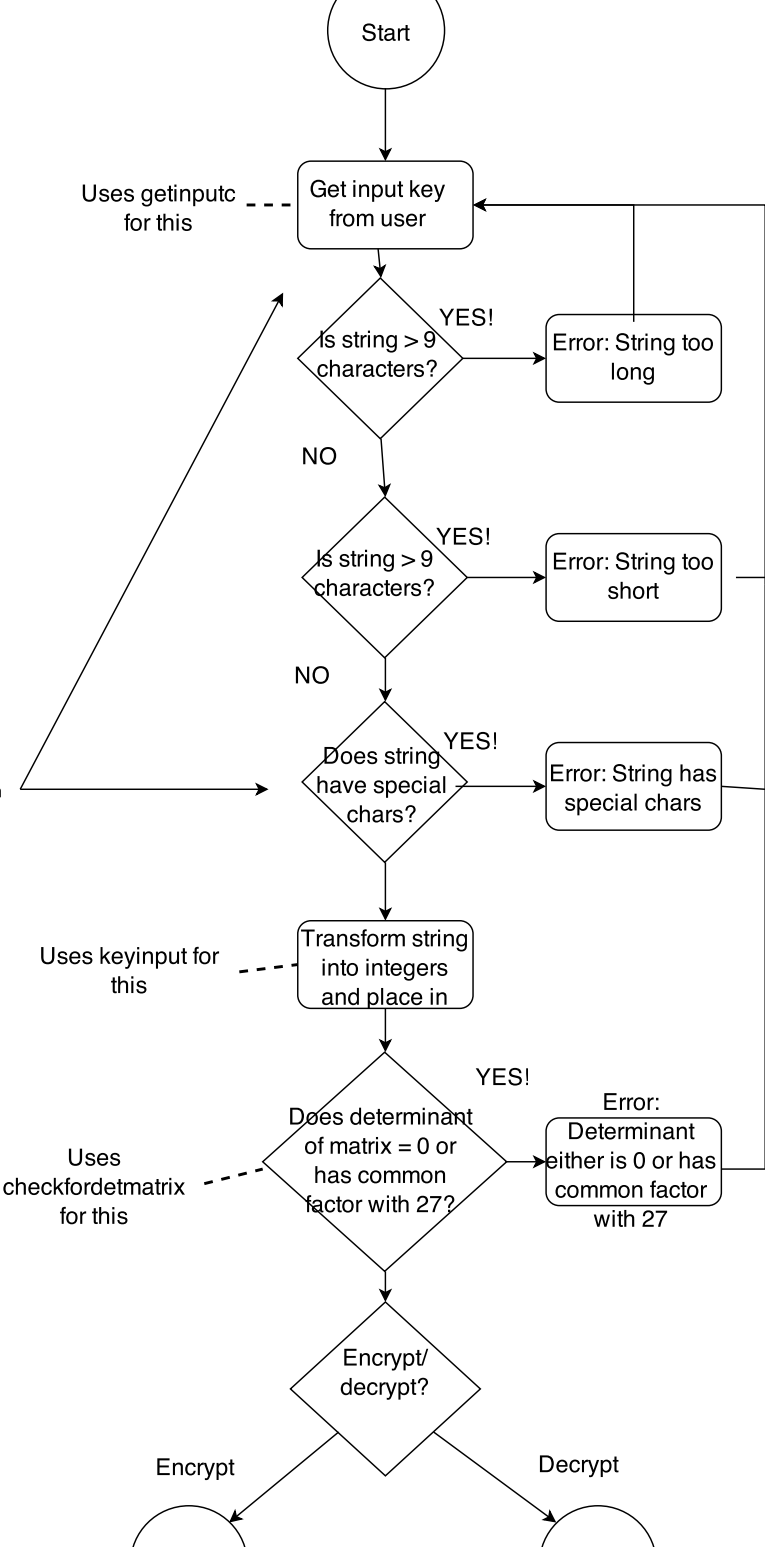
int matrixinvert

Inputs: matrixsource[[3],
matrixdest[[3], int
modmultinverse

Gets every element of matrixsource[3][3] and inverts the matrix using given formula. Afterwards, multiplies each resultant element with modmultinverse to get the correct element, then places each new element into matrixdest[3][3].

Functions bordered by this vertical line are part of the key validity group of functions

These are used only for the decryption process



Other functions of note/flowcharts for clarity

