REPUBLIQUE TUNISIENNE MINISTERE DE L'EDUCATION ❖❖❖❖❖ **EXAMEN DU BACCALAUREAT** ❖❖❖❖❖ SESSION DE JUIN 2015	**EPREUVE PRATIQUE D'INFORMATIQUE** **SECTIONS** MATHEMATIQUES SCIENCES EXPERIMENTALES SCIENCES TECHNIQUES **DATE : 21/05/2015** **DUREE :** 1h **COEFFICIENT :** 0.5

Important :

1) Une solution modulaire au problème posé est exigée.

*2) Enregistrer au fur et à mesure votre programme dans le dossier **bac2015** se trouvant sur la racine du disque C en lui donnant comme nom votre **numéro d'inscription (6 chiffres).***

Pour sécuriser l'envoi des messages, deux chercheurs cryptent leurs messages en utilisant le principe suivant :

1. Saisir le message à crypter **msg**, sachant qu'il est composé uniquement par des lettres,
2. Remplir un tableau **T** par les ordres alphabétiques des lettres de **msg** de façon à ce que **T[i]** lui correspond de **msg[i]** (Sachant que "**A**" et "**a**" sont d'ordre 1, "**B**" et "**b**" sont d'ordre 2, ...),
3. Remplacer chaque **T[i]** par $(T[i])^e$ **mod (p*q)** avec **p**, **q** et **e** trois constantes ayant pour valeurs respectivement **17**, **19** et **5**.

   Le tableau **T** ainsi obtenu représente le code de la chaine **msg**.

Exemple :

Pour la chaîne **msg**="Bonjour", T sera remplit initialement comme suit :

	1	2	3	4	5	6	7
T	2	15	14	10	15	21	18

En effet "B" et d'ordre alphabétique 2, "o" est d'ordre alphabétique 15, …

Après avoir coder en remplaçant chaque **T[i]** par $(T[i])^e$ **mod (p*q) on obtient :**

	1	2	3	4	5	6	7
T	32	2	29	193	2	89	18

En effet :
T[1] est remplacé par $(T[1])^e$ mod (p*q)= 2^5 mod (17*19) = 32
T[2] est remplacé par $(T[2])^e$ mod (p*q)= 15^5 mod (17*19) = 2
Etc.

Travail demandé :

Ecrire un programme Pascal qui permet de saisir une chaîne non vide formée uniquement par des lettres, de la crypter selon le principe décrit ci-dessus et d'afficher le tableau de code obtenu.

Grille d'évaluation :

Questions	Nombre de points
Décomposition en modules	**2**
Appels des modules	**2**
Si exécution et tests réussis avec respect des contraintes	**16**
Sinon	
▪ Structures de données adéquates au problème posé	**3**
▪ Saisie de **msg** avec respect des contraintes	**4**
▪ Cryptage de la chaîne (**1er remplissage** de T + **2ème remplissage** de T)	**7 = (3.5 + 3.5)**
▪ Affichage	**2**