TEXT:. *Computer Engineers: Architects of the Future in a Digital World*

A computer engineer possesses a unique blend of technical skills and personal qualities that make them highly sought after in today's digital age. They are known for being authentic problem-solvers with a solid foundation in mathematics, programming, and hardware design, computer engineers excel at creating innovative solutions and optimizing system performance.

Computer engineers can find employment in various sectors and industries. They are in demand by technology companies, Finance, healthcare, both large and small, where they can contribute to software development, network design, and system architecture. These professionals are also valuable assets to research institutions and academic organizations, where they can engage in cutting-edge projects and advance the boundaries of technology.

Additionally, computer engineers can thrive in the field of cybersecurity. With the growing concerns surrounding data breaches and online threats, companies require experts who can develop robust security systems and safeguard sensitive information. They play a vital role in designing effective defense mechanisms, ensuring the protection of valuable digital assets. Moreover, these engineers are well suited for positions in the field of embedded systems. Their presence in a workplace is impactful since their personality is apparent, they are analytical, detail-oriented, curious, and persistent as they can fit in the teamwork with their possession of key ethical mindset and self-motivation.
In recent years, artificial intelligence (AI) and machine learning have gained significant prominence. Computer engineers with a background in AI can contribute to the development of intelligent systems, predictive analytics, and automation. They play a crucial role in leveraging data to extract insights, train models, and create intelligent algorithms that improve processes and decision-making.

Overall, a computer engineering degree opens up a world of opportunities. Whether working for technology giants like Google, Microsoft, or Apple, or joining cutting-edge startups and research institutions, computer engineers have a wide range of career paths to explore. Their expertise is invaluable in shaping the future of technology, they can explore a multitude of career paths and make a significant impact in the digital world.

QUESTIONS:

I/ Comprehension: (6pts)

a) Read the text and answer the questions: **/4.5pts**

1- What technical skills and qualities make computer engineers highly sought after in today's digital age? (0.75p)

2- In which sectors and industries can computer engineers find employment? (0.75p)

3- How do computer engineers contribute to the field of cybersecurity? (0.75p)

4- What role do computer engineers play in the development of artificial intelligence and machine learning systems? (0.75p)

5- What are some of the personality traits that can be found in a computer engineers? (0.75p)

6- How do computer engineers contribute to the optimization of system performance and the creation of innovative solutions? (0.75p)

b) Extract word synonyms from the text: **/1.5pts**

Firm (§1) = ……. Meticulous (§3) = ……. Important (§3) = ……

II/ Mastery of language: (10pts)

a) Conjugate the verbs between brackets using the right tense **/4pts**

1- By this time next year, I *(to finish)* the Java course and *(to start)* to program with ease. **(Future perfect continuous)**

2- I *(to delete)* all the unnecessary files from my computer because I *(to need)* space. **(Present perfect continuous) (Past simple)**

3- Indians *(to be)* skilled mathematicians for thousands of years. **(Present perfect)**

4- The court *(to find)* him guilty on all charges. **(Past perfect)**

5- By this time next year, I (to *work)* as a computer engineer after I *(to hopefully get)* my master's degree in computer science. **(Future continuous) (Present simple)**

b) Use the correct modal verb (Need- could – couldn't – ought to – mustn't – might – will) **/2pts**

1- Despite efforts, the team ……. fix a rare software bug causing intermittent system crashes
2- User interfaces ……. to be intuitive and user-friendly to enhance the experience
3- Computer engineers ……. eventually play a crucial role in integrating (IoT) devices into everyday life.
4- In AI field, it's possible that deep learning techniques ……. revolutionize various industries and transform the way we live.

c) Transform the following sentences from active voice into passive voice. **/2pts**

1- The professor is assigning weekly homework to the students.
2- They have implemented a new security system to protect sensitive data.
3- The teacher teaches the students a complex math concept.
4- She will complete the project by the end of the week.

III/ Written expression: (6pts)

Write a motivation letter consisting of a text ranging from 6 to 12 lines, describing your personality and your drive to join a computer engineering company (optional name) for an internship. In this letter, focus on mentioning key elements and strategies that show your enthusiasm, qualifications, and compatibility with the company.

You can use adjective likes (Self-motivated/ self-confident/ creative/ ambitious/ responsible/ courageous/ curious/ driven/ committed...etc)

GOOD LUCK!

Correction (solution):

I/ Comprehension: (6pts)

1- Computer engineers are highly sought after in today's digital age due to their **possession of technical skills and their ability to solve complex problems. /0.75pts**

2- Computer engineers can find employment in **technology companies, finance, healthcare, research institutions, and academic organizations. /0.75pts**

3- Computer engineers contribute to the field of cyber security by **developing robust security systems and defense mechanisms** to safeguard sensitive information. **/0.75pts**

4- With their background in AI, they contribute to it by **creating intelligent systems, predictive analytics, and automation**. They **leverage data to extract insights, train models, and design intelligent algorithms**. **/0.75pts**

5- Some of the personality traits commonly found in computer engineers include **being analytical, detail-oriented, curious, and persistent, possessing a strong ethical mindset, and being self-motivated**. **/0.75pts**

6- Computer engineers contribute to the optimization of system performance and the creation of innovative solutions **through their technical skills and problem-solving abilities**. **/0.75pts**

b) Extract word synonyms from the text: **/1.5pts (0.5 each)**

Firm (§1) = Solid Meticulous (§3) = Detail-Oriented Important (§3) = Crucial/ Vital

II/ Mastery of language: (10pts)

a) Conjugate the verbs between brackets using the right tense **/4pts (0.5 each)**

1- By this time next year, I *will have been finishing* the Java course and *will have been starting* to program with ease. **(Future perfect continuous)**

2- I *have been deleting* all the unnecessary files from my computer because I *needed* space. **(Present perfect continuous) (Past simple)**

3- Indians *have been* skilled mathematicians for thousands of years. **(Present perfect)**

4- The court *had found* him guilty on all charges. **(Past perfect)**

5- By this time next year, I will be working as a computer engineer after I *hopefully get* my master's degree in computer science. **(Future continuous) (Present simple)**

b) Use the correct modal verb (Need- could – couldn't – ought to – mustn't – might – will) **/2pts (0.5 each)**

1- Despite efforts, the team could not fix a rare software bug causing intermittent system crashes
2- User interfaces need to be intuitive and user-friendly to enhance the experience
3- Computer engineers will eventually play a crucial role in integrating (IoT) devices into everyday life.
4- In AI field, it's possible that deep learning techniques might revolutionize various industries and transform the way we live.

c) Transform the following sentences from active voice into passive voice. **/2pts (0.5 each)**

1- Weekly homework is being assigned to the students by the professor.
2- A new security system has been implemented to protect sensitive data.
3- The students are taught a complex math concept by the teacher.
OR - A complex math concept is taught to students by the teacher.
4- The project will be completed by the end of the week by her.

***III/ Written expression*: (6pts)**

Write a motivation letter consisting of a text ranging from 6 to 12 lines, describing your personality and your drive to join a computer engineering company (optional name) for an internship. In this letter, focus on mentioning key elements and strategies that show your enthusiasm, qualifications, and compatibility with the company.

Key expressions:

- Description of personality's qualities (mentioned adjectives)

- Description of the willingness and the plus that could be brought to the company

- Use of polite and formal words.

- A plus : Use of modal verbs or passive voice.

Example:

Dear [Company Name],

I am writing to express my enthusiasm for joining your computer engineering company. As a self-motivated and ambitious individual with a passion for technology, I am driven to push boundaries and seek innovative solutions.

With a strong foundation in computer engineering and a commitment to excellence, I am confident in my ability to contribute effectively to your team. Your company's culture of innovation aligns perfectly with my aspirations. I am eager to collaborate with like-minded individuals and contribute to groundbreaking technologies. I possess strong interpersonal and communication skills, thriving in collaborative environments that value teamwork and idea exchange. I am excited to bring my expertise and learn from the talented professionals at your company.

In conclusion, my self-motivation, creative mindset, and technical proficiency make me an ideal fit for your computer engineering company. I am thrilled about the opportunity to join your team and play a part in developing cutting-edge technologies.

Thank you for considering my application.

Sincerely,

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Belahdj Bouchaib Ain Temouchent
Faculté des Sciences et Technologies
Département Mathématiques et Informatique

Master 1 CYSIA

Examen de la matière cryptographie

Questions

1- Pourquoi le générateur de clé constitue un élément crucial dans un schéma de chiffrement en particulier le chiffrement symétrique. Expliquez (1points)
2- Est-ce qu'on peut exécuter un chiffrement d'un message par blocs en parallèle ? (1 point)
3- Est-ce que le chiffrement à l'aide double DES est fiable (1 point)
4- Dans le chiffrement AES expliquez comment on obtient SubBytes**(**C2)=25?(3points)
5- Supposons que nous avons accès à un oracle le calcul du MAC d'un message donné à l'aide de la fonction suivante :

FMAC(m) = a + b m (mod 1249) où a et b sont des entiers positifs inférieurs à 1249. 1249 est un nombre premier.

Expliquez pourquoi FMAC est sécurisé si l'utilisateur utilise FMAC qu'une seule fois pour obtenir le MAC d'un message, mais insécurisé s'il dispose de plusieurs accès (sur deux messages ou plus). ? (3 points).

6- Qu'elle serait la meilleure solution pour assurer la confidentialité ainsi que l'intégrité des données et pourquoi ? 2 points
7- **a.** Si dans un système de chiffrement à base de RSA dans lequel les deux utilisateurs ALI et Mohamed décident d'utiliser la même clé publique qu'est-ce que cela impliquera et est-ce que cette manière de faire causera des problèmes coté confidentialité et intégrité. ? (3 points)

   b. si on connait N=187 et $\varphi(N) = 160$ que pouvons-nous calculer (donnez le résultat) qu'elle problème mathématique nous avons résolu avec ces données ? (2 points)
8- Mohamed choisit un entier premier p = 17 et un générateur α = 3 du groupe $(Z^*_p, \times)$. Il choisit l'entier k=6 pour clef privée (ElGamal).

   a. Calculez β afin que Mohamed diffuse sa clef publique (p, α, β). (1 point)

   b. Ali envoie le chiffré C = (11, 16) à Mohamed, déchiffrez le message chiffré 16. (3points).

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Belahdj Bouchaib Ain Temouchent
Faculté des Sciences et Technologies
Département Mathématiques et Informatique

Solution

1- Tout chiffrement qu'il soit symétrique ou Asymétrique repose sur une clé. Le chiffrement parfait one time pad repose sur clé aléatoire dont la suite de bit est impossible à déduire cependant dans des générateurs randomisés elle dépend d'un certain seed. Trouver la clé signifie le break du crypto-système en particulier dans un chiffrement symétrique qui utilise la même clé pour chiffrer et déchiffrer le message. Un exemple une weak key peut rendre un système de chiffrement fiable tel que AES ou DES moins sûr.

2- Oui dans le mode de chiffrement vu durant le cours ECB et CTR peuvent être exécutés en parallèle car le calcule de chaque bloque est indépendant.

3- Non double DES n'est pas fiable car il suffit de moins de 2112 tentatives Attaque par milieu de Double DES (2 DES), Étant donné un couple clair-chiffré (M,C):

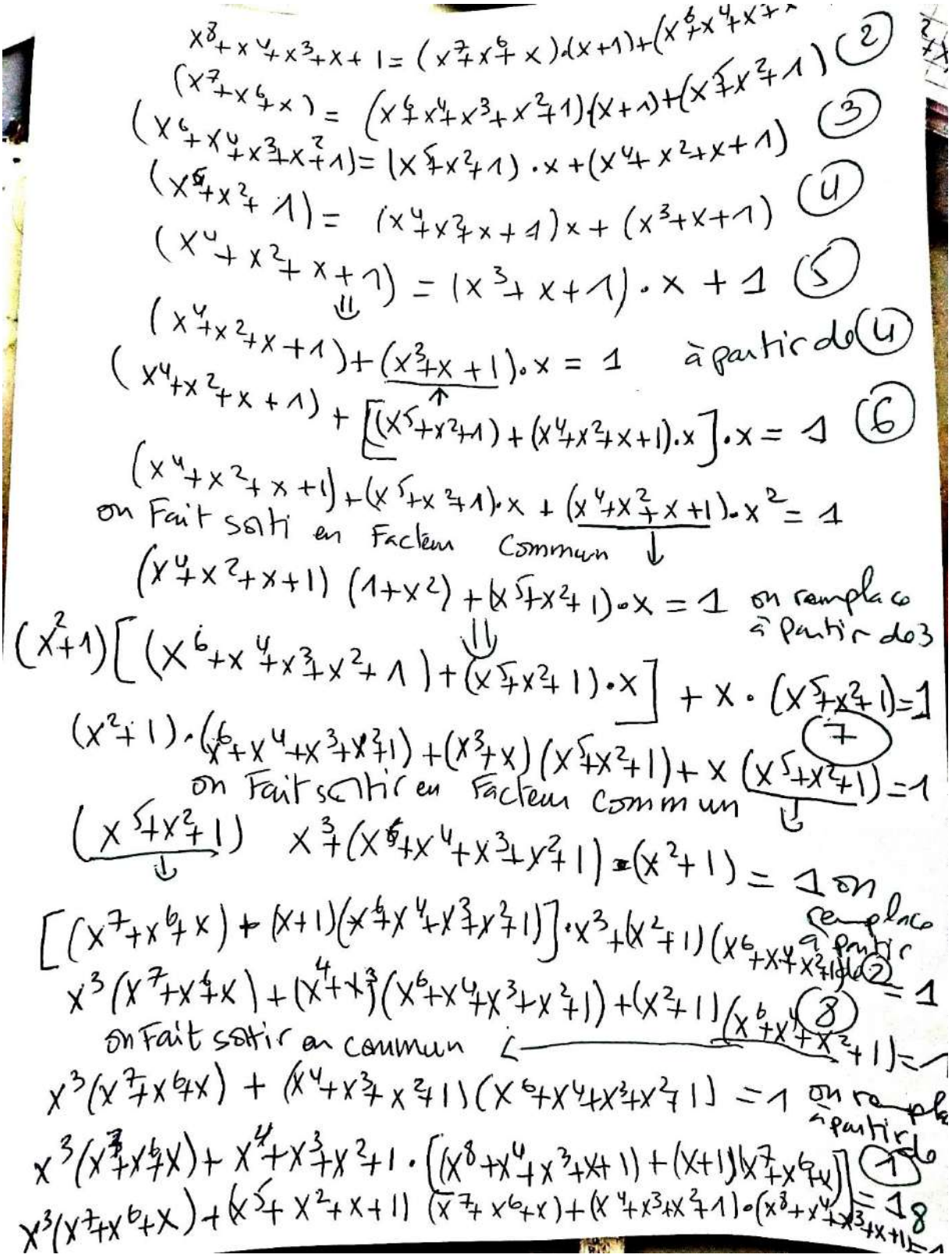
– Calculer $Ni = DESi(M)$ pour 0 ≤ i < 2^56 (i.e. pour chacune des 2^56 valeurs possibles de $k1$)

– Calculer $Pj = DESj^{-1}(C)$ pour 0 ≤ j < 2^56 (i.e. pour chacune des 2^56 valeurs possibles de $k2$) – On cherche les indices (i,j) tels que $Pj = Ni$

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Belahdj Bouchaib Ain Temouchent
Faculté des Sciences et Technologies
Département Mathématiques et Informatique

$x^7+x^6+x = (11000010)2 = (C2)$ on calcul son inverse dans GF(2) les corps de Galois

(2 points)



$GF(2^8)$ modulo $P(x) = x^8 + x^4 + x^3 + x + 1$

donc l'inverse du polynome est $(2F)_{hex} = (00101111)_2 = x^5+x^3+x^2+x+1$.

Qu' on va multiplier par la matrice en y ajoutant le vecteur mod2 on obtient 25 (1 point)

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \mod 2.$$

3- Supposons que nous utilisions la formule suivante pour calculer des MAC (codes d'authentification de message) : FMAC(m) = a + bm (mod 1249) où a et b sont des entiers positifs inférieurs à 1249. 1249 est un nombre premier. Expliquons pourquoi ce MAC est sécurisé s'il est utilisé sur un seul message, mais non sécurisé s'il est utilisé sur deux messages ou plus. Lorsqu'un seul message est utilisé, et que les valeurs secrètes a et b sont choisies de manière aléatoire, chaque nombre inférieur à 1249 est également probable. Par conséquent, il est impossible de déduire des informations sur a ou b, et donc le FMAC est sécurisé car il est difficile de falsifier un nouveau MAC. Maintenant, supposons que nous utilisions FMAC sur au moins deux messages m1 et m2, où m1 est différent de m2. Soit c1 = FMAC(m1) et c2 = FMAC(m2). En soustrayant c2 de c1, nous obtenons c1 - c2 = b(m1 - m2). Comme m1 - m2 est inversible puisque 1249 est un nombre premier, nous pouvons déduire la valeur de b. Étant donné m1, c1 (ou m2, c2) et b, il est facile de calculer la valeur de a. Ainsi, si FMAC est utilisé sur un seul message, il est sécurisé car il est difficile de deviner les valeurs a et b. Cependant, si FMAC est utilisé sur plusieurs messages, les différences entre les MACs peuvent être utilisées pour déduire la valeur de b, ce qui rend le système moins sécurisé.

4- Le chiffrement authentifié l'approche Encrypt-then-MAC est prouvée comme étant sécurisée. Elle garantit l'intégrité des textes chiffrés (INT-CTXT), ce qui signifie qu'il est pratiquement impossible pour un attaquant de construire un texte chiffré valide autre que ceux qu'il parvient à convaincre le détenteur de la clé de générer.exemple IP-SEC.

5- **A.** Si Ali utilise la même valeur n que Mohamed, alors elle devrait connaître sa factorisation en nombres premiers pour générer ses propres valeurs e et d correspondantes. Cependant, si elle connaît la factorisation en nombres premiers de n et si elle connaît la valeur publique de e de Mohamed, alors elle pourrait utiliser l'algorithme d'Euclide étendu pour calculer la valeur secrète d de Mohamed. Ensuite, elle pourrait falsifier un message de la part de Mohamed en utilisant sa valeur d, et la signature numérique de Mohamed ne serait plus une preuve qu'il a envoyé le message. Ainsi, si Ali et Mohamed utilisent la même clé publique n, cela peut conduire à une vulnérabilité dans le système, car Ali pourrait forger des messages de la part de

Mohamed en utilisant ses valeurs secrètes, compromettant ainsi l'intégrité et la sécurité des communications.

B. si on connait $\varphi(N) = 160$ cela implique que la factorisation de N =187 en nombre premier est possible donc le système RSA de déchiffrement est cassé (la notion de sens unique) $\varphi(N) = (p-1)(q-1) = pq - q - p + 1 = n - p - q + 1$, $N = p.q$.

p+q=28 et p*q=187 en remplace p par 28-q ça donne 28-q*q=187 => -q2-28-187=0 on calcul $\Delta = 36$ q a deux valeur 17 et 11 donc soit p=17 et q=11 soit le contraire.

8.

a. $\beta \equiv 3^6 \bmod 17 \equiv 15 \bmod 17$

b . On calcul d'abord la clé de chiffrement qui est $\equiv 11^6 \bmod 17 \equiv 8$ modulo 17

Maintenant on calcul l'inverse de 8 mod 17 à l'aide de l'algorithme d'Euclide entendu on obtient 15 on peut vérifier que $15.\ 8 \equiv 1 \bmod 17$. Il suffit pour déchiffrer le ciphertext 16 de le multiplier par 15=> $15.16 \bmod 17 \equiv 2 \bmod 17$

Université Ain Témouchent -Belhadj Bouchaib
Faculté des Sciences et de la Technologie
Département de Mathématiques et Informatique

Corrigé type examen

Exercice 1 : (8 pts) Choisir la (ou les) bonne(s) réponse(s) :

1. Pour programmer la communication dans une application distribuée on utilise :
   a. Ajax et JQuery.
   b. **les flux d'entrées/sorties non bloquantes.**
   c. **Les sockets et RMI.**
2. L'instruction : ServerSocket ss=new ServerSocket('3000') ; signifie :
   a. Créer un socket de communication coté serveur sur le port 3000.
   b. Créer un socket de communication coté client sur le port 3000.
   c. **Créer un socket de connexion coté serveur sur le port 3000.**
   d. Créer un socket de connexion coté client sur le port 3000.
3. L'instruction : Socket s= serverSocket.accept() ; permet de :
   a. **Créer un socket coté serveur.**
   b. Créer un socket coté client.
   c. Lire les messages arrivés dans le socket.
4. Pour pouvoir gérer plusieurs clients dans un programme distribués avec les sockets :
   a. **On utilise les Threads.**
   b. On exécute plusieurs serveurs.
   c. **On utilise les flux d'entrées/sorties non bloquantes.**
5. Si on exécute le client et le serveur dans deux machines différentes:
   a. On doit préciser l'adresse IP du client dans le code serveur.
   b. **On doit préciser l'adresse IP du serveur dans le code client.**
   c. On doit préciser l'adresse IP "localhost" dans le code serveur et client.
6. Quelles informations sont-elles nécessaires à un client pour créer une "DatagramPacket" à destination d'un serveur ?
   a. L'adresse IP du client ainsi son numéro de port.
   b. **L'adresse IP du serveur ainsi son numéro de port.**
   c. **La longueur des données à envoyer.**
7. Soit un objet quelconque Obj qui est une instance de la classe A qui n'hérite pas d'une autre classe et qui implémente l'interface AInt. En Java RMI, il est très facile de transformer cet objet en un objet distribué. Pour cela il suffit de :
   a. Faire que la classe A implémente aussi l'interface Remote.
   b. Faire que la classe A implémente l'interface Serializable, puis écrire cet objet dans un annuaire RMI.
   c. **Créer un proxy de A. Ce proxy hérite de UnicastRemoteObject et implémente l'interface AInt qui hérite de l'interface Remote.**
8. L'enregistrement d'un Objet Distribué (ou Objet Distant) dans l'annuaire peut s'effectuer à l'aide de la méthode :
   a. lookup()
   b. **bind()**

Exercice 2 : (12 pts)

1. Le serveur est la classe **program2 (il contient le ServerSocket)** le client est la classe **program1**. **(1 pts)**
2. Que fait cette application ? **le client envoie deux nombre au serveur via le socket. Le serveur récupère ces deux nombre, calcule leur pgcd et renvoie le résultat au client via le socket, ce dernier le récupère et l'affiche à l'écran. (2 pts)**
3. Cette application contient des erreurs qui empêchent son exécution. Trouver et corriger ces erreurs ? **(3 pts)**

```
import java.net.*;
import java.io.*;
public  class program1
{  int x=15; int y=6;
  public static void main (String args[]) throws IOException
  {    Socket socket = new Socket("localhost", 3000);
       BufferedReader in = new BufferedReader(new InputStreamReader(socket.getInputStream()));
       PrintWriter out= new PrintWriter(socket. getOutputStream (),true);
       out.println(x);
       out.println(y);
       String resultat=in.readLine() ;
       System.out.println(resultat) ;
       out.close() ;  in.close() ;
       socket.close() ;
  }}
```

```
import java.net.*;
import java.io.*;
public class program2
{ int port = 3000 ;
  public static void main (String args[]) throws IOException
  { ServerSocket sersoc= new ServerSocket(port) ;
    Socket socket = sersoc.accept();
    BufferedReader in = new BufferedReader(new InputStreamReader(socket.getInputStream()));
    PrintWriter out= new PrintWriter(socket.getOutputStream(),true);
    int x=in.readLine();
    int y=in.readLine();
    while (x != y)
    {  if(x>y)    x=x-y;
       else  y=y-x; }
   out.println('le résultat = '+x );
  out.close() ;  in.close() ;
  socket.close() ;  sersoc.close() ;
  }}
```

4. Qu'est-ce que nous devons changer si on exécute le client est le serveur dans deux machines différentes ? **(2 pts)**
   le client doit préciser l'adresse IP du serveur lors de la connexion (au lieu de mettre localhost) : Socket socket = new Socket(adresseIP_serveur, port);
5. Modifier l'application pour pouvoir gérer plusieurs clients ? **(4 pts)**
   - **Le client ne change pas.**
   - **Dans le serveur on doit utiliser les threads.**

```
import java.net.*;
import java.io.*;
public class program2
{ int port = 3000 ;
  public static void main (String args[]) throws IOException
  { ServerSocket sersoc= new ServerSocket(port) ;
    While (true){
      Socket socket = sersoc.accept();
       new thread_seveur(socket).start();  }
  sersoc.close() ;
  }}
```

```
import java.net.*;
import java.io.*;
public class thread_serveur
{ Socket soket;
 public thread_serveur(Socket sok)
{socket=sok;}
 Public void run()
 {
   BufferedReader in = new BufferedReader(new InputStreamReader(socket.getInputStream()));
   PrintWriter out= new PrintWriter (socket.getOutputStream(),true);
   int x=in.readLine();
    int y=in.readLine();
    while (x !=y)
    {  If(x>y) x=x-y;
        else y=y-x; }
    out.println('le résultat = '+x);
    in.close() ; out.close() ; soket.close() ; }
```

Corrigé type d'Examen

Ex1 : 1/

La forme canonique du mot « admirablement » est :

- ✓ admirable
- ○ admirer
- ○ admirablement
- ○ Aucune réponse correcte.

La forme canonique du mot « rendez-vous» est :

- ○ Rendre
- ○ Vous
- ○ Rendre et vous
- ✓ Aucune réponse correcte.

2/ 2.5pts

a) arbres : arbre naturellement : nature iront : aller manteau : manteau

b) En définissant des règles de passage :
   - pour les noms ; du pluriels au singulier, du féminin au masculin,
   - pour les verbe du conjugué à infinitif
   - et en supprimant les affixes, préfixes ; suffixes),
   - …

3/ 2.5pts

Réponse : Il doit donner les différentes possibilités lexicales :

Le	*Livre*	*Est*	*bon*
• *Article défini <Le>* • *Pronom <Le>*	• *Nom Commun féminin Singulier <Livre>* • *Nom Commun masculin Singulier <Livre>* • *Verbe <Livrer>, Temps présent de l'indicatif, 1ère personne du singulier .* • *Verbe <Livrer>, Temps présent de l'indicatif, 3ème personne du singulier.*	• *Verbe <Etre>, Temps présent de l'indicatif, 3ème personne du singulier.* • *Nom Commun Masculin singulier <Est>*	• *Nom Commun Masculin singulier <Bon>* • *Adjectif Masculin singulier <Bon>*

4/ 1pts

	Méthode	Avantages	Inconvénients
1	Représenter toutes les formes au niveau d'un même lexique	Le lexique est complet	Volume important du lexique
2	Représenter le minimum dans un lexique et le reste doit être reconnu ou généré grâce à des algorithmes automates	Lexique plus léger	Nécessité d'écriture des automates et temps de traitement

Réponses :

i) TALN : Traitement'processing' automatique de la langue naturelle'humaine'= !langue artificielle',
TALN : Ensemble de recherches et développements visant à modéliser et reproduire à l'aide de machine la capacité humaine à produire et comprendre des énoncés linguistiques.

ii) quelques 'au moins 8' domaines d'application du TALN :
- recherche d'information
- Résumé automatique
- traduction automatique
- vérification d'hortographe
- correction d'ortographe
- extraction de connaissance
- classification de texte
-annotation de document
-système Q/R
-…

iii) Il s'agit d'un procédé de formation de mots nouveaux par addition, suppression ou remplacement d'un élément grammatical d'un mot simple.
Ex. : normal → anormal- normalement.

iv) Ces mots découlent tous de la même racine, le verbe « marcher ». Ils sont des formes fléchies du verbe « marcher ». Le processus qui permet de les générer est la « flexion verbale ».

v) Il y a une ambiguïté entre : - Avocat : profession d'une personne. - Avocat : fruit. Cette ambiguïté sera levée au niveau sémantique.

vi) Bruit : C'est l'ensemble d'informations non pertinents trouvés en réponse à une question, lors d'une recherche d'information. L'information pertinente est noyée dans la masse.
Silence : C'est l'ensemble des informations pertinents non affichés lors d'une recherche documentaire. L'information pertinente n'est pas trouvée et celui qui cherche peut penser qu'il n'y en a pas.

vii) La traduction est une application difficile parce qu'elle implique à la fois **l'analyse** et la **génération**. Autre application de la même catégorie : résumé automatique.

viii) le processus qui permet de passer de la structure profonde à la structure de surface d'une phrase : **Analyse** . le processus inverse : **Génération**.