ENSIAS, Rabat, 2012-2013

CRYPTOGRAPHIE et MAPLE
QCM (14 points)
Version A
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 p un nombre premier et a un entier non nul. On dit que a est un résidu quadratique modulo p si :

A. $x \equiv a^2 \pmod{p}$ admet une solution.

B. $x^2 \equiv a \pmod{p}$ n'a pas de solutions.

C. $x^2 \equiv a \pmod{p}$ admet une solution.

D. x est inversible modulo p.

E. $x^2 \equiv -a \pmod{p}$ admet une solution.

Question 2. (1 point)
Soit n un nombre entier. Soit a un nombre entier avec $\text{pgcd}(a, n) = 1$ et $a^{n-1} \not\equiv 1 \pmod{n}$. Alors :

A. n est premier.

B. n est composé.

C. n est pseudo premier en base a.

D. n est pseudo premier fort en base a.

E. $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$.

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

```
pi :=proc(n)
local i,L ;
L :=[] ;
if n < 0 then
return( "Try n > 1") ;
else
for i from 1 to n do
L :=[op(L),ithprime(i)] ;
end do ;
end if ;
return L ;
end proc :
```

On exécute pi(6). La réponse est alors :

A. $[2, 3, 5, 7, 9, 11]$.

B. $[13, 11, 7, 5, 3, 2]$.

C. $[1, 2, 3, 4, 5, 6]$.

D. $[2, 3, 5, 7, 11, 13]$.

E. $[1, 2, 3, 5, 7, 11]$.

Question 4. (1 point)
On considère le cryptosystème RSA avec la clé publique $N = 15$, $e = 4$. Le chiffrement du message $M = 12$ est :

A. 12.

B. 1.

C. 3.

D. 9.

E. 6.

Question 5. (1 point)
On considère le cryptosystème RSA avec $N = 221$ et la clé privée $d = 11$. Le déchiffrement du message crypté $C = 2$ est :

A. 59.

B. 11.

C. 4.

D. 16.

E. 20.

Question 6. (1 point)
On donne un module RSA $N = pq$ avec $q < p < 2q$. Alors p et q vérifient :

A. $\frac{1}{2}\sqrt{N} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N}$.

B. $\frac{1}{4}\sqrt{N} < q < \frac{\sqrt{2}}{2}\sqrt{N} < p < \sqrt{N}$.

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

D. $\frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N} < p < \frac{5}{4}\sqrt{N}$.

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

Question 7. (2 point)
On considère le cryptosystème RSA avec la clé publique $N = 437$, $e = 17$. La clé privée est :

A. $d = 11$.

B. $d = 113$.

C. $d = 233$.

D. $d = 11$.

E. $d = 201$.

Question 8. (2 point)
On considère le protocole d'échange de clés de Diffie-Hellman avec le groupe $(\mathbb{Z}/101\mathbb{Z})^*$ et le generateur $g = 11$. Pour échanger une clé K, la personne A choisit une clé privé $a = 4$ et la personne B choisit une clé privé $b = 6$. La clé commune est alors :

A. $K = 11$.

B. $K = 17$.

C. $K = 21$.

D. $K = 56$.

E. $K = 22$.

Question 9. (2 point)
On considère le cryptosystème El Gamal avec le groupe $(\mathbb{Z}/71\mathbb{Z})^*$ et le generateur $g = 7$. Pour recevoir des messages, la personne A choisit une clé privé a secrète et publie $41 \equiv g^a \pmod{71}$. La personne B choisit une clé privé $k = 3$ et veut envoyer le message $M = 10$. Les valeurs de γ, δ que doit envoyer B sont :

A. $\gamma = 12$, $\delta = 24$.

B. $\gamma = 59$, $\delta = 13$.

C. $\gamma = 17$, $\delta = 34$.

D. $\gamma = 45$, $\delta = 11$.

E. $\gamma = 62$, $\delta = 28$.

Question 10. (2 point)
On considère la procédure suivante :

```
pi10 :=proc(a,b)
local m,n,c ;
m :=abs(a) ;
n :=abs(b) ;
while n > 0 do
c :=m mod n ;
m :=n ;
n :=c ;
od ;
return(m) ;
end proc ;
```

On exécute pi10(378,308). La réponse est alors :

A. 1.

B. 99.

C. 117.

D. 14.

E. 9.

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					