UNIVERSITÉ DU BURUNDI

GRENIER DU SAVOIR DU BURUNDI

Dépôt institutionnel officiel

https://repository.ub.edu.bi

Conception et réalisation d’une application d’e-commerce

NDAYIRAGIJE, Audifax

2021-09

Université du Burundi

https://repository.ub.edu.bi/handle/123456789/33

Document téléchargé depuis le **Grenier du Savoir du Burundi** — https://repository.ub.edu.bi

Université du Burundi

Faculté des sciences de l'ingénieur (FSI)
Département des Technologies de l'Information et de la Communication
Master en Génie informatique
Année académique : 2019-2020



Conception et réalisation d'une application d'e-commerce

Par

Audifax NDAYIRAGIJE

MEMOIRE

Présenté

En vue de l'obtention du grade de

MASTER

en

Génie Informatique

Sous la direction de : Dr Longin NDAYISABA

Bujumbura, Septembre 2021

IDENTIFICATION DES MEMBRES DU JURY

Dr.	NDAYISABA Longin	: Directeur
Pr.	MANIRABONA Audace	: Président
Dr.	SAHINGUVU William	: Secrétaire
Pr.	NDIKUMAGENGE Jérémie	: Membre

Dédicaces

A Dieu tout puissant ;

A mon épouse ;

A mes chers enfants ;

A mes parents ;

A mes frères et sœurs ;

A mes cousins et cousines ;

A mes oncles et tantes ;

A toutes mes connaissances ;

NDAYIRAGIJE Audifax

Remerciements

Je tiens tout d'abord à remercier Dieu le Tout-Puissant pour la bonne santé qu'il m'a prodigué durant mes études.

Je remercie tout particulièrement le directeur de ce mémoire, Dr. NDAYISABA Longin, qui a accepté de diriger ce mémoire malgré ses multiples responsabilités, son assiduité, son organisation et sa franche collaboration m'ont vraiment facilité la tâche et me serviront d'exemple.

Je remercie aussi toutes les personnes avec lesquelles j'ai eu le plaisir de collaborer et qui ont pu par la même occasion m'aider durant toute la durée de réalisation de mon projet.

Je remercie très spécialement le Responsable de master en génie informatique et tous les professeurs qui nous ont enseigné en Master. J'ai apprécié leur sacrifice ; ce qui me servira d'exemple dans ma future vie professionnelle.

Enfin, je voudrais aussi remercier mon épouse, mes enfants et mes amis, pour leur soutien inconditionnel.

RESUME

Le e-commerce est « l'échange pécuniaire de biens, de services et d'informations par l'intermédiaire des réseaux informatiques, notamment l'internet ». Grace à l'avènement de ce dernier, le commerce électronique a connu des avancées très significatives offrant ainsi de nouvelles possibilités d'affaires aux entreprises.

Notre projet de fin d'étude se focalise sur **l'analyse, la conception et la réalisation d'une application web d'e-commerce** qui permettra aux entrepreneurs de voir grand leurs entreprises et d'atteindre leurs objectifs.

En outre, notre application permet la mise en place d'une boutique en ligne ; comme dans un magasin réel, on peut choisir et payer des articles. Pour acheter dans cette boutique en ligne, il suffit de visiter la page de catalogue des articles, de cliquer sur les produits sélectionnés puis de les ajouter dans un panier d'achat virtuel. L'acheteur peut ensuite payer à l'aide d'une carte bancaire ou d'un autre système de paiement autorisé par la boutique en ligne comme LumiCash ou EcoCash. Enfin, le client peut choisir le point de livraison selon les modalités définies par la boutique.

Mots clés : **e-commerce, boutique en ligne, panier d'achat virtuel, système de paiement**

ABSTRACT

E-commerce is "the monetary exchange of goods, services and information, via computer networks, including the Internet". Due to the advent of internet, electronic commerce has experienced very significant advances, thus offering new business opportunities to companies. Our graduation project focuses on the analysis, design and implementation of an e-commerce web application that will allow entrepreneurs to grow their businesses and achieve their goals.

In addition, our application allows the establishment of an online store; just like in a real store, one can choose and pay for items.

To buy from this online store, simply visit the item catalog page, click on the selected products and then add them to a virtual shopping cart. The customer can then pay, using a bank card or another payment system, authorized by the online store such as LumiCash or EcoCash.

Finally, the customer can choose the point of delivery.

Keywords: e- commerce, online shop, virtual shopping cart, payment system

Liste des abréviations

B2B	: Business-to- Business
B2C	: Business-to-Consumer
B2E	: Consumer-to-Empoyee
B2G	: Consumer-*to*-Government
BBS	: BackBone System
C2C	: Consumer-to-Consumer
FN	: Forme Normale
IP	: Internet Protocol
MCD	: Modèle Conceptuel de Données
MERISE	: Méthode d'étude et de réalisation informatique pour les systèmes d'entreprise
MLD	: Modèle logique de Données
MPD	: Modèle physique de Données
MVC	: Model-View-Controller
ORM	: Object-Relational-Mapping
PMC	: Package Manager Console
SGBD	: Système de Gestion de Base de Données
TCP	: Transmission Control Protocol

Table des matières

IDENTIFICATION DES MEMBRES DU JURY i
Dédicaces ii
Remerciements iii
RESUME iv
Liste des abréviations v
Table des matières vi
Tables des illustrations ix
Liste des tableaux x
AVANT-PROPOS xi
CHAPITRE I : INTRODUCTION GENERALE 1
I.1.Introduction 1
I.2. Objectifs du projet 2
I.2.1. Objectif global 2
I.2.2. Objectifs spécifiques 2
I.3. Problématique 2
I.4. Solutions proposées 3
I.5. Résultats attendus 3
I.6. Apport scientifique et technologique 3
I.7. Domaine d'application 3
I.8. Méthodologie 3
I.9. Outils mathématiques 4
I.10. Généralités sur l'e-commerce ou commerce électronique 4
I.10.1. Essor du e-commerce 5
I.10.2. Impact négatif d'e-commerce 5
I.10.3. Impact positif d'e-commerce 6
I.11. Conclusion 7
CHAPITRE II : ANALYSE DE L'EXISTANT ET EXPRESSION DES BESOINS 8
II.1. Introduction 8
II.2. Analyse de la vente traditionnelle et de la vente électronique 8
II.2.1. Vente traditionnelle 8

II.2.2. Vente électronique 8
II.2.3. Critique à l'endroit du commerce traditionnelle 9
II.2.4. Comparaison entre commerce traditionnel et le commerce électronique 9
II.2.5. Tableau comparatif entre le commerce traditionnel et le commerce électronique 10
II.3. Expression de besoins 12
II.3.1. Besoins fonctionnels 12
II.3.2. Besoins non fonctionnels 12
CHAPITRE III : CONCEPTION ET MODELISATION DU NOUVEAU SYSTEME INFORMATIQUE 15
III.1. Introduction 15
III.2. Outils et méthodes utilisés 15
III.2.1. Méthode d'Étude et de Réalisation Informatique pour les Systèmes d'Entreprise 15
III.2.2. Éléments constitutifs du modèle entités-associations 16
III.2.3. Normalisation des type-entités et type-associations 22
III. 3. Modèle conceptuel de données 27
III. 4. Modèle logique de données 29
III.5. Dictionnaire des données 30
III. 6. Modèle physique de données 34
III.7. Conclusion 35
CHAPITRE IV : MODELE MATHEMATIQUE UTILISE POUR LA CONCEPTION DE LA BASE DE DONNEES 36
IV.1. Introduction 36
IV.2. Problématiques des graphes 37
IV.3. Historique des graphes 38
IV.4. Modélisation du système à l'aide de la théorie des graphes 41
IV.4.1. Représentation de la base de données à l'aide d'un graphe 41
IV.4.2. Matrice d'adjacence obtenu à partir du graphe 42
IV.4.3. Matrice d'incidence 43
IV.4.4. Calcul de la matrice de fermeture transitive 44
IV.4.5. Matrice des plus courts chemins dans le parcours de la base de données. 47
IV.4.6. Algorithme de Floyd-Warshall 48
IV.5. Conclusion 54

CHAPITRE V : SECURISATION DE L'APPLICATION D'E-COMMERCE A L'AIDE DU CRYPTOSYSTEME RSA 55
V.1. Introduction 55
V.2. Comparaison des algorithmes de chiffrement 55
V.3. Historique de RSA 56
V.4. Principe de fonctionnement. 57
V.5. Explication mathématique du principe de fonctionnement de RSA 57
V.5.1. Chiffrement asymétrique des données à l'aide de RSA 58
V.5.2. Déchiffrement du message 59
V.6. Conclusion 62
CHAPITRE VI : IMPLEMENTATION DE L'APPLICATION.. 63
VI.1. Introduction 63
VI.2. Modèles-Vues-Controlleurs 63
VI.3. Packages de NuGet utiles pour l'application 64
VI.4. Entity Framework et Echafaudage 64
VI.5. Présentation de principales fonctionnalités de l'application 67
VI.5.1. Page d'Accueil ou d'affichage du « Catalogue de produits » 67
VI.5.2. Page « Index de produits » 68
VI.5.3. Pages « d'enregistrement de produits » 69
VI.5.4. Pages de « suppression de produits » 69
CONCLUSION ET RECOMMANDATIONS 70
1. Conclusion 70
2. Recommandations 70
REFERENCES BIBLIOGRAPHIQUES 71

Tables des illustrations

Figure 1: Exemple d'une fenêtre de vente en ligne 9
Figure 2: Interface de l'outil JMERISE 26
Figure 3: Modèle conceptuel de données 28
Figure 4: Modèle Physique de Données 34
Figure 5: Packages utilisés pour le développement de l'application 64
Figure 6: Commandes utilisée pour migrer les tables vers les classes C# 65
Figure 7: Classes C# obtenues après Echafaudage 66
Figure 8: Page d'accueil de l'application 67
Figure 9: Page index de produits 68
Figure 10: Page d'enregistrement de produits 69
Figure 11: Page de suppression d'un produit 69

Liste des tableaux

Tableau 1: Comparaison entre le commerce traditionnel et le commerce électronique 10
Tableau 2: Dictionnaire des données 31
Tableau 3: Etude comparative des modèles mathématiques 36
Tableau 4: Matrice d'adjacence 43
Tableau 5: Etude comparative des algorithmes de chiffrement 55

AVANT-PROPOS

Ce mémoire s'inscrit dans le cadre d'un projet de fin d'études du deuxième cycle universitaire afin d'obtenir un diplôme de Master en Génie Informatique. Il se focalise sur la promotion d'e-service dans le domaine commercial par la « *conception et réalisation d'une application d'e-commerce*».

Certes, aucun site de commerce électronique de renommé bien connu au Burundi. Cela rend nos entrepreneurs moins compétitifs sur plan international puisqu'il leur est difficile de vendre leurs produits et services partout au monde. De plus l'opération de vente devient complexe parce que le vendeur est obligé de tout faire alors qu'une partie aurait été effectuée par le client via l'internet. Ce thème a été donc choisi, d'une part pour contribuer à la promotion d'e-service et d'autre part pour proposer à nos entreprises une solution e-commerce leurs permettant de booster le chiffre d'affaires et étendre leurs zones cibles.

En effet, nous avons commencé par identifier la problématique liée au non utilisation de l'internet comme support incontournable dans le domaine commercial et se documenter par rapport à la conception des sites de commerce électronique (Amazon, eBay, etc.). Par après, nous avons proposé des solutions aboutissant à la mise en place d'une application d'e-commerce interactive implémentée avec le langage de programmation C Sharp et HTML (Asp.net core) et le gestionnaire de base de données MySQL.

Au cours de la réalisation de ce projet, la seule difficulté rencontrée est liée à l'accès aux données. D'ailleurs, au départ, j'entreprenais à promouvoir l'e-Gouvernement par la mise en place *« d'une application de gestion des élections et des journées électorales, cas de la CENI* ». Cela nous a contraints à choisir un thème qui ne demande pas forcément un cas d'étude.

CHAPITRE I : INTRODUCTION GENERALE

I.1.Introduction

Depuis l'avènement de la fibre optique, l'essentiel des capacités internet est fourni via cette voie. Deux opérateurs disposant des infrastructures nationales, VIETTEL Burundi et BackBone System (BBS), transportent à partir de la frontière, les capacités internet achetées de l'étranger.

Le marché de l'internet au Burundi est exploité par neuf fournisseurs d'accès internet qui proposent aux clients plusieurs offres de services internet via différentes technologies : VSAT, FO, WIMAX, ADSL, MPLS, etc.

Par ailleurs, il se trouve que ces fournisseurs d'accès internet peinent à vendre localement les capacités internet achetées à l'étranger.

En 2017, la moyenne trimestrielle des capacités internet achetées à l'étranger est de 4341 Mbps, tandis que la demande locale ne se limite qu'à 1583 Mbps, soit 36% de la capacité achetée [1].

De ce qui précède le constant est clair, l'internet est disponible au Burundi mais il n'est pas suffisamment exploité. Plusieurs entreprises possèdent des sites web simples pour de fins de publication et beaucoup d'internautes n'utilisent l'internet que pour de fins de simples messageries. Seules les entreprises œuvrant dans le secteur médiatique essaient d'exploiter l'internet en l'utilisant en plus pour de fins commerciales (abonnement des clients).

Or, dans le contexte actuel, on ne peut pas ignorer l'importance des nouvelles technologies de l'information et de la communication au sein de l'entreprise qu'elle soit de négoce, industrielle ou de services.
En effet, aucun site de commerce électronique de renommé bien connu au Burundi. Cela rend nos entrepreneurs moins compétitifs sur plan international puisqu'il leur est difficile de vendre leurs produits et services partout au monde. De plus l'opération de vente devient complexe parce que le vendeur est obligé de tout faire alors qu'une partie aurait été effectuée par le client via l'internet.

I.2. Objectifs du projet

I.2.1. Objectif global

L'objectif global du projet est de concevoir une application web d'e-commerce qui permettra aux entreprises d'améliorer leur compétitivité grâce à l'extension de la part du marché et la flexibilité des opérations commerciales.

I.2.2. Objectifs spécifiques

Pour y réussir l'objectif global du projet, les objectifs spécifiques suivants seront menés :

1) Créer une application web d'e-commerce ;
2) Permettre aux clients de s'inscrire en ligne
3) Publier le catalogue de produits et/ou services en vente ainsi que leurs prix et caractéristiques
4) Ajouter des produits préférés au panier de vente virtuel ;
5) Passer une commande tout en renseignant le mode de payement et le point de livraison ;
6) Payer en ligne et générer la facture seront mis en œuvre.

I.3. Problématique

Nous savons que tout projet vient en réponse à une problématique qui hante la société. Jusqu'à nos jours, nos entreprises ne sont pas compétitives sur le plan mondial, cela est dû au fait qu'elles ne profitent pas encore de nombreux avantages présentés par l'e-commerce. Ce dernier permet un achat plus rapide ainsi que la possibilité de toucher un large public 24 heures sur 24, 7 jours sur 7. Par ailleurs, tout semble être là pour la mise en place d'e-commerce.

En outre, notre projet a été donc motivé par les problèmes suivants :

1) Les capacités d'internet achetées à l'étranger ne sont pas suffisamment utilisées ;
2) Les sites web dont disposent nos entreprises ne sont utilisés qu'à des fins de simples publications ;
3) Les entreprises éprouvent la difficulté de vendre partout au monde ;
4) Il est difficile de servir les clients à temps réel car, chaque fois, pendant l'opération de vente l'employé vendeur commence à zéro pour chaque client qui vient pour acheter ;
5) Les entreprises ne vendent pas 24H/24, 7/7 ;
6) Le client peut parcourir de longues distances et, arriver au point de vente, il trouve le stock du produit recherché épuisé ;

7) Le client n'a pas la possibilité de choisir simplement le vendeur le moins disant ;
8) La possibilité de vol avant l'achat parce que le client a sur lui l'argent liquide ;
9) La possibilité d'erreur pendant le payement.

I.4. Solutions proposées

Pour résoudre cette problématique, notre projet comme solutions :

1) Créer une application web d'e-commerce ;
2) Imprimer les rapports de vente et archivage de données y relatif ;
3) Doter les entreprises d'un équipement informatique suffisant pour que l'application soit d'usage ;
4) Former les utilisateurs pour ce nouveau système.

I.5. Résultats attendus

Après la mise en place des solutions proposées, les résultats attendus seront que :

1) Une application web d'e-commerce est disponible au niveau des entreprises ;
2) Les opérations d'achat et de vente se font 24H/24, 7J/7 ;
3) La visibilité des entreprises est améliorée ;
4) Le chiffre d'affaires des entreprises est augmenté ;
5) Un gain remarquable en termes de ressource humaines est observé.

I.6. Apport scientifique et technologique

Modélisation de la base de données à l'aide de la théorie des graphes, clonage d'une application réseau intranet aux sites web interactifs.

I.7. Domaine d'application

Industries de transformation de biens et services, réseautage informatique, système informatique de gestion marketing des entreprises

I.8. Méthodologie

Comme méthodologie de recherche nous allons utiliser les approches suivantes :

- Etude de l'existant
- Visite de certains sites bien reconnus pour apprécier leurs formes et contenus ;

- Lecture de documents et rapports publiés.
- Internet.

I.9. Outils mathématiques

Les outils mathématiques à utiliser seront les procédures et fonctions récursives, le langage de programmation C#, MySQL et la théorie des graphes ;

I.10. Généralités sur l'e-commerce ou commerce électronique

Le e-commerce ou commerce électronique, consiste à échanger des biens et des services entre deux personnes à distance sur les réseaux informatiques, c'est-à-dire via Internet.

Apparu dans les années 1980, il s'est surtout démocratisé à la fin des années 1990 avec l'apparition des paiements en ligne et la démocratisation de l'accès à Internet dans les foyers.

IBM et Microsoft étant les premiers pionniers de ce nouveau concept, au début, les produits mis en vente étaient principalement des biens informatiques.

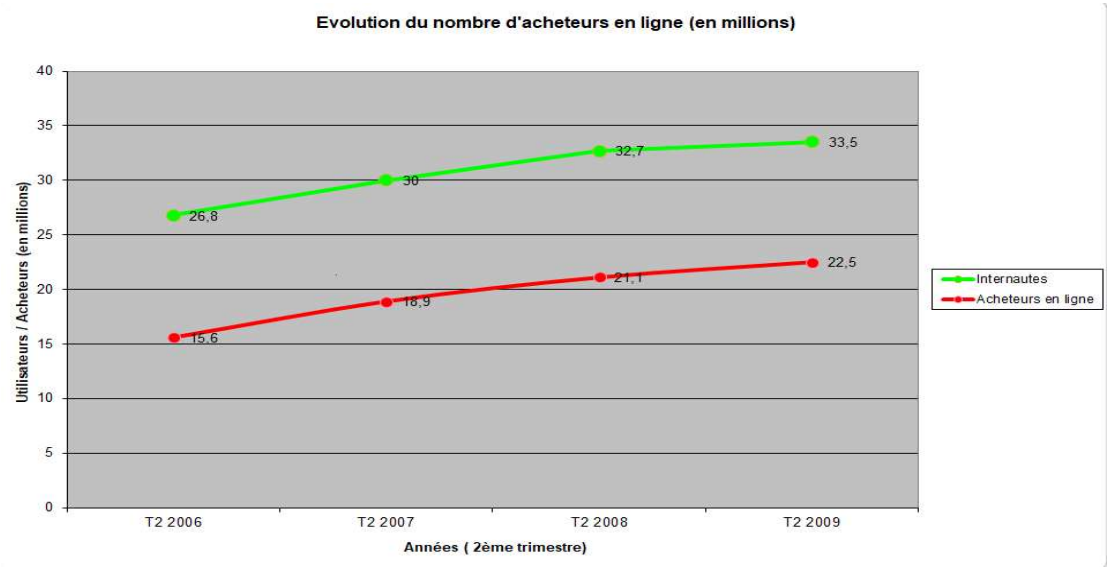
A ses débuts, le e-commerce ne rencontre pas un franc succès, à cause de la crainte des investisseurs et la prudence des acheteurs sur l'utilisation de ce nouveau canal. Cela est notamment du à 3 facteurs essentiels au e-commerce : la livraison, les moyens de paiements et la démocratisation d'Internet dans les foyers.

Petit à petit, ces facteurs se développant et devenant de plus en plus fiables, on assiste à l'essor du e-commerce dans le monde. Il existe plusieurs types de e-commerce : l'e-commerce entre entreprises, souvent appelé B2B, acronyme anglais de *Business to business*, le commerce électronique à destination des particuliers, ou B2C, acronyme anglais de *Business to consumer*. Il s'agit de sites Internet marchands. Exemple : sites de E-commerce : EBay, Amazon …, le commerce électronique entre particuliers, ou C2C, acronyme anglais de *Consumer-to-consumer*. Il s'agit de sites Internet permettant la vente entre particuliers. Le site en plein essor actuellement en France entre particuliers est Leboncoin.fr, l'échange électronique entre une entreprise et ses employés, souvent appelé Intranet ou B2E, acronyme anglais de *Business to employee*, l'échange électronique entre les entreprises privées et le gouvernement, souvent appelé B2G, acronyme anglais de *Business to government*. Nous allons principalement nous focaliser sur le B2C et C2C, qui concernent les ménages.

I.10.1. Essor du e-commerce

Au cours des 10 dernières années, le e-commerce a connu une évolution fulgurante. Avec l'apparition d'Internet dans les foyers, le nombre de cyberacheteurs a augmenté à une vitesse folle. L'utilisation du e-commerce s'est très vite démocratisé et concerne donc aujourd'hui toutes les populations, sans distinction d'âge, de localité ou de sexe. [3]

Evolution du nombre d'utilisateurs/acheteurs



(Source FEVAD : Fédération du E-commerce et de la Vente A Distance)

I.10.2. Impact négatif d'e-commerce

L'essor fulgurant du e-commerce comporte hélas un aspect négatif pour le commerce traditionnel français.

En effet, certains secteurs d'activité physique se sont vu concurrencés, puis très rapidement dépassés par leurs **cyber-concurrents**. Ces derniers proposant des prix souvent plus attractifs, un choix de produits plus grand (grâce à la comparaison entre les différents sites) et plus facile d'accès, et surtout le gros avantage pour le consommateur de pouvoir effectuer ses achats sans se déplacer, 24H/24, 7J/7, et où qu'il soit dans le monde (avec la seule condition d'avoir un accès internet). [4]

I.10.3. Impact positif d'e-commerce

Le e-commerce est aujourd'hui le canal de distribution le plus simple d'accès, et donc le meilleur moyen de faire de la publicité. L'utilisation de ce canal en complément (voir en substitution) d'une activité au niveau "physique" est clairement bénéfique pour l'entreprise.

Ainsi, le e-commerce est utilisé dans deux cas de figures. Il est utilisé d'une part, par les petites entreprises ayant besoin de se faire connaitre, et d'autre part, par les entreprises à plus forte notoriété pour augmenter leurs chiffres d'affaires. [5]

Dans le premier cas de figure, on retrouve toutes les **start-ups** ou indépendants. Ces-derniers voient en Internet le meilleur moyen d'étendre leur **zone d'activité**, et ainsi de gagner des clients. Grâce au e-commerce, leur zone d'activité ne se limite plus à un espace géographique restreint autour de leur lieu de travail, mais à la totalité du territoire (voire du Monde).

Dans le second cas, on retrouve toutes les grandes enseignes, chaines de magasins, etc. L'utilisation de ce nouveau canal de distribution n'a pour but que d'augmenter le chiffre d'affaires de ces entreprises ayant déjà percées au niveau physique. Le Web s'avère être un réel soutien pour le réseau de boutiques de ces entreprises. En effet, le site Web d'une entreprise peut par exemple mettre en places des animations ou des jeux de concours en ligne et créer ainsi une base de données d'individus, à qui on enverra ensuite une invitation par mail, les invitant à se rendre dans la boutique la plus proche de chez eux (même méthode que les petites entreprises, expliqué précédemment). Le but étant ici de booster le chiffre d'affaire des boutiques physiques.

Ce procédé est également utilisé en sens inverse (de la boutique vers le site Web), mais de façons différentes. En effet, les boutiques physiques de ces entreprises sont de gros pourvoyeurs d'avantages pour leurs sites Web. De nombreux moyens existent pour attirer les clients sur le site (cadeaux à gagner en ligne, annonce de réduction en commandant par internet, ...), mais le plus couramment utilisé reste une publicité de masse concernant l'adresse internet du site. La chaîne de parfumeries Séphora, par exemple, a affiché, dès 2005, sur tous ses sacs en papier, l'adresse de son site Web, en indiquant : "Votre boutique Séphora ouverte 24H/24".

Partant de ce principe, le site Web de ces entreprises devient la boutique pouvant réaliser le plus gros chiffre d'affaires de l'entreprise.

I.11. Conclusion

Afin de réussir à ses missions, l’e-commerce ou le commerce électronique est le meilleur enjeu pour toute entreprise commerciale. Toutefois, le commerce électronique et le commerce traditionnel se complètent. Il faut donc coupler les deux car chacun a ses avantages et inconvénients.

CHAPITRE II : ANALYSE DE L'EXISTANT ET EXPRESSION DES BESOINS

II.1. Introduction

Avant de se lancer dans la réalisation de tout projet informatique, il indispensable de bien étudier et analyser l'existant et de faire référence aux autres projets similaires afin de produire un ouvrage de qualité qui réponde mieux aux besoins exprimés. Comme le commerce électronique n'est pas beaucoup exploité dans notre pays, le Burundi, l'analyse et l'expression des besoins a porté sur l'étude du commerce traditionnel, la consultation de sites d'e-commerce populaires (eBay, Amazone, etc.) ; pour justement passer d'une vente traditionnelle vers la vente électronique.

Ainsi, dans ce deuxième chapitre, nous allons nous plonger dans le bain du projet en étudiant la manière dont se déroule la vente traditionnelle. Par la suite, nous allons consulter certains sites d'e-commerce populaires pour comprendre le déroulement de la vente en ligne. Enfin, nous allons dégager une comparaison afin de pouvoir mettre en évidence l'intérêt apporté par le commerce électronique. En outre, ce chapitre présente un ensemble des besoins fonctionnels et non fonctionnels du système du futur système informatisé.

II.2. Analyse de la vente traditionnelle et de la vente électronique

II.2.1. Vente traditionnelle

Pour la vente traditionnelle, le client se présente physiquement dans une boutique, choisit des produits dont il a besoins, négocie le prix ; puis le vendeur produit une facture. Enfin, le client procède au paiement de la facture. Le client peut aussi passer une commande, puis payer la facture correspondante ; le vendeur procède à servir la commande et à la livraison de produits qui peut être une livraison à domicile ou pas.

II.2.2. Vente électronique

Comme pour la vente traditionnelle, ici nous avons aussi une boutique ; mais une boutique virtuelle ou boutique en ligne. La boutique étant en ligne le client n'a pas besoins de se présenter physiquement dans la boutique. Pour lui, il suffit de visiter la boutique en ligne, de consulter le catalogue de produits, d'ajouter des produits dont il a besoin dans un panier d'achat virtuel avec possibilité de consulter les détails du produit et supprimer des produits qui sont précédemment ajoutés au panier, de sélectionner le point de livraison et le mode de payement et, enfin, de valider la vente.

En général, la page d'accueil des sites de e-commerce présente deux parties essentielles : la partie réservée aux publicités et la partie pour le catalogue de produits.

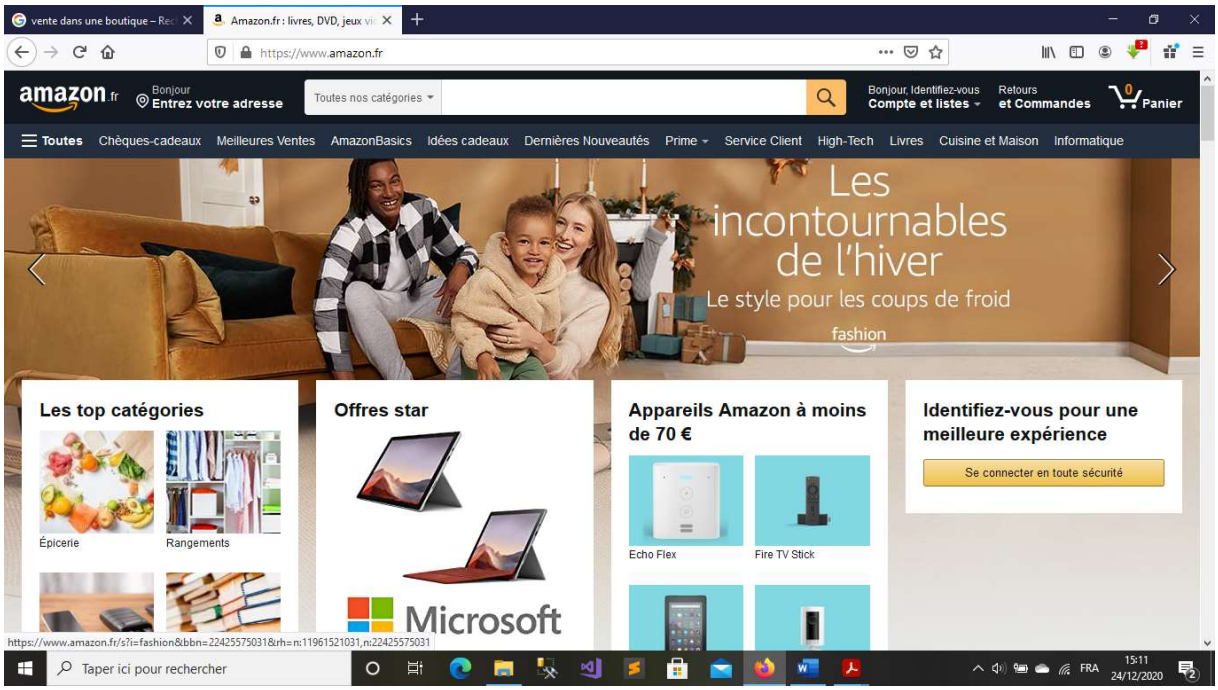


Figure 1: Exemple d'une fenêtre de vente en ligne

II.2.3. Critique à l'endroit du commerce traditionnelle

Le commerce traditionnel, bien qu'il y ait possibilité d'effectuer toutes les opérations commerciales (la vente, le paiement, marketing, etc.), il présente encore certaines limités car il ne concerne qu'un nombre limité de clients ; ceux qui sont très proches de la boutique pour pouvoir la visiter, voir les produits exposés et savoir la disponibilité en stock de ces derniers ainsi que leurs prix et leurs caractéristiques techniques. Ce nombre limité de clients représente une entrave pour nos entreprises dans la compétitivité et la commercialisation des produits et services.

Notre application d'e-commerce va apporter une solution car elle permettra la mise en place d'une boutique virtuelle sur Internet.

II.2.4. Comparaison entre commerce traditionnel et le commerce électronique

Avec l'avènement de l'internet, le moment est venu où tout le monde devrait comprendre l'intérêt de coupler le commerce traditionnel avec le commerce électronique. Grace à la boutique en ligne, les clients peuvent acheter des biens et services, payer des factures ou transférer de l'argent en un seul clic. Par contre, dans la boutique physique, toutes les opérations

relatives à la vente sont presque réalisées en totalité par le vendeur et sont nombreuses par rapport à la boutique en ligne. Dans la boutique physique, le client n'a qu'à choisir ses produits préférés et payer sa facture. Toutefois, les deux modes ont leurs avantages et leurs inconvénients.

Le tableau ci-dessous simplifie la différence entre commerce traditionnel et commerce électronique [7].

II.2.5. Tableau comparatif entre le commerce traditionnel et le commerce électronique

Tableau 1: Comparaison entre le commerce traditionnel et le commerce électronique

Base de comparaison	Commerce traditionnel	Commerce électronique	Commentaires
Sens	Le commerce traditionnel est une branche d'activité qui met l'accent sur l'échange de produits et de services et comprend toutes les activités qui encouragent l'échange, d'une manière ou d'une autre.	Le commerce électronique consiste à effectuer des transactions commerciales ou des échanges d'informations par voie électronique sur Internet.	Le e-commerce peut se montre comme un désavantage car il y une réduction de la main d'œuvre (activités physiques)
Traitement des transactions	Manuel	Automatique	Avec l'automatisation il y a le gain en temps et d'efficacité, donc c'est l'avantage de l'e-commerce
Accessibilité	Temps limité	24 × 7 × 365	La boutique en ligne est ouverte en permanence ce qui est très important en commerce.
Inspection physique	Les marchandises peuvent être inspectées	Les marchandises ne peuvent pas être	Ce point présente un désavantage pour l'e-

	physiquement avant l'achat.	inspectées physiquement avant l'achat.	commerce, mais cela ne puisse pas mettre en cause le e-commerce car certains produits ont des spécifications techniques précisés.
Interaction client	Face à face	Écran à face	Donc, en e-commerce, pas de relation directe entre le client et le vendeur
Champ d'activité	Limité à une zone particulière.	Portée mondiale	Le e-commerce est avantageant car on vend partout au monde
Échange d'informations	Pas de plate-forme uniforme pour l'échange d'informations.	Fournit une plate-forme uniforme pour l'échange d'informations.	Pour le e-commerce la collecte des données devient facile et fiable.
Focus sur les ressources	Côté de l'offre	Côté de la demande	Grace à l'e-commerce, on produit pour vendre et non pour stocker
Relation d'affaires	Linéaire	De bout en bout	La relation d'affaires est beaucoup plus développée grâce à l'e-commerce
Commercialisation	Marketing à sens unique	Marketing personnalisé	Le marketing personnalisé est beaucoup plus adapté que le marketing à sens unique
Paiement	Argent comptant, chèque, carte de crédit, etc.	Carte de crédit, virement de fonds, etc.	Il n'a pas de grande différence entre les deux types de commerce.

Livraison de marchandises	Immédiatement	Prend du temps	Le temps que prend la livraison en e-commerce est dû à une grande distance qui peut séparer le client et le point de vente

II.3. Expression de besoins

Dans cette partie du chapitre, nous nous intéressons aux besoins et soucis des utilisateurs de l'application qui sont les gestionnaires des boutiques en lignes, les internautes et les autres systèmes informatique comme les systèmes de payement en ligne. Ces besoins et soucis sont spécifiés en besoins fonctionnelles et non fonctionnelles.

II.3.1. Besoins fonctionnels

Les besoins fonctionnels expriment les fonctionnalités concrètes du système, ces besoins sont directement liés au fonctionnement du système, ils influencent sur les résultats de l'application. Pour notre application sont entre autres : exposition des produits ainsi que leurs prix et caractéristiques, inscription des clients, ajout des produits au panier, l'enregistrement en ligne de la commande tout en renseignant le mode de paiement et point de livraison, payement en ligne, génération et impression de la facture et publication de nouvelles informations à l'endroit des clients.

II.3.2. Besoins non fonctionnels

Les besoins non fonctionnels sont des indicateurs de qualité de l'exécution des besoins fonctionnels, ils ne sont pas directement liés au fonctionnement de l'application mais jouent un rôle important sur la qualité de l'application.

L'application dispose d'une partie réservée au catalogue de produits avec possibilité de navigation selon la catégorie de produits. Les produits sont présentés avec leurs prix et caractéristiques techniques. On peut aussi consulter les détails sur chaque produit.

L'application est dotée d'une page d'inscription. Le client peut s'inscrire juste avant toute opération d'achat ; sinon il sera redirigé à la page d'inscription pour s'identifier ou s'inscrire

avant de valider sa commande. Les clients non-inscrits ne pourront pas valider leurs commandes.

L'ajout des produits au panier consiste à cliquer sur un produit exposé sur le catalogue afin de l'ajouter au panier d'achat. La quantité est automatiquement déterminée par le nombre de clics sur le même produit. On pourra également diminuer la quantité voire la suppression complète du produit en cliquant sur le bouton « supprimer » devant le produit ciblé.

Au moment de la commande, on a une option (liste déroulante) permettant de préciser un point de livraison de son choix. De plus au moment de la commande, on a une autre option permettant le choix d'un mode de paiement parmi ceux proposés par le système informatisé comme LumiCash, EcoCash, carte de crédit, etc. Pour cette option, je vais utiliser des services web que je proposerais à l'une des prestataires de ce genre de services faute de quoi je faire recours à la simulation.

Apres le choix de produits, d'un mode de paiement et d'un point de livraison sont terminés, il suffit d'un seul clic sur le bouton de validation pour que toutes les transactions puissent se dérouler séquentiellement ainsi que la génération et impression de la facture. En l'absence de l'imprimante, la facture peut être sauvegardée pour l'imprimer ultérieurement. En fin, pour des fins marketings, l'application aura un espace publicitaire pour communiquer de nouvelles informations aux clients et une option permettant d'ajouter de nouvelles publicités.

II.3.2. Besoins non fonctionnels

Les besoins non fonctionnels sont eux aussi importants car ils agissent de façon indirecte sur le résultat et sur le cycle de vie de l'application. Ils définissent le comportement et la performance de notre solution, ce qui fait qu'ils ne doivent pas être négligés, pour cela il faut répondre aux exigences suivantes :

L'application doit fonctionner de façon cohérente sans erreurs. La fiabilité désigne son aptitude à assurer sa mission dans des conditions d'environnement données et pendant une durée donnée. Elle caractérise ainsi la confiance que l'utilisateur peut placer dans le service rendu par un système.

Les cas d'exception doivent être signalées par des messages d'erreurs bien gérés pour bien guider l'utilisateur et l'aider à se retrouver en cas d'ambiguïtés.

Le système sera compatible avec plusieurs environnements d'exécution (Lunix, Mac Os, …). En outre le système doit être facile à l'adaptation, à l'installation et interchangeable.

Le système doit être documenté pour être facile d'analyse et de modification. Il doit être fondé sur une architecture standard et claire permettant sa maintenance et son déploiement.

L'application doit garantir au maximum possible d'intégrité et de confidentialité des données personnelles des clients. Pour y arriver, étant donné que l'on ne peut se prévenir d'attaques par l'homme du milieu, le système d'authentification des utilisateurs et un système de cryptage de données seront intégrés au niveau de l'application.

L'application sera accessible depuis les quatre coins du monde et à n'importe quel moment. Il s'agit d'une application full web hébergée sur un serveur distant disponible 24H/24, 7j/7.

II.4. Conclusion

L'analyse permet de comprendre le domaine à modéliser et ainsi aboutir à l'expression des besoins fonctionnels et non fonctionnels pour avoir un système informatisé répondant aux attentes des utilisateurs finaux. Ces besoins trouveront les solutions dans les chapitres III et IV

CHAPITRE III : CONCEPTION ET MODELISATION DU NOUVEAU SYSTEME INFORMATIQUE

III.1. Introduction

Une méthode d'analyse et de conception a pour objectif de permettre de formaliser les étapes préliminaires du développement d'un système afin de produire un système informatisé qui répond fidèlement aux besoins du client.

La conception prend en compte les résultats de l'analyse de l'existant. Il s'agit donc d'élaborer un modèle, à l'aide d'outils et méthodes adaptés, qui permettent la représentation schématique des données qui circulent dans l'entreprise qui fait objet d'informatisation. Ce modèle reflétant une réalité physique, doit être compréhensible par tous (client et concepteur). De ce modèle, il en découle le modèle logique de données, puis une base de données physique implémentée dans un gestionnaire de base de données (SGBD). Ce dernier contiendra toutes les données du système d'information informatisé.

III.2. Outils et méthodes utilisés

Pour mener à bien la conception d'un système d'information, plusieurs outils et méthodes peuvent être utilisés selon leurs facilités. Les plus connus de ces méthodes étant **MERISE** et **UML**

A ce stade, nous avons préféré d'utiliser l'outil **JMerise** intégrant la méthode **MERISE** (Méthode d'Étude et de Réalisation Informatique pour les Systèmes d'Entreprise) pour la conception de notre système d'information. Cette méthode est basée sur la séparation des données et des traitements à effectuer en plusieurs modèles conceptuels et physiques.

Pour l'implémentation de la base de données physique, nous avons préféré d'utilise **MySQL**.

III.2.1. Méthode d'Étude et de Réalisation Informatique pour les Systèmes d'Entreprise

La méthode d'Étude et de Réalisation Informatique pour les Systèmes d'Entreprise, MERISE, est issue de l'analyse (l'étude d'un problème) systémique, elle est le résultat des travaux menés par une équipe de chercheurs et d'ingénieurs aixois (Jean-Louis le Moigne, Hubert Tardieu, Dominique Nancy, Henry Hechenroth, Daniel Pasco, Bernard Espinasse) qui en posèrent les bases dans le milieu des années 1970. [6]

Reconnu comme standard, Merise devient un outil de communication. En effet, Merise réussit le compromis difficile entre le souci d'une modélisation précise et formelle, et la capacité

d'offrir un outil et un moyen de communication accessible aux non-informaticiens. Un des concepts clés de la méthode Merise est la séparation des données et des traitements. Cette méthode est donc parfaitement adaptée à la modélisation des problèmes abordés d'un point de vue fonctionnel. Les données représentent la **statique** du système d'information et les traitements sa **dynamique**. L'expression conceptuelle des données conduit à une modélisation des données en entités et en associations. Merise propose une démarche, dite par niveaux, dans laquelle il s'agit de hiérarchiser les préoccupations de modélisation qui sont de trois ordres : la conception, l'organisation et la technique. En effet, pour aborder la modélisation d'un système, il convient de l'analyser en premier lieu de façon globale et de se concentrer sur sa fonction : c'est-à-dire de s'interroger sur ce qu'il fait avant de définir comment il le fait. Ces niveaux de modélisation sont organisés dans une double approche données/traitements.

Les trois niveaux de représentation des données sont :

- Le modèle conceptuel des données (MCD) décrit les entités du monde réel, en termes d'objets, de propriétés et de relations, indépendamment de toute technique d'organisation et d'implantation des données. Ce modèle se concrétise par un schéma entités-associations représentant la structure du système d'information, du point de vue des données.
- Le modèle logique des données (MLD) précise le modèle conceptuel par des choix organisationnels. Il s'agit d'une transcription (également appelée dérivation) du MCD dans un formalisme adapté à une implémentation ultérieure, au niveau physique, sous forme de base de données relationnelle ou réseau, ou autres. Les choix techniques d'implémentation (choix d'un SGBD) ne seront effectués qu'au niveau suivant.
- Le modèle physique des données (MPD) permet d'établir la manière concrète dont le système sera mis en place (SGBD retenu).

III.2.2. Éléments constitutifs du modèle entités-associations

La représentation du modèle entités-associations s'appuie sur trois concepts de base : l'objet ou entité, l'association, la propriété.
L'objet est une entité ayant une existence propre. L'association est un lien ou relation entre objets sans existence propre. La propriété est la plus petite donnée d'information décrivant un objet ou une association.

Libelle
Liste des Propriétés . .

Une entité est un objet, une chose concrète ou abstraite qui peut être reconnue distinctement et qui est caractérisée par son unicité.
Exemples d'entité : Audifax NDAYIRAGIJE, ordinateur, livre que je tiens entre les mains, etc.
Les entités ne sont généralement pas représentées graphiquement.

Un type-entité désigne un ensemble d'entités qui possèdent une sémantique et des propriétés communes.
Les personnes, les articles et les livres sont des exemples de type-entité. En effet, dans le cas d'une personne par exemple, les informations associées (les propriétés), comme le nom et le prénom, ne changent pas de nature.
Une entité est souvent nommée occurrence ou instance de son type-entité.

Les type-entité Personne, caractérisé par un nom et un prénom, et article, caractérisé par un nom et prix, ne peuvent pas être regroupés car ils ne partagent leurs propriétés (le prénom est une chaîne de caractères et le prix un nombre). Les type-entité Personne, caractérisé par un nom et un prénom, et Livre, caractérisé un titre et un auteur, possèdent tous les deux attributs du type chaîne de caractères. Pourtant, ces deux type-entités ne peuvent pas être regroupés car ils ne partagent pas une même sémantique : le nom d'une personne n'a rien à voir avec le titre d'un livre, le prénom d'une personne n'a rien à voir avec un auteur.
Par abus de langage, on utilise souvent le mot entité en lieu et place du mot type entité, il faut cependant prendre garde à ne pas confondre les deux concepts.

Attribut ou propriété, valeur

Clients
nomClient **prenomClient** **adresse**

Un attribut (ou une propriété) est une caractéristique associée à un type-entité ou à un type-association.
Exemples d'attribut : le nom d'une personne, le titre d'une livre, le prix d'un article.

Au niveau du type-entité ou du type-association, chaque attribut possède un domaine qui définit l'ensemble des valeurs possibles qui peuvent être choisies pour lui (entier, chaîne de caractères, booléen, …). Au niveau de l'entité, chaque attribut possède une **valeur** compatible avec son domaine.

La figure 2.2 montre la représentation graphique d'un exemple de type-entité
(Personne) avec trois attributs.

Règle :

- Un attribut ne peut en aucun cas être partagé par plusieurs type-entités ou type-associations.
- Un attribut est une donnée élémentaire, ce qui exclut des données calculées ou dérivées
- Un type-entité et ses attributs doivent être cohérents entre eux (ne traiter que d'un seul sujet).

Par exemple, si le modèle doit comporter des informations relatives à des articles et à leur fournisseur, ces informations ne doivent pas coexister au sein d'un même type entité. Il est préférable de mettre les informations relatives aux articles dans un type-entité Article et les informations relatives aux fournisseurs dans un type-entité Fournisseur. Ces deux type-entités seront probablement ensuite reliés par un type-association.

Identifiant ou clé

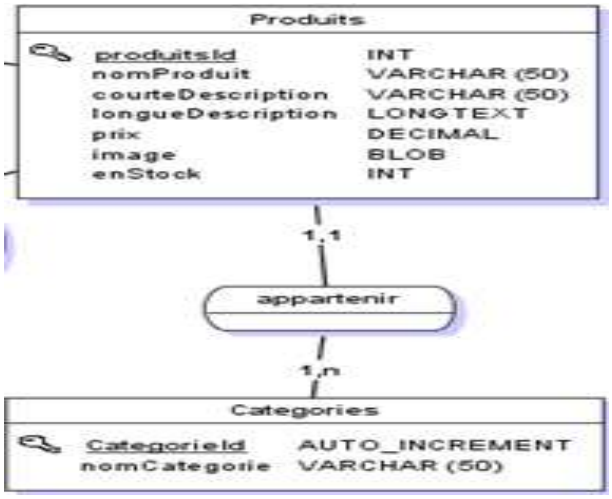
Clients
ClientId
nomClient
prenomClient
adresse

Cette figure est une représentation graphique d'un exemple de type-entité comportant quatre attributs dont un est un identifiant : deux personnes peuvent avoir le même nom, le même prénom et le même âge, mais pas le même identifiant.

Un identifiant (ou clé) d'un type-entité ou d'un type association est constitué par un ou plusieurs de ses attributs qui doivent avoir une valeur unique pour chaque entité ou association de ce type.

Exemples d'identifiant : le numéro de la commande, numéro de l'employé. Chaque type-entité possède au moins un identifiant, éventuellement formé de plusieurs attributs.
Ainsi, chaque type-entité possède au moins un attribut qui, s'il est seul, est donc forcément l'identifiant.
Dans la représentation graphique, les attributs qui constituent l'identifiant sont soulignés et placés en tête.

Association ou relation



Association : Une association (ou une relation) est un lien entre plusieurs entités.
Exemples d'association : l'appartenance de plusieurs produits à une catégorie.

Les associations ne sont généralement pas représentées graphiquement.
Un type-association (ou un type-relation) désigne un ensemble de relations qui possèdent les mêmes caractéristiques. Le type association décrit un lien entre plusieurs type-entités. Les associations de ce type association lient des entités de ces type-entités.
Comme les type-entités, les type-associations sont définis à l'aide d'attributs qui prennent leur valeur dans les associations. Un attribut peut être placé dans un type-association uniquement lorsqu'il dépend de toutes les entités liées par le type-association.
Un type-association peut ne pas posséder d'attribut explicite et cela est relativement fréquent, mais on verra qu'il possède au moins des attributs implicites.
Exemples de type-association : l'emprunt d'un livre à la bibliothèque.
Une association est souvent nommée occurrence ou instance de son type-association.

Par abus de langage, on utilise souvent le mot association en lieu et place du mot type-association, il faut cependant prendre garde à ne pas confondre les deux concepts.
Les type-entités intervenant dans un type-association sont appelés les **participants** de ce type-association.
L'ensemble des participants d'un type-association est appelé la **collection** de ce type-association.
Cette collection comporte au moins un type-entité, mais elle peut en contenir plus, on parle alors de type-association n-aire (quand n=2 on parle de type-association binaire, quand n=3 de type-association ternaire, …).

La **dimension**, ou **l'arité** d'un type-association est le nombre de type-entités contenu dans la collection.
Comme un type-entité, un type-association possède forcément un identifiant, qu'il soit explicite ou non. La concaténation des identifiants des type-entités liés à un type association constitue un identifiant de ce type-association et cet identifiant n'est pas mentionné sur le modèle (il est implicite).
Cette règle implique que deux instances d'un même type-association ne peuvent lier un même ensemble d'entités.
Souvent, un sous-ensemble de la concaténation des identifiants des type-entités liés suffit à identifier le type-association.
On admet également un identifiant plus naturel et explicite, à condition qu'il ne soit qu'un moyen d'exprimer plus simplement cette concaténation.

Cardinalité d'une patte reliant un type-association et un type-entité précise le nombre de fois minimal et maximal d'interventions d'une entité du type-entité dans une association du type-association. La cardinalité minimale doit être inférieure ou égale à la cardinalité maximale.
Exemple de cardinalité : une personne peut être l'auteur de 0 à n livre, mais un livre ne peut être écrit que par une personne.
L'expression de la cardinalité est obligatoire pour chaque patte d'un type association.
Une cardinalité minimale est toujours 0 ou 1 et une cardinalité maximale est toujours 1 ou n.

Ainsi, si une cardinalité maximale est connue et vaut 2, 3 ou plus, alors nous considérons qu'elle est indéterminée et vaut n. En effet, si nous connaissons n au moment de la conception, il se peut que cette valeur évolue au cours du temps. Il vaut donc mieux considérer n comme inconnue dès le départ. De la même manière, on ne modélise pas des cardinalités minimales qui valent plus de 1 car ces valeurs sont également susceptibles d'évoluer. Enfin, une cardinalité maximale de 0 n'a pas de sens car elle rendrait le type-association inutile.
Les seules cardinalités admises sont donc :
0,1 : une occurrence du type-entité peut exister tout en étant impliquée dans aucune association et peut être impliquée dans au maximum une association.
0, n : c'est la cardinalité la plus ouverte ; une occurrence du type-entité peut exister tout en étant impliquée dans aucune association et peut être impliquée, sans limitation, dans plusieurs associations.
1,1 : une occurrence du type-entité ne peut exister que si elle est impliquée dans exactement (au moins et au plus) une association.
1, n : une occurrence du type-entité ne peut exister que si elle est impliquée dans au moins une association.
Une cardinalité minimale de 1 doit se justifier par le fait que les entités du type-entité en question ont besoin de l'association pour exister. Dans tous les autres cas, la cardinalité minimale vaut 0. Ceci dit, la discussion autour d'une cardinalité minimale de 0 ou de 1 n'est intéressante que lorsque la cardinalité maximale est 1. En effet, lors de la traduction vers un schéma relationnel, lorsque la cardinalité maximale est n, nous ne ferons pas la différence entre une cardinalité minimale de 0 ou de 1.

La seule difficulté pour établir correctement les cardinalités est de se poser les questions dans le bon sens. Pour ne pas augmenter le risque d'erreurs, il faut noter que, les cardinalités d'un type association sont « à l'envers » (par référence à UML) pour les type-associations binaires et « à l'endroit » pour les n-aires avec n>2.

La notion de cardinalité n'est pas définie de la même manière dans le modèle
Américain et dans le modèle Européen (Merise). Dans le premier n'existe que la notion de cardinalité maximale.
Avec un SGBD relationnel, nous pourrons contraindre des cardinalités à des valeurs comme 2, 3 ou plus en utilisant des déclencheurs (trigger).
Voici les dénominations des types-associations selon le nombre participants :

- Une type-association **récursive** (ou réflexive) relie la même classe d'entité
- Une type-association **binaire** relie deux classes d'entité
- Une type-association **ternaire** relie trois classes d'entité
- Une type-association **n-aire** relie n classes d'entité

III.2.3. Normalisation des type-entités et type-associations

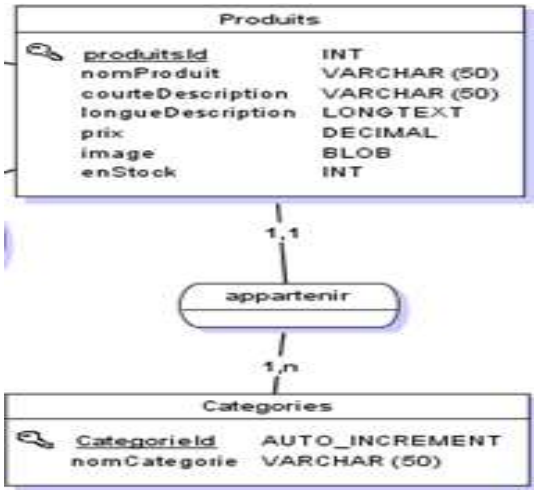
Les formes normales sont différents stades de qualité qui permettent d'éviter la redondance, source d'anomalies. La normalisation peut être aussi bien effectuée sur un modèle entités-associations, où elle s'applique sur les type-entités et type-associations, que sur un modèle relationnel.

Il existe 5 formes normales principales et deux extensions. Plus le niveau de normalisation est élevé, plus le modèle est exempt de redondances. Un type-entité ou un type-association en forme normale de niveau n est automatiquement en forme normale de niveau n−1. Une modélisation rigoureuse permet généralement d'aboutir directement à des type-entités et type-associations en forme normale de Boyce-Codd.

Première forme normale (1FN)

Produits
produitsId
nomProduit
courteDescription
longueDescription
prix
image
enStock
Categorie

1FN



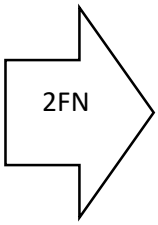
Un type-entité ou un type-association est en première forme normale si tous ses attributs sont élémentaires, c'est-à-dire non décomposables.

Un attribut composite doit être décomposé en attributs élémentaires (comme l'attribut Adresse sur la figure ci-dessus) ou faire l'objet d'une entité supplémentaire (comme l'attribut Occupants sur la figure ci-dessus.

L'élémentarité d'un attribut est toutefois fonction des choix de gestion. Par exemple, la propriété Adresse peut être considérée comme élémentaire si la gestion de ces adresses est globale. Par contre, s'il faut pouvoir considérer les codes postaux, les noms de rues, …, il convient d'éclater la propriété Adresse en Adresse (au sens numéro d'appartement, numéro et nom de rue, …), Code postal et Ville. En cas de doute, il est préférable (car plus général) d'éclater une propriété que d'effectuer un regroupement.

Deuxième forme normale (2FN)

Contenir
commandeId
produitsId
quantite





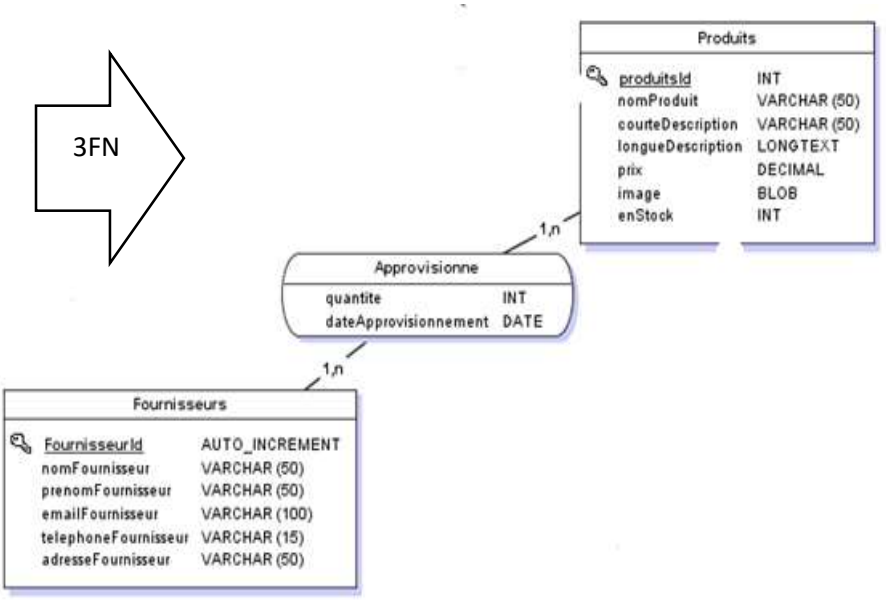
Un type-entité ou un type-association est en deuxième forme normale si, et seulement si, il est en première forme normale et si tout attribut n'appartenant pas à la clé dépend de la totalité de cette clé.

Autrement dit, les attributs doivent dépendre de l'ensemble des attributs participant à la clé. Ainsi, si la clé est réduite à un seul attribut, ou si elle contient tous les attributs, le type-entité ou le type-association est, par définition, forcément en deuxième forme normale.

La figure 2.31 montre un type-entité Article décrivant des produits provenant de différents fournisseurs. On suppose qu'un même fournisseur peut fournir plusieurs produits et qu'un même produit peut être fourni par différents fournisseurs. Dans ce cas, les attributs Produit ou Fournisseur ne peuvent constituer un identifiant du type-entité Article. Par contre, le couple Produit/Fournisseur constitue bien un identifiant du type-entité Article. Cependant, l'attribut Adresse fournisseur ne dépend maintenant que d'une partie de la clé (Fournisseur). Opter pour une nouvelle clé arbitraire réduite à un seul attribut N° article permet d'obtenir un type-entité Article en deuxième forme normale. On va voir dans ce qui suit que cette solution n'a fait que déplacer le problème.

Troisième forme normale (3FN)

Produits
produitsId
nomProduit
courteDescription
longueDescription
Prix
Image
enStock
Categorie
Fournisseur
AdresseFournisseur

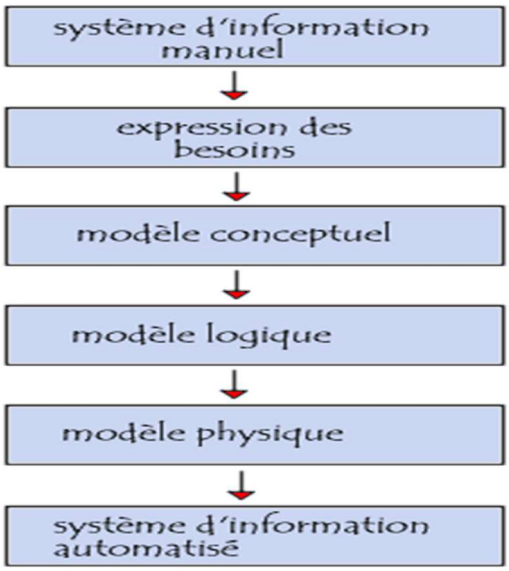


Dans cet exemple, l'attribut Adresse fournisseur dépend de l'attribut Fournisseur.

Un type-entité ou un type-association est en troisième forme normale si, et seulement si, il est en deuxième forme normale et si tous ses attributs dépendent directement de sa clé et pas d'autres attributs.

Un type-entité ou un type-association en deuxième forme normale avec au plus un attribut qui n'appartient pas à la clé est, par définition, forcément en troisième forme normale.

Succession d'étapes pour la conception des systèmes d'information :



Fenêtre d'accueil de l'outil JMerise

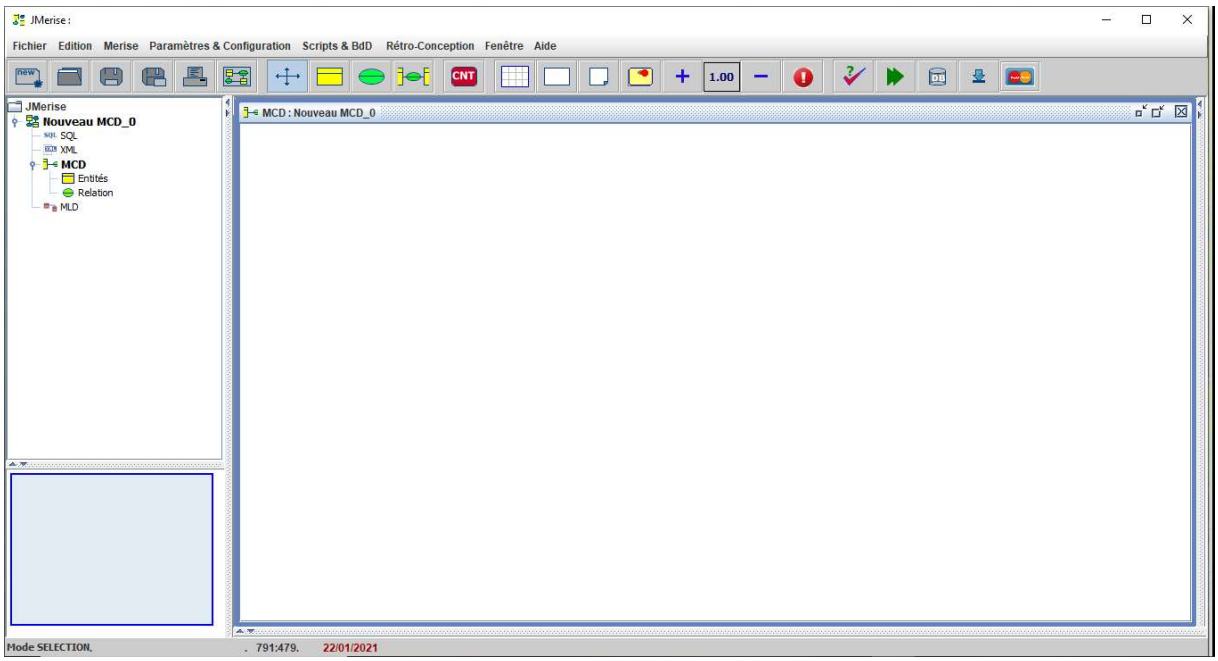


Figure 2: Interface de l'outil JMERISE

III. 3. Modèle conceptuel de données

Le modèle conceptuel des données (MCD) a pour but d'écrire de façon formelle les données qui seront utilisées par le système d'information. Il s'agit donc d'une représentation des données, facilement compréhensible, permettant de décrire le système d'information à l'aide d'entités.

Le modèle conceptuel de données est la représentation schématique du futur système informatisé. Il est une solution proposée par le concepteur pour répondre aux besoins exprimés au moment de l’analyse et doit être compréhensible par tous les intervenants.

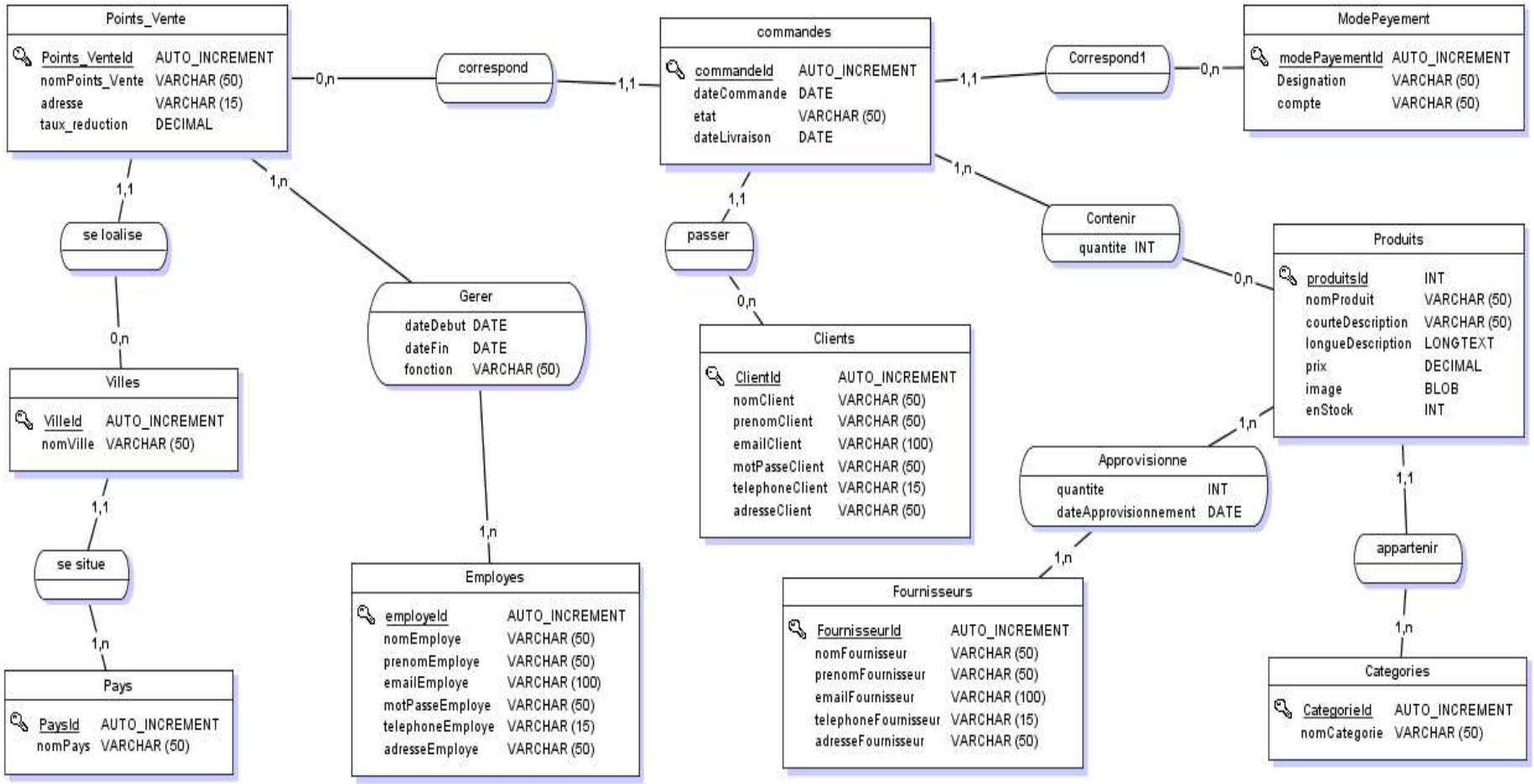


Figure 3: Modèle conceptuel de données

III. 4. Modèle logique de données

Le modèle logique des données (MLD) consiste à décrire la structure de données utilisée sans faire référence à un langage de programmation. Il s'agit donc de préciser le type de données utilisées lors des traitements. Ainsi, le modèle logique est dépendant du type de base de données utilisé.

Le passage du modèle conceptuel au modèle logique au niveau des classes de relation se fait selon les cardinalités des classes d'entité participant à la relation :

- Si une des classes d'entités possède une cardinalité faible : la table aura comme attributs, les attributs de la classe ayant une cardinalité faible, puis le (ou les) attribut(s) de relation et enfin les attributs de la seconde classe précédé du nom de la classe
- Si les deux classes d'entités possèdent une cardinalité forte : la table aura comme attributs, les attributs des deux classes de relation précédés des noms des classes respectives, puis le (ou les) attribut(s) de relation

Ainsi le Modèle logique de données (MLD) se traduit comme suit :

Clients(**ClientId** ,nomClient, prenomClient, email, motPasse, telephone, adresse, Clients)

ModePeyement(**modePayementId**, Designation, compte, ModePeyement)

Categorie(**categorieId**, nomCategorie, Categorie)

Produits(**produitsId**, nomProduit, courteDescription, longueDescription, prix, image, enStock, **#categorieId**)

Employes(**employeId**, nomEmploye, prenomEmploye, email, motPasse, telephone, adresse)

Fournisseurs(**FournisseurId**, nomFournisseur, prenomFournisseur, email, telephone, adresse)

Pays(**PaysId**, nomPays)

Villes(**VilleId**, nomVille, **#PaysId**)

Points_Vente(**Points_VenteId**, nomPoints_Vente, adresse, taux_reduction, **#VilleId**)

commandes(**commandId**, dateCommande, etat « payée, livrée », dateLivraison, **#ClientId**, **#Points_VenteId**, **#modePayementId**)

Gerer(**employeId, Points_VenteId**, dateDebut, dateFin, fonction)

Contenir(**commandeId**, **produitsId**, quantite)

Approvisionne(**FournisseurId**, **produitsId**, quantite, dateApprovisionnement)

III.5. Dictionnaire des données

Le dictionnaire des données est un document qui regroupe toutes les données que vous aurez à conserver dans votre base (et qui figureront donc dans le MCD). Pour chaque donnée, il indique :

- le **code mnémonique :** il s'agit d'un libellé désignant une donnée (par exemple «*nomClient*» pour le nom du client) ;
- la **désignation :** il s'agit d'une mention décrivant ce à quoi la donnée correspond (par exemple «*l'agresse du client*») ;
- le **type de donnée :**
    - **A** ou **Alphabétique :** lorsque la donnée est uniquement composée de caractères alphabétiques (de 'A' à 'Z' et de 'a' à 'z'),
    - **N** ou **Numérique :** lorsque la donnée est composée uniquement de nombres (entiers ou réels),
    - **AN** ou **Alphanumérique :** lorsque la donnée peut être composée à la fois de caractères alphabétiques et numériques,
    - **Date :** lorsque la donnée est une date (au format AAAA-MM-JJ),
    - **Booléen :** Vrai ou Faux ;
- la **taille :** elle s'exprime en nombre de caractères ou de chiffres. Dans le cas d'une date au format AAAA-JJ-MM, on compte également le nombre de caractères, soit 10 caractères. Pour ce qui est du type booléen, nul besoin de préciser la taille (ceci dépend de l'implémentation du SGBDR) ;
- et parfois des **remarques** ou **observations** complémentaires (par exemple si une donnée est strictement supérieure à 0, etc.).

Ainsi notre dictionnaire des données s'établit comme suit :

Tableau 2: Dictionnaire des données

Entités	Code mnémonique	Désignation	Type	Taille	Contraintes, règle de calcul
Clients	ClientId	Identifiant numérique du client	N	11	Automatique
	nomClient	Nom du client	A	50	Obligatoire
	prenomClient	Prénom du client	A	50	Obligatoire
	emailClient	Email du client	AN	100	Obligatoire
	telephoneClient	Numéro de téléphone du client	AN	15	Obligatoire
	adresseClient	Adresse du client	AN	50	Obligatoire
ModePeyement	modePayementId	Identifiant numérique du mode de paiement	N	50	Automatique
	Designation	Le nom du mode de paiement	A	50	Obligatoire
	Compte	Le compte de l'entreprise correspondant au mode de paiement	AN	50	Obligatoire
Categorie	categorieId	Identifiant numérique de la catégorie de produit	N	11	Automatique
	nomCategorie	Nom de la catégorie de produit	A	50	Obligatoire
Produits	produitsId	Identifiant numérique du produit	N	11	Automatique
	nomProduit	Nom du produit	A	50	Obligatoire
	courteDescription	Courte description du produit	A	50	Obligatoire
	longueDescription	Longue description du produit	A	50	Obligatoire
	prix	Prix d'un produit	N	11	Obligatoire
	Image	Image d'un produit	AN	200	Obligatoire
	enStock	Quantité de produit en stock	N	11	Obligatoire

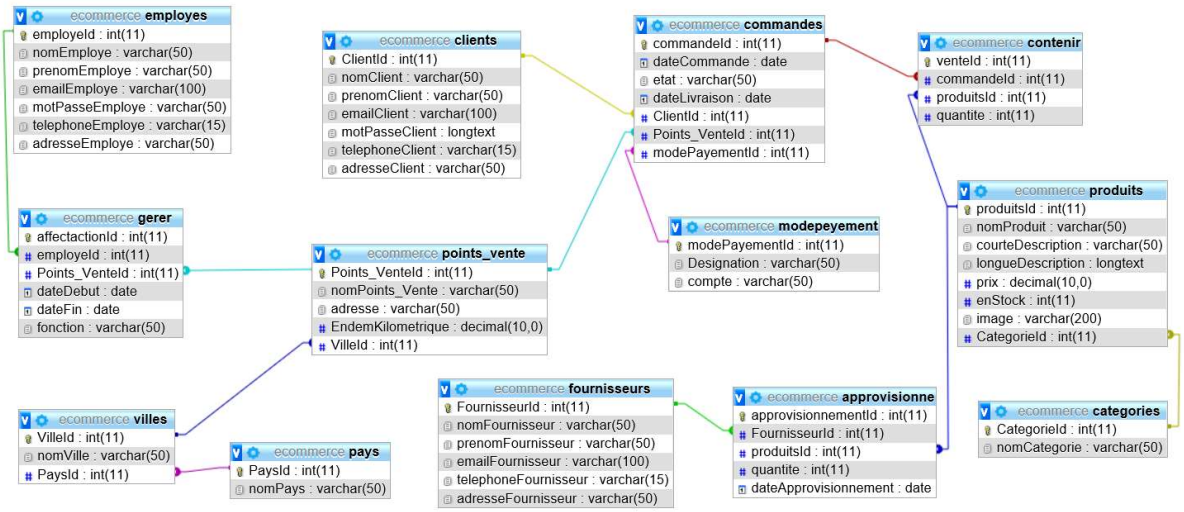
Employes	employeId	Identifiant numérique d'un employé	N	11	Automatique
	nomEmploye	Nom d'un employé	A	50	Obligatoire
	prenomEmploye	Prénom d'un employé	A	50	Obligatoire
	emailEmploye	Email d'un employé	AN	100	Obligatoire
	motPasse	Mot de passe d'un employé	AN	50	Obligatoire
	telephoneEmploye	Téléphone d'un employé	AN	15	Obligatoire
	adresseEmployé	Adresse d'un employé	A	50	Obligatoire
Fournisseurs	FournisseurId	Identifiant numérique d'un fournisseur	N	11	Automatique
	nomFournisseur	Nom d'un fournisseur	A	50	Obligatoire
	prenomFournisseur	Prénom d'un fournisseur	A	50	Obligatoire
	emailFournisseur	Email d'un fournisseur	AN	100	Obligatoire
	telephoneFournisseur	Numéro de téléphone d'un fournisseur	AN	15	Obligatoire
	adresseFournisseur	Adresse d'un fournisseur	AN	50	Obligatoire
Pays	PaysId	Identifiant numérique d'un pays	N	11	Automatique
	nomPays	Nom d'un pays	A	50	Obligatoire
Villes	VilleId	Identifiant numérique d'une ville	N	11	Automatique
	nomVille	Nom d'une ville	AN	50	Obligatoire
Points_Vente	Points_VenteId	Identifiant numérique d'un point de vente	N	11	Automatique
	nomPoints_Vente	Nom d'un point de vente	AN	50	Obligatoire
	adressePoints_Vente	Adresse d'un point de vente	A	50	Obligatoire

	taux_reduction	Taux de réduction pour un point de vente	N	11	Obligatoire
commandes	commandId	Identifiant numérique d'une commande	N	11	Automatique
	dateCommande	Date de commande	DATE		Obligatoire
	etat	Etat d'une commande	A	50	Obligatoire
Gerer	dateLivraison	Date de livraison d'une commande	DATE		Obligatoire
	dateDebut	Date d'affectation dans un point de vente	DATE		Obligatoire
	dateFin	Date de fin d'affectation dans un point de vente	DATE		Obligatoire
	fonction	Fonction d'un employé	A	50	Obligatoire
Contenir	quantite	Quantité de produit achetée	N	11	Obligatoire
	commandeId	Identifiant numérique de la commande	N		Obligatoire, clé étrangère
	produitsId	Identifiant numérique du produits	N		Obligatoire, clé étrangère
Approvisionne	dateApprovisionnement	Date d'approvisionnement	DATE		Obligatoire
	FournisseurId	Identifiant numérique du Fournisseur	N		Obligatoire, clé étrangère
	produitsId	Identifiant numérique du produits	N		Obligatoire, clé étrangère

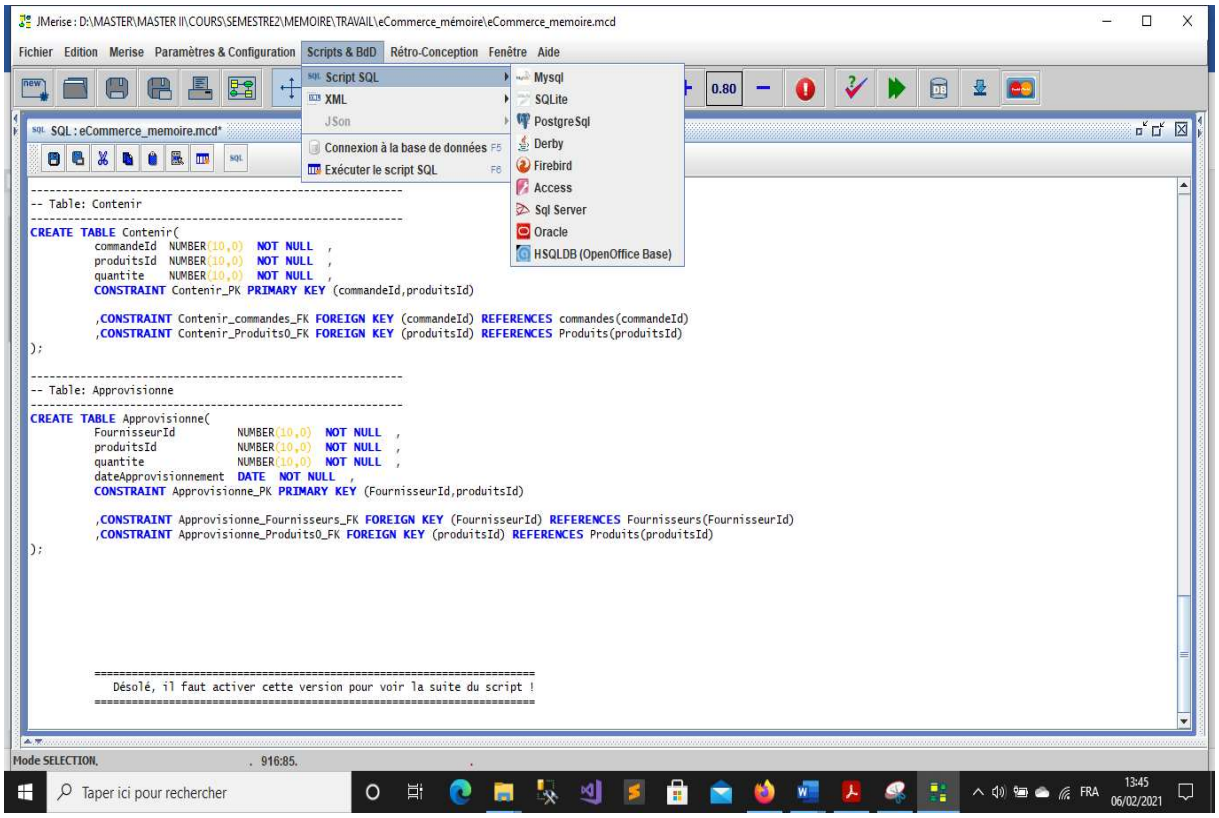
III. 6. Modèle physique de données

Avec la méthode Merise, le modèle physique des données (MPD) consiste à implémenter une base de données dans un système de gestion de basé de données (SGBD), le plus souvent relationnel (SGBDR). Ce modèle est dépendant d'un SGBD utilisé.

Figure 4: Modèle Physique de Données



L'outil **JMerise** permet de générer un script d'un modèle physique de données selon neufs SGBD comme le montre la figure ci-dessous :



III.7. Conclusion

La conception est l'étape clé dans la réalisation d'un système informatisé. Elle doit prendre en compte tous les besoins identifiés au cours de l'analyse. La conception a une série d'étapes à suivre. Pour la méthode MERISE, il s'agit du modèle conceptuel de données, modèle logique des données et le modèle physique des données (Base de données physique)

CHAPITRE IV : MODELE MATHEMATIQUE UTILISE POUR LA CONCEPTION DE LA BASE DE DONNEES

IV.1. Introduction

Plusieurs outils mathématiques sont à notre disposition pour modéliser des problèmes de la vie courante, les plus utilisés étant le Réseau de Pétri, les Files d'attente, Algèbre relationnelle, la Théorie des Graphes, Réseau des neurones, etc.

Tableau 3: Etude comparative des modèles mathématiques

Le nom modèle	**Rôle du modèle**
Réseau Pétri	Les réseaux de Pétri sont des outils graphiques et mathématiques permettant de modéliser et de vérifier le comportement dynamique des systèmes à événements discrets
Files d'attente	Elle consiste à modéliser le système dans lequel les serveurs sont soumis à un flux de requêtes qu'ils doivent être traités si les clients arrivent aléatoirement
Algèbre relationnelle	Elle décrit un ensemble d'opérations qui permettent de manipuler des relations, considérées comme des ensembles de n-uplets
Théorie des graphes	Elle permet de décrire un ensemble d'objets et leurs relations, c'est à dire les liens entre les objets
Réseau des neurones	Un réseau neuronal s'inspire du fonctionnement des neurones biologiques et prend le corps dans un ordinateur sous forme d'un algorithme

Parmi ceux outils mathématiques, j'ai trouvé que la Théorie des graphes est la mieux adaptée pour modéliser le système étudié.

IV.2. Problématiques des graphes

Certaines problématiques complexes ont été particulièrement étudiées. Parmi celles-ci on trouve la coloration des graphes. Il s'agit d'affecter une couleur à chaque nœud de telle sorte que deux nœuds reliés entre eux ne soient pas de la même couleur. Si cette problématique est mathématiquement intéressante et a capté l'attention de nombreux chercheurs, elle ne trouve que relativement peu d'applications concrètes. [8]

Les problématiques rencontrées dans le monde réel concernent principalement la réduction des graphes, la répartition de la charge des graphes, la polarisation des graphes et le parcours des graphes. Les graphes auxquels nous avons à faire sont généralement des graphes non homogènes, non structurés, présentant des cycles et des pôles locaux.

La problématique liée à la **réduction** des graphes consiste à produire un graphe équivalent disposant de moins d'arcs. Cette problématique se rencontre dans les réseaux notamment. Comment optimiser le nombre de points de raccordement de mon réseau de gaz pour diminuer le cout de l'installation et de la maintenance par exemple.

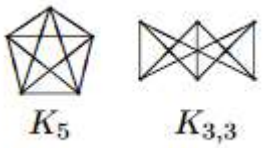
La problématique de **répartition de la charge** des graphes consiste à rechercher un graphe équivalent dans lequel les coefficients affectés aux arcs soient dans des intervalles de valeurs plus resserrées. Comment équilibrer la charge de mon réseau de distribution de l'électricité pour satisfaire les besoins évolutifs des consommateurs par exemple.

La problématique de **polarisation** de graphe consiste à remplacer le graphe par un graphe polaire équivalent. En formant des « grappes » on peut optimiser le réseau internet, par exemple en utilisant des gros tuyaux entre des pôles puis des ramifications vers les points de raccordement individuels.

La problématique de **parcours** des graphes consiste à rechercher le meilleur chemin entre deux nœuds. Par exemple pour optimiser le transport pour une société de logistique ou au contraire pour allonger la visite d'un client dans un centre commercial.

IV.3. Historique des graphes

En 1736, Euler s'intéresse au problème des ponts de Königsberg. Il s'agit de savoir s'il existe un chemin passant une fois et une seule par chaque pont de la ville. Ce problème deviendra ensuite le problème du postier qui vise à minimiser la distance parcourue par un postier voulant desservir toute la ville. En 1856, Hamilton étudie un problème apparemment aussi simple, celui de trouver un chemin passant une fois et une seule par chaque sommet d'un graphe. En fait, ce problème est beaucoup plus difficile à résoudre. [9]



Au début des années 1930, Kuratowski s'intéresse à la décomposition des graphes planaires. Il montre qu'on peut «décomposer» en temps linéaire tout graphe non-planaire en graphes K_5 ou $K_{3,3}$. Le dernier grand résultat concernant les graphes a été obtenu en 1976 par Appel et Haken qui ont montré qu'on peut colorier les faces de tout graphe planaire avec seulement 4 couleurs (les faces tangentes doivent être coloriées avec des couleurs différentes). Cependant, on ne connaît toujours pas de démonstration simple de ce résultat.

Définition (Graphe non-orienté). Un graphe non-orienté est un couple (X, E) où X est un ensemble de sommets et E est inclus dans $P_2(X)$ (ensemble des parties à deux éléments de X). Les éléments de E sont appelés arêtes. Parfois, on autorise les boucles (arêtes de mêmes extrémités), ou les arêtes multiples. L'arête{x, y} est souvent notée xy.

Définition (Graphe orienté).Un graphe orienté est un couple (X, U) où X est un ensemble de sommets et U est inclus dans $X\times X\backslash\{(x, x)|x \in X\}$.U est un ensemble d'arcs.

On autorise également parfois les boucles ou arcs multiples.

Définitions (Adjacence, incidence, voisinage, degré). Deux sommets x et y d'un graphe G = (X, E) sont adjacents si $xy \in E$.

Deux arêtes e et f d'un graphe G = (X, E) sont adjacentes si $e \cap f \neq \emptyset$. L'arête xy est incidente aux sommets x et y. Le voisinage d'un sommet x est défini par $\Gamma(x) = \{y \in X \mid xy \in E\}$. Le degré du sommet x est alors $d(x) = |\Gamma(x)| = \text{Card } \Gamma(x)$.

Pour un graphe orienté, les définitions peuvent être précisées :

Définitions (Voisinages extérieurs et intérieurs). Soit G = (X, U) un graphe orienté et x un sommet. Le voisinage extérieur de x est défini par $\Gamma^+(x) = \{y \in X \mid (x, y) \in U\}$. Son voisinage intérieur est $\Gamma^-(x) = \{y \in X \mid (y, x) \in U\}$. Le voisinage $\Gamma(x)$ est la réunion de $\Gamma^+(x)$ et $\Gamma^-(x)$. On appelle parfois voisinages sortant et entrant les voisinages extérieurs et intérieurs. On peut alors définir les degrés sortant d^+ et entrant d^- par le cardinal des ensembles $\Gamma^+(x)$ et $\Gamma^-(x)$.

Définitions (Point isolé, pendant, dominant). Si d(x) = 0, le sommet x du graphe est dit isolé. Si d(x) = 1, le sommet x est dit pendant. Si d(x) = |X|−1, le sommet x est dit dominant. Notons n = |X| et m = |E| ou |U|.

Proposition 1.1. Soit G = (X, E) un graphe non-orienté.

1. $m \leq \frac{1}{2}n(n-1)$;

2. $\sum_{x \in X} d(x)$ est pair ;

3. Il y a un nombre pair de sommets de degré impair.

Démonstration.1. Le graphe étant supposé sans boucle ni arête multiple, ce résultat est immédiat.

2. La somme des degrés des sommets est le nombre d'extrémités d'arêtes. Chaque arête possède deux extrémités et compte donc pour deux dans la somme des degrés. On a donc $\sum_{x \in X} d(x) = 2m$.

3. Ce résultat se déduit immédiatement du 2.

Proposition. Soit G= (X, E) un graphe. Il existe deux sommets différents ayant le même degré

Démonstration.

Supposons que tous les sommets aient des degrés différents. Ces degrés sont des entiers compris entre 0 et n −1. Ils prennent donc une fois et une seule chaque valeur entière entre 0

et n − 1. Il y a donc un sommet isolé et un sommet dominant, ce qui est impossible simultanément. Il y a contradiction.

Pour un entier n donné, il existe deux uniques graphes différents possédant deux sommets de mêmes degrés et les autres sommets de degrés tous différents.

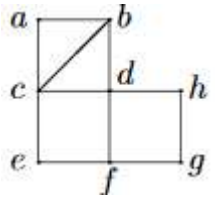
Définitions (Sous-structures). $G' = (X, E')$ est un graphe partiel de $G = (X, E)$ si $E' \subset E$.
$G' = (X', E')$ est un **sous-graphe** de $G = (X, E)$ si $X' \subset X$ et $E' = E \cap P_2(X')$.
$G' = (X', E')$ est **un sous-graphe partiel** de $G = (X, E)$ si $X' \subset X$ et $E' \subset E \cap P_2(X')$.
Définitions (Graphes particuliers). On note K_n le graphe complet à n sommets et S_n le graphe sans arête à n sommets. Un sous-graphe de G isomorphe à K_p est appelé **clique** tandis qu'un sous-graphe isomorphe à S_p est appelé **stable**.

Définition (Parcours, chaîne, cycle, longueur). Un parcours de G est une suite d'arêtes $\mu = (x_1, \ldots, x_k)$ telle que $x_i x_{i+1} \in E$ pour tout $i \in \{1, \ldots, k-1\}$.Un parcours $(x_1, \ldots, x_k)$ est fermé si $x_i = x_k$. Une chaîne de $G = (X, E)$ est un parcours sans répétition d'arête. Un cycle est une chaîne fermée. Une chaîne élémentaire est un chemin sans répétition de sommet. La longueur d'une chaîne est le nombre d'arêtes que contient cette chaîne.

On peut noter que la longueur d'une chaîne est toujours définie tandis que pour un parcours, ce n'est pas toujours le cas (un parcours peut être infini s'il contient des cycles).

Exemple.

- (a, b, c, d, c, a) est un parcours fermé.
- (e, f, d, c, b, d, h, g, f) est une chaîne.
- (a, b, d, c, a) est un cycle élémentaire.
- (a, b, d, c) est une chaîne élémentaire.



Proposition. Soit G = (X, E) un graphe non orienté. De toute chaîne, on peut extraire une chaîne élémentaire ayant les mêmes extrémités.

Démonstration. Soit $\mu = (x_1, \ldots, x_k)$ une chaîne. Si μ n'est pas élémentaire, il existe $i < j$ tel que $x_i = x_j$. Alors $\mu' = (x_1, \ldots, x_i, x_{j+1}, \ldots, x_k)$ est une sous- chaîne de μ, de mêmes extrémités.

La longueur de μ′ est strictement inferieure à la longueur de μ. On construit donc une suite de chaînes de mêmes extrémités, et de longueur strictement décroissante. Comme ces longueurs sont des entiers, cela ne peut pas se poursuivre indéfiniment. L'hypothèse de base devient donc fausse à partir d'un certain nombre d'itérations. La chaîne obtenue est alors élémentaire.

IV.4. Modélisation du système à l'aide de la théorie des graphes

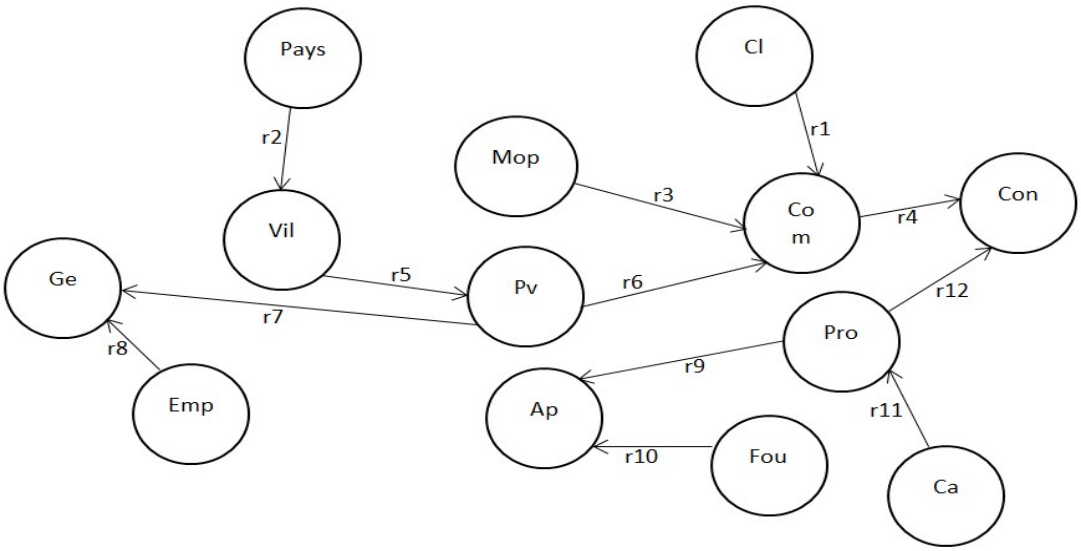
IV.4.1. Représentation de la base de données à l'aide d'un graphe

La base de données ou le modèle physique de données est composée de tables reliées par des relations. Dans notre graphe les tables sont des nœuds et les relations sont des arêtes qui relient les nœuds. Pour faire simples, les noms des tables et les noms des relations seront simplifiés comme le montre les tableaux ci-dessous :

Nom de table	**Nom simplifié pour le nœud correspondant**
Approvisionne	Ap
Categories	Ca
Clients	Cl
Commandes	Com
Contenir	Con
Employes	Emp
Fournisseurs	Fou
Gerer	Ge
Modepeyement	Mop
Pays	Pays
PointsVentes	Pv
Produits	Pro
Villes	Vil

Les relations	**Désignation simplifiée pour l'arête correspondant**
(Cl, Com)	r1
(Pays, Vil)	r2
(Mop, Com)	r3
(Com, Con)	r4
(Vil, Pv)	r5
(Pv, Com)	r6
(Pv, Ge)	r7
(Emp, Ge)	r8
(Pro, Ap)	r9
(fou, Ap)	r10
(Ca, Pro)	r11
(Pro, Con)	r12

On a alors le graphe suivant :



IV.4.2. Matrice d'adjacence obtenu à partir du graphe

En théorie des graphes, la matrice d'adjacence pour un graphe fini à n sommets est une matrice de dimension n × n dont l'élément non diagonal a_{ij} est le nombre d'arêtes liant le sommet i au sommet j.

A tout graphe d'ordre |X| = n, on associe une matrice M de n lignes et n colonnes dont les éléments sont notés M_{ij} :

Tableau 4: Matrice d'adjacence

	Ap	**Ca**	**Cl**	**Com**	**Con**	**Emp**	**Fou**	**Ge**	**Mop**	**Pays**	**Pv**	**Pro**	**Vil**
Ap	0	0	0	0	0	0	0	0	0	0	0	0	0
Ca	0	0	0	0	0	0	0	0	0	0	0	1	0
Cl	0	0	0	1	0	0	0	0	0	0	0	0	0
Com	0	0	0	0	1	0	0	0	0	0	0	0	0
Con	0	0	0	0	0	0	0	0	0	0	0	0	0
Emp	0	0	0	0	0	0	0	1	0	0	0	0	0
Fou	1	0	0	0	0	0	0	0	0	0	0	0	0
Ge	0	0	0	0	0	0	0	0	0	0	0	0	0
Mop	0	0	0	1	0	0	0	0	0	0	0	0	0
Pays	0	0	0	0	0	0	0	0	0	0	0	0	1
Pv	0	0	0	1	0	0	0	1	0	0	0	0	0
Pro	1	0	0	0	1	0	0	0	0	0	0	0	0
Vil	0	0	0	0	0	0	0	0	0	0	1	0	0

IV.4.3. Matrice d'incidence

En théorie des graphes, la matrice d'incidence d'un graphe est une matrice qui décrit le graphe en indiquant quels liens arrivent sur quels sommets.

$$aij = \begin{cases} +1 \text{ si le sommet est l'extrémité initiale de l'arc} \\ -1 \text{ si le sommet est l'extrémité finale de l'arc} \\ 0 \text{ si le sommet n'est ni l'extrémité initiale ni l'extrémité finale de l'arc} \end{cases}$$

	r1	r2	r3	r4	r5	r6	r7	r8	r9	r10	r11	r12
Ap	0	0	0	0	0	0	0	0	-1	-1	0	0
Ca	0	0	0	0	0	0	0	0	0	0	+1	0
Cl	+1	0	0	0	0	0	0	0	0	0	0	0
Com	-1	0	-1	+1	0	-1	0	0	0	0	0	0
Con	0	0	0	-1	0	0	0	0	0	0	0	-1
Emp	0	0	0	0	0	0	0	+1	0	0	0	0
Fou	0	0	0	0	0	0	0	0	0	+1	0	0
Ge	0	0	0	0	0	0	-1	-1	0	0	0	0
Mop	0	0	+1	0	0	0	0	0	0	0	0	0
Pays	0	+1	0	0	0	0	0	0	0	0	0	0
Pv	0	0	0	0	-1	+1	+1	0	0	0	0	0
Pro	0	0	0	0	0	0	0	0	+1	0	-1	+1
Vil	0	-1	0	0	+1	0	0	0	0	0	0	0

IV.4.4. Calcul de la matrice de fermeture transitive

$$M=\begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&1&0&0&0&1&0&0&0&0&0\\
1&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0
\end{pmatrix}$$

La matrice M, matrice d'adjacence montre tous les chemins de longueur 1

$M^2=$

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

La matrice ci-dessus montre les chemins de longueur 2 que l'on ajoute comme arrêtes.

$M^3=$

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

La matrice montre les chemins de longueur 3 que l'on ajoute comme arrêtes

$M^4=$

$$\begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}$$

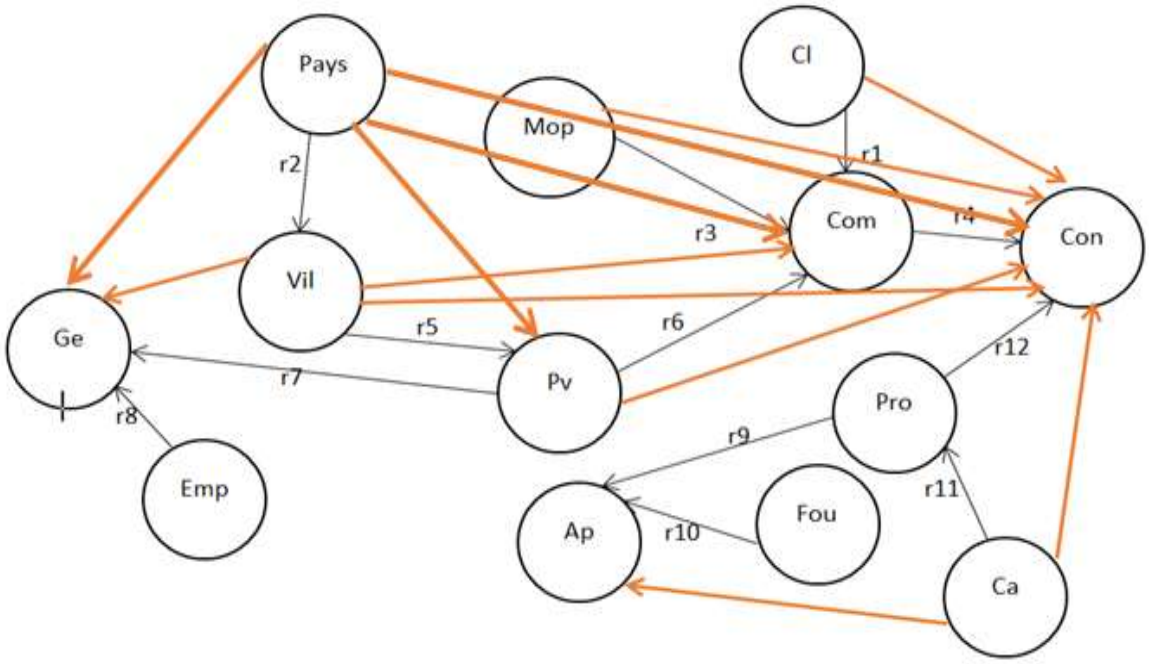
La matrice montre les chemins de longueur 4 que l'on ajoute comme arrêtes

En effectuant progressivement la somme $T = M \oplus M^2 \oplus M^3 \oplus M^4 \oplus \dots M^n$ (n = 13)….On peut observer qu'à partir d'une certaine valeur de n, la somme ne peut plus changer. La matrice T obtenue est la matrice de la fermeture transitive du graphe.

$T=$

$$\begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&0&0&0&0&0&1&0\\
0&0&0&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&0&0&0&0&0&0&0&0\\
0&0&0&1&1&0&0&1&0&0&1&0&1\\
0&0&0&1&1&0&0&1&0&0&0&0&0\\
1&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&1&1&0&0&1&0&0&1&0&0
\end{pmatrix}$$

Le graphe obtenu par fermeture est alors le suivant :



IV.4.5. Matrice des plus courts chemins dans le parcours de la base de données.

Notre graphe étant non pondéré, nous considérons que tous les arcs ont le même poids, soit le poids 1.

Plusieurs algorithmes sont donc utilisés pour le calcul des plus courts chemins. Les plus utilisés sont : l'Algorithme de Dijkstra, l'Algorithme de Bellman-Ford et Algorithme de Floyd-Warshall

Chacun de ces algorithmes est utilisé pour résoudre un problème spécifique de calcul des plus courts chemins. [18]

L'Algorithme de Dijkstra résout le problème de plus courts chemins depuis une source unique, le sommet **S**. L'Algorithme de Dijkstra ne fonctionne que pour des poids positifs.

L'algorithme de Bellman-Ford résout le problème de recherche de plus court chemin depuis une source unique, mais en autorisant des arcs portant des poids négatifs.

Il permet de détecter l'existence d'un circuit absorbant, c'est-à-dire de poids total strictement négatif, accessible depuis le sommet source. Cependant, si le graphe contient un circuit absorbant, il n'existe pas de solution.

Si l'on veut trouver pour toutes les paires de sommets les chemins les plus courts, l'algorithme décrit précédemment peut être appliqué en considérant successivement chaque sommet comme sommet de départ.

L'algorithme de Floyd-Warshall est cependant plus efficace pour le problème de plus courts chemins entre tous les sommets. Nous allons donc utiliser cet algorithme de Floyd-Warshall pour construire la matrice des plus courts chemins.

IV.4.6. Algorithme de Floyd-Warshall

L'algorithme de Floyd-Warshall consiste à calculer inductivement l'ensemble des chemins les plus courts entre tout couple de sommets dans un graphe en n'empruntant qu'un sous-ensemble E des sommets comme sommets intermédiaires.
En faisant croître E jusqu'à couvrir l'ensemble des sommets du graphe, on obtient alors l'ensemble des chemins les plus courts.

Soit la matrice W la matrice de pondération du graphe étudié.

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	∞	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	∞	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	0	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

Exécution de l'algorithme de Floyd-Warshall ; on calcule à chaque étape les valeurs de la partie non coloriée de la matrice en considérant le sommet k comme sommet intermédiaire.

W°=

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	∞	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	∞	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0	

W¹=

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	∞	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	∞	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

W¹=

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	∞	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	∞	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

W²=

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	∞	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	∞	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

W²=

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	∞	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	∞	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

W³=

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	∞	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	∞	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

$W^3=$

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	∞	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	∞	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

$W^4=$

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

$W^4=$

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

$W^5=$

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

$W^5=$

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

$W^6=$

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

$W^6=$

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

$W^7=$

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

$W^7=$

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

$W^8=$

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

$W^9=$

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

$W^9=$

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

$W^{10}=$

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞	0

$W^{10}=$

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	2	3	∞	∞	2	∞	∞	1	∞	0

$W^{11}=$

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	2	3	∞	∞	2	∞	∞	1	∞	0

$W^{11}=$

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
∞	0	∞	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	2	3	∞	∞	2	∞	∞	1	∞	0

$W^{12}=$

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
2	0	∞	∞	2	∞	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	2	3	∞	∞	2	∞	∞	1	∞	0

W^{12}=

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
2	0	∞	∞	2	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞	0	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0
∞	∞	∞	2	3	∞	∞	2	∞	∞	1	∞	0

W^{13}=

0	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
2	0	∞	∞	2	∞	∞	∞	∞	∞	1	∞
∞	∞	0	1	2	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	0	1	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	0	∞	∞	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	0	∞	1	∞	∞	∞	∞
1	∞	∞	∞	∞	∞	0	∞	∞	∞	∞	∞
∞	∞	∞	∞	∞	∞	∞	0	∞	∞	∞	∞
∞	∞	∞	1	2	∞	∞	∞	0	∞	∞	∞
∞	∞	∞	3	4	∞	∞	3	∞	0	2	∞	1
∞	∞	∞	1	2	∞	∞	1	∞	∞	0	∞	∞
1	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	0	∞
∞	∞	∞	2	3	∞	∞	2	∞	∞	1	∞	0

Interprétation de ces matrices trouvées

La matrice $\mathbf{W^1}$ est la matrice qui représente les plus courts chemins entre toutes paires de tables en passant par la table 1 (Ap) comme intermédiaire.

La matrice $\mathbf{W^2}$ est la matrice qui représente les plus courts chemins entre toutes paires de tables en passant par la table 2 (Ca) comme intermédiaire.

La matrice $\mathbf{W^3}$ est la matrice qui représente les plus courts chemins entre toutes paires de tables en passant par la table 3 (Cl) comme intermédiaire.

La matrice $\mathbf{W^4}$ est la matrice qui représente les plus courts chemins entre toutes paires de tables en passant par la table 4 (Com) comme intermédiaire.

La matrice $\mathbf{W^5}$ est la matrice qui représente les plus courts chemins entre toutes paires de tables en passant par la table 5 (Con) comme intermédiaire.

La matrice $\mathbf{W^6}$ est la matrice qui représente les plus courts chemins entre toutes paires de tables en passant par la table 6 (Emp) comme intermédiaire.

La matrice $\mathbf{W^7}$ est la matrice qui représente les plus courts chemins entre toutes paires de tables en passant par la table 7 (Fou) comme intermédiaire.

La matrice $\mathbf{W^8}$ est la matrice qui représente les plus courts chemins entre toutes paires de tables en passant par la table 8 (Ge) comme intermédiaire.

La matrice $\mathbf{W^9}$ est la matrice qui représente les plus courts chemins entre toutes paires de tables en passant par la table 9 (Mop) comme intermédiaire.

La matrice $\mathbf{W^{10}}$ est la matrice qui représente les plus courts chemins entre toutes paires de tables en passant par la table 10 (Pays) comme intermédiaire.

La matrice W11 est la matrice qui représente les plus courts chemins entre toutes paires de tables en passant par la table 11 (Pv) comme intermédiaire.
La matrice $\mathbf{W^{12}}$ est la matrice qui représente les plus courts chemins entre toutes paires de tables en passant par la table 12 (Pro) comme intermédiaire.
La matrice $\mathbf{W^{13}}$ est la matrice qui représente les plus courts chemins entre toutes paires de tables en passant par la table 13 (Vil) comme intermédiaire.
Donc la dernière matrice $\mathbf{W^{13}}$ est la **matrice des plus courts** chemins entre toutes les paires de tables.
En mettant à 1 toutes les valeurs non nulles et différentes à l'infini, on trouve la **matrice de fermeture transitive**.

IV.5. Conclusion

La théorie des graphes permet la représentation mathématique de plusieurs problèmes qui se présente sous forme de situation discrète. Dans le contexte de ce projet, la théorie des graphes a été utilisée pour représenter la base des données. Les tables correspondent aux sommets du graphe et les relations aux arcs du graphe. Ainsi on peut résoudre le problème d'optimisation des requêtes en étudiant le graphe.

CHAPITRE V : SECURISATION DE L'APPLICATION D'E-COMMERCE A L'AIDE DU CRYPTOSYSTEME RSA

V.1. Introduction

La sécurité des applications web est encore plus alarmante. D'après un rapport de Positive Technologies, 100% des applications analysées contiennent des failles de sécurité dont 85% pouvant toucher les utilisateurs.

De plus, d'après le rapport « State of Web Application Vulnerabilities » il y a eu une augmentation de plus de 700% de vulnérabilités entre 2014 et 2018. [12]

Plusieurs attaques peuvent être évitées grâce aux mesures de sécurité déjà connus comme l'authentification et le contrôle d'accès, mais malheureusement, il s'est montré que l'on ne peut pas se prévenir de l'Homme du milieu « Main in de middle ». Pour cela, il faut chiffrer nos informations transitant sur le réseau afin qu'elles soient compréhensibles uniquement par leurs destinateurs.

V.2. Comparaison des algorithmes de chiffrement

Tableau 5: Etude comparative des algorithmes de chiffrement

Algorithme	Avantages	Inconvénients
Chiffre de César	Très simple à mettre en œuvre	Le chiffre de César n'est pas fiable du tout : - Le nombre de combinaisons limites (26 possibles) - Le chiffre de César est très vulnérable à l'analyse des fréquences
Chiffre de Playfair	Analyse des fréquences difficile	Facile à casser car il conserve la structure du texte clair
Chiffre de Hill	Un Cryptage par bloc - La simplicité de l'implémentation - La bonne vitesse d'exécution et le grand débit du	- La vulnérabilité aux « Attaque à Texte Clair Choisi » - La mauvaise qualité de cryptage pour les images - Difficile de trouver de bonnes clés : l'inverse d'une matrice peut ne pas exister

	Cryptage - La résistance à l'analyse des fréquences - Dans le Cryptage d'image	
Chiffre de Vigenère	- Résiste à l'analyse des fréquences - La même lettre sera chiffrée de différentes manières	- Pour un message long, c'est même que le Playfair
Chiffrement de RSA	Réputé incassable Utilise deux clés : publique et privée Asymétrique	Cryptogramme de grande taille Encombrement de la base de données

Parmi ces algorithmes cités en haut, le RSA a été retenu pour le chiffrement les mots de passes seulement, les autres données seront hachées avant leurs stockage au niveau de la base de données.

V.3. Historique de RSA

La méthode de cryptographie RSA a été inventée en 1977 par Ron Rivest, Adi Shamir et Len Adleman, à la suite de la découverte de la cryptographie à clé publique par Diffie et Hellman, d'où le sigle RSA. RSA a été breveté par le MIT en 1983 aux Etats-Unis d'Amérique, mais le brevet a expiré le 21 septembre 2000. Au départ, Rivest, Shamir et Adlman voulaient prouver que tout système à clé publique possède une faille. [13]

V.4. Principe de fonctionnement.

Si Bob souhaite recevoir des messages en utilisant le RSA, il procède de la façon suivante :

1) **Création des clés** : Bob crée 4 nombres p ; q; e et d:
   - p et q sont deux grands nombres premiers distincts. Leur génération se fait au hasard, en utilisant un algorithme de test de primalité probabiliste.
   - e est un entier premier avec le produit (p-1)(q-1).
2) d est tel que ed ≡ 1 [(p - 1)(q - 1)]. Autrement dit, ed – 1 est un multiple de (p - 1)(q - 1). On peut fabriquer d à partir de e, p et q, en utilisant l'algorithme d'Euclide.
3) **Distribution des clés** : Le couple (n, e) constitue la clé publique de Bob. Il la rend disponible par exemple en la mettant dans un annuaire. Le couple (n, d) constitue sa clé privée. Il la garde secrète.
4) **Envoi du message codé** : Alice veut envoyer un message codé à Bob. Elle le représente sous la forme d'un ou plusieurs entiers M compris entre 0 et n – 1. Alice possède la clé publique (n, e) de Bob. Elle calcule $C \equiv M^e [n]$. C'est ce dernier nombre qu'elle envoie à Bob.
5) **Réception du message codé** : Bob reçoit C, et il calcule grâce sa clé privée $D \equiv C^d[n]$. D'après un théorème du mathématicien Euler, $D = M^{de} \equiv M [n]$. Il a donc reconstitué le message initial.

V.5. Explication mathématique du principe de fonctionnement de RSA

La RSA, s'appuie principalement sur les concepts mathématiques de nombre premiers, modulo et l'indicatrice d'Euler

Nombre premier : un nombre premier est un nombre entier qui n'est divisible que par lui-même ou par 1, par exemple 3, 5, 7, 11, 13 sont des nombres premiers. 91 n'est pas un nombre premier car 91 = 7 x 13.

Nombres premiers entre eux : deux nombres entiers sont premiers entre eux s'ils n'ont aucun diviseur commun à part 1, 15 et 8 sont des nombres premiers entre eux, 34 et 51 ont un diviseur commun : 17, ils ne sont donc pas premiers entre eux. [14]

Reste d'une division euclidienne :

L'opérateur % du C retourne le reste d'une division entre entiers.

55 % 12 = 7 car 55 = 4 * 12 + 7,

55 = 7 [12]. // On dit que 55 est égal à 7 modulo 12.

Le modulo, c'est 12 et non 7 comme on l'entend souvent dire par erreur.

L'indicatrice d'Euler : C'est une fonction notéeϕ. Elle est définie de la manière suivante : ϕ(N) est le nombre d'entiers inférieurs à N, premiers avec N.

Un exemple pour calculer ϕ(55). On écrit tous les entiers entre 1 et 55, on barre ceux qui ne sont pas premiers avec 55, on compte combien il en reste, c'est ϕ(55)

- 1,2,3,4,~~5~~,6,7,8,9,~~10~~,~~11~~,12,13,14,~~15~~,16,17,18,19,~~20~~,21, ~~22~~,23,24,~~25~~,26,27,28,29,~~30~~,31,32,~~33~~,34,~~35~~,36,37,38,39,~~40~~,41,42,43,~~44~~,~~45~~,46,47,48,49,~~50~~,51,52,53,54,~~55~~
- ϕ(55)=40.

Théorème : Si P et Q sont premiers, et si N = P x Q, alors ϕ(N) = (P-1)(Q-1). ϕ(55) = ϕ(5x11) = (5-1)(11-1) = 40.

V.5.1. Chiffrement asymétrique des données à l'aide de RSA

Prenons par exemple N = 55, P = 5, Q = 11, ϕ(55) = 40 et message à chiffrer : **Audifax**.

Nous savons que l'ordinateur ne comprend que des entiers, donc pour procéder au chiffrement d'un message, il faut représenter chaque caractère par son code ASCII correspondant.

On a: A = 65, u = 117, d = 100, I = 105, f = 102, a = 97 et x = 120. Ainsi le message à chiffrer devient : **65117100105102971120.**

Ensuite, on découpe le message en nombres < N (55) et l'on obtient : **6 51 17 10 0 10 51 0 29 7 12 0**, on détermine un nombre **e** qui soit premier avec ϕ(N) = 40, soit **e** = 3.

Élevons maintenant chaque partie du message à la puissance e, le message devient : **6^3 51^3 17^3 10^3 0^3 10^3 51^3 0^3 29^3 7^3 12^3 0^3**

Calculons enfin l'équivalent modulo N de chaque partie du message élevée à la puissance e :

- 6^3 modulo 55 = 51
- 51^3 modulo 55 = 46
- 17^3 modulo 55 = 18
- 10^3 modulo 55 = 10
- 0^3 modulo 55 = 0
- 10^3 modulo 55 = 10
- 51^3 modulo 55 = 46
- 0^3 modulo 55 = 0
- 29^3 modulo 55 = 24
- 7^3 modulo 55 = 13
- 12^3 modulo 55 = 23
- 0^3 modulo 55 = 0

Le message chiffré devient : **51 46 18 10 0 10 46 0 24 13 23 0**

Nous concluons que le chiffrement répond à la formule mathématique suivante : M^e mod N. M étant le message à chiffrer. Clef publique = (N, e), seuls N et e sont divulgués. P et Q sont secrets

V.5.2. Déchiffrement du message

Le déchiffrement consiste à décoder le message chiffré pour revenir au message d'origine, message clair.

On a chiffré le message en élevant des blocs à la puissance e modulo N. On va déchiffrer en utilisant le même principe. On va élever les blocs chiffrés à une puissance d modulo N.

Pour ça, déterminons d entier tel que : ed = 1 [ϕ(N)], $((M_1)^e)^d$ [N] = M1 [N], e x d = 1 + (k x ϕ(N))

Dans notre exemple : 3d = 1 + 40k, c'est-à-dire que 3d % 40 = 1

On considère d comme un compteur.
On part de d = 1 et on l'incrémente tant que 3d % 40 ! = 1. On trouve d = 27

Déchiffrement consiste à effectuer l'opération inverse,

Message déchiffré :

- 51^{27} modulo 55 = 6
- 46^{27} modulo 55 = 51
- 18^{27} modulo 55 = 17
- 10^{27} modulo 55 = 10
- 0^{27} modulo 55 = 0
- 10^{27} modulo 55 = 10
- 46^{27} modulo 55 = 46
- 0^{27} modulo 55 = 0
- 24^{27} modulo 55 = 29
- 13^{27} modulo 55 = 7
- 23^{27} modulo 55 = 12
- 0^{27} modulo 55 = 0

Voici finalement le message déchiffré, message initial : **651171001051029712 0**. d est la clef privée

Robustesse : Longueur de clef = longueur N (Ex : 128 bits = 2^{128} = 38 chiffres), Trouver d nécessite de calculer $\phi(N)$, Calculer $\phi(N)$, c'est très long sans connaître P et Q, Connaître P et Q nécessite de décomposer N en facteurs premiers. C'est long !

Cela est illustré par cet exemple donné par R, S et A :

- N=3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609

- P=16347336458092538484431338838650908598417836700330923121811108523893331001045081512121181675115 79
- Q=19008712816648221131268515739354139754718967899685154936666385390880271038021044989571912614655 71

Factorisé en 5 mois par 80 machines, 640 bits = 193 chiffres. La longueur conseillée : 2048 bits.

Clé publique en base 64 :

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAskgPKBcNpz71mi4NSYa5
mazJrO0WZim7T2yy7qPxk2NqQE7OmWWakLJcaeUYnI0kO3yC57vck66RPCjKxWuW
SGZ7dHXe0bWb5IXjcT4mNdnUIalR+lV8czsoH/wDUvkQdG1SJ+IxzW64WvoaCRZ+
/4wBF2cSUh90LwGEXiodUJ90JXFZVPKGCEjPcBI0vC2ADBRmVQ1sKsZg8zbHN+gu
U9rPLFzN4YNrCnEsSezVw/W1FKVS8J/Xx4HSSg7AyVwniz8eHi0e3a8VzFg+H09I
5wK+w39sjDYfAdnJUkr6PjtSbN4/Sg/NMkKB2Ngn8oj7LCfe/7RNqIdiS+dQuSFg
Eqidaqab

Clé privée en base 64 :

MIIEpAIBAAKCAQEAskgPKBcNpz71mi4NSYa5mazJrO0WZim7T2yy7qPxk2NqQE7O
mWWakLJcaeUYnI0kO3yC57vck66RPCjKxWuWSGZ7dHXe0bWb5IXjcT4mNdnUIalR
+lV8czsoH/wDUvkQdG1SJ+IxzW64WvoaCRZ+/4wBF2cSUh90LwGEXiodUJ90JXFZ
VPKGCEjPcBI0vC2ADBRmVQ1sKsZg8zbHN+guU9rPLFzN4YNrCnEsSezVw/W1FKVS
8J/Xx4HSSg7AyVwniz8eHi0e3a8VzFg+H09I5wK+w39sjDYfAdnJUkr6PjtSbN4/
Sg/NMkKB2Ngn8oj7LCfe/7RNqIdiS+dQuSFgeQIDAQABAoIBAQCtAyEyVqz5UTAn
n+llIUmcyQIuvyatnnIYcfRzgsY9soy6O8BjPSbypSTp31ozEwXGdN7U5Ir7Br4L
E8s0K2R8fnfwXTMPcJ8I9qXyj82lFO+4ewkDV1KewRn/cCIJs4s0caL48ZpDMt/V
6kC58QruFIA6pdwxtij09RPwDg7E3U1MrL9PqgGXXQcAwtboP7gHs2ac+0b6CwV0
Cyev09Xpni3ID0iKX8yKsxi6wOh+2O4Mz8B3R2gIXq7Gzw8oeho0nSBD19B7fWs+
w4vFlHIl57zbeISQK10cvvJ8BB4byy/bn5V2O2lESgU10d48csD5IUcjdV4/yuFx
vI8S9vfBAoGBAOqbw03WXnhZQu8O7Gos8P7lrBi3eYdF45hHAfWbK5ub6O7fC0kQ
FYZqO0AR70EAzuApWP0uGxQFALZ0QPyFZbpnKinE9T9a4M5AaP1Ex8WmeWbto96b
md6jVRXKXz24x5GDk+UdF7PJF91DufpUB5ZaO/AXpB9/3R9BDu7JHTjzAoGBAMKJ

grfZmyH3B9Cslnb8HUSlbXZQ/tnLoc3DpXnaENpYKWz/FMjqxTHuVRRqH86tYL33
/ow3UCaN3EYgIguoVC+DTbzk3/I9IXXeDXrocH1qCUy+x6dohzPoKZMoILLs+VeF
eAJfIptgVIfcD5teKdEY4lYPbV0m47Q2ET8pgNvjAoGADWgDPBJw6Y2oPoLqzZJt
3xL+x5bMcgdzXwNHwGIylrzNDcFfIrixkjHF2v5rU6HZMIQMWsNktrsmdEamZAe3
bXRxu1tO7GTkDcUuerKQe+HsdA5GW/UmUMuilBExahSCCvWq4N/Nt+9Y1sMFAKIG
oPfdDvY64bXry9pq4QhLDDMCgYAGs90vH24641n/lJKyksknXlPBKdU+B8gRYNZI
tnyyKSt0N+2tZnlY2Q9RXr6tzkdxBCRfDGDUkzqtp9nEcQ5FfM6m3XPh0r1eZEIu
o+eMSqT7Ye9bEzzlSvBzw4Qs5gFJRK331vNISy9eZvSas8nZDHRv5qQr+3UI9nvt
oy5vZQKBgQCK5z2IeL1NFd5OuJaR07Y+xwO7IOiZ+nn+fXWYkZ4bD08Dg0ACnd/w
OcS+2fU2/IIuXnhT/f5M5r0AJI1lG/V8TBo4gxN2dm7yBLgczbK3u+tex+pEnfEZ
qxAE0159q3iGvU5nmtX6VC0Z/IJIUCVgiEMwoKct0T5eOV2iQf5PaQ==

Texte claire : Jean*123

Cryptogramme :

e4X9ILaahBDOB6UdYH4p9r7LWV+AR2yNLObMETBa0Z4YAQ9Qq8q1ySU5pvdj7fJaLWqtQsz
Tg1dJ6CdgNTSJh+GJCmH33/0HlZ4PILjSHfSJffkH5Xh5mQyaLvsRaP7dd4y9SNlxjSWOX7/64a2
o018+7lGuAwLEpiVx499rOkYcrZFkykOf0UTXK2pyo/iQRax8gydq8GXl0FwtYi4AoTDgGAUNEbu
W43DsERR910aWZKOjpdSu6IveW/jjUfqJVJP3yid+xiteRZw5utSuPagVKfIqOBQAMQA0RYDkI
oTdHID1joGWi91LRiF50N2Qiq/PUJKZm726N7mkrlONTlQ==

V.6. Conclusion

Le RSA a deux types de clés : la clé publique (e, N) et la clé secrète ou privée (d, N). C'est donc un cryptosystème asymétrique ce qui renforce sa sécurité. De plus, la taille de N détermine sa robustesse car le problème est la factorisation de N pour trouver P et Q. En plus de cela, si N est de grande taille, on n'aura pas à réarranger les blocs car tous les codes ASCII correspondants aux caractères à chiffrer seront inférieurs à N.

CHAPITRE VI : IMPLEMENTATION DE L'APPLICATION..

VI.1. Introduction

Au niveau de cette dernière partie, nous allons mettre en place une application répondant aux besoins fonctionnels et non fonctionnels énumérés dans les chapitres précédents. Pour y arriver nous utiliserons des outils et l'architecture adaptés.

Ainsi nous avons utilisé comme environnement de développement : Visual studio 2019 via son Framework web ASP.NET core permettant la création d'applications multiplateformes et la publication d'application avec des packages utiles seulement. Nous avons également utilisé comme architecture : MVC (Models-Views-Controllers) et comme langages de programmation : C Sharp et le HTML.

Nous avons utilisé MySQL comme gestionnaire de base de données.

VI.2. Modèles-Vues-Controlleurs

Trop de développeurs, et pas seulement les débutants, ne savent pas organiser leur code, ce qui peut par la suite poser des problèmes. En fait, il y a des problèmes en programmation qui reviennent tellement souvent qu'on a créé toute une série de bonnes pratiques que l'on a réunies sous le nom de design patterns. En français, on dit « patron de conception ».
Le MVC est un design pattern très répandu. MVC est un acronyme signifiant Modèle - Vue - Contrôleur. Ce patron de conception, permet de bien organiser son code pour son application web. [15]
Voici ce que nous trouvons dans chaque partie :

- **Modèle** : les modèles vont gérer tout ce qui a trait aux données de l'application.
  Ces données se trouvent en général dans une base de données. Les données vont être traitées par les modèles pour ensuite être récupérées par les contrôleurs.
- **Vue** : comme son nom l'indique, une vue s'occupe de l'affichage. On y trouve uniquement du code HTML, les vues récupèrent la valeur de certaines variables pour savoir ce qu'elles doivent afficher. Il n'y a pas de calculs dans les vues.
- **Contrôleur** : un contrôleur va jouer le rôle d'intermédiaire entre le modèle et la vue.

Le contrôleur va demander au modèle les données, les analyser, prendre des décisions et renvoyer le texte à afficher à la vue. Les traitements se font dans le contrôleur. Un contrôleur ne contient que du code en C# et réalise une action.

VI.3. Packages de NuGet utiles pour l'application

Le développement d'une application web dans Visual Studio demande l'installation de certains packages selon les besoins. Dans mon projet nous avons utilisé les packages ci-dessous :

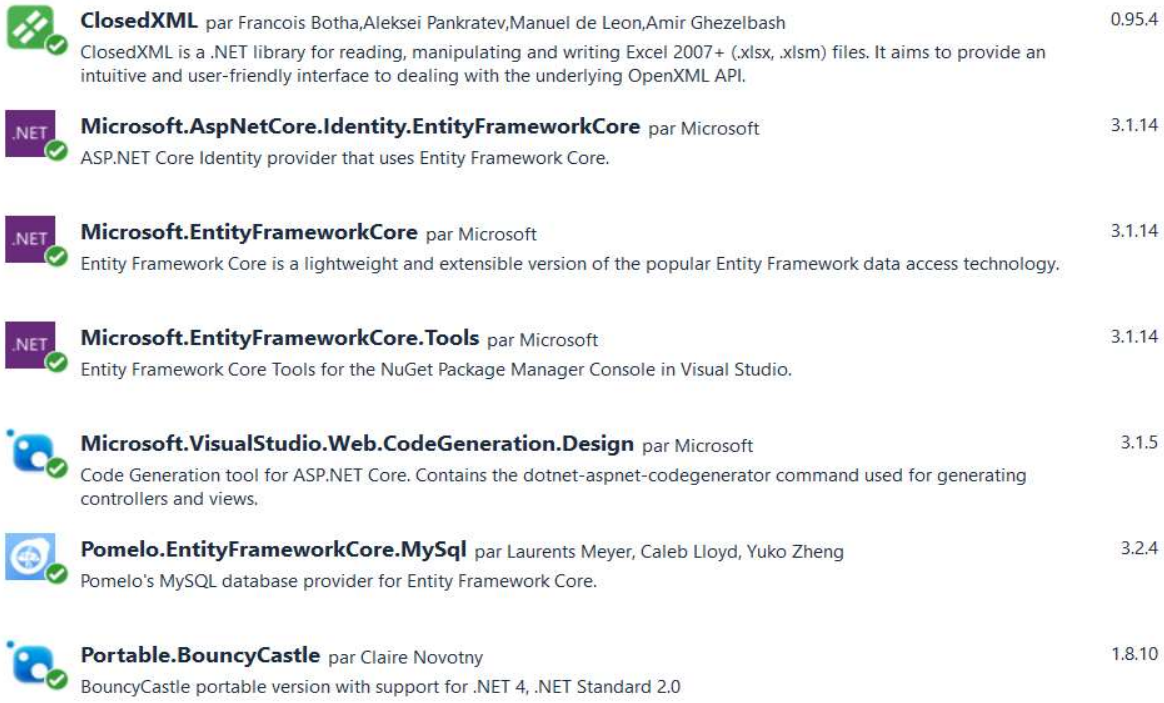


Figure 5: Packages utilisés pour le développement de l'application

VI.4. Entity Framework et Echafaudage

Entity Framework est un ORM qui va nous permettre d'accéder à une source de données sans que nous ayons la sensation de travailler avec une base de données. Cela paraît étrange, mais signifie simplement que grâce à cet ORM, nous n'allons plus écrire de requêtes, ni créer de tables, etc., via un système de gestion de base de données mais directement manipuler les données dans notre code C#. Un ORM très populaire avec C# est Entity Framework.

En utilisant cet ORM, trois approches peuvent être utilisées selon les cas. Il s'agit de :

- L'approche Model First
- L'approche Database First,
- L'approche Code First

Nous avons préféré d'utiliser la deuxième approche.

Echafaudage (Scaffolding) est une commande exécutée grâce aux outils PMC (Package Manager Console). Pour Entity Framework Core exécutent des tâches de développement au moment de la conception. Par exemple, ils créent des migrations, appliquent des migrations et génèrent du

code pour un modèle basé sur une base de données existante. Les commandes s'exécutent à l'intérieur de Visual Studio à l'aide de la console du gestionnaire de packages. Ces outils fonctionnent avec les projets .Net Framework.NET core.

L'Echafaudage consiste donc au mappage des tables d'une base de données en des classes C# et inversement. On peut donc commencer par la création d'une base de données (Database First) ou par la création des classes en C#. A l'aide des commandes de la console du gestionnaire de packages, on peut faire des migrations d'un côté vers l'autre.

```
PM> Scaffold-DbContext "Server = localhost;Database = ecommerce;user= root;" "Pomelo.EntityFrameworkCore.MySql" -
OutputDir Models -DataAnnotations
Build started...
Build succeeded.
PM>
```

Figure 6: Commandes utilisée pour migrer les tables vers les classes C#

Après Echafaudage, toutes les tables d'une base de données sont mappées en classes C#.

A partir de là on peut créer des classes C# et créer des tables correspondantes dans la base de données par migration via la console du gestionnaire de packages.

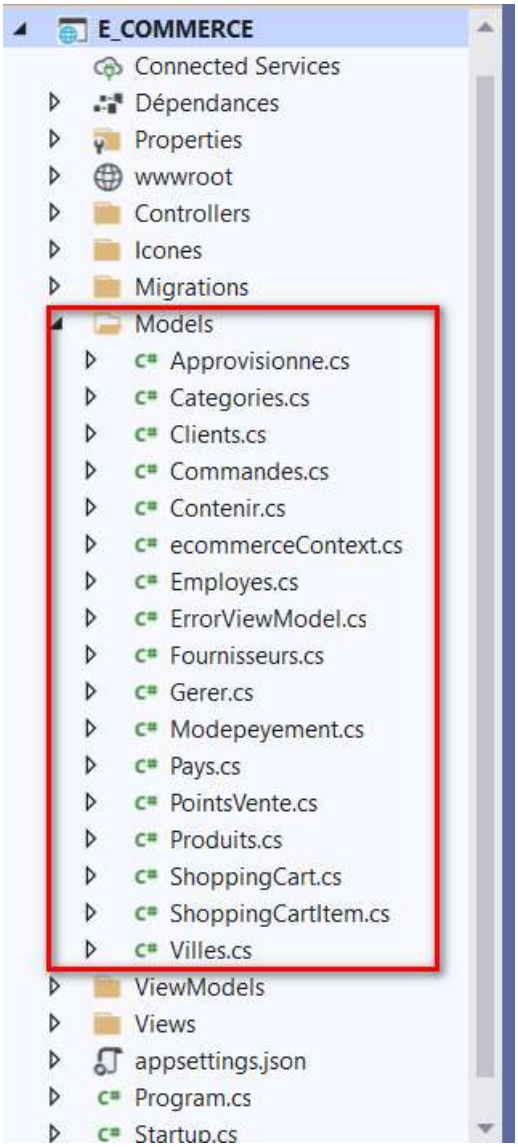


Figure 7: Classes C# obtenues après Echafaudage

VI.5. Présentation de principales fonctionnalités de l'application

VI.5.1. Page d'Accueil ou d'affichage du « Catalogue de produits »

La page d'accueil est la première page qui apparait quand un internaute visite notre site. Elle représente le catalogue de produits.

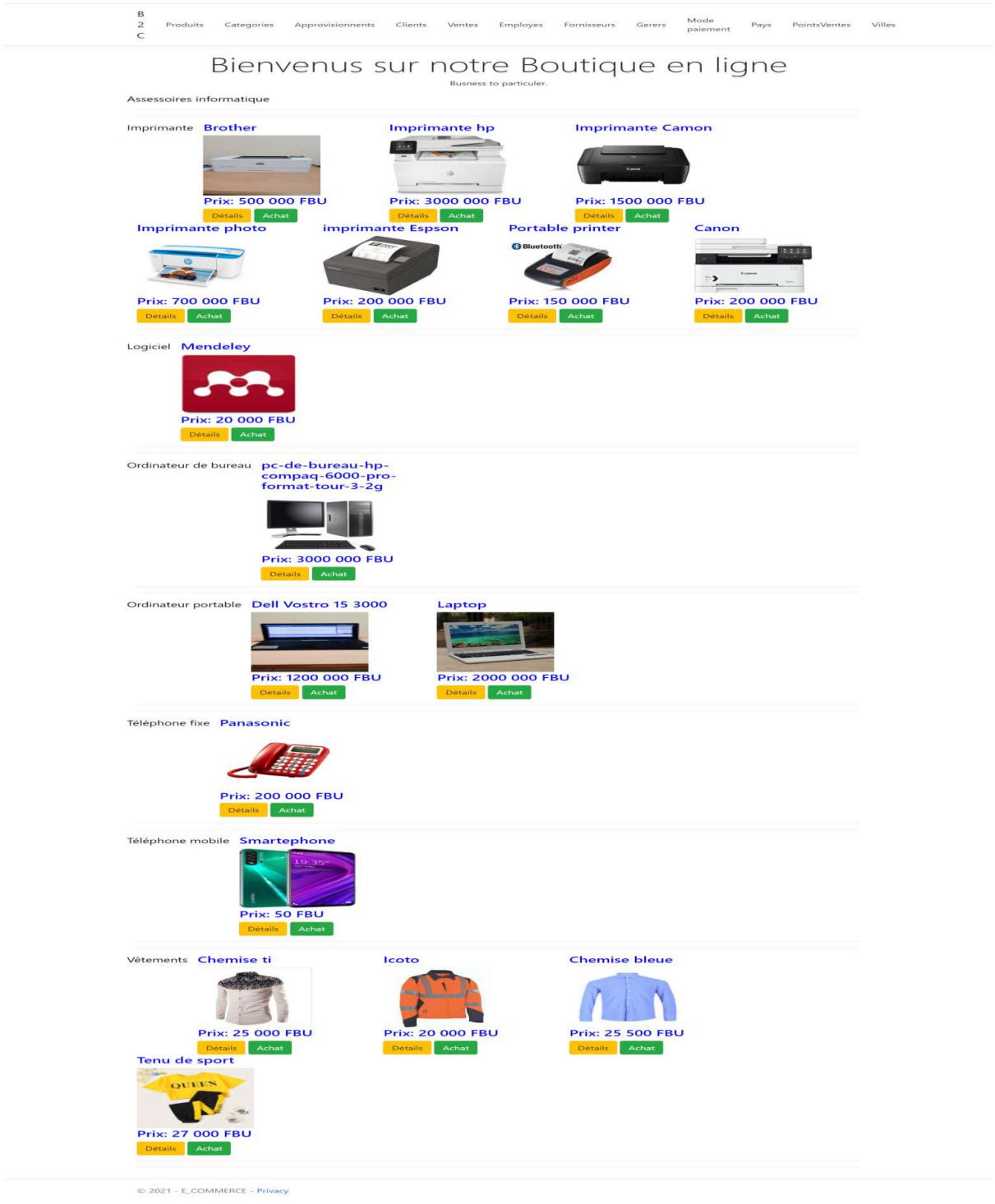


Figure 8: Page d'accueil de l'application

VI.5.2. Page « Index de produits »

Cette permet au gestionnaire de la boutique en ligne de gérer les produits, c'est-à-dire ajouter, modifier, supprimer un produit.

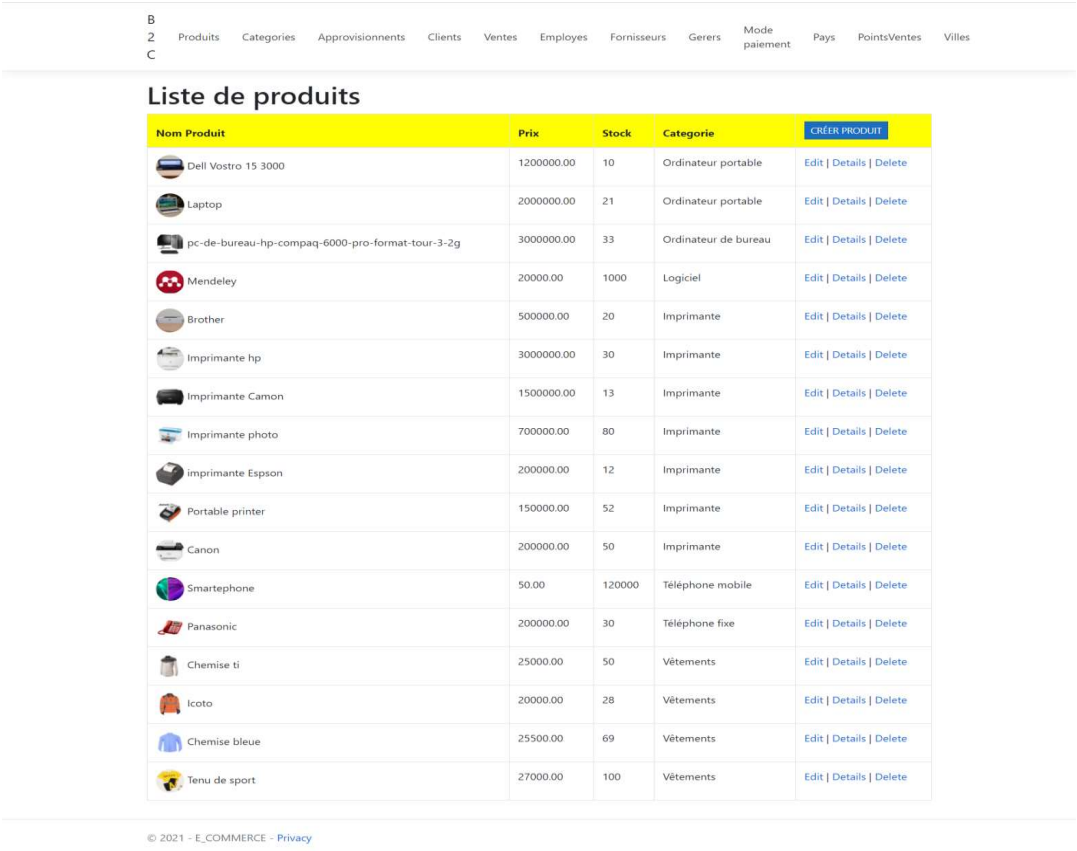


Figure 9: Page index de produits

VI.5.3. Pages « d'enregistrement de produits »

Cette page apparaît quand on clique sur le bouton **CREER PRODUIT** de la page d'index de produits, elle permet d'enregistrer un nouveau produit en même temps que son image.

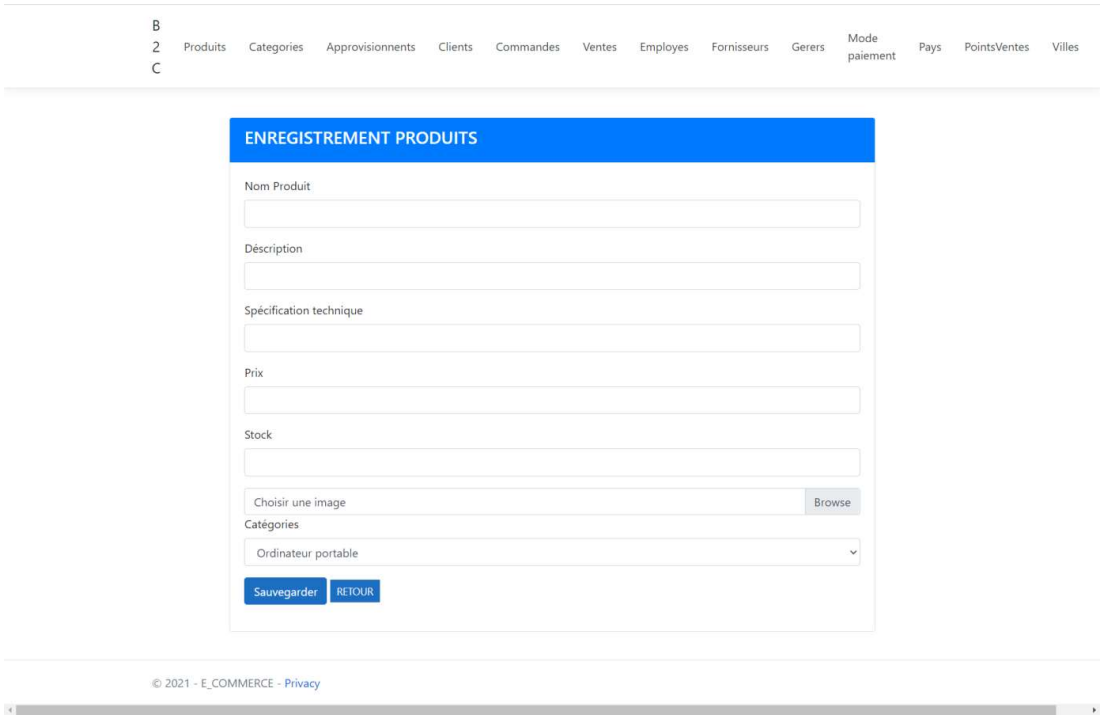


Figure 10: Page d'enregistrement de produits

VI.5.4. Pages de « suppression de produits »

Cette page apparaît quand on clique sur le bouton **Delete** de la page d'index de produits, elle permet supprimer un nouveau produit en même temps que son image.

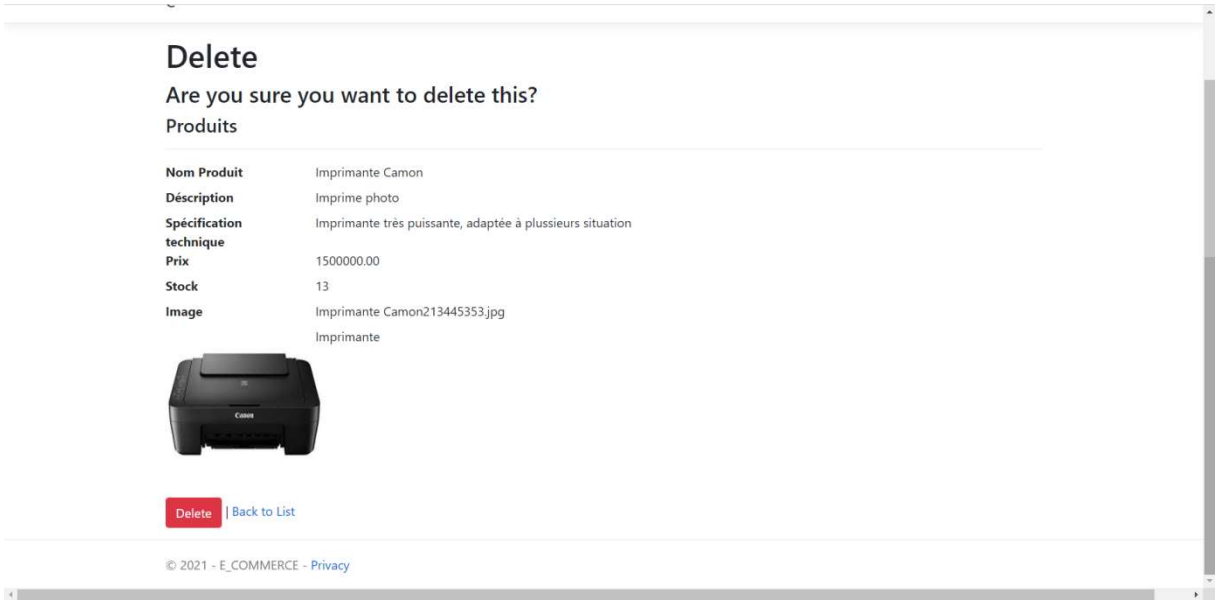


Figure 11: Page de suppression d'un produit

CONCLUSION ET RECOMMANDATIONS

1. Conclusion

A nos jours, le secteur du commerce est un secteur où l'on observe une grande concurrence. L'avènement de l'internet a permis aux entreprises d'accroitre leur part du marché. Or, dans notre pays, mêmes les capacités d'internet achetées à l'étranger par les fournisseurs d'accès internet ne sont pas suffisamment exploitées. L'enjeu de toute entreprise qu'elle soit de négoce, industrielle ou de services est de mettre en place un système de commerce électronique pour pouvoir vendre partout au monde.

Dans le cadre de mon projet de fin d'études, il a été intéressant de concevoir et développer une application web d'e-commerce permettant la mise en place d'une boutique virtuelle.

L'architecture MVC, une méthode appréciée des professionnels et des passionnés de la programmation, a été utilisée pour le développement de l'application. Ce modèle nous a permis de réaliser une application qui réponde mieux aux besoins fonctionnels et non fonctionnels de cette application. Aussi pour garantir l'intégrité et la fiabilité de l'application, nous avons mis en place plusieurs mécanismes de sécurité : l'authentification des utilisateurs, la gestion de rôles pour maitriser l'accès à certaines fonctionnalités et enfin, nous avons utilisé la cryptographie RSA pour chiffrer les flux de données de notre application qui transitent sur la toile.

Ainsi l'utilisation de notre application d'e-commerce apportera une solution à la problématique énoncée précédemment.

2. Recommandations

Le développement d'une telle application est un travail qui demande du temps suffisant et tous les services de paiement sont tiers. Cela a fait que certains modules ne soient pas développés. Je recommanderais aux futurs étudiants chercheurs d'améliorer cette application en développant le module de paiement en ligne à travers les services de paiement proposés par les opérateurs financiers disponibles dans notre pays comme LumiCash, EcoCash, etc.

REFERENCES BIBLIOGRAPHIQUES

[1] "akeza.net – TIC au Burundi : Quelques chiffres clés du marché de l'internet." http://akeza.net/tic-au-burundi-quelques-chiffres-cles-du-marche-de-linternet/ (accessed Feb. 11, 2021).

[2] "Qu'est-ce que le e-commerce?" http://tpemaxanthorobin.e-monsite.com/pages/le-e-commerce-generalites/qu-est-ce-que-le-e-commerce.html (accessed Feb. 12, 2021).

[3] "L'essor du e-commerce." http://tpemaxanthorobin.e-monsite.com/pages/le-e-commerce-generalites/l-essor-du-e-commerce.html (accessed Feb. 12, 2021).

[4] "Impact négatif : désintermédiation* de la vente, branches d'activités en chute libre." http://tpemaxanthorobin.e-monsite.com/pages/impact-sur-le-commerce-traditionnel/impact-negatif-desintermediation-de-la-vente-branches-d-activites-en-chute-libre.html (accessed Feb. 12, 2021).

[5] "Impact positif : utilisation du e-commerce pour booster le commerce physique." http://tpemaxanthorobin.e-monsite.com/pages/impact-sur-le-commerce-traditionnel/impact-positif-utilisation-du-e-commerce-pour-booster-le-commerce-physique.html (accessed Feb. 12, 2021).

[7] "Différence entre le commerce traditionnel et le commerce électronique." https://fr.gadget-info.com/difference-between-traditional-commerce (accessed Feb. 12, 2021).

[8] "Du rôle majeur des graphes - cleverm8." https://cleverm8.com/les-graphes/ (accessed Feb. 12, 2021).

[9] "Graphes et algorithmique des graphes." [Online]. Available: http://opencontent.org/opl.shtml.

[10] "Processus et protocoles de routage." http://mbaudin.free.fr/walkonthegrass/routage.html (accessed Feb. 13, 2021).

[11] rolin and pi, "Chapitre 7."

[12] "Sécurité des applications web : pourquoi devez-vous vous en soucier ?" https://www.synbioz.com/blog/securite-applications-web (accessed Feb. 17, 2021).

[13] "Histoire des maths : Cryptographie (RSA)." [Online]. Available: http://www.chez.com/myismail1Historique.

[14] "Réalisation d'un logiciel de Chiffrement RSA. - ppt télécharger." https://slideplayer.fr/slide/5468770/ (accessed Feb. 17, 2021).

[15] asp.net-core-mvc. (n.d.).

[16] "Théorie des graphes et applications," 2013.

[17] A. De Graphes, L. Info, and L. Math-info, "- TP 5. Plus courts chemins entre tous couples. Algorithme de Floyd-Warshall -," pp. 2016–2017, 2017.

[18] Ripphausen-lipa, H., & Science, A. (n.d.). court chemin Objectif.