Cryptographie

1ère partie

Jules César, pendant la guerre des Gaules, eu l'idée simple mais efficace, de transmettre des messages en décalant chacune des lettres de 3 crans dans l'alphabet. Ainsi, *a* devient *d*, *b* devient *e*, etc...
Depuis, tout système par décalage, quel que soit le nombre de crans choisi, est appelé "alphabet de Jules César".
1) Créer une fonction **[b]=codage_cesar(a,n)** avec un décalage donné par **n** et permettant de coder une phrase constituée de lettres en majuscules et de blancs. (une seconde version pourra transformer la chaîne en majuscules)
2) Créer une fonction de décodage permettant, par exemple, de lire la phrase, suite à un décalage de 7 crans :

"SL KLCVPY LZA ALYTPUL".

2ème partie

Il s'agit de construire deux fonctions, l'une servant à coder un texte, l'autre le décrypter.
Pour transmettre un message, on peut utiliser le système de cryptage à clé secrète suivant :

1ère étape : On supprime tout d'abord les caractères qui ne sont pas des lettres et on transforme les lettres restantes en leurs majuscules.
A chaque lettre du message en clair, on associe son rang dans l'alphabet (précédé de 0 si ce numéro est inférieur ou égal à 9) : A → 01, B → 02, ..., Z → 26
Exemple, pour le message Le contact aura lieu demain, il devient successivement LECONTACTAURALIEUDEMAIN, puis :
12 05 03 15 14 20 01 03 20 01 21 18 01 12 09 05 21 04 05 13 01 09 14

2ème étape : la clé secrète est un mot, par exemple NATUREL, que l'on transforme en chiffres comme dans la première étape. Ici, 14 01 20 21 18 05 12.

3ème étape : on aligne l'un en-dessous de l'autre le message en chiffres et la clé en chiffre (répétée autant de fois que nécessaire) :
12 05 03 15 14 20 01 03 20 01 21 18 01 12 09 05 21 04 05 13 01 09 14
14 01 20 21 18 05 12 14 01 20 21 18 05 12 14 01 20 21 18 05 12 14 01
On additionne en colonne les nombres écrits ; lorsque la somme dépasse 26, on diminue le résultat obtenu de 26.
Dans l'exemple, on obtient ainsi le message (secret) suivant :
01 06 23 10 06 25 13 17 21 21 16 10 06 24 23 06 15 25 23 18 13 23 15

Ecrire la fonction **[b]=codage_crypto(a,cle)** qui effectue la tache suivante.
On peut tout d'abord supposer que toutes les lettres des chaînes sont transformées en leurs majuscules et que tous les blancs ont été supprimés.
Vous devrez construire un premier tableau faisant correspondre à chaque lettre de la chaîne **a** son rang dans l'alphabet.
Vous devrez ensuite créer une chaîne **c** constituée de la chaîne **cle** répétée autant de fois que nécessaire pour atteindre la longueur de la chaîne **a** et coder la chaîne **c** dans un autre tableau comme pour la chaîne **a**.
Vous pourrez ensuite effectuer le codage grâce aux tableaux ainsi construits :

- construction de la somme des tableaux au décalage de 26 près
- constitution de la chaîne correspondant à ces rangs dans l'alphabet

Création du programme de décodage : **[b]=codage_crypto(a,cle)**
On suppose dans ce cas que l'on connaît le texte à décrypter a (il est constitué de la suite des chiffres) et la clé du codage (cle).
Utilisez et modifiez les éléments de codage pour construire cette fonction de décodage.

```
function [b]=codage_crypto(a,cle)

//transformation en majuscules
e='';
for i=1:length(a) do
if part(a,i)==' ' then e=e
elseif str2code(part(a,i))>0 then e=e+code2str(-(str2code(part(a,i))));
else e=e+part(a,i);
end
end
a=e

e='';
for i=1:length(cle) do
if part(cle,i)==' ' then e=e
elseif str2code(part(cle,i))>0 then e=e+code2str(-(str2code(part(cle,i))));
else e=e+part(cle,i);
end
end
cle=e

// une cle de longueur la chaine
n=modulo(length(a),length(cle))
c=''
for i=1:((length(a)-n)/length(cle)) do
c=c+cle;
end
for i=1:n do
c=c+part(cle,i);
end

//construction des tableaux
taba=zeros(1,length(a))
for i=1:length(taba) do
taba(i)=ascii(part(a,i))-ascii('A')+1;
end
disp(taba)

tabc=zeros(1,length(a))
for i=1:length(tabc) do
tabc(i)=ascii(part(c,i))-ascii('A')+1;
end
disp(tabc)

tabb=taba
for i=1:length(tabb) do
tabb(i)=modulo(tabb(i)+tabc(i)-1,26)+1
end
disp(tabb)
```

```
//construction de b
b="
for i=1:length(tabb) do
if tabb(i)<10 then b=b+'0'+string(tabb(i));
else b=b+string(tabb(i));
end
end

function [b]=decodage_crypto(a,cle)

e='';
for i=1:length(cle) do
if part(cle,i)==' ' then e=e
elseif str2code(part(cle,i))>0 then e=e+code2str(-(str2code(part(cle,i))));
else e=e+part(cle,i);
end
end
cle=e

// une cle de longueur la chaine
n=modulo(length(a)/2,length(cle))
c="
for i=1:((length(a)/2-n)/length(cle)) do
c=c+cle;
end
for i=1:n do
c=c+part(cle,i);
end

//construction des tableaux
taba=zeros(1,length(a)/2)
for i=1:length(taba) do
taba(i)=evstr(part(a,[2*i-1 2*i]));
end

tabc=zeros(1,length(a)/2)
for i=1:length(tabc) do
tabc(i)=ascii(part(c,i))-ascii('A')+1;
end

tabb=taba
for i=1:length(tabb) do
tabb(i)=modulo(tabb(i)-tabc(i)-1,26)+1
if tabb(i)<0 then tabb(i)=tabb(i)+26; end
end

//construction de b
b="
for i=1:length(tabb) do
b=b+ascii(tabb(i)+64);end
```