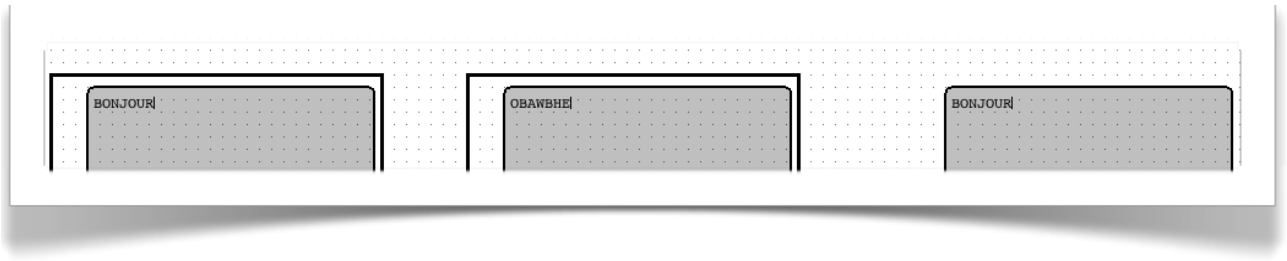
Ave César

Objectif

Obtenir un circuit permettant de chiffrer un texte. Le chiffre à utiliser est celui appelé « chiffre de César » ou « rot13 » chez les informaticiens. Son principe est très élémentaire puisqu'il s'agit de la simple permutation (A N) (B O) ... (M Z). Ce chiffre fait partie de la famille des chiffres à décalage qui n'offrent aucune résistance cryptographique, mais sont simplement mentionnés pour des raisons historiques ou pédagogiques. Rot13 n'est qu'une des variantes du chiffre de César qui est en réalité paramétré par le décalage de l'alphabet (donc 25 chiffres de César possible). La particularité de rot13 est qu'il est involutif. On cherchera donc à vérifier cette propriété par exemple en chiffrant puis chiffrant à nouveau et à la suite le texte d'entrée comme dans la figure suivante :



Élements utiles

Les éléments pouvant servir sont :

- keyboard (permettant de saisir le texte à chiffer)
- tty (pour affiche le résultat)
- portes arithmétiques diverses
- constantes
- bit extender (pour convertir les données 7 bits en 8 bits et vice-versa)

Réalisation

La difficulté ici est essentiellement de bien comprendre comment l'arithmétique est réalisée. Diverses constructions peuvent être obtenues :

1. dans un premier temps, à obtenir un circuit convertissant une donnée 7 bits en une donnée 8 bits équivalente (sous réserve que l'entrée est un caractère alphabétique majuscule)
2. modifiez le circuit de sorte que les caractères autres que les lettres majuscules soient conservés à l'identique (via des opérateur de comparaison, etc)
3. modifiez le circuit de sorte que le chiffre s'applique sur les lettres alphabétiques majuscules et minuscules
4. faites du circuit de chiffrement un sous-circuit en rajoutant un autre circuit (Project ☛ Add circuit) et en faisant du nouveau le circuit principal (sélectionnez-le et faites apparaître le menu contextuel Set As Main Circuit), puis ajoutez keyboard et tty(s) pour saisir un texte et voir son chiffrement et déchiffrement opérer (via une horloge manuelle ou non).

Un projet pour lycéen pourrait être de réaliser un circuit réalisant le chiffrement DES (Data Encryption Standard). Cet algorithme de chiffrement est utilisé pour chiffrer les mots de passe de presque tous les systèmes d'exploitation depuis plus de 30 ans. Attention : c'est assez difficile à réaliser mais intéressant car pour obtenir un circuit raisonnable, il faut faire « tourner » les données à l'intérieur du circuit...