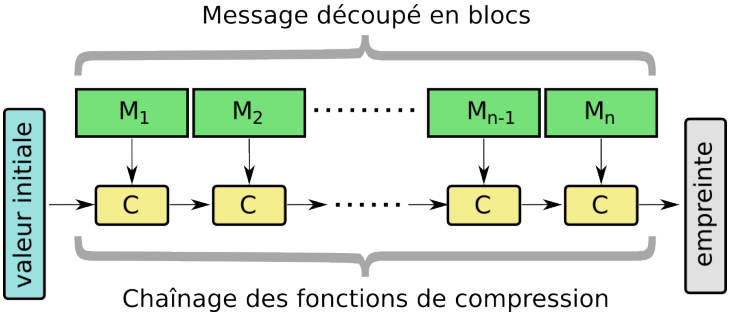
TD 4 : Hachage. Signatures numériques

• Fonction de hachage TTH

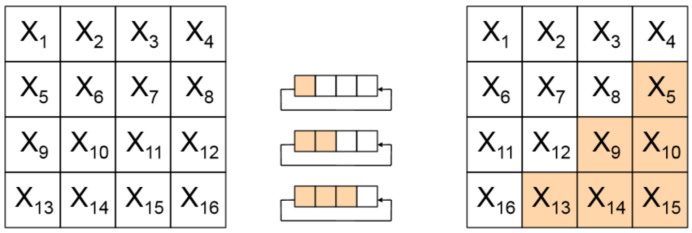
On construit une fonction de hachage appelée **Toy Tetragraph Hash** (TTH) qui travaille sur l'alphabet $\{A, ..., Z\}$. Etant donnée une suite de lettres, TTH fournit une empreinte sous la forme d'une suite de 4 lettres dont l'équivalent numérique modulo 26 s'appelle **Total**. Il a pour valeur initiale **(IV)** qui vaut $(0, 0, 0, 0)$.
On utilisera l'encodage usuel de l'alphabet :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- **Pas 0 :** Tout d'abord, TTH scinde le message en blocs de 16 lettres en ignorant les espaces et la ponctuation.
  Si la longueur du message n'est pas un multiple de 16, TTH complète avec le caractère A d'équivalent numérique 0.



- **Pas 1 :** On applique une **fonction de compression** au bloc courant :
  – On arrange les 16 lettres en un tableau 4×4 en arrangeant les lettres ligne par ligne.
  – On convertit ce tableau en une matrice d'entiers modulo 26.
  – On calcule la somme de chaque colonne modulo 26 et on l'ajoute à la valeur de **Total**.



- **Pas 2 :** En utilisant le tableau du même bloc, on fait subir une permutation circulaire à chacune des lignes :
  – une permutation circulaire d'une position vers la gauche pour la seconde ;
  – une permutation circulaire de deux positions vers la gauche pour la troisième ;
  – une permutation circulaire de trois positions vers la gauche pour la 4e.
- **Pas 3 :** On calcule la somme de chaque colonne mod 26 et on l'ajoute à la valeur de **Total**. Cette nouvelle valeur de **Total** constitue l'entrée de la fonction de compression pour le bloc suivant.

anca.nitulescu@ens.fr

Exercice 1
Utilisez la fonction TTH pour calculer l'empreinte du message :

LE HACHAGE AVEC TTH EST FACILE.

- **Pas 0 :**

LEHACHAGEAVECTTH

ESTFACILEAAAAAAA

- **Pas 1 :**

L	E	H	A
C	H	A	G
E	A	V	E
C	T	T	H

E	S	T	F
A	C	I	L
E	A	A	A
A	A	A	A

Total := | 0 | 0 | 0 | 0 | $\bigoplus$ | · | · | · | · |

• Paradoxe des anniversaires

Exercice 2
En utilisant le paradoxe des anniversaires, donnez le nombre de messages à considérer pour avoir plus d'une chance sur deux de trouver une collision pour TTH.

• Signature ElGamal

Exercice 3 On considère les paramètres suivants pour la signature ElGamal : $(p = 467, g = 2, x = 65)$.

1. Justifiez la validité du choix de p et g. (Regardez l'ordre de $g \in \mathbb{Z}_p^\star$.)
2. Calculez la clé publique $X = g^x \mod p$.
3. Calculez la signature du message $m = 100$ en utilisant les valeurs aléatoires $r_1 = 5$ et $r_2 = 213$.
4. Montrez que la vérification fonctionne pour les deux signatures obtenues.

• Signature RSA

Exercice 4 Bob a une clé privée RSA pour signer des messages : $(d = 7, p = 11, q = 3)$.

1. Pour authentifier ses messages, il doit publié sa clé de vérification. Choisissez une clé publique valide pour Bob : (e, n).
2. Bob veut envoyer le message signé $m = 13$ à Alice. Pourriez-vous aider Bob à calculer la signature pour ce message ?
3. Alice reçoit la signature $\sigma = 24$. Donnez la valeur d'un message provenant de Bob pour lequel la signature σ est valide.