TP - Félix Leturgez

Puissance modulo n et chiffrement/déchiffrement d'un entier

Question 11 :
cf script

5^11 = 5x2^1 + 5x2^2 + 5x2^0 + 5x2^8
17^154 = 17x2^0 + 17x2^2 + 17x2^0 + 17x2^8 + 17x2^16 + 17x2^0 + 17x2^0 + 17x2^128
4^13 = 4x2^1 + 4x2^0 + 4x2^4 + 4x2^8

Question 12:

Les attributs de cette classe sont ***int p***, ***int q***, ***int* e**, ***int n*** qui sont nécessaire à trouver **d**.

Question 13 :

les conditions à respecter :
- n = p x q
- z = (p - 1) x (q - 1)
- e est premier avec z

Question 14 :

d = e^-1 modulo z

Question 15 :
(5, 7, 35) a pour clé de déchiffrement d = 11.

Question 16:
cf script

Question 17 :
Le message clair 222 devient chiffré en : 52 avec le triplet (5, 17, 5).

Question 18 :
cf script

Question 19 :
ex avec la valeur 147 pour le triplet (5, 17, 5).
La valeur déchiffrée est : 7

Question 21 :
On peut utiliser la valeur ASCII de chaque caractère.

Question 22 :

Cette méthode sera dans la classe RSA car elle permet le chiffrement également.

Question 23 :

Codé par bloc est plus sécurisé car on crypte par bloc et non par lettre. Il est donc plus difficile de décoder des combinaisons de lettres plutôt qu'une lettre par une lettre.