ENSIAS, Rabat, 2012-2013

CRYPTOGRAPHIE et MAPLE
QCM (14 points)
Version B
Durée : 1 heure

Chaque question n'a qu'une seule bonne réponse.
Cocher la bonne réponse dans le tableau de la page 5, qui est à rendre.
Aucun document n'est autorisé.
Les machines à calculer sont interdites.

Question 1. (1 point)
Soit $a \in (\mathbb{Z}/101\mathbb{Z})^*$. On sait que a n'est pas un générateur de $(\mathbb{Z}/101\mathbb{Z})^*$ et que son ordre est supérieur à 30. Alors son ordre est

A. 101.

B. 100.

C. 50.

D. 51.

E. 75.

Question 2. (1 point)
Soit n un nombre entier impair. Soit a un nombre entier avec $\text{pgcd}(a, n) = 1$ et $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$. Alors :

A. n n'est pas premier.

B. $\frac{n-1}{2}$ est premier.

C. n n'est pas pseudo premier fort en base a.

D. $a^{n-1} \equiv -1 \pmod{n}$.

E. n est pseudo premier en base a.

Question 3. (1 point)
On considère la procédure suivante :

```
pi :=proc(n)
local i,S,a;
if n < 2 then
return( "Try n > 1");
else
S :=0;
for i from 1 to n do
if isprime(i) then
S :=S+i;
end if;
end do;
end if;
return S;
end proc :
```

On exécute pi(12). La réponse est alors :

A. 30.

B. 25.

C. 24.

D. 28.

E. 12.

Question 4. (1 point)
On considère le cryptosystème RSA avec $N = 391$ et la clé privée $d = 5$. Le déchiffrement du message crypté $C = 101$ est :

A. 169.

B. 144.

C. 121.

D. 100.

E. 81.

Question 5. (1 point)
On donne un module RSA $N = pq$ avec $q < p < 3q$. Alors p et q vérifient :

A. $\frac{1}{3}\sqrt{N} < q < \sqrt{N} < p < \sqrt{3}\sqrt{N}$.

B. $\frac{\sqrt{3}}{3}\sqrt{N} < q < \sqrt{N} < p < \sqrt{3}\sqrt{N}$.

C. $\sqrt{N} < q < \sqrt{2}\sqrt{N} < p < \sqrt{3}\sqrt{N}$.

D. $\frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N} < p < 3\sqrt{N}$.

E. $\frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N}$.

Question 6. (1 point)
On considère le cryptosystème RSA avec la clé publique $N = 35$, $e = 3$. Le chiffrement du message $M = 32$ est :

A. 12.

B. 1.

C. 8.

D. 9.

E. 6.

Question 7. (2 point)
On considère le cryptosystème RSA avec la clé publique $N = 451$, $e = 117$. La clé privée est :

A. $d = 119$.

B. $d = 113$.

C. $d = 233$.

D. $d = 263$.

E. $d = 253$.

Question 8. (2 point)
On considère le cryptosystème El Gamal avec le groupe $(\mathbb{Z}/83\mathbb{Z})^*$ et le generateur $g = 28$. Pour recevoir des messages, la personne A choisit une clé privé a secrète et publie $16 \equiv g^a \pmod{83}$. La personne B choisit une clé privé $k = 6$ et veut envoyer le message $M = 25$. Les valeurs de γ, δ que doit envoyer B sont :

A. $\gamma = 23$, $\delta = 25$.

B. $\gamma = 41$, $\delta = 75$.

C. $\gamma = 63$, $\delta = 34$.

D. $\gamma = 23$, $\delta = 26$.

E. $\gamma = 61$, $\delta = 63$.

Question 9. (2 point)
On considère la procédure suivante :

```
pi2 := proc (n, b)
local k, L, q, i ;
if n=0 then return [0]
else
k := floor(ln(n)/ln(b))+1 ;
L := [] ;
q := n ;
for i from 0 to k-1 do
L := [op(L), iquo(q, b^(k − 1 − i))] ;
q := q mod b^(k − 1 − i) ;
end do ;
end if ;
return L ;
end proc :
```

On exécute pi2(13,2). La réponse est alors :

A. $[1, 1, 1, 0]$.

B. $[1, 1, 0, 1]$.

C. $[1, 0, 0, 0]$.

D. $[1, 1, 0, 0]$.

E. $[1, 0, 0, 1]$.

Question 10. (2 point)
On considère le protocole d'échange de clés de Diffie-Hellman avec le groupe $(\mathbb{Z}/151\mathbb{Z})^*$ et le generateur $g = 7$. Pour échanger une clé K, la personne A choisit une clé privé $a = 6$ et la personne B choisit une clé privé $b = 4$. La clé commune est alors :

A. $K = 91$.

B. $K = 19$.

C. $K = 35$.

D. $K = 49$.

E. $K = 17$.

ENSIAS, Rabat, 2012-2013

CRYPTOGRAPHIE et MAPLE
QCM (15 points)

NOM :.....

Prénom : .....

	Réponse A	Réponse B	Réponse C	Réponse D	Réponse E
Question 1 : 1 point					
Question 2 : 1 point					
Question 3 : 1 point					
Question 4 : 1 point					
Question 5 : 1 point					
Question 6 : 1 point					
Question 7 : 2 point					
Question 8 : 2 point					
Question 9 : 2 point					
Question 10 : 2 point					