REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de **T**echnologie

Département **I**ngénierie des **S**ystèmes **E**lectriques

Mémoire de Master

Présenté par

Mr. FILALI Farid

Mr. BERREKBIA Akram

Filière : Electronique

Spécialité : Electronique des **S**ystèmes **E**mbarqués

Conception d'un système de contrôle d'accès combiné RFID-Mot de passe

Soutenu le 12 / 07 /2022 devant le jury composé de :

MESSAOUDI	**Noureddine**	**MCA**	**UMBB**	**Président**
MOUATSI	**Abdelmalek**	**MCA**	**UMBB**	**Examinateur**
KAOUANE	**Mohamed**	**MCB**	**UMBB**	**Rapporteur**

Année Universitaire : 2021/2022

Remerciements

A dieu, le tout puissant, nous rendons grâce pour nous avoir donné la santé, la volonté et la patience pour réaliser ce travail.

Nos remerciements vont à Dr Mohamed KAOUANE notre encadreur, pour son aide, son suivi, ses conseils et directives et pour son dévouement.

Nous tenons à gratifier aussi les membres de jury pour l'intérêt qu'ils ont porté pour nous en acceptant d'examiner ce travail.

J'adresse mes sincères sentiments de gratitude et de reconnaissance à toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail.

Dédicaces

Je dédie ce mémoire

***A** toute ma famille*
***A** tous mes amis*
***A** tous ceux qui me sont chers*

Farid FILALI

A mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études.

A mes chères sœurs et frères pour leurs encouragements permanents, et leur soutien moral.

A toute la famille BERREKBIA et GEUSSOUM

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fruit de votre soutien.

Merci d'être toujours là pour moi.

Akram BERREKBIA

Résumé

Dans ce projet, nous avons réalisé un système de contrôle d'accès sécurisé basé sur la technologie RFID; géré par la carte Arduino afin de commander l'ouverture d'une porte ou d'une barrière, dans lequel l'utilisateur devra d'abord scanner la bonne étiquette et ensuite il devra entrer son mot de passe. Nous avons également ajouté d'autres témoins tels que, les LEDs et le Buzzer afin que l'utilisateur sache gérer son système, et d'un écran LCD I2C qui garantit l'affichage des informations utiles du système à l'utilisateur.

Le système proposé permet de sauvegarder toutes les informations des gens qui l'utilisent dans le but d'exploiter la base de données. On peut également utiliser ce système dans des magasins commerciaux ou dans des administrations et des établissements d'enseignement.

Abstract

In this project, we have realised a secure access system based on RFID technology and managed by the Arduino board to control the door or barrier in which the user will first have to scan the correct tag and then he will have to enter his password. we have also added other indicators such as LEDs and buzzers so that the user can manage their system, and an I2C LCD screen which guarantees the display of useful information from the system to the user

The proposed system saves all the details and information of the people they have used to operate the database. The system can also be used in commercial and educational establishments.

ملخص

في هذا المشروع، أدركنا نظامًا آمنًا للتحكم في الوصول يعتمد على تقنية RFID؛ تدار بواسطة لوحة Arduino من أجل الأمر بفتح باب أو حاجز، حيث يجب على المستخدم أولاً مسح العلامة الصحيحة ثم إدخال كلمة المرور الخاصة به. لقد أضفنا أيضًا مؤشرات أخرى مثل LEDs وBuzzer حتى يعرف المستخدم كيفية إدارة نظامه، وشاشة I2C LCD التي تضمن نقل المعلومات المفيدة من النظام إلى المستخدم.

يتيح النظام المقترح إمكانية حفظ جميع المعلومات الخاصة بالأشخاص الذين يستخدمونها من أجل استغلال قاعدة البيانات. يمكن استخدام هذا النظام أيضًا في المتاجر التجارية أو في المؤسسات الحكومية والتعليمية .

SOMMAIRE

Sommaire

Liste des abréviations

Abréviation	Signification
RFID	Radio frequency identification
AIDC	Automatic Identification and Data Capture
OCR	Optical Character Recognition,
IFF	Identify: Friend or Foe
EPC Global	Electronic Product Code.
OEM	Original Equipment Manufacturer – Fabricant d'équipement original
NFC	National Financial Credit
UID	Identifiant unique
SPI	**S**erial **P**eripheral **I**nterface
UHF	**U**ltra **H**aute **F**réquence
USB	**U**niversal **S**erial **B**us
LED	Light Emitting Diode
DC	**D**irect **C**urrent
BF	**B**asse **F**réquence
HF	**H**aute **F**réquence
ISO	**I**nternational **O**rganization for **S**tandardization
IDE	**I**ntegrated **d**evelopment **E**nvironment
NFC	**N**ear **F**ield **C**ommunication
I2C	Inter Integrated Circuit

Liste des figures

Chapitre I : **Généralités sur les systèmes de contrôle d'accès à RFID**

Chapitre II : **Etud*e* d'un système de contrôle d'accès RFID-Mot de passe**

Chapitre III **: Réalisation d'un système de contrôle d'accès RFID-Mot de passe**

Liste des tableaux

INTRODUCTION GENERALE

INTRODUCTION GENERALE

Les nouvelles technologies de l'information et de la communication (les NTIC) ont un rôle fondamental dans notre société moderne. Elles participent à sa transformation par différents effets sur les plans économiques et sociaux. Le développement de ces technologies est initié par des découvertes scientifiques, lesquelles permettant de nouvelles applications technologiques, elles-mêmes participant au partage de la connaissance. Les technologies d'identification font partie de ces technologies de l'information. Elles trouvent leurs applications depuis nombreuses années dans différents secteurs d'activité : transports (pour gérer l'accès aux transports publics), contrôle d'accès (aux immeubles, aux autoroutes), billetterie et gestion événementielle, et plus récemment, cartes d'identité et passeports. Elles sont aussi très répandues dans la chaîne d'approvisionnement manufacturière et la logistique de distribution des produits. Jusque-là les technologies d'identifications étaient soit sans contact : marquage, code à barres, soit nécessitaient un contact : carte bancaire, carte d'appels téléphoniques…etc. Grâce au développement récent des systèmes sans fil et de la micro- électronique, d'autres nouvelles technologies d'identification sans contacts ont vu le jour : les technologies de radio-identification (ou RFID pour Radio-Frequency IDentification). Ces nouvelles technologies, par leurs plus grande souplesse, rendent l'échange d'informations nettement plus rapide et efficace.

La technologie RFID est largement utilisée dans plusieurs domaines, l'identification d'objets ou de personnes, d'en suivre le cheminement et elle permet d'en connaitre les caractéristiques à distance grâce à une étiquette émettant des ondes radio attachée ou incorporée à l'objet ou à la personne (traçabilité), contrôler l'accès à une zone, puisque dans tous les endroits il y a un groupe de personnes qui partagent un espace commun, et personne ne souhaite voir son personnel mis en danger, et il n'existe pas de meilleures solutions que de sécuriser les accès (aux bâtiments, aux universités…etc.) avec un système de contrôle d'accès intelligent et fiable, qui permet d'isoler des zones précises et d'identifier tous les mouvements dans cette zone. Le système permet de gérer les ouvertures de portes automatiquement sans intervention humaine, garder un historique sur les entrées en temps réel pour chaque personne demandant l'accès grâce à un badge personnel (tag RFID) qui identifie chaque personne. La lecture de ces tags se fait par le lecteur RFID.

INTRODUCTION GENERALE

Le déploiement de l'identification par radiofréquence (RFID) dans un grand nombre de domaines d'application paraît prometteur. Sur ce présent projet et afin de mieux cerner notre étude nous avons exposé dans le premier chapitre un aperçu général sur la RFID et les systèmes de contrôle d'accès, les principales caractéristiques de la RFID, et une présentation générale des applications de la RFID.

Le deuxième chapitre est dédié à l'étude des différents éléments qui constituent notre projet y compris essentiellement la carte ARDUINO UNO et le module RFID.

Le dernier chapitre est consacré à la présentation de notre système de sécurité et les différentes étapes de programmation (codes utilisés), câblage et réalisation, ainsi que l'environnement de développement et les divers composants implémentés dans l'architecture de notre système.

Nous finirons ce rapport par une conclusion générale

CHAPITRE I :

GENERALITES SUR LES SYSTEMES DE CONTROLE D'ACCES A RFID

I.1. Introduction

L'identification par radiofréquence RFID (*radio frequency identification*) est une technologie automatique qui encode des données numériques dans un « tag » RFID, ou étiquette RFID, et permettant à un dispositif à ondes radioélectriques de les lire à distance. Le but de ces technologies est de permettre l'identification d'objets ou d'individus par des machines. La technologie RFID a la particularité de fonctionner à distance, sur le principe suivant : un lecteur émet un signal radio et reçoit en retour les réponses des étiquettes ou tags qui se trouvent dans son champ d'action.

La RFID permet de transmettre les données en temps réel, sans liaison filaire ni aucune intervention humaine. Elle convient parfaitement aux situations qui exigent l'obtention instantanée de données [1].

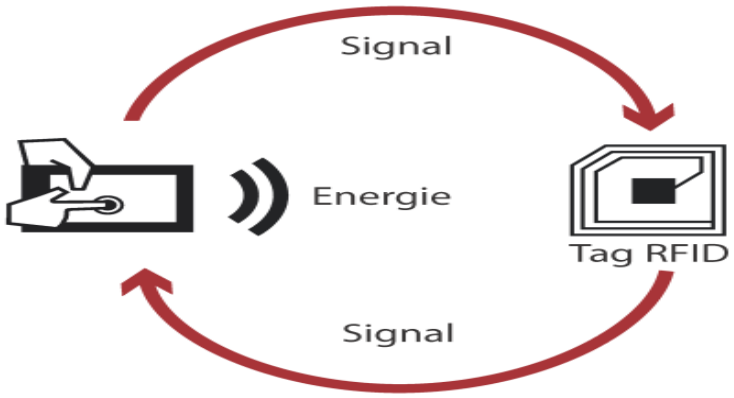


Figure I- 1: Echange de données entre un lecteur et un tag RFID

I.2. Différents systèmes d'identification automatique

Les systèmes RFID font partie des technologies d'identification automatique, que l'on appelle aussi AIDC (Automatic Identification and Data Capture). Nous présentons quelques-unes de ces technologies importantes à connaître pour comprendre le fonctionnement des systèmes RFID **[1]**.

I.2.1. Code à barres

Omniprésents dans notre vie quotidienne, les codes barre dominent les systèmes d'identification automatique depuis plus de 20 ans. Le code barre est un code binaire représenté par une séquence de barres vides et de barres pleines, larges ou étroites, disposées parallèlement (voir la Fig.II.1). La séquence peut être interprétée numériquement ou alpha numériquement. Elle est lue par balayage optique au laser, c'est-à-dire d'après la différence

de réflexion du rayon laser par les barres noires et les espaces blancs.

Malgré son grand âge, le code barre conserve des avantages importants comme son coût quasiment nul, et sa large diffusion. En revanche, il présente plusieurs inconvénients : il est fragile et doit être lu de manière optique. De plus, il ne peut pas être modifié à distance, contient peu d'informations et n'a bien sûr aucune capacité de traitement de données.

Figure I- 2: Code à barres

I.2.2. Reconnaissance optique de caractères

La reconnaissance optique de caractères (Optical Character Recognition, OCR) est utilisée depuis les années 1960. Elle fonctionne avec des polices de caractères conçues pour être lisibles aussi bien par les hommes que par les machines. Elle est utilisée aujourd'hui dans le domaine administratif et les services bancaires, notamment pour l'encaissement de moyens de paiement, tels que les chèques ou les bulletins de versement. Si les systèmes OCR ne sont pas plus répandus, c'est notamment dû à la complexité des lecteurs et à leur prix élevé.

Figure I- 3 : Reconnaissance optique du caractère

I.2.3. Smart cards

Une smart card (« carte intelligente » ou « carte à puce »), est un système électronique de stockage de données, éventuellement avec une capacité de traitement (carte microprocesseur) qui, par commodité, est incorporé dans une carte en plastique de la taille d'une carte de crédit. Les premières smart cards sontapparues en 1984, sous la forme de cartes téléphoniques prépayées. Pour fonctionner, les smart cards doivent être placées dans un lecteur,

qui entre en contact avec la surface de contact de la smart card. Le lecteur fournit à la smart card l'énergie et la pulsation d'horloge. Les transferts de données entre lelecteur et la carte se font par une interface série bidirectionnelle (port E/S). Un des principaux avantages des smart cards est que les données qui y sont stockées peuvent être protégées contre les accès (lecture et/ou écriture) non désirés. Les smart cards simplifient et sécurisent de nombreux services, à commencer par les transactions financières. Les smart cards comptent plusieurs inconvénients, basés sur la nécessité du contact et des manipulations : elles sont vulnérables à la corrosion et la poussière. Les lecteurs qui sont utilisés fréquemment (cabines téléphoniques, automates à billets. . .) tombent en panne et sontchers à entretenir. De plus, les lecteurs accessibles au public ne peuvent pas être protégés contre les mal intentionnés.

Figure I- 4: Smart cards

I.3. Généralités sur Les systèmes RFID

La technologie RFID est une solution qui ne nécessite ni contact physique ni contact visuel, entre le lecteur et le transpondeur fixé sur la pièce. Elle utilise les champs magnétiques ou électriques pour communiquer.

Les champs magnétiques traversant la matière, à l'exception des matériaux métalliques, il est donc possible de mettre le transpondeur aussi bien en surface de la pièce que directement dans la pièce où il sera alors non visible. Le transpondeur ne porte pas uniquement un identifiant, il peut aussi porter tous types d'informations numériques comme les codes à barres. **[3].**

I.3.1. Historique

La radio-identification est une technologie d'identification relativement moderne qui a été développée récemment. Cependant, la première application RFID fut utilisée pendant la Seconde Guerre mondiale lorsque Watson et Watt avaient développé une application dans le domaine militaire permettant de vérifier l'appartenance « amie » ou « ennemie » des avions arrivant dans l'espace aérien britannique et cela en 1935. Ce système dit IFF (Identify: Friend or Foe) reste le principe de base utilisé de nos jours pour le contrôle du trafic aérien. À partir

des années 40, l'idée de l'identification radio fréquence commence à germer avec les travaux de Harry Stockman, suivi des travaux de F. L. Vernon en 1952 et ceux de D.B. Harris. Leurs articles sont considérés comme les fondements de la technologie RFID et décrivent les principes qui sont toujours utilisés aujourd'hui. En 1975, la démonstration de la rétrodiffusion des étiquettes (tags) RFID, à la fois passives et semi-passives a été réalisée par Steven Depp, Alfred Koelle et Robert Freyman au laboratoire scientifique de Los Alamos. Le système portable fonctionne à la fréquence 915 MHz. Cette technique est utilisée par la majorité des transpondeurs (tags) RFID fonctionnant en UHF (ultra Hautes Fréquences) et microonde. À la fin des années 70, l'utilisation de la RFID pour l'identification de bétail commence en europe et aux États-Unis. Il a fallu attendre l'année 1990 pour commencer la standardisation des puces RFIDs. L'organisme ISO (International Organization for Standardization) se penche d'abord sur les puces puis sur les lecteurs et commence son travail de normalisation. Aujourd'hui encore la technologie RFID n'est pas encore complètement encadrée par une règlementation à l'échelle mondiale. L'année 1999 a connu la création du centre « Auto-ID Center », formé par le MIT (Massachusetts Institute of Technology) et des partenaires industriels, une organisation sans but lucratif ayant pour mission la standardisation et la construction d'une infrastructure pour un réseau mondial de la RFID. En 2010-2013, il a été prévu dans le Projet de Loi sur la santé que tous les Américains se verront implanter une micro-puce dans le but de créer un registre national d'identification, pour permettre un meilleur suivi des patients en ayant toutes les informations relatives à leur santé **[4]**.

I.3.2. Infrastructure de système RFID

Les premières générations des systèmes RFID ont été déployées sur un seul site avec généralement peu de lecteurs communicants à travers des liens dédiés vers un seul ou plusieurs serveurs d'application. Une telle architecture (Fig.III.2) marche bien pour un essai ou pour la validation d'un principe, mais devient plus difficile à exploiter pour des implémentations d'Enterprise avec plus de lecteurs, plus de sites et plus d'applications.

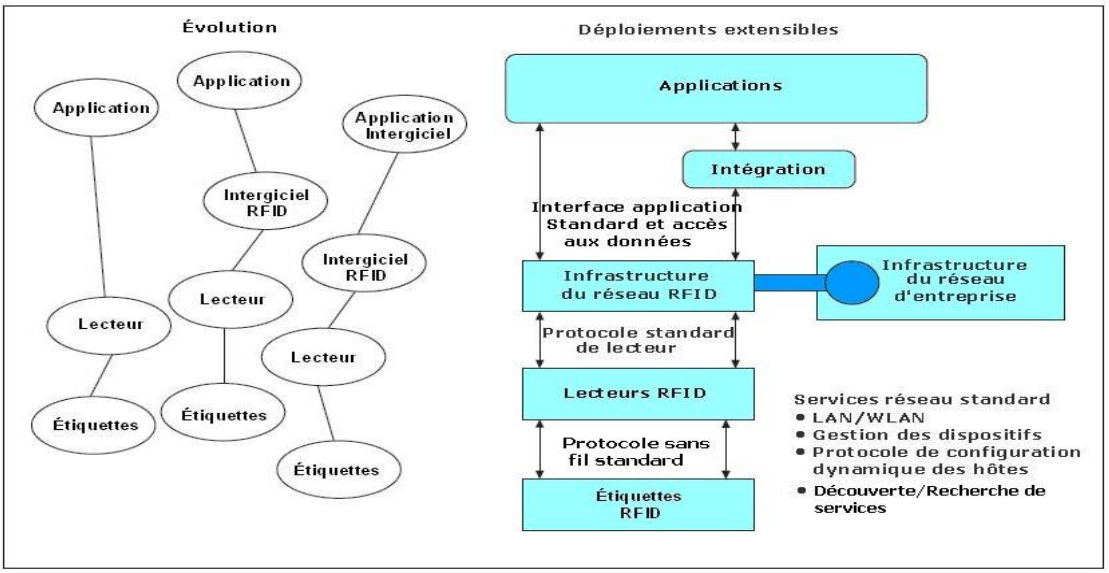


Figure I- 5: Évolution vers une infrastructure de RFID

Cette technologie permet d'identifier un objet, d'en suivre le cheminement et d'en connaître les caractéristiques à distance grâce à une étiquette émettant des ondes radio, attachée ou incorporée à l'objet. La technologie RFID permet la lecture des étiquettes même sans ligne de vue directe et peut traverser de fines couches de matériaux (peinture, neige, etc.) **[5]**.

I.4. L'identification électronique et la RFID

L'identification électronique se divise classiquement en deux branches :l'identification « à contact » et l'identification « sans contact »

Dans l'identification à contact, on a des dispositifs comportant un circuit électronique dont l'alimentation et la communication sont assurées par des contacts électriques. Les deux principaux exemples d'identification à contact sont **les circuits « mémoire »**, comportant des fonctions mémoire embarqués sur des modules de formes et de tailles variées, et les **cartes à puces** telles que les cartes bancaires, la carte vitale ou la carte SIM.

Dans l'identification sans contact, on distingue trois sous-branches principales :

I.4.1. Vision optique :

Ce type de liaison nécessite une vision directe entre l'identifiant et le lecteur (laser, camera CCD...). La technologie la plus répandue est le code à barre linéaire et les codes 2D (PDF417, QR Code, etc.). La technologie OCR (Optical Character Recognition) est également largement utilisée (scan MRZ (Machine Readable Zone) sur les passeports ou Carte National d'Identité).

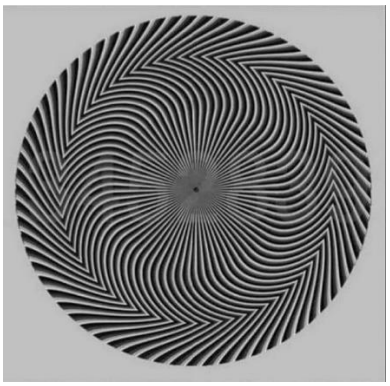


Figure I- 6: Vision optique

I.4.2. Liaison infrarouge :

Ce type de liaison assure un grand débit d'information,une grande directivité qu'une bonne distance de fonctionnement. Ces systèmes nécessitent également une visibilité directe.

Figure I- 7: Liaison infrarouge

I.4.3. Liaisons radiofréquences :

Ce type de liaison permet la communication entre l'identifiant et un interrogateur, sans nécessité de visibilité directe. De plus, il est également possible de gérer la présence simultanée de plusieurs identifiants dans le champ d'action du lecteur (anticollisions).

Cette dernière sous-branche constitue la **Radio Frequency IDentification ou** RFID dont on peut donner la définition suivante : Technologie d'identification automatique qui utilise le rayonnement radiofréquence pour identifier les objets porteurs d'étiquettes lorsqu'ils passent à proximité d'un interrogateur. Cela dit, la RFID ne peut pas se résumer à une seule technologie.

En effet, il existe plusieurs fréquences radio utilisées par la RFID et **plusieurs types d'étiquettes** ayant différents types de mode de communication et d'alimentation (Fig.I.8).

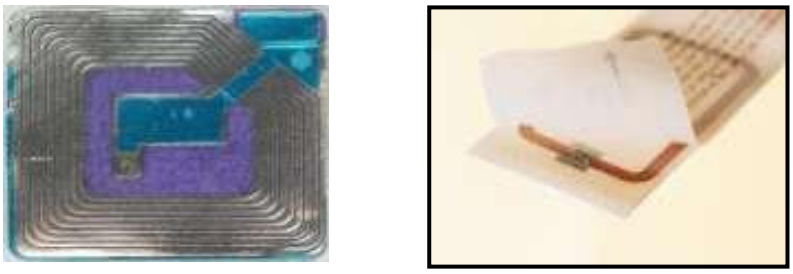


Figure I- 8: Exemples de Tags HF à 13.56 MHz

L'interrogateur ou lecteur est un dispositif actif, émetteur de radiofréquences activantles transpondeurs (ou tags) qui passent devant lui en leur fournissant à courte distancel'énergie dont ceux-ci ont besoin.

Pour transmettre des informations à l'interrogateur (encore appelé station de base ou plus généralement lecteur), un **tag RFID** est généralement **muni d'une puce électronique associée à une antenne**. Cet ensemble, appelé **inlay**, est ensuite packagé pour résister aux conditions dans lesquelles il est amené à vivre. L'ensemble ainsi formé est appelé tag, label ou encore transpondeur **[6]**.

I.5. Fonctionnement d'un système RFID et ses composants

Un système RFID se compose principalement d'un ou de plusieurs lecteurs, d'une ou plusieurs étiquettes (tags) et d'un logiciel d'application (middleware). La figure suivante décrit le schéma général d'un système RFID.

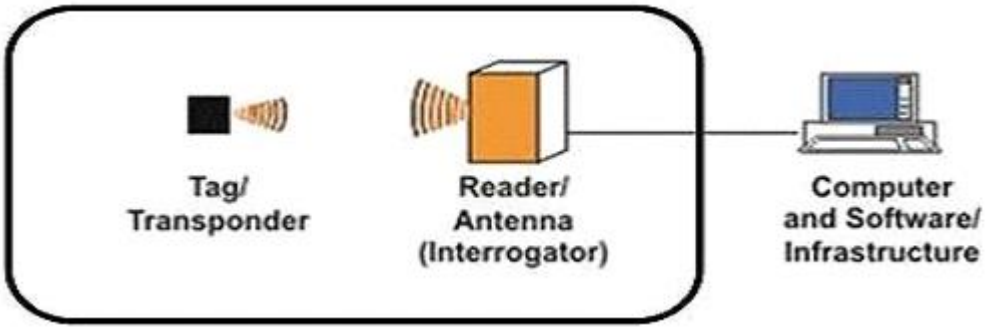


Figure I- 9: Les éléments d'un système RFID

Le lecteur agit généralement en maître par rapport au tag ; si le tag est dans la zone de lecture du lecteur, ce dernier l'active en lui envoyant une onde électromagnétique puis entame la communication et l'échange de données. Le lecteur est relié à un hôte d'application qui récupère l'information pour le logiciel d'application. Un lecteur RFID est donc chargé de l'interface avec le système global relatif à l'application et de la gestion de l'identification des tags qui se présentent à lui. Le tag est, quant à lui, constitué d'une antenne et d'une puce électronique miniature.

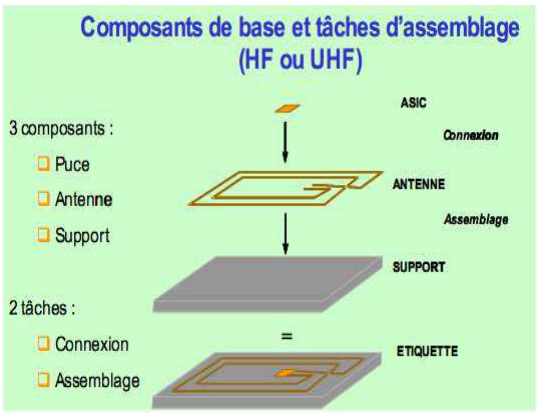
La liaison entre le lecteur et l'hôte de l'application peut être une liaison sans fil. Le lecteur interroge les étiquettes passives ou semi-actives en leurs envoyant la commande et l'énergie nécessaire pour interagir avec lui et dans le cas où le tag est actif c'est à dire possède sa propre batterie, il peut initier la communication **[7]**.

I.5.1. Composants

I.5.1.1. L'étiquette :

L'étiquette (tag) appelée aussi transpondeur, comprend une puce, dotée d'une mémoire et d'un microprocesseur, reliée à une antenne bobinée et lue par un lecteur captant et transmettant l'information.

Ces tags peuvent alors être incorporés dans des objets ou être collés sur des produits. Le format des données inscrites sur les étiquettes est standardisé à l'initiative d'EPC Global (*Electronic Product Code).*



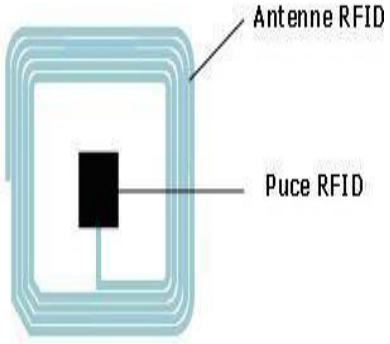


Figure I- 10: Étiquette RFID

Il existe trois types d'étiquettes (tag) (voir fig.I.11):

1- RFID passive : fonctionne en **lecture seule** puisque la puce ne possède pas de batterie et doit être déplacé vers le lecteur pour être lu. Un puissant signal électromagnétique lui est alors envoyé, ce qui permet d'activer la puce RFID et de lire les informations qu'elle contient. [8]

2- RFID active : fonctionne avec **une source d'énergie** telle qu'une petite pile ou une batterie, ce qui permet de **lire la carte à plus longue distance**. Cette technique est principalement utilisée pour la **traçabilité de personnes**, de véhicules ou encore pour la **traçabilité logistique**.

3- RFID semi-passive : est alimenté par une source d'énergie. Cependant, la batterie alimente la puce RFID à des intervalles de temps réguliers. Celle-ci n'envoie pas de signal. Cette technologie s'avère utile pour la **traçabilité alimentaire** notamment pour enregistrer les changements de température durant le transport.

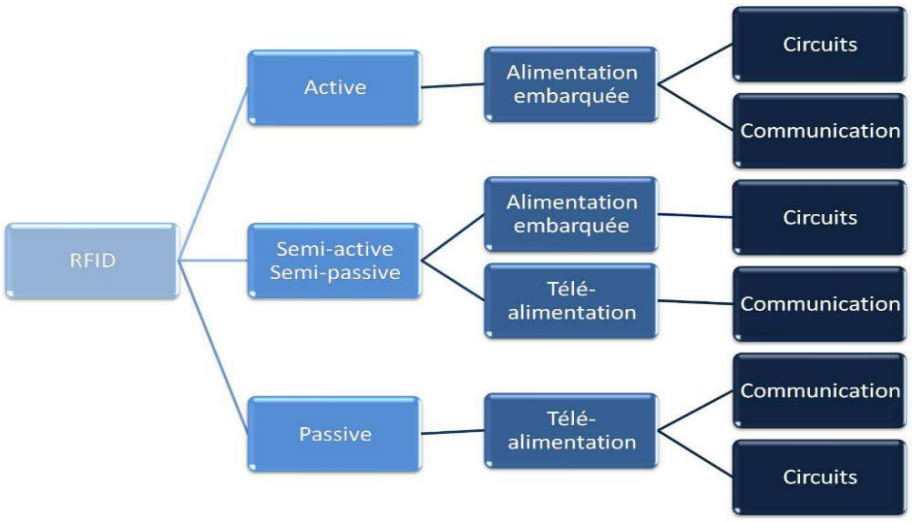


Figure I- 11: Types de tags

I.5.1.2. Lecteur

Le lecteur RFID est un émetteur-récepteur radio spécialisé. Il doit générer des signaux à la fréquence porteuse et moduler ces signaux pour transmettre des informations aux tags. Il doit recevoir et identifier sélectivement des réponses à partir des tags. Pour cela, il est doté de circuits de démodulation et de fonctions de traitement lui permettant d'adresser et de communiquer sélectivement et individuellement avec tout tag dans son champ de lecture.

Ainsi le lecteur RFID est l'élément responsable de la lecture des tags radiofréquence et de la transmission des informations qu'elles contiennent (code EPC, information d'état, clé cryptographique…) vers le niveau suivant du système (middleware).

Les conceptions de lecteurs couvrent un spectre étendu basé sur différents facteurs :

1. **Nombre d'antennes** : antennes multiples (typiquement 4 à 8) ou une simple antenne intégrée.
2. **Complexité de traitement :** le traitement inclut des processus intelligents, ou juste une intelligence RF.
3. **Fonctions d'accès à l'étiquette** : certaines exécutent toutes les opérations du air-protocol (read, write,look et kill étiquette), d'autres juste inventorient les étiquettes.
4. **Connectivité :** Ethernet, série, ou Wireless (non filaires).

Figure I- 12: Lecteur RFID Mifare RC522

I.5.1.3. Le middleware (ou intergiciel):

Un middleware, est un logiciel intermédiaire entre le réseau et le matériel d'une part, et les applications d'autre part. Cet intergiciel permet de collecter, de filtrer et d'agréger les données. Cela permet aussi une gestion plus facile des différents lecteurs. [9]

Un intergiciel pour étiquettes électroniques est un logiciel tiers destiné à simplifier l'accès et l'exploitation des informations stockées dans des étiquettes RFID.

Le but d'un intergiciel entre le réseau et les applications est d'accomplir les tâches techniques et les échanges de données. Dans les systèmes RFID, un intergiciel doit gérer les lecteurs, qui sont souvent hétérogènes, doit traiter les évènements issus des lecteurs RFID, et doit être connecté aux applications. Dans certains cas, il n'y a pas besoin d'intergiciel, comme dans le cas d'une petite et unique application telle que « compter le nombre d'identifiants lus », ou encore « lire les étiquettes dans le champ du lecteur ».

I.5.2. Composants matériels

Les puces et les lecteurs sont les composants matériels de base d'un système RFID. [10]

I.5.2.1. Puce RFID

La technologie des puces d'identification RFID est très étendue, elle permet de s'adapter à des multitudes de situations, l'identification, et d'embarquer d'autres informations sur letranspondeur (tag). Mais le besoin de chaque entreprise étant différent, il existe différents modes de fonctionnement des transpondeurs que l'on peut regrouper sous deux différentes catégories :

1. Les puces à usage unique (lecture seule) : la puce contient des données qui sont lues par le lecteur RFID sans possibilité de les modifier. C'est le mode de fonctionnement le plus simple du transpondeur et qui sert principalement pour les problèmes traitant seulement l'identification. Le transpondeur peut être lu uniquement par le lecteur, le transpondeur possède juste les informations qui ont été écrites par le fabriquant du tag. Ces informations peuvent être choisies par l'entreprise, mais une fois ces informations écrites, le transpondeur ne peut être que lu.

2. Les puces réinscriptibles (lecture/écriture) : les données inscrites sur la puce peuvent être modifiées par le lecteur RFID selon les deux modes suivants :

- **Lecture/écriture unique** : ce mode de fonctionnement est similaire à la lecture seule sauf que cette fois ci, le transpondeur livré par le fabriquant est vierge, il ne contient aucune information. C'est l'utilisateur du transpondeur qui va pouvoir écrire des informations dessus. Les informations ne peuvent être écrites qu'une seule fois, ensuite le transpondeur se comporte comme un transpondeur en lecture seule.

- **Lecture/écriture multiple** : dans ce mode de fonctionnement, le transpondeur peut être livré vierge ou avec des informations. Mais les informations peuvent être effacées et réécrites par l'utilisateur du transpondeur presque autant de fois qu'il le souhaite. Ce type de transpondeur est très utile lorsque l'on vient écrire des informations à différents moments d'un processus ou bien lorsque l'on souhaite réutiliser les transpondeurs avec de nouvelles informations.

Figure I- 13: Puce RFID

I.5.2.2. Antenne RFID

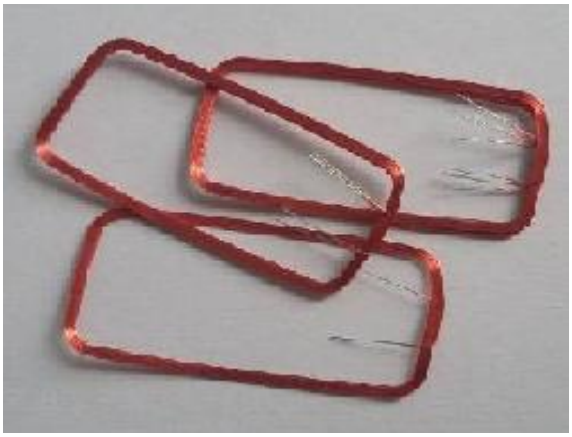


Figure I- 14: Antenne RFID

L'antenne RFID est un élément primordial du système RFID qui est généralement intégré au lecteur RFID et à l'étiquette RFID, elle permet de transmettre les informations et d'activer les tags afin de recevoir des données dans le cas des étiquettes passives et semi-passives.

Le choix du type de l'antenne à intégrer au lecteur RFID diffère selon le type de lecture, le type d'étiquette, l'utilisation du système RFID…etc. Ainsi, deux types principaux d'antennesse distinguent :

1. Les antennes intégrées : elles sont intégrées au lecteur, leur utilisation est conseillée pour les lecteurs de basse fréquence à portée limitée.

2. Les antennes externes : elles ne font pas partie du lecteur, elles sont plus puissantes et s'avèrent donc utiles pour obtenir une plus grande portée.

I.5.3. Classes RFID

Il existe différentes classes concernant la RFID : [11]

Tableau I - 1 : Tableau illustrant les différentes classes de la RFID

Classe	Tag	Fonction	Avantages / inconvénients
Classe0 **Classe1**	Passif	Lecture de l'identifiant unique	Moins onéreux que les tags actifs, utile pour un gros volume de marchandises pour être lues à courte distance. Cependant, la distance de lecture est aussi un frein car le lecteur doit se trouver à proximité.
Classe2	Passif	Fonctions additionnelles : lecture, écriture avec mémoire	
Classe3	Semi-passif	Tags assistés par une batterie	Plus performant et moins onéreux que la RFID active. En revanche, l'incertitude repose sur la fiabilité en cas de traçabilité.
Classe4	Actif	Communication sans transiter par un serveur central	Technologie autonome grâce à son énergie propre qui permet une lecture à longue distance. Les inconvénients sont : le coût des étiquettes et leur durée limitée, la faible sécurité des ondes émisses et son impact sur la santé.
Classe5	Interrogateur	Alimentent les tags de classe 0 à 3 et communiquent avec les tags de classe 4.	

I.5.4. Normes RFID

Pour une interopérabilité, les équipements RFID (lecteurs et tags) doivent impérativement être normalisés quant à leur mode de fonctionnement soit, pour une fréquence d'utilisation donnée,que n'importe quel tag soit lu par n'importe quel lecteur. On parle alors de protocole de communication. [9]

Le développement de standards est la responsabilité du comité technique de l'ISO.

L'ISO est l'union internationale des institutions nationales de standardisation, comme la DIN (Allemagne), l'ANSI (USA), l'AFNOR (France) ou la SNV (Suisse).

Les tags RFID fonctionnent selon des normes comme l'ISO 14443 (13.56 MHz) ou EPCglobal 96-bits (915 MHz).

I.5.5. Avantages et les inconvénients

Comme toute technologie, la RFID a des avantages comme elle a des inconvénients[12]

I.5.1.1. Avantages :

Par rapport aux techniques d'identification classiques, les technologies RFID apportent une souplesse et des gains de productivité considérables. Elles permettent un gain de temps ainsi qu'une optimisation des opérations de lecture et améliorent la fiabilité et les capacités du système de traçabilité.

- **Une sécurité d'accès au contenu**

Comme tout support numérique, l'étiquette radio fréquence peut être protégée par mot de passe en écriture ou en lecture. Les données peuvent être chiffrées. Dans une même étiquette,

Une partie de l'information peut être en accès libre, et l'autre protégée. Cette faculté fait de l'étiquette RF, un outil adapté à la lutte contre le vol et la contrefaçon

- **Lecture en masse d'étiquettes :**

La technologie permet de lire un grand nombre d'étiquettes simultanément. Une palette complète de cartons ou produits peut ainsi être lue automatiquement au passage dans un système de lecture RFID.

- **Evolutivité des informations :**

La fonctionnalité de lecture/écriture permet de faire évoluer les informations stockées dans l'étiquette et ainsi de suivre le cycle de vie d'un objet ou d'un produit. Elle permet également une réutilisation des étiquettes.

- **Une plus grande durée de vie**

Dans les applications où un même objet peut être utilisé plusieurs fois, comme l'identificationdes supports de manutention, une étiquette radio fréquence peut être réutilisée 1 000 000 de fois.

- **Une plus grande souplesse de positionnement**

Avec l'étiquette radio fréquence, il est possible de s'abstraire des contraintes liées à la lecture optique, elle n'a pas besoin d'être vue. Il lui suffit d'entrer dans le champ du lecteur pour que sa présence soit détectée.

- **Identification d'un produit de manière unique :**

La technologie RFID permet de disposer d'un numéro unique d'identification dans chaque puce RFID afin d'identifier chaque objet d'une manière unique.

I.5.5.2. Inconvénients :

Comme tout système, la RFID n'est pas sans contraintes. Nous allons présenter les principales :

- **Perturbation par l'environnement physique**

La lecture des étiquettes radio fréquence est perturbée par la présence, par exemple, de métaux dans leur environnement immédiat.

- **Perturbations induites par les étiquettes entre elles**

Dans de nombreuses applications, plusieurs étiquettes radio fréquence peuvent se présenter en même temps dans le champ du lecteur volontairement ou involontairement. Ceci peut être voulu en magasin, au moment du passage à la caisse ou entre les portiques antivols.

- **Sensibilité aux ondes électromagnétiques parasites**

Les systèmes de lecture RFID sont dans certaines circonstances sensibles aux ondes électromagnétiques parasites émises par des équipements informatiques (des écrans d'ordinateurs) ou des systèmes d'éclairage plus généralement par les équipements électriques.Leur emploi doit donc être testé en tenant compte de l'environnement.

- **Interrogations sur l'impact de la radio fréquence sur la santé**

Cette question fait débat depuis quelques années, en particulier concernant les portiques antivols et les téléphones portables. Les étiquettes passives ne présentent aucun risque quel quesoit leur nombre puisqu'elles ne sont actives que lorsqu'elles se trouvent dans le champ d'un lecteur. Les études portent donc essentiellement sur les lecteurs et visent à définir les critères de régulation de leur puissance d'émission afin d'éviter qu'ils ne créent des perturbations sur les équipements de santé tels que les pacemakers (stimulateur cardiaque), mais aussi sur l'organisme humain.

- **Sécurité et vie privée**

L'utilisation d'ondes électromagnétiques pour transmettre des données entre deux dispositifs rend cette technologie intrusive et vulnérable aux attaques basées sur l'utilisation de la radiofréquence.

I.5.6. Gammes de fréquences RFID

I.5.6.1. La RFID dans le spectre radio *:*

Le système RFID utilise le canal hertzien pour ses communications. L'utilisation de ressourcesradio est soumise à autorisation et suit des règlements nationaux ou internationaux, on les classes ainsi en quatre catégories : [13]

BF : pour des fréquences inferieures à 135 MHz

HF : pour des fréquences qui avoisinent les 135 MHz

UHF : pour des fréquences autour de 434 MHz, de 869-915 MHz, 2,5 GHz

SHF : pour des fréquences aux alentours de 2,5 GHz. Voici un aperçu des fréquences de la RFID dans le spectre radio :

Tableau I - 2Tableau illustrant les gammes de fréquence de la RFID dans le spectre radio

Fréquence	125 et 134,2 kHz LF	13,56 MHz HF	868 à 915 MHz UHF	2,45 et 5,8 GHz SHF
Portée typique max	0,5 m	1 m	3 à 6 m	1 m
Caractéristiques générales	-Relativement cher même par gros volumes - L'antenne nécessite un nombre de tours important - Faible dégradation des performances en milieu métallique ou liquide	-Moins cher que les tags LF - Bien adapté aux applications qui ne demande pas de lire beaucoup de tags à grande distance -Fréquence unique dans le monde	-En gros volume, les tags UHF sont moins chers que les tags HF et LF - Adapté à la lecture en volume à longue distance - Performances dégradées par rapport à la HF en milieu métallique ou aqueux	-Performances similaires à l'UHF - Très forte sensibilité aux métaux et liquides - Liaison lecteur/tag plus directive que pour les fréquences plus basses
Principales Normes	ISO 14223/1 ISO 18000-2	ISO 14443 ISO 15693 ISO 18000-3	ISO 18000-6	ISO 18000-4

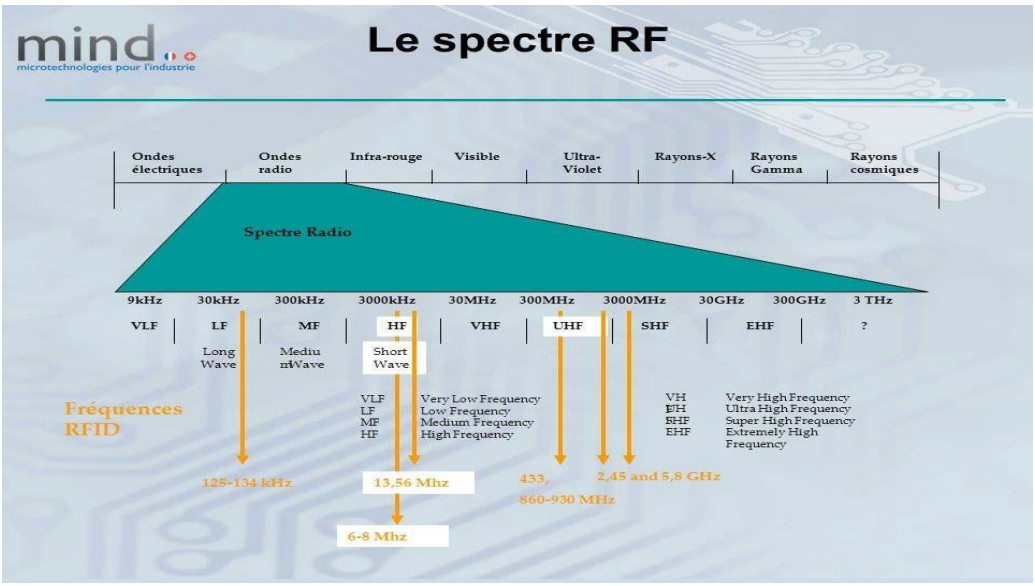


Figure I- 15: Les fréquences RFID dans le spectre radio

I.5.7. Marché de la RFID

Selon l'étude « RFID Forecasts, Playersand Opporunities 2014-2024 » d'ID TechEx, l'estimation du nombre de tags RFID passifs qui seront vendus sur le marché en 2020, toutes applications et marchés confondus sont présentés ci-dessous : [6]

- **LF** : 1308 millions (646.5 en 2013)
- **HF** : 5904 millions (2182 en 2013)
- **UHF** : 30000 millions (3079 en 2013)

I.5.8. Systèmes RFID dans la bande 13,56 MHz

La fréquence à 13,56 MHz a été choisie pour diminuer les coûts et s'adresse à des applications nécessitant de grandes quantités d'étiquettes.

Ces étiquettes RFID se présentent sous la forme de films fins qui peuvent être intégrés dans des étiquettes papier, des étiquettes textiles, des badges personnalisables ou du cartonnage. Elles peuvent être imprimées comme une étiquette papier standard et contenir des données électroniques.

La portée de lecture va de quelques centimètres à plusieurs dizaines de centimètres. Toutefois, le métal est une importante source d'interférences et de perte de performance.

Figure I- 16: Exemple d'étiquettes RFID 13.56 MHz.

Les applications à 13,56 MHz comprennent notamment l'identification du linge, des livres de bibliothèque, le contrôle d'accès ou les applications OEM

Les avancées technologiques apportées par l'utilisation de la fréquence 915 MHz et les nouvelles capacités de fabrications à 125 kHz ont toutefois freiné l'avancée de la technologie à 13,56 MHz, qui conserve cependant des applications spécifiques, en particulier dans le marché des fabricants d'équipement original.

I.5.9. Couplage inductif et couplage radiatif

Le principe de communication des systèmes RFID est divisé en deux grands groupes.Le premier se base sur le couplage inductif entre le lecteur et le tag. L'encombrement des antennes est alors beaucoup plus petit que la longueur d'onde. Le deuxième groupe se basesur le principe de couplage radiatif. La longueur de l'antenne du tag est comparable à la longueur d'onde. [6]

En LF et HF la communication s'établit majoritairement par couplage inductif (Figure VII.8.a**)**. Les tags, généralement en forme de boucle, ont une portée de quelques dizaines de centimètres. En effet presque toute l'énergie disponible est contenue dans la région située à proximité de l'antenne lecteur. Ces tags sont dédiés aux applications en champ proche tels que les badges pour le contrôle d'accès ou les passeports biométriques.

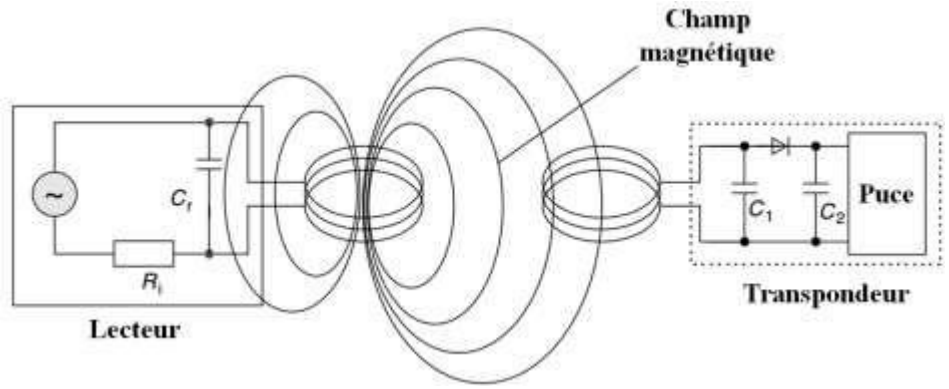


Figure I- 17: Principe du couplage inductif en RFID LF et HF

En UHF, les tags sont de formes dérivées du dipôle. Ils fonctionnent en champ lointain (Figure VII.8.b) et leurs portées peuvent aller jusqu'à quelques dizaines de mètres. Ils sont surtout utilisés pour la traçabilité des palettes et conteneurs dans les entrepôts.

Il est important de noter que l'utilisation de la RFID dépend directement des réglementations des autorités publiques de chaque pays. Ces réglementations, pour ce qui est la bande de fréquence 860MHz - 960MHz, bande de fréquence étudiée dans cette thèse, respectent le protocole EPC (Tableau 3).

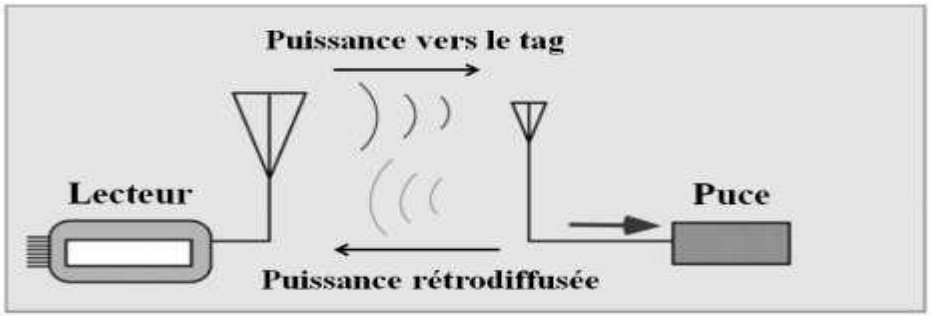


Figure I- 18: Principe du couplage radiatif en RFID UHF

Tableau I - 3 : Bandes de fréquence et puissance maximale autorisée pour différentes zones du monde

Région		Bande de Fréquence	Puissance rayonnée
Europe (ETSI)		$865-868MHz$	$100mW_{erp}$
		$865,5-868MHz$	$500mW_{erp}$
		$865,6-867,6MHz$	$2W_{erp}$
Amérique (FCC)		$902-928MHz$	$4W_{eirp}$
Asie Pacifique	Japon	$952-956,4MHz$	$4W_{eirp}$
	Chine	$840,5-844,5MHz$	$2W_{erp}$
		$920,5-924,5MHz$	$2W_{erp}$
	Australie	$918-926MHz$	$1W_{eirp}$
		$920-926MHz$	$4W_{eirp}$
	Nouvelle Zélande	$864-868MHz$	$4W_{eirp}$
		$921,5-928MHz$	$4W_{eirp}$

I.5.10. Domaines applicatifs

La qualité ainsi que l'authentification et la sécurité des objets achetés, des transactions financières mais aussi de leur transport physique est un enjeu de plusieurs milliards d'Euros pour l'industrie. La technologie RFID est à ce jour le moyen le plus utilisé pour résoudre cette partie de l'équation, que ce soit sous forme de contrôle d'accès (HF14443), de sécurisation bancaire (NFC), ou bien d'Authentification (HF15693, UHF Gen2). La technologie RFID permet d'associer une quantité d'information personnelle à chaque objet et ce de façon unique. Les origines et le cheminement ainsi que les preuves de qualité et d'authenticité peuvent désormais faire partie intégrante de la fiche signalétique des objets. On liste ci-dessous des domaines applicatifs dans lesquels la RFID a démontré tout son intérêt. [14]

a) Marquage d'objets : Système implanté d'identification et mémorisation pour maintenance et suivi : Identification de containers de substances chimiques, de médicament, de

mobilier urbain, jeux publics, d'arbres d'ornement. La traçabilité d'objets tels que des livres dans les librairies et les bibliothèques ou la localisation des bagages dans les aéroports utilisent plutôt la classe haute fréquence (13.56 MHz).

b) Contrôle d'accès : il se fait par badge de *« proximité »* ou *« mains-libres »*. Le contrôle d'accès à des bâtiments sensibles est un domaine où le système de radio-identification remplace les badges magnétiques, permettant l'authentification des personnes sans contact. La radiofréquence de la plupart des badges d'accès ne permet qu'une utilisationà quelques centimètres, mais ils ont l'avantage de permettre une lecture-écriture dans la puce, pour mémoriser des informations (biométriques, par exemple). Certaines « clés électronique » d'accès permettent la protection « sans serrures » de bâtiments ou portières automobiles. Les badges mains-libres, permettent une utilisation jusqu'à 150 cm (selon le type d'antenne utilisée). Ils peuvent contenir une Identité numérique ou un certificat électronique ou y réagir et permettent l'accès à un objet communicant ou son activation. Utilisé par exemple pour le contrôle d'accès à des systèmes de transports en commun (exemple Passe Navigo).

Figure I- 19 : RFID pour le contrôle d'accès

c) Inventaires : Saisie automatique d'une liste de produits achetés ou sortis du stock. Une analyse effectuée chez Wal-Mart a démontré que la radio-identification peut réduire les ruptures d'inventaire de 30 % pour les produits ayant un taux de rotation entre 0,1 et15 unités/jour.

Figure I- 20: RFID pour inventaire manuel

d) Logistique : La technologie RFID permet le contrôle des flux en temps réel entre les sites de la chaîne de valeur et d'approvisionnement, apportant une traçabilité au niveau des

objets, optimisant les processus de fabrication mais aussi de distribution et d'approvisionnement. Elle apporte également la traçabilité des services en donnant les preuves que la chaîne de distribution a respecté les conditions déterminées pour le stockage et le transport (chaîne du froid par exemple).

Figure I- 21: Principe d'une chaîne logistique complète contrôlé par RFID

e) Traçabilité distante d'objets (fixes ou mobiles) : Par exemple, des palettes et conteneurs peuvent être suivis dans des entrepôts ou sur les docks via des tags UHF. Des tags actifs micro-ondes (2.45 GHz) permettent le contrôle d'accès à longue distance de véhicules, comme par exemple sur de grandes zones industrielles. Dans la chaîne du froid, desaliments peuvent théoriquement être suivis par une puce enregistrant les variations de température.

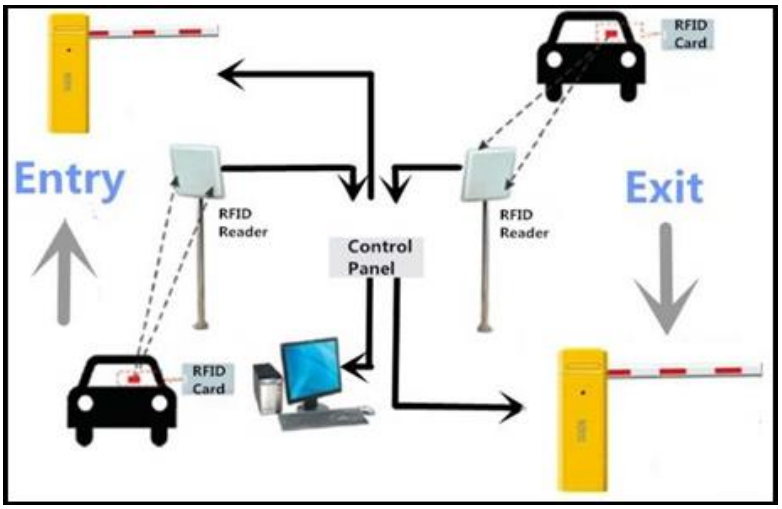


Figure I- 22: Principe d'objets dans le cadre de la réception d'un camion de la traçabilité

f) Marquage d'êtres vivants : Identification de plantes, d'animaux d'élevage (suivi d'un cheptel : nourriture, lactation, poids), d'animaux de compagnie ou sauvages grâce à une puce installée sous la peau dans le cou, d'animaux sauvages ; Ce sont généralement des puces basse fréquence (125 à 135 kHz).

Figure I- 23: Marquage RFID d'animaux

g) Transactions financières : Carte de crédit permettant le paiement sans contact ou titre de transport.

h) Relevés scientifiques : des tags sont aussi des moyens de communication pour la collecte des données issues des relevés scientifiques (monitoring) produits dans un organisme ou par des stations de mesure isolées et autonomes (stations météorologiques, volcaniques ou polaires).

i) Chez l'Homme : Combinés à des capteurs sensibles aux fonctions principales du corpshumain, ces systèmes sont aussi proposés comme solution intégrée de supervision de l'état de santé d'un patient. Implants corporels

j) Autres applications : Télépéages d'autoroutes (5.8 GHz), contrôle des forfaits de remontée mécanique, suivis industriels en chaîne de montage, antivols utilisés dans les magasins, épreuves populaires de course à pied, échange de cartes de visites lors d'évènements, …

I.5.11. SECURITE DE LA TECHNOLOGIE RFID

À ce jour et au niveau actuel de la technologie du système RFID, il ressort que les risques Sur le plan de la sécurité sont observables à trois niveaux, notamment : [15]

a) L'intégrité :

Sur le plan des équipements notamment les puces RFID utilisées pour l'identification et le stockage de données, il y a risque de piraterie ou contrefaçon par clonage. Et de plus en Plus, on parle de virus RFID. Ces virus sont capables de se reproduire et ainsi perturber les identifications des étiquettes ou le transfert des données dans le réseau.

b) La confidentialité :

II y a risque de fuites d'informations contenues dans les puces, c'est à dire. Les informations Peuvent être lues par un lecteur non autorisé dans le cas où de précautions ne sont pas prises, mais il faut noter que le cryptage assure une protection très efficace.

c) La disponibilité :

Les risques existant en ce qui concerne la disponibilité des informations contenues dans une puce est la non capture de l'information par le lecteur. Ces erreurs de lecture peuvent subvenir dans 3% des cas.

I.6. Conclusion

Dans ce chapitre nous avons présenté le système de contrôle d'accès à RFID, nous avons focalisé notre étude sur la technologie RFID ou l'identification par radiofréquence, cette technologie est de systèmes sans fil permettant une lecture d'information sans contact. Ce type de système fonctionne sur la base des informations et données qui sont collectées des étiquettes par de lecteurs spécifique. Nous avons également présenté, le principe de fonctionnement de la technologie RFID, ses avantages et inconvénients ainsi les différents domaines d'applications.

CHAPITRE II :

ETUDE D'UN SYSTEME DE CONTROLE D'ACCES RFID – MOT DE PASSE

II.1. Introduction

L'objectif de ce travail consiste à l'étude d'un système de contrôle d'accès à base de la technologie RFID et la saisie d'un code personnel d'identification (mot de passe), pour la reconnaissance des individus.

Afin de réaliser le système décrit précédemment, on doit utiliser un ensemble de composants matériels en interaction, chacun réalise une tâche précise :

- Unité de commande et de traitement : Arduino UNO.
- Unité de sortie et de communication : Afficheur I2C LCD 16 x 2.
- Unité d'entrée : un clavier électronique et le module RFID.
- En plus, d'autres composants auxiliaires.
- Fonctionnement du système
- Synoptique et algorithme de fonctionnement

II.2. Schéma synoptique du système

Le schéma synoptique illustré ci-dessous représente les principaux composants du système :

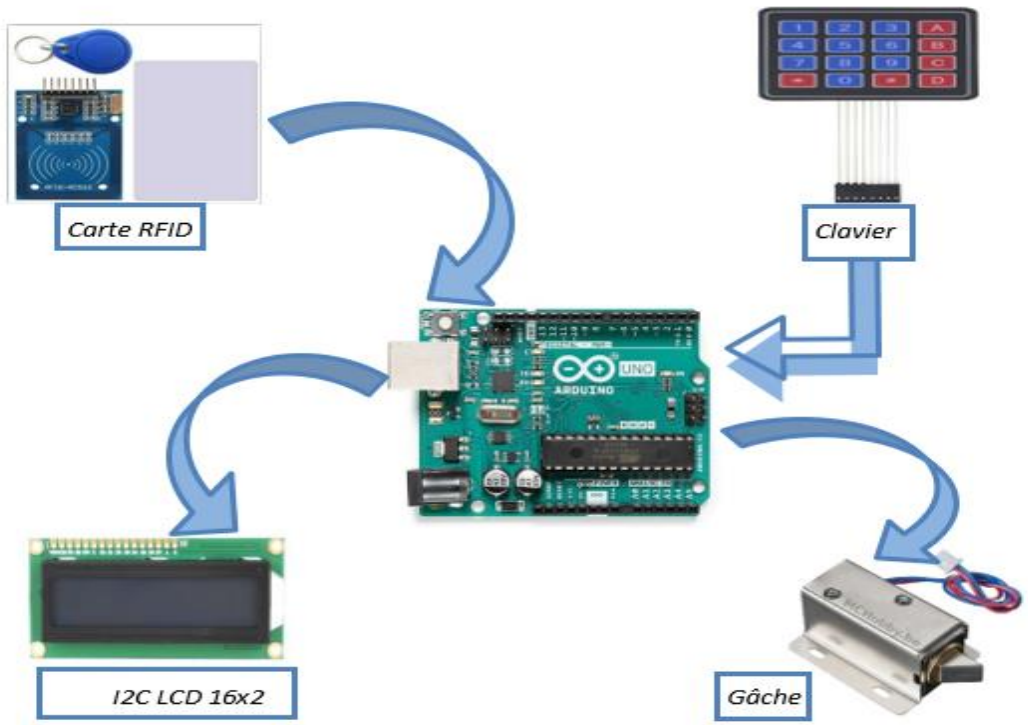
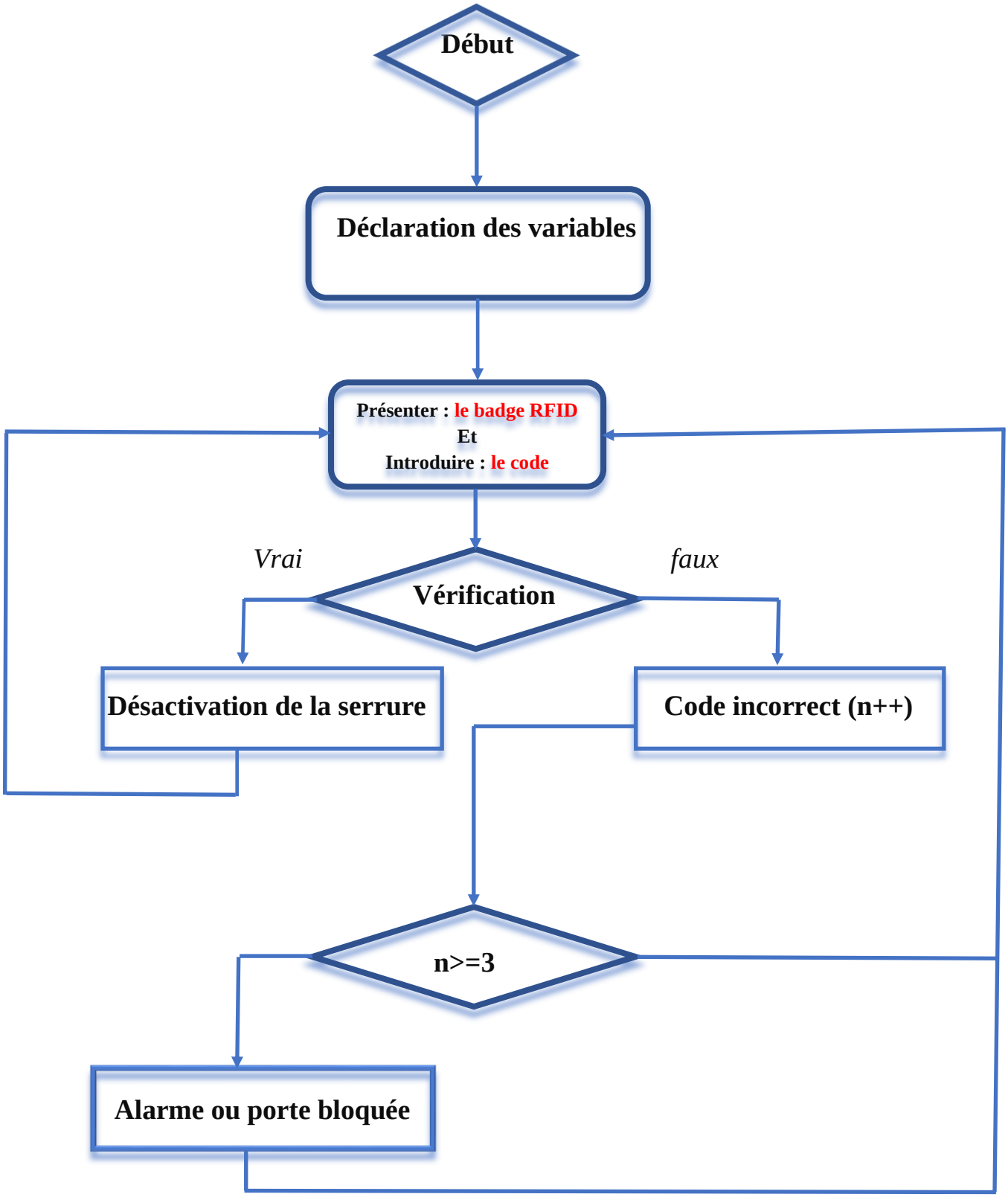


Figure II- 1: Schéma synoptique du système

II.3. Algorithme de fonctionnement



Lors de la demande d'accès, l'utilisateur doit présenter son badge, ayant un identifiant unique et introduire son code (mot de passe).

Le système doit alors remplir les fonctionnalités suivantes :

- Attente d'un évènement (présentation d'un badge)

- Extraction du contenu (Identifiant)
- Introduction du mot de passe
- Vérification des droits d'accès
- Enregistrement des informations d'identification en cas d'autorisation
- Enregistrement des tentatives d'accès.
- L'envoi de la réponse (autoriser ou refuser)

II.4. Fonctionnement du système de contrôle d'accès par badge commandé par Arduino

L'application consiste l'ouverture d'une porte en utilisant un badge. Le lecteur RFID couplé à la carte Arduino permet de détecter un badge enregistré ou non. Lorsque l'utilisateur est reconnu, le système déclenche l'ouverture de la porte ou une alarme dans le cas échéant. [28]

Ci-dessous les éléments constituant le projet ainsi leurs fonctionnements.

RFID-RC522 à fréquence 13.56 Mhz : sert à la lecture du badge
Carte Arduino : Elle est couplée avec le lecteur RFID. Elle permet de détecter la présence du badge, reconnaitre son identifiant (code du badge). Elle sert également à activer l'ouverture de la porte ou l'alarme

LED verte : Voyant indiquant l'ouverture de la porte. La LED s'allume, lorsqu'un badge reconnu est détecté. Elle reste éteinte dans le cas contraire

LED rouge : Voyant indiquant la détection d'un Faux badge (identifiant non reconnu du badge). La LED rouge s'allume et le buzzer émet un signal acoustique signifiant une alarme.

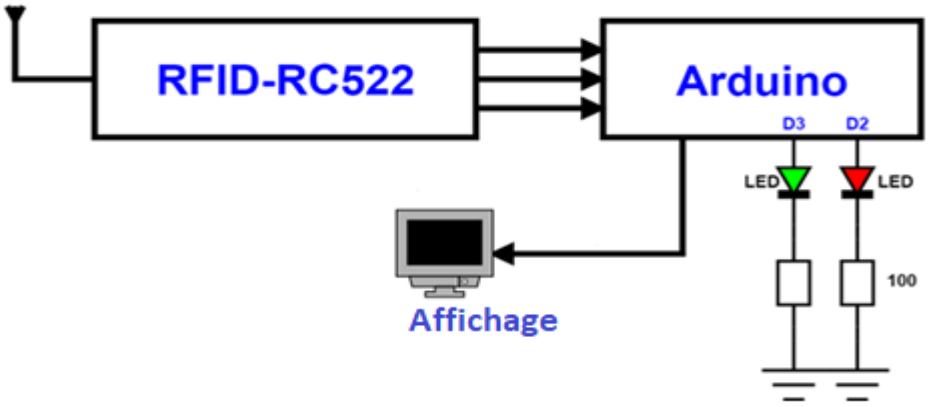


Figure II- 2: Schéma illustratif du système

II.5. Unité de commande et de traitement

II.5.1. La carte Arduino UNO

C'est une petite carte électronique (5,33 × 6,85 cm) équipée d'un microcontrôleur, ce dernier permet, à partir des d'événements détectés par des capteurs, de programmer et de commander des actionneurs ; la carte Arduino est donc une interface programmable. **[19]**

Le modèle UNO de la société ARDUINO est une carte électronique dont le cœur est un microcontrôleur ATMEL de référence ATMega328. Le microcontrôleur ATMega328 est un microcontrôleur 8bits de la famille AVR dont la programmation peut être réalisée en langage C [20].

Figure II- 3: La carte Arduino UNO

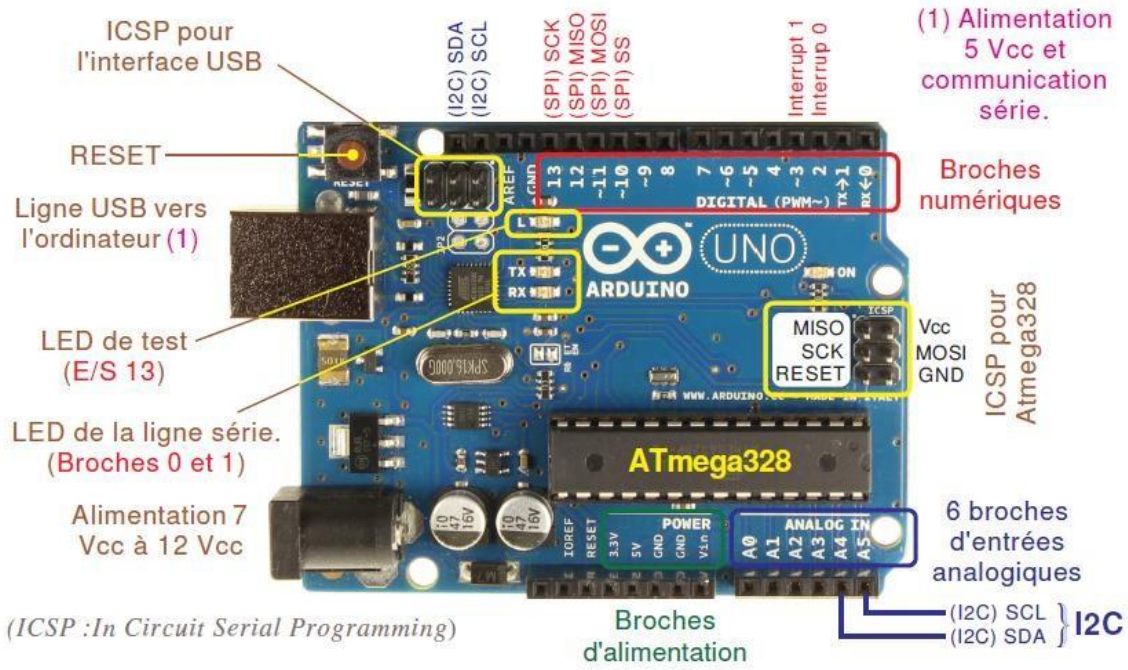


Figure II- 4: Les E/S d'une carte Arduino UNO

II.5.2. Caractéristiques techniques de la carte Arduino UNO

- Microcontrôleur : ATmega328.
- Fréquence horloge : 16 MHz.
- Tension d'alimentation interne : 5Vcc.
- Tension d'alimentation externe recommandée : 7-12Vcc. (Limites : 6-20 Vcc)
- Courant max sur la sortie 3,3V généré par le régulateur interne : 50mA.
- Entrées/sorties binaires : 14 broches.
- Courant MAX par broches en sortie : 40 mA. (85 mA en court-circuit)
- Courant MAX cumulé par les broches en sorties : 200 mA. (Soit 14 mA en moyenne)
- Les E/S binaires 0 et 1 sont mobilisées par le dialogue sur la ligne série.
- S0 pour RX et S1 pour TX. Chaque broche est reliée à une LED via R = 1kΩ.
- Les E/S binaires 3, 5, 6, 9, 10, et 11 sont dédiées au mode PWM.
- L'E/S 13 est reliée sur la carte à la LED de test via une résistance de 1kΩ.
- Entrées analogiques : 6, le niveau logique maximal doit être de +5Vcc.
- Mémoire Flash 32 KB dont 0.5 KB utilisée par le Boot loader.
- Mémoire SRAM 2 KB, Mémoire EEPROM 1 KB.
- La carte s'interface au PC par l'intermédiaire de sa prise USB.
- La carte s'alimente par le jack d'alimentation [21].

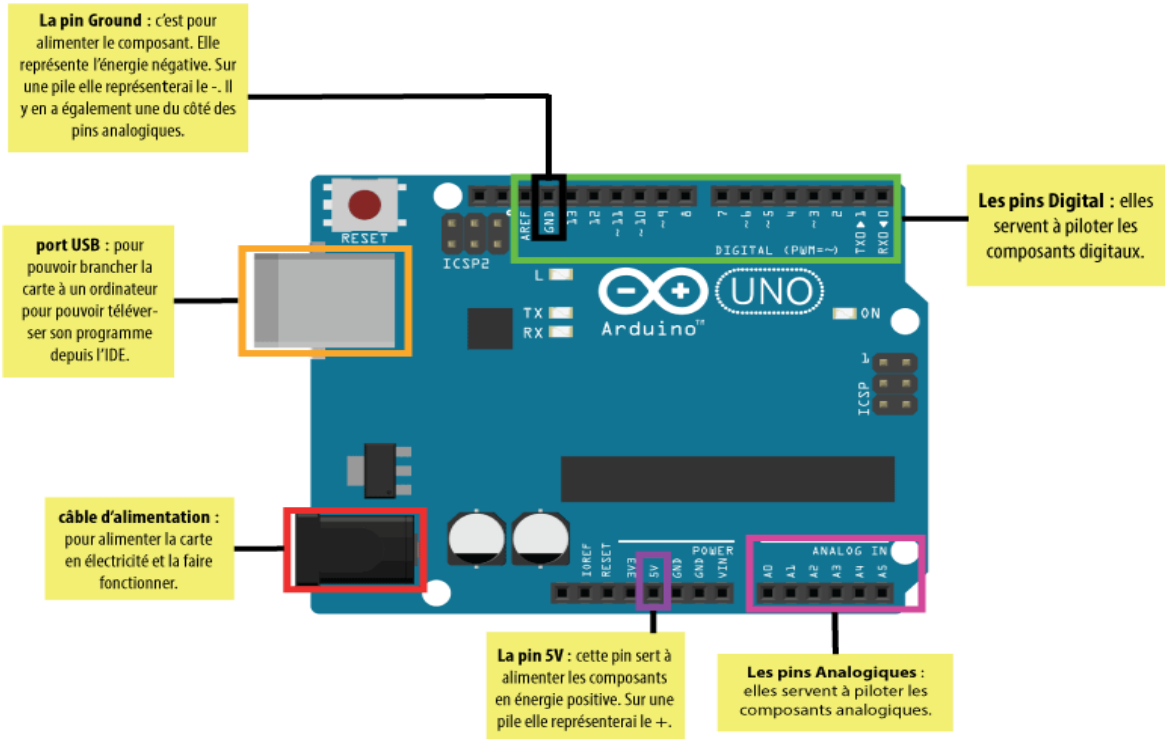


Figure II- 5 : Anatomie d'une carte Arduino UNO

II.5.3. Schéma simplifié de la carte Arduino UNO

Le microcontrôleur utilisé sur la carte Arduino UNO est un microcontrôleur ATMega328, ce dernier [22], est un circuit intégré qui rassemble sur une puce plusieurs éléments complexes dans un espace réduit dont la programmation peut être réalisée en langage C.

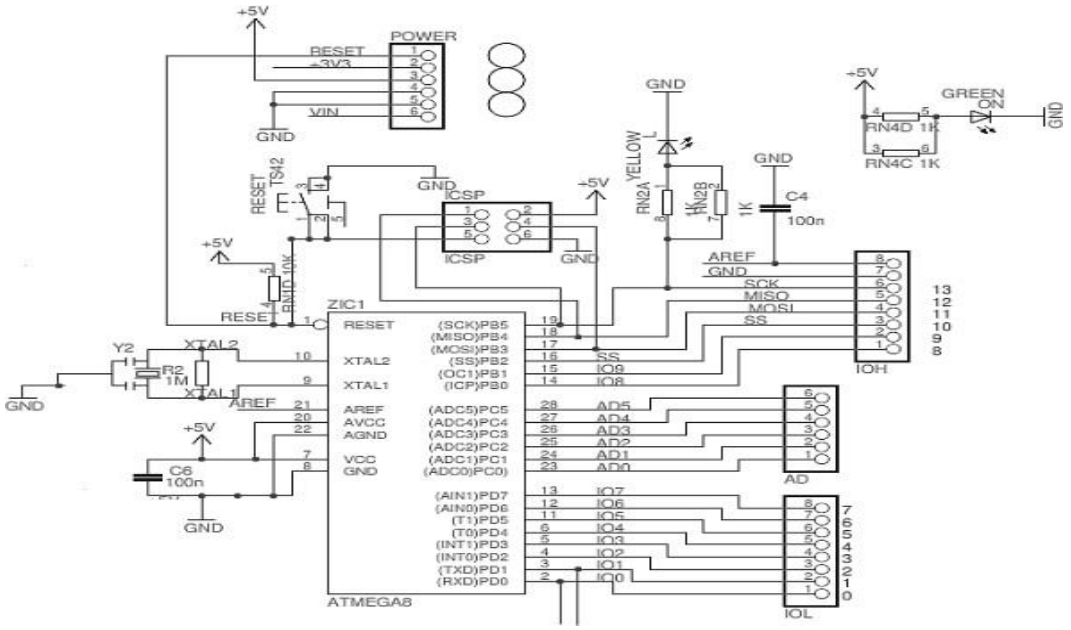


Figure II- 6: Schéma simplifié de la carte Arduino UNO

Le ATMEL ATMega328 est un microcontrôleur ATMEL de la famille AVR 8bit [22], il se caractérise par :

- **FLASH :** mémoire programme de 32Ko
- **SRAM :** données (volatiles) de 2Ko
- **EEPROM :** données (non volatiles) de 1Ko
- **Digital I/O (E/S Tout Ou Rien) :**3 ports PortB, PortC, PortD (soit 23 broches I/O).
- **Timers/Counters :** Timer0 et Timer2 (comptage 8 bits), Timer1 (comptage 16bits) Chaque timer peut être utilisé pour générer deux signaux PWM. (6 broches OCxA/OCxB).
- **Plusieurs broches multi-fonctions :** certaines broches peuvent avoir plusieurs fonctions différentes choisies par programmation.
- **PWM:**6 broches OC0A(PD6), OC0B(PD5), 0C1A(PB1), OC1B(PB3), OC2A(PB3), OC2B(PD3)
- **Analog to Digital Converter (résolution 10bits) :** 6 entrées multiplexées ADC0(PC0)à ADC5(PC5).
- **Gestion bus I2C (TWI Two Wire Interface) :** le bus est exploité via les broches

SDA(PC5) /SCL(PC4).

- **Port série (USART) :** émission/réception série via les broches TXD(PD1) /RXD(PD0)
- **Comparateur Analogique :** broches AIN0(PD6) et AIN1 (PD7) peut déclencher « interruption Watch dog Timer programmable ».
- Gestion d'interruptions (24 sources possibles (interrupt vectors)) : en résumé
    - Interruptions liées aux entrées INT0 (PD2) et INT1 (PD3)
    - Interruptions sur changement d'état des broches PCINT0 à PCINT23
    - Interruptions liées aux Timers 0, 1 et 2 (plusieurs causes configurables)
    - Interruption liée au comparateur analogique
    - Interruption de fin de conversion ADC
    - Interruptions du port série USART Interruption du bus TWI (I2C) [22].

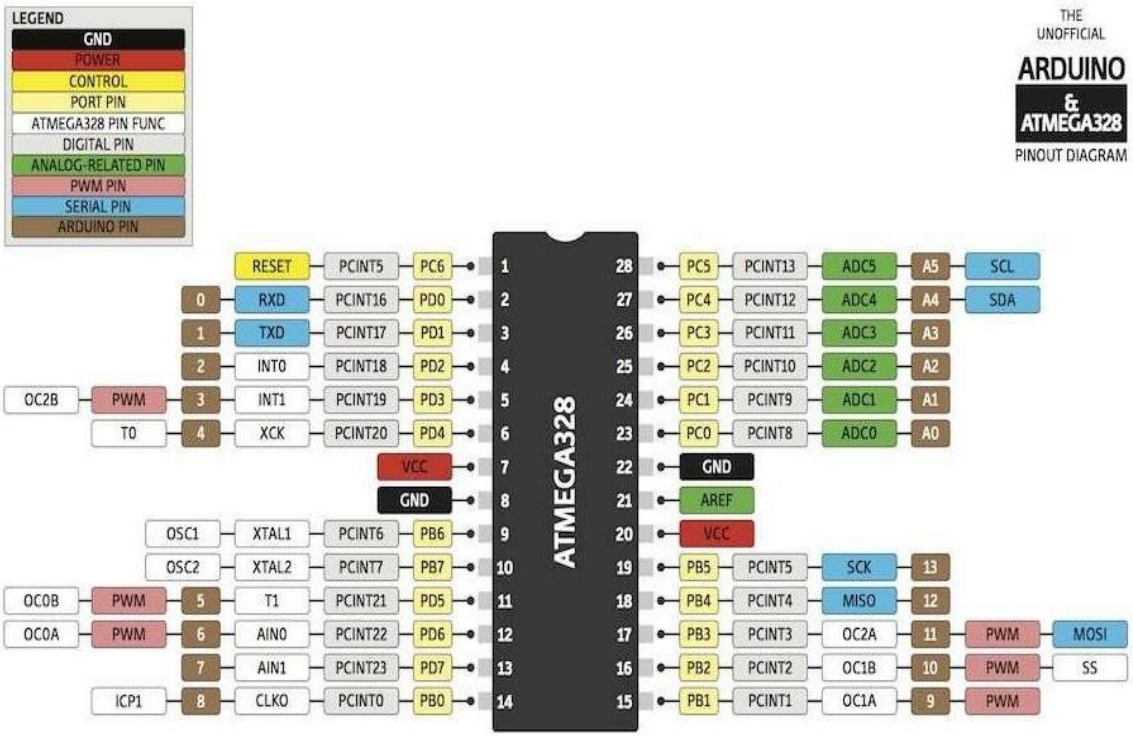


Figure II- 7: Brochage du Microcontrôleur ATMega328

II.5.4. Alimentation de la carte ARDUINO UNO

La carte Arduino UNO peut être alimentée via la connexion USB ou avec une alimentation externe, la source d'alimentation est automatiquement sélectionnée. Une alimentation externe peut provenir soit d'un adaptateur AC-DC ou d'une batterie. L'adaptateur peut être connecté en branchant une prise 2.1mm dans la prise d'alimentation de la carte ou à partir d'une batterie connectée dans le pin (ou broche) GND et Vin (alimentation externe) [18].

- Le processeur peut fonctionner sur une alimentation externe de 6 à 20 V. Cependant, si la tension est inférieure à 7V, le pin 5V peut fournir moins de 5 V et le processeur peut devenir instable.
- Si la tension est supérieure à 12V, le régulateur de tension peut surchauffer et endommager la carte, la plage recommandée est de 7 à 12 V [17].

II.5.5. Module RFID

a) Porte clé

Le porte clé RFID est un produit simple et pratique qui s'adapte à toutes les situations. La clé RFID assure un contrôle d'accès fiable et sécuritaire à l'entrée des immeubles, des parkings ou de portes sécurisées.

b) Badge RFID

Le badge RFID devient incontournable pour faciliter et sécuriser l'accès aux endroits à usage professionnel. Ces badges RFID sont munis d'une antenne et d'une puce aussi**,** pour permettre la transmission de données avec un lecteur. Il est réalisé à partir d'un PVC ultra blanc offrant une résistance parfaite lors de manipulations répétées. Le badge RFID est au format ISO : 84 x 56 x 0.76 mm.

II.5.6. Le module RFID RC522

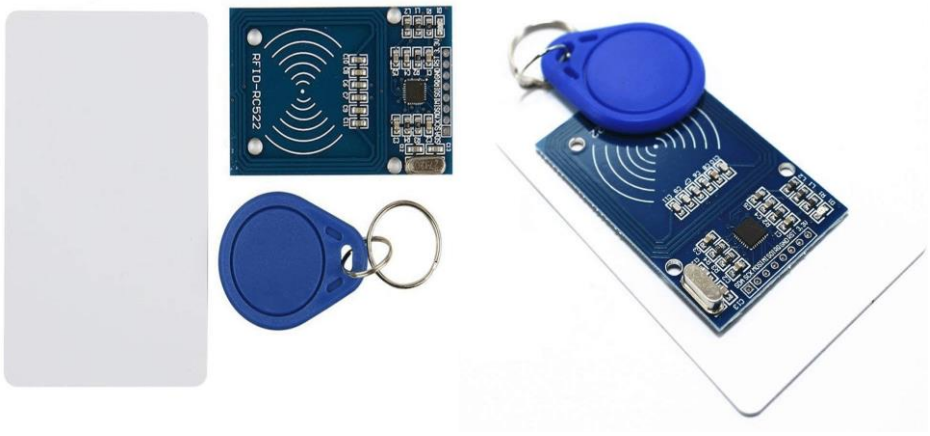


Figure II- 8 : Lecteur RFID aves ses accessoires

C'est une interface qui permet l'identification sans contact à partir d'un badge ou d'une clé RFID. Il est basé sur le circuit intégré Philips RC522. Il utilise la bande 13,56 MHz, la distance de communication peut aller jusqu'à 6cm.

Ci-dessous les caractéristiques du module :

Basé sur le circuit MFRC522

Fréquence de fonctionnement: 13,56 MHz

Tension d'alimentation: 3.3V

Courant: 13-26mA

Portée de lecture: Environ 3 cm avec la carte et le porte-clés fournis

Interface de communication : SPI

Taux de transfert de données maximum: 10 Mbit / s

Dimensions : 60mm × 39mm

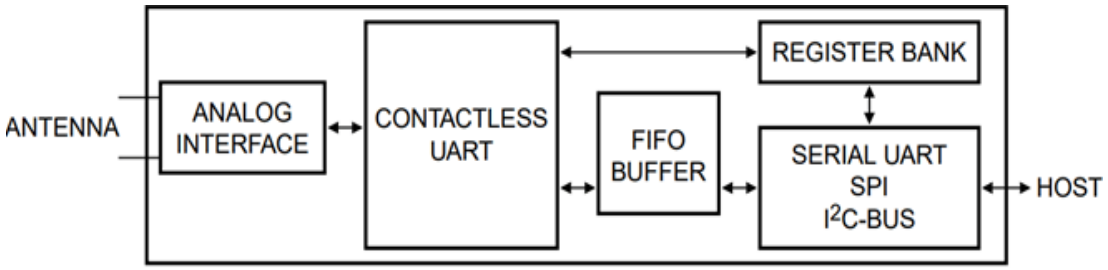


Figure II- 9: Schéma synoptique simplifié du MFRC522

II.6. Unité de sortie et de communication

II.6.1. Afficheur I2C LCD 16x2

Les afficheurs à cristaux liquides, autrement appelés afficheurs LCD (Liquid Crystal Display), sont des modules compacts intelligents et nécessitent peu de composants externes,

Pour un bon fonctionnement. Ils consomment relativement peu de courant (de 1 à 5 mA).

L'afficheur I2C LCD 16x2 utilisé est un écran permettant l'affichage de 16×2 caractères, c'est-à-dire deux lignes de 16 caractères. Ce type d'afficheur LCD est très répandu dans les projets Arduino, permettant de réduire les raccordements à quatre fils (SDA et SCL, masse et alimentation) entre Arduino et l'afficheur I2C. L'interface I2C en l'arrière utilise un empattement de 2.54mm, ce qui permet d'utiliser des connecteurs du pont pour effectuer les raccordements sur breadboard (ou directement sur un Arduino).

L'avantage d'un bus I2C, c'est qu'il permet de connecter plusieurs périphériques sur le même bus, pour autant que chaque périphérique dispose d'une adresse unique sur le bus.

Cet afficheur dispose de cavaliers permettant de configurer son adresse sur le bus entre 0x20 et 0x27. Un potentiomètre à l'arrière permet d'ajuster le contraste de l'afficheur [23].

Le potentiomètre du module I2C permet d'ajuster le contraste de l'écran. Le transfert des données sous forme de bits est pris en compte par la bibliothèque**''Liquid Crystal''**.

Figure II- 10: Afficheur LCD I2C

Tout projet qui nécessite tant de convivialité ou de contrôle pour l'utilisateur doit comporter un afficheur. En effet, celui-ci permet de manière très rapide de révéler n'importe quelle information qui pourrait être utile au programmeur ou à l'usager.

II.6.2. Principe de fonctionnement d'un écran LCD

L'afficheur LCD est constitué de deux polariseurs dont les directions de polarisation forment un angle de 90°, de chaque côté d'un sandwich formé de deux plaques de verre enserrant des cristaux liquides. À chacune des interfaces avec les cristaux liquides, une couche de polymère, généralement un polyamide, rainurée assure l'ancrage des molécules au repos **[24].**

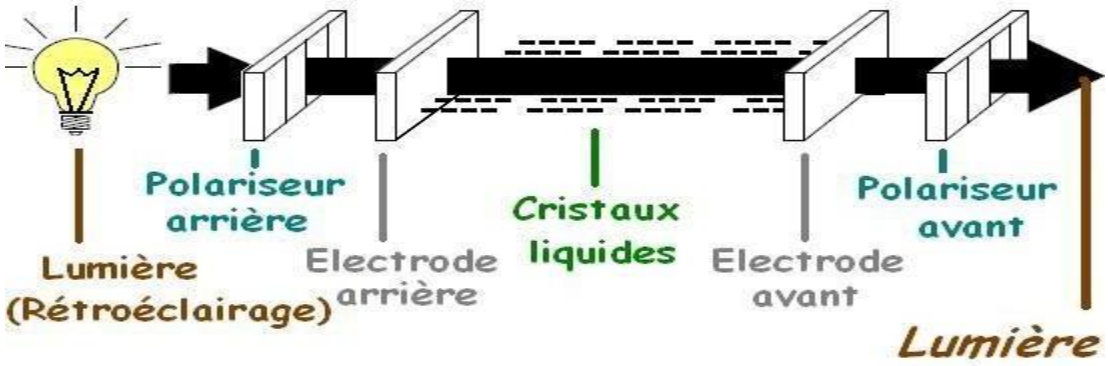


Figure II- 11: Principe de fonctionnement d'un écran LCD

II.7. Unité d'entrée

Les puces, les lecteurs RFID ainsi que la communication entre eux sont exposés à un grand nombre de risques qui impliquent les trois dimensions traditionnelles de la sécurité : disponibilité, intégrité et confidentialité. Ces risques sont par exemple le déni de service, le brouillage, le clonage, l'interception des données et la lecture non-autorisée (*skimming*).

Assurer la sécurité de l'identification par radiofréquence nécessite tout un ensemble de dispositions techniques. Pour prévenir et atténuer les risques. Un certain nombre de moyens techniques existent, et afin de remédier à cette défaillance l'intronisation du dispositif clavier

matricielle qui nous permet de protéger notre système par un mot de passe est plus qu'indispensable.

I1.7.1. Clavier matriciel

Le clavier matriciel ou à membrane est plus aisé et plus pratique à utiliser, il présente la communication Homme-Machine. Il comporte 16 touches dont 10 numériques (0-9), et 6 touches #*ABCD, il est matriciel car au lieu d'avoir 16 fils (1 par touche) et une masse, le multiplexage n'utilise que 8 sorties : 4 lignes et 4 colonnes.

C'est un élément fondamental dans les systèmes à microcontrôleur, afin d'affecter les performances des fonctions à exécuter, de saisir des données et de pouvoir interagir avec la machine [16].

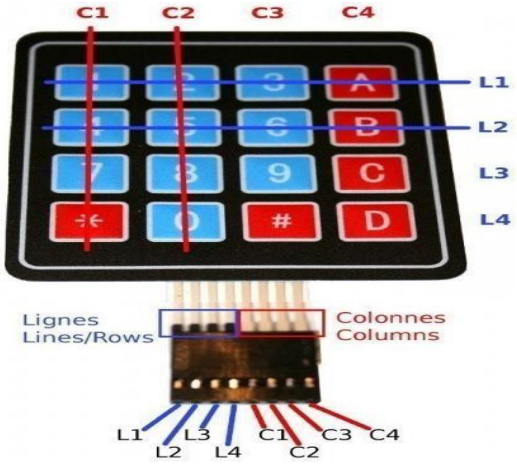


Figure II- 12: Clavier matriciel

Le code étant numérique, donc il nous suffit de choisir un clavier seize touches dont il y'a deux boutons spéciaux, un capable de changer facilement le mot de passe et l'autre efface l'écran en cas d'erreur de frappe [16].

- **Caractéristiques** :

-L'épaisseur très réduite lui permet d'être installé confortablement et avec n'importe quel appareil.
- le clavier peut se coller sur un support, il est étanche.
-Saisie de données numérique facile.
Ses principales utilisations : téléphonie, clavier de digicode, saisie de données numérique dans un programme Arduino (programme)…

II.8. Composants auxiliaires

II.8.1. Buzzer

Buzzer est un composant piézoélectrique qui transforme l'énergie électrique en onde acoustique variable en fonction de l'amplitude et la fréquence de la vibration, il est constitué d'un

diaphragme piézoélectrique, accepte une plage de tension : 3V à 20 V **[27].** Une échelle de décibels (dB) est utilisée pour décrire le niveau acoustique.

Figure II- 13: Buzzer

II.8.2. Cable USB

Ce câble USB permet à la fois l'alimentation de la carte Arduino et le chargement des programmes nécessaires au fonctionnement des cartes programmables à travers IDE-Arduino. La longueur du câble est d'environ 1 m.

Figure II- 14: Cable USB

II.8.3. Plaque d'essai

Une plaque d'essai (Fig.II.15) permet de réaliser des montages électroniques sans soudure. En règle générale les plaques d'essais sont de forme rectangle. Il y a plusieurs rangés de trous, certaines rangés sont verticales tandis que d'autres sont horizontales.

Plusieurs modèles existent, nous utiliserons des plaques d'essai comme celle représentée ci-dessous. La plaque d'essai comporte des connexions cachées, chaque bande de cuivre met en contact 5 trous. Les trous sont espacés exactement de 2,54 mm.

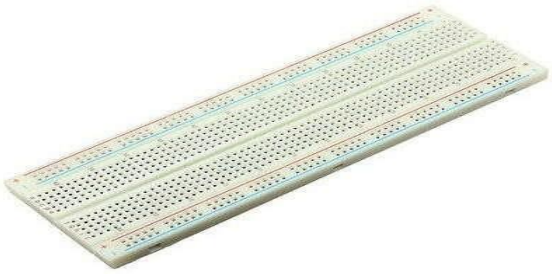


Figure II- 15: Plaque d'essai

II.8.4. Fils de connexions

Ils servent de connexions entre les différents composant et la plaque d'essai. Ils sont en cuivre isolés, de longueur et de couleurs variables.

Ils existent sous plusieurs types : male/male, femelle/femelle, ou male/ femelle

Figure II- 16: Fils de connexion

II.8.5. LEDs

Lorsqu'un tag RFID comportant un code admissible sera détecté, une LED verte va s'allumer. Lorsqu'un tag comportant un code inadmissible sera détecté, c'est plutôt une LED rouge qui s'allumera.

Figure II- 17: LEDs

II.8.6. Relais

Un relais est un organe électrique permettant de dissocier la partie puissance de la partie commande. Il sert à faire une transition entre un courant faible et un courant fort. Il est constitué d'une bobine ou solénoïde qui lorsqu'elle est sous-tension attire par un phénomène électromagnétique une armature ferromagnétique qui déplace des contacts **[25].**

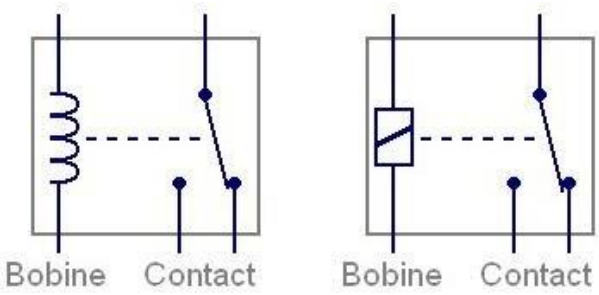


Figure II- 18: Symbole de relais

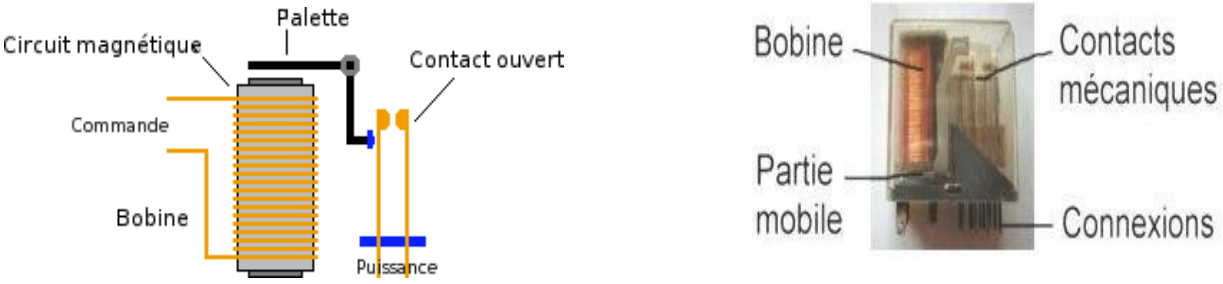


Figure II- 19: schéma interne du relais

II.8.6.1. Principe de fonctionnement d'un Relais

Le passage d'un courant de quelques dizaines de milliampères dans le circuit d'excitation (bobine) suffit pour commander un relais. Lorsque le relais est commandé, le contact initialement en position repos passe en position travail et reste dans cette position tant qu'un courant circule dans le circuit d'excitation. Lorsque le courant dans le circuit d'excitation disparaît, le contact revient en position repos **[26].**

Position normale position activée

Figure II- 20: Principe de fonctionnement d'un Relais

II.8.8. La gâche électrique 12 V DC

Les solénoïdes (fig.II.21) sont des actionneurs à entraînement électromagnétique. Lorsqu'une tension est appliquée à la bobine du solénoïde, la force électromagnétique tire le piston central vers l'intérieur.

Les solénoïdes se trouvent le plus souvent dans les mécanismes de verrouillage et de type déclencheur. Ce produit permet de commander l'ouverture par un clavier à code, un lecteur de badge, un bouton poussoir ou tout autre dispositif de commande fonctionnant en 12v.

Figure II- 21: Gâche électrique

II.8.8.1. Fonctionnement de la gâche connectée avec Arduino

Cette serrure, pré câblée (2 câbles avec embout JST) nous permet d'ajouter un contrôle électrique de fermeture pour nos projets Arduino, le câble rouge est à raccorder au positif, le vert au négatif.

Lors de la mise sous tension, le courant fera rétracter la serrure et lorsqu'il n'y a plus de courant (0V), la serrure ressortira.

II.8.8.2. Caractéristiques techniques d'une gâche électrique

Alimentation à prévoir: 12 Vcc

Consommation: 650 Ma

Impulsion: 1 à 10 secondes maxi

Sortie: 2 fils de 20 cm sur connecteur JST

Dimensions: 56 x 43 x 28 mm

II.9. Conclusion

Dans le présent chapitre nous avons présenté la partie théorique des différents modules constituant notre système de contrôle d'accès.

Dans la première partie du présent chapitre on a décrit le schéma synoptique, fonctionnement du système accompagné d'un schéma illustratif, et d'un l'algorithme de fonctionnement. La deuxième partie pour la présentation des caractéristiques techniques et le schéma simplifie de la carte Arduino.

La troisième partie de ce chapitre, présente l'unité d'entré avec les différents protocoles de communications entre l'unité de commande et les périphériques d'entrés/sortie et le clavier matriciel.

Dans la troisième partie nous avons présenté l'unité de sortie et de communication (Afficheur I2C LCD).

La quatrième partie présente les composants auxiliaires nécessaire au bon fonctionnement du montage.

CHAPITRE III :

REALISATION D'UN SYSTEME DE CONTROLE D'ACCES RFID – MOT DE PASSE

III.1. Introduction

Nous présenterons dans ce chapitre les différentes étapes de conception de notre projet et comment réaliser un système de contrôle d'accès sécurisé à base de la technologie RFID et par utilisation d'un clavier matriciel, géré par une carte Arduino. Parmi les applications de ce système, nous avons choisi la commande d'ouverture automatique en utilisant une gâche électrique.

Et pour les besoins de notre projet nous avons utilisé un afficheur LCD I2C 2x16 caractères rétro-éclairé pour afficher les messages du système et d'un dispositif MFRC522AN de RFID (13,56 MHz MiFare RC522AN avec communication SPI).

III.2. Outils de développement utilisés

Le choix des outils de développement détermine énormément le coût en temps de programmation, ainsi que la flexibilité du produit à réaliser. Dans un premier temps, nous allons procéder à la spécification de l'environnement matériel et logiciel utilisé dans notre projet.

Ensuite, nous nous intéresserons, à la description des différentes étapes de réalisation de notre système « Contrôle d'accès ».

Pour développer notre système, nous avons eu recours à divers éléments notamment les outils logiciels, les langages de programmation et les outils matériels qui nous ont permis la mise en œuvre de notre système.

III.3. Outils logiciels :

III.3.1. Logiciel de programmation IDE Arduino:

Figure III - 1: Logo Arduino

L'environnement de programmation Arduino (IDE en anglais) est une application écrite en Java. L'IDE permet d'écrire, de modifier un programme et de le convertir en une série d'instructions compréhensibles pour la carte. Le logiciel va nous permettre de programmer la carte Arduino, il nous offre une multitude de fonctionnalités**.**

La structure des programmes Arduino est un peu particulière, en apparence, des structures habituelles du langage C. La syntaxe est la même qu'en langage C.

Au début du programme, la déclaration des librairies utilisée par le programme à compiler.

- Nouveau : pour créer un nouveau programme (sketch).

- **Ouvrir** : ouvrir un programme existant. Le menu n'est pas déroulant à cause d'un bug...pour obtenir un menu déroulant passer par file/open

- **Enregistrer** : sauvegarder le programme, et pour sauvegarder sous un autre nom, passer par file/Save as.

- **Moniteur série :** pour ouvrir la fenêtre qui permet de visualiser les données transmises par le port série de l'Arduino.

- Le programme est lu par le microcontrôleur de haut vers le bas.

- Une variable doit être déclarée avant d'être utilisée par une fonction.

La structure minimale est constituée :

- En tête : déclaration des variables, des constantes, indication de l'utilisation de bibliothèques etc...

- **un setup (ou initialisation)** : cette partie n'est lue qu'une seule fois, elle comprend les fonctions qui doivent être réalisées au démarrage (utilisation des broches en entrées ou en sortie)

- **Une boucle (loop)** : cette partie est lue en boucle, c'est ici que les fonctions sont réalisées [30].

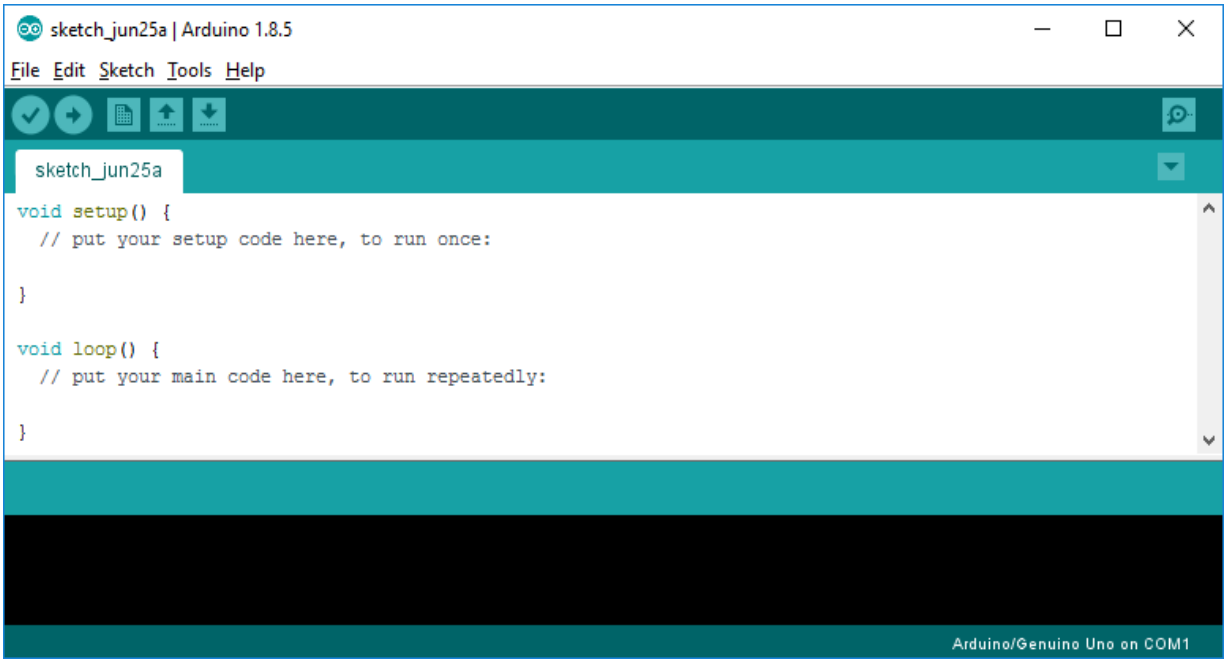


Figure III - 2: Interface de l'environnement de développement Arduino

III.3.2. Fritzing

Fritzing est un logiciel d'édition de circuit imprimé. Il a notamment pour vocation de favoriser l'échange de circuits électroniques libres et d'accompagner l'apprentissage de la conception de circuit.

Il est adapté aux débutants ou confirmés en électronique pour faire rapidement des circuits simples, et est également un bon outil didactique pour apprendre à bidouiller en électronique par la pratique

Le logiciel comporte trois vues principales :

- ✓ La « Platine d'essai », où l'on voit les composants tels qu'ils sont dans la réalité et où l'on construit le montage.
- ✓ La « Vue schématique », représentant le schéma fonctionnel du circuit.
- ✓ Le « Circuit imprimé », représentant la vue du circuit imprimé tel qu'il sera généré en PDF pour être imprimé **[29]**.

Figure III - 3: Logo fritzing

III.3.3. Langage utilisé

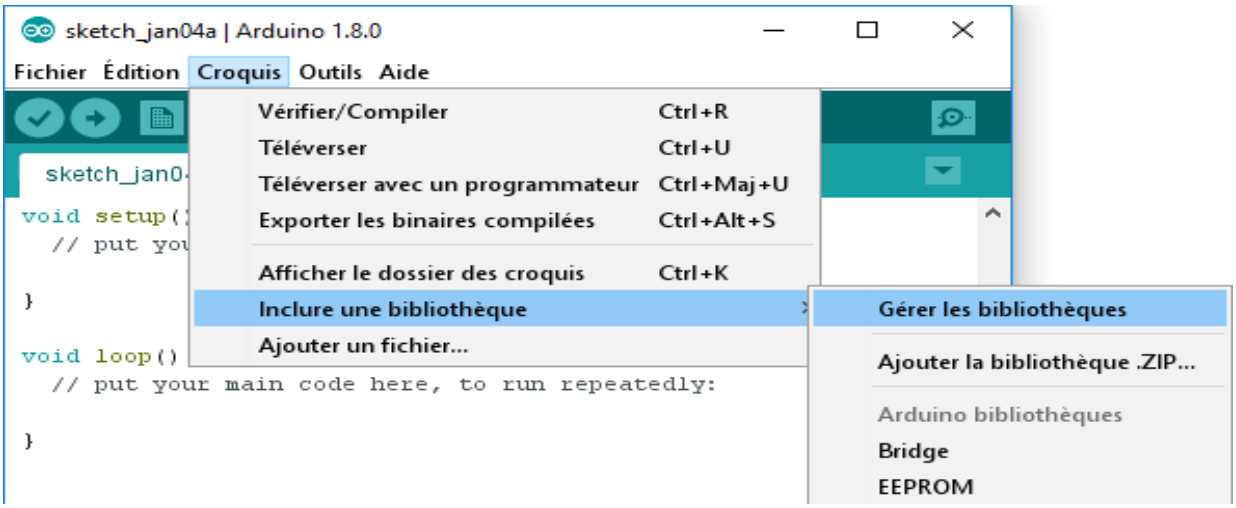
III.3.3.1. Langage C

Est un langage de programmation impératif généraliste, de moyen niveau. Inventé au début des années 1970 pour réécrire Unix. C, est devenu un des langages les plus utilisés, encore de nos jours. De nombreux langages plus modernes comme C++, Java et PHP ou JavaScript ont repris une syntaxe similaire au C et reprennent en partie sa logique. C offre au développeur une marge de contrôle importante sur la machine (notamment sur la gestion de la mémoire) et est de ce fait utilisé pour réaliser les « fondations » (compilateurs, interpréteurs…) de ces langages plus modernes.

III.4. Installation des bibliothèques

III.4.1. Bibliothèque MFRC522

- Ouvrir l'IDE Arduino
- Aller dans Croquis
- Inclure une bibliothèque
- Gérer les bibliothèques

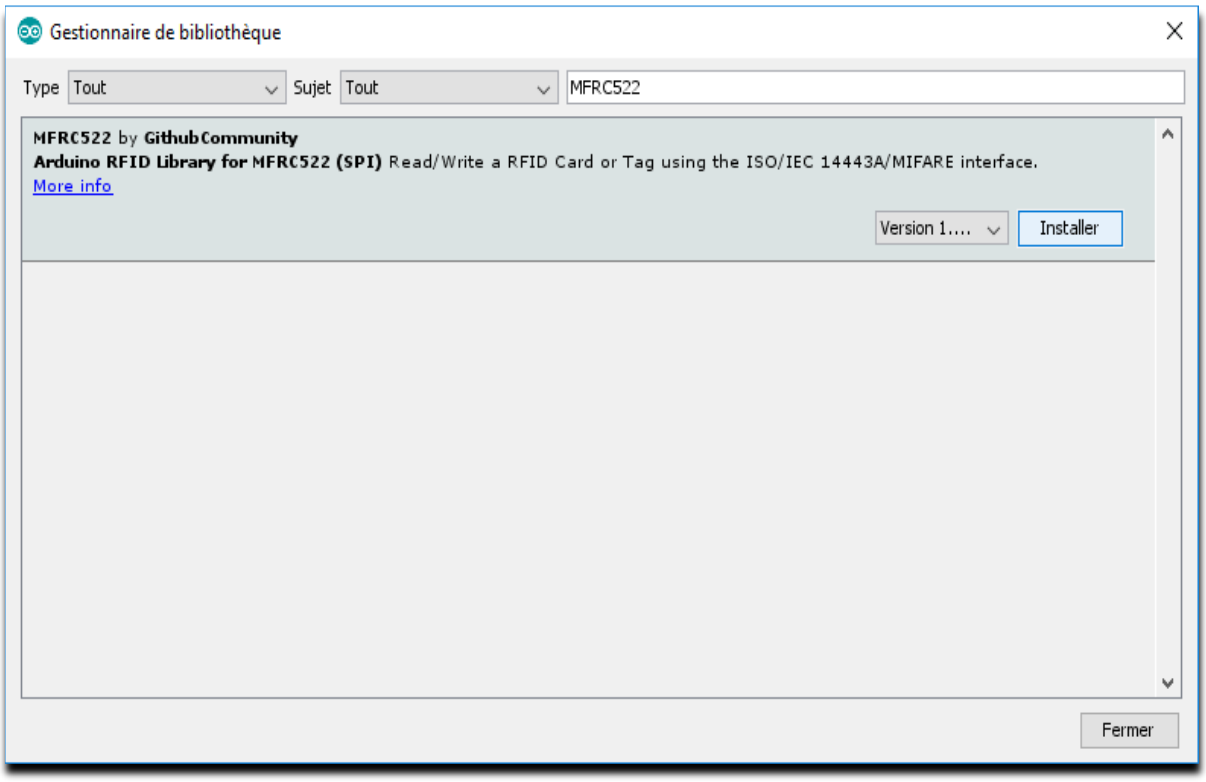


Dans le gestionnaire de bibliothèques :

- Rechercher « MFRC522 »

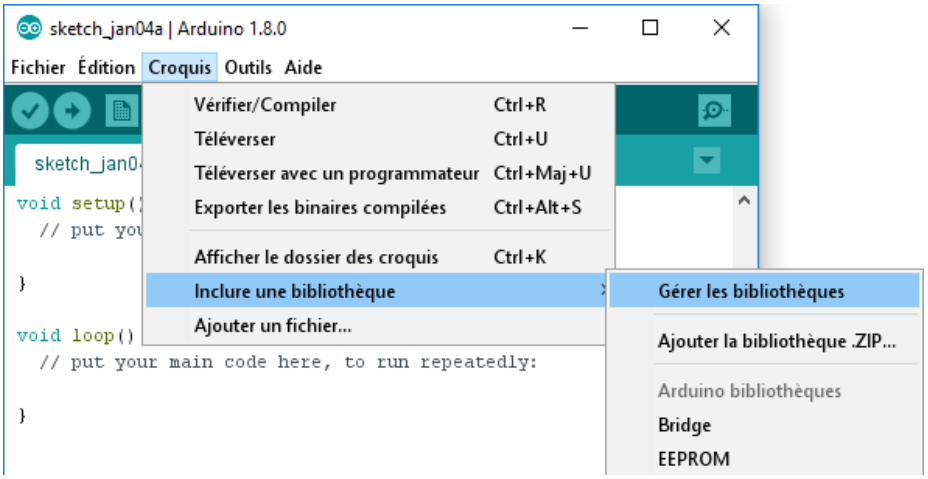
-Installer MFRC522 :

- Fermer la fenêtre une fois l'installation terminée.

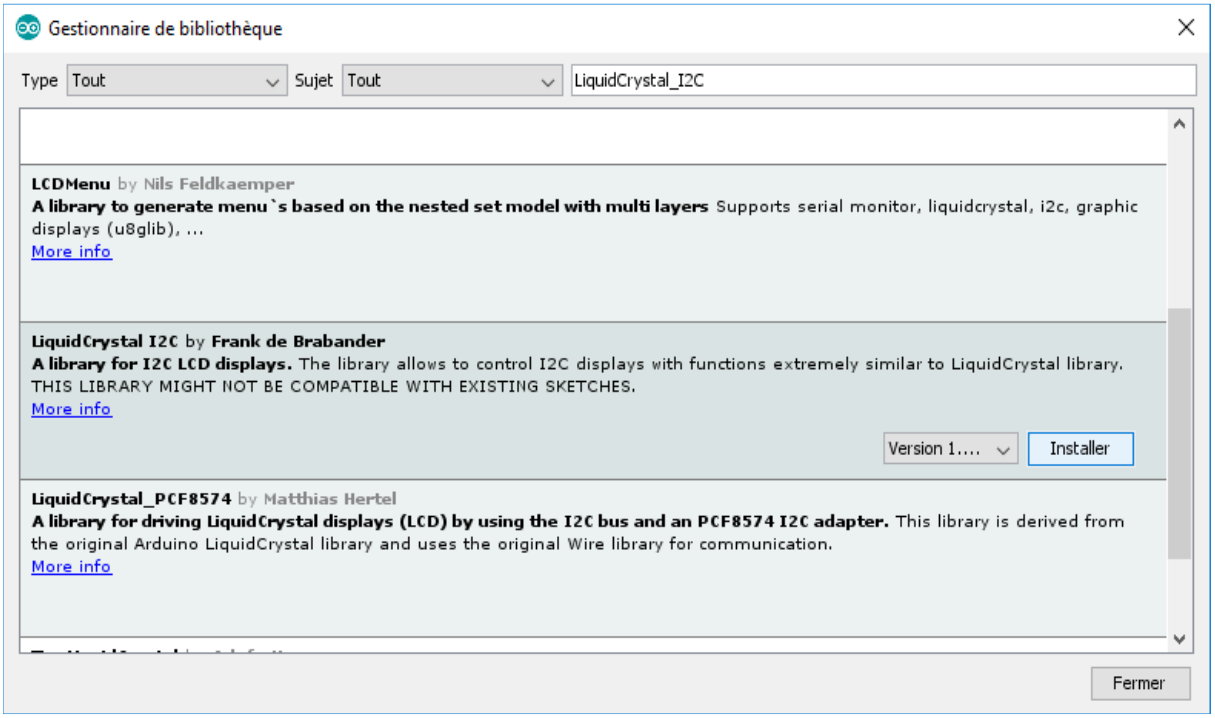


II.4.2. Bibliothèque de l'afficheur LCD I2C

Pour pouvoir utiliser l'afficheur LCD, la bibliothèque *LiquidCrystal_I2C* doit être installée : Ouvrir l'IDE Arduino et aller dans *Croquis* ⟶ *Inclure une bibliothèque* ⟶ Gérer les bibliothèques



Dans le gestionnaire de bibliothèques, rechercher « LiquidCrystal_I2C » et installer LiquidCrystal I2C :



Fermer la fenêtre une fois l'installation terminée.

III.4.3. Bibliothèque du clavier matriciel

Installation de la librairie Keypad.h via le lien : http://arduino.cc/fr/Main/LibrairieKeypad
Ce programme crée un objet de type Keypad, puis lit les entrées clavier et affiche sur le serial monitor les entrées saisies.

On peut faire avec cette librairie :

- **Lire la touche appuyée** : char getKey ()
- **Surveiller l'état du clavier** : KeypadState, getState ()
- **Définir un délai d'appui pour valider la saisie** : SetHoldTime (unsignedint time)
- **Paramétrer une pause anti-rebond** : setDebouceTime (unsignedint time)
- **Créer un évènement si le clavier est utilisé** : addEventListener (KeypadEvent)

III.5. Raccordement des différents dispositifs à la carte Arduino

III.5.1. Raccordement relais

Le relais est utulisé pour controler des equipements de grande puissance avec des commandes de faible puissance (exemple arduino).

Le branchement du relais aux broches de l'Arduino est représenté selon la correspondance ci-dessous :

- **VCC** → +5V d'Arduino
- **GND** → GND Arduino
- **IN** → Pin 13 Arduino (servira à commander le relais)

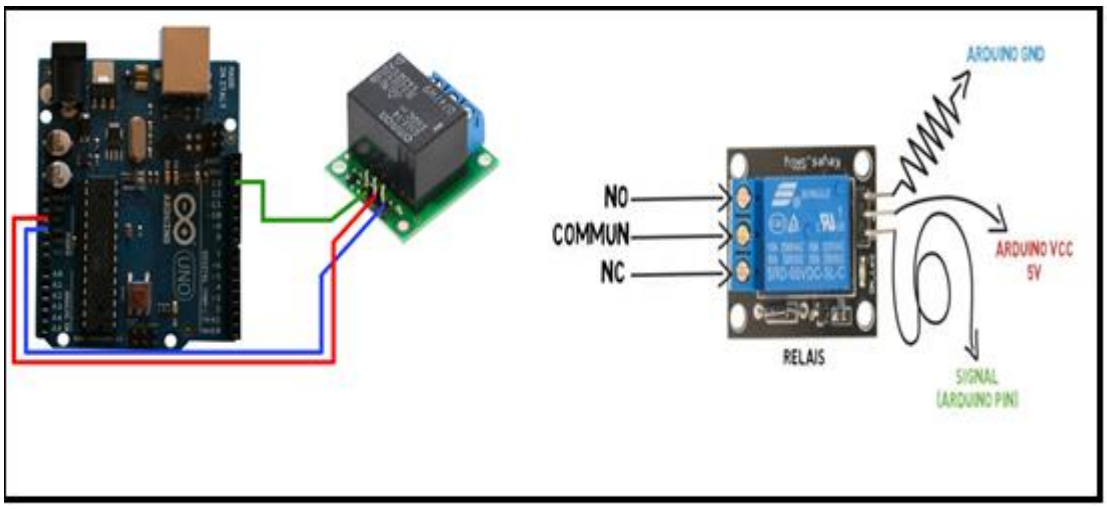


Figure III - 4: Raccordement du relais

III.5.2. Raccordement du solénoïde

Les 03 broches du module relais en liaisons avec le solénoïde et la batterie sont : **NC** (normaly close), **NO** (normaly open) et la broche **COM** (commun).

La borne **(-)** de la batterie 12V est branché directement sur le solénoïde, le **(+)** est branché sur le COM du relais, l'autre borne du solénoïde est branchée sur la borne NO du relais. Dès que la bobine du relais excitée par la commande **IN** de l'Arduino, le solénoïde commence à fonctionner.

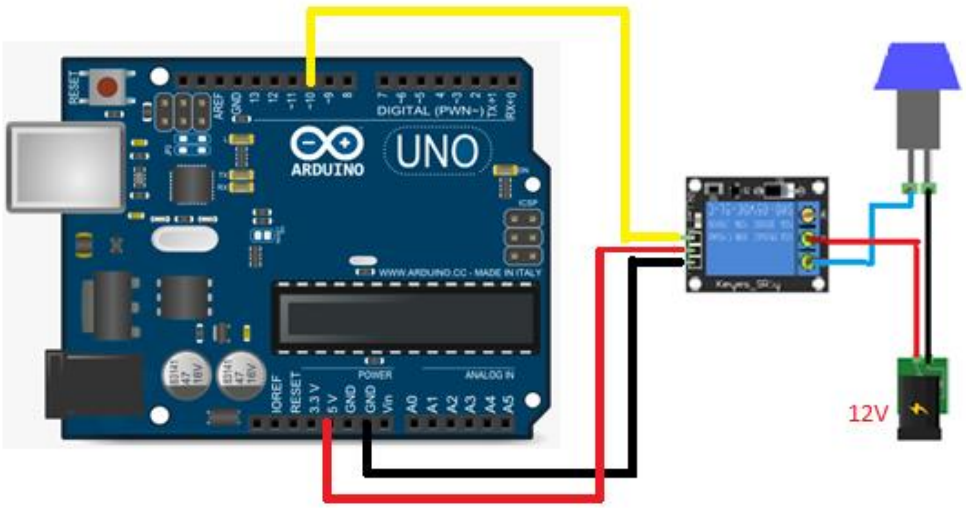


Figure III - 5: Raccordement du solénoïde

III.5.3. Raccordement du clavier matriciel à membrane

Utilisation d'un clavier matriciel à membrane avec Arduino

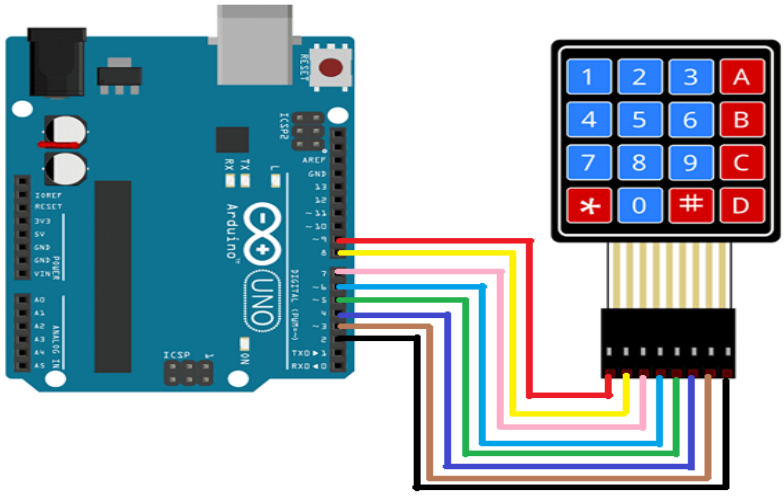


Figure III - 6: Raccordement du clavier matriciel à membrane

III.5.3.1. Composants utilisés :

- ✓ Clavier à membrane à 16 touches
- ✓ Carte Arduino Uno
- ✓ Nappe de fils de câblage male/male Dupont

III.5.3.2. Principe de fonctionnement

Le clavier comporte 16 touches, dont 10 numériques (0-9) et 6 touches marquées #*ABCD.

Il est matriciel : au lieu d'avoir 16 fils (1 par touche) et une masse, le multiplexage n'utilise que 8 sorties : 4 lignes et 4 colonnes.

III.5.3.3. Câblage

Il y a 8 fils en sortie du clavier, 4 lignes et 4 colonnes
Vu de face, de gauche à droite :
Pin 1-4 les 4 lignes, pin 5-8 les 4 colonnes.
On le branche sur les 8 entrées digitales successives de la carte Arduino Uno de D9 à D2.

Pin 1 ⟶ D9

Pin 2 ⟶ D8

Pin3 ⟶ D7

Pin4 ⟶ D6

Pin 5 ⟶ D5

Pin 6 ⟶ D4

Pin 7 ⟶ D3

Pin 8 ⟶ D2

III.5.4.Raccordement de l'afficheur I2C LCD 16x2

Vcc pour le **+5V**

GND à la **masse**

SCL sur **l'entrée analogique A5** de la carte Arduino

SDA sur **l'entrée analogique A4** de la carte Arduino

Remarque **:**

Si le câblage est bon, nous devons avoir le rétroéclairage allumé et l'écran qui n'affiche rien, nous devons varier sur potentiomètre intégré au connecteur série I2C à l'aide d'un tournevis, pour trouver la position où les pixels de l'écran apparaissent.

Si le contraste n'est pas bien réglé nous ne verrons pas le texte affiché.

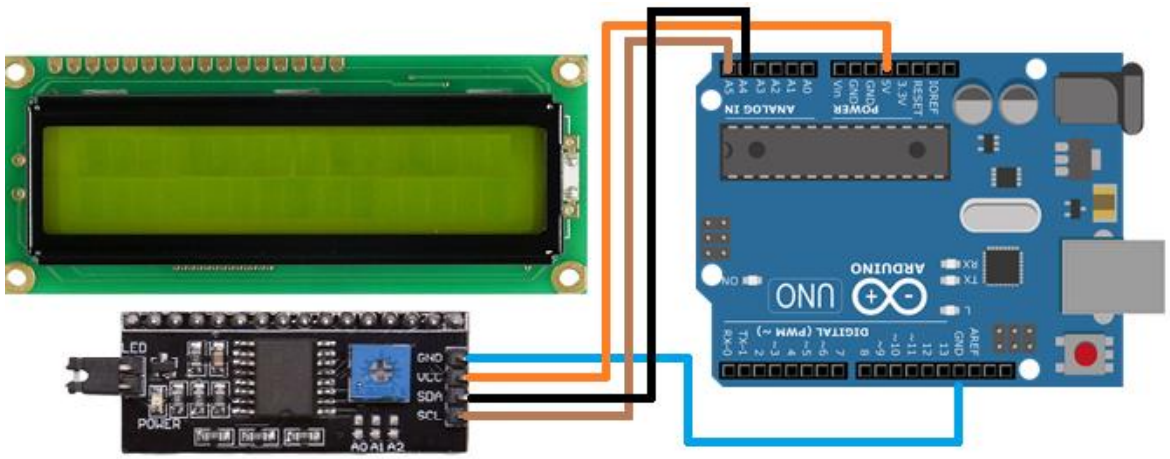


Figure III - 7: Raccordement de l'afficheur I2C LCD16x2

III.5.5. Raccordement du buzzer

Dans notre cas on a utilisé un buzzer actif car ce dernier fonctionne avec une tension continue. Le câblage du buzzer est directement sur une sortie digitale de la carte Arduino.

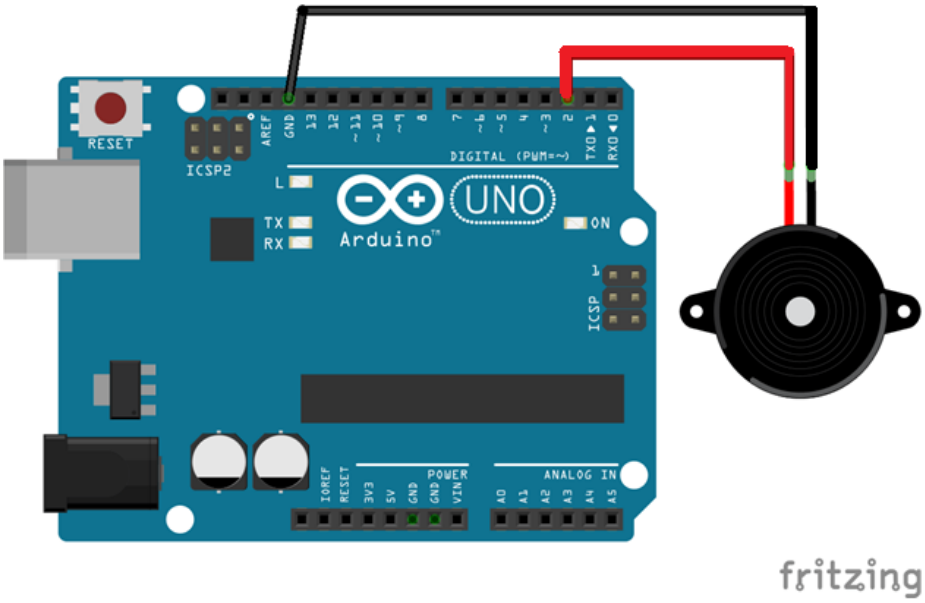


Figure III - 8: Raccordement du buzzer

III.6. Les tests

Nous présentons dans cette partie les schémas de câblage de nos modules et les différents tests effectués sur ces derniers.

III.6.1. Test d'identification des UID (carte à puce et badge)

Le module RFID est accompagné de deux badges de formes différentes (voir fig.III.7) : l'un se forme d'une carte et l'autre d'une clé.

Pour lire le contenu d'un TAG RFID ou d'une carte à puce nous utilisons l'application **DumpInfo** implémentée sur Arduino.

Etape1 : Brancher le module RC522 aux broches de l'Arduino comme représenté ci-dessous avec les connexions correspondantes :

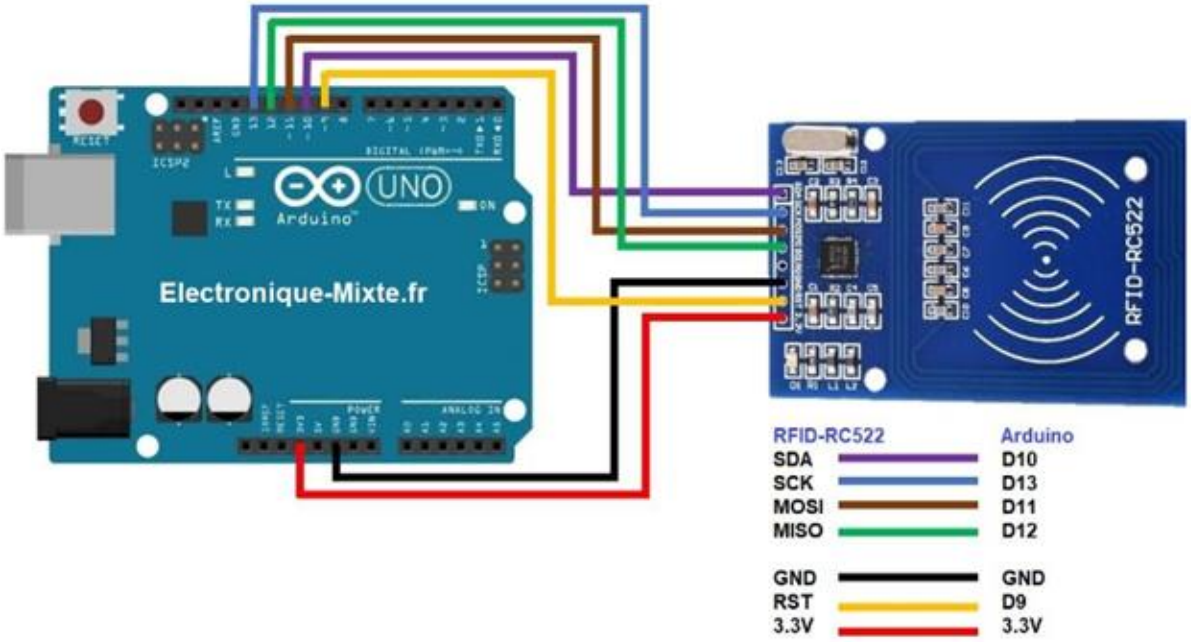


Figure III - 9: Raccordement RC522-Arduino

Etape2 : présentation de la carte à puce ou la clé au lecteur RFID à une distance qui ne doit pas dépasser 30mm

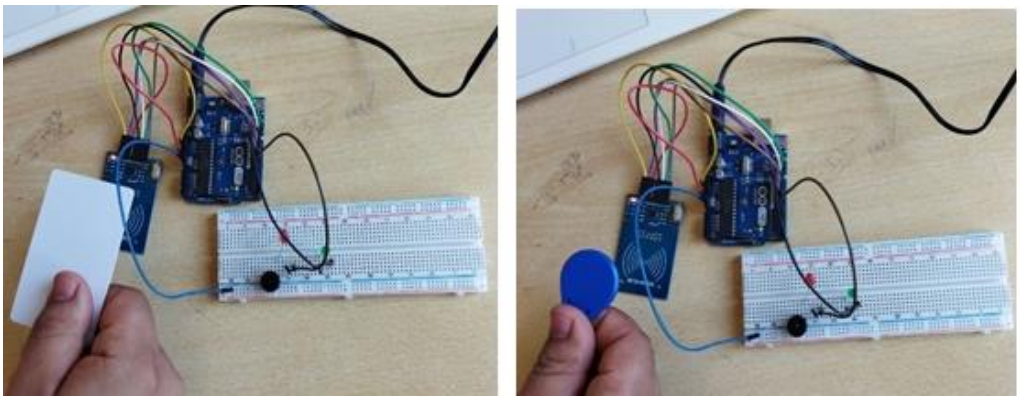


Figure III - 10 : Test de récupération des identifiants de la carte et de la clé

III.6.2. Récupération d'identifiant de la carte à puce en code hexadécimale

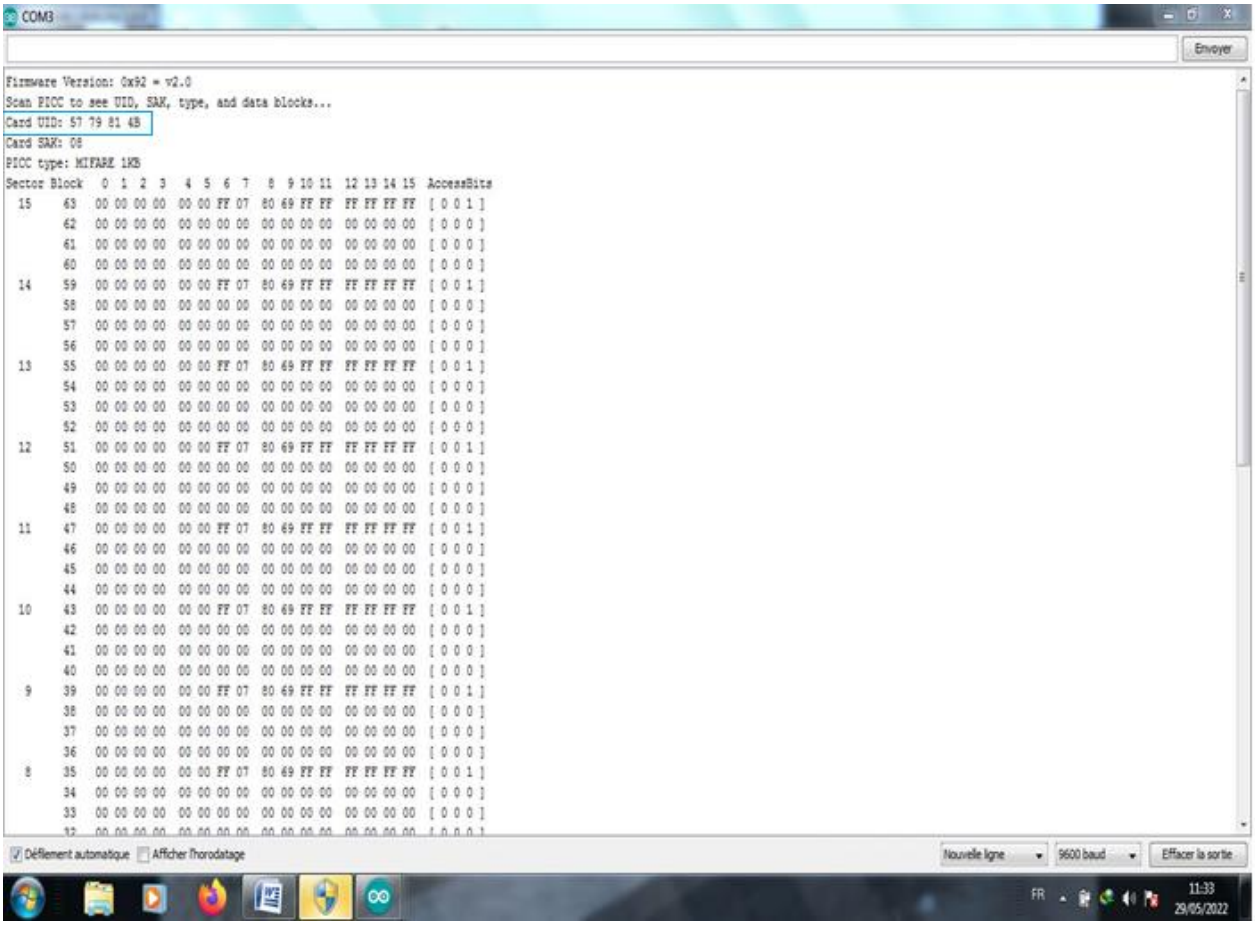


Figure III - 11: Récupération d'identifiant de la carte

La figure ci-dessus montre le résultat de présentation de la carte à puce au lecteur. On peut voir ce résultat sur le moniteur série d'Arduino.
Le code UID en hexadécimale associé à la carte à puce est : **57 79 81 4B**.

III.6.3. Récupération d'identifiant de la clé en code hexadécimale

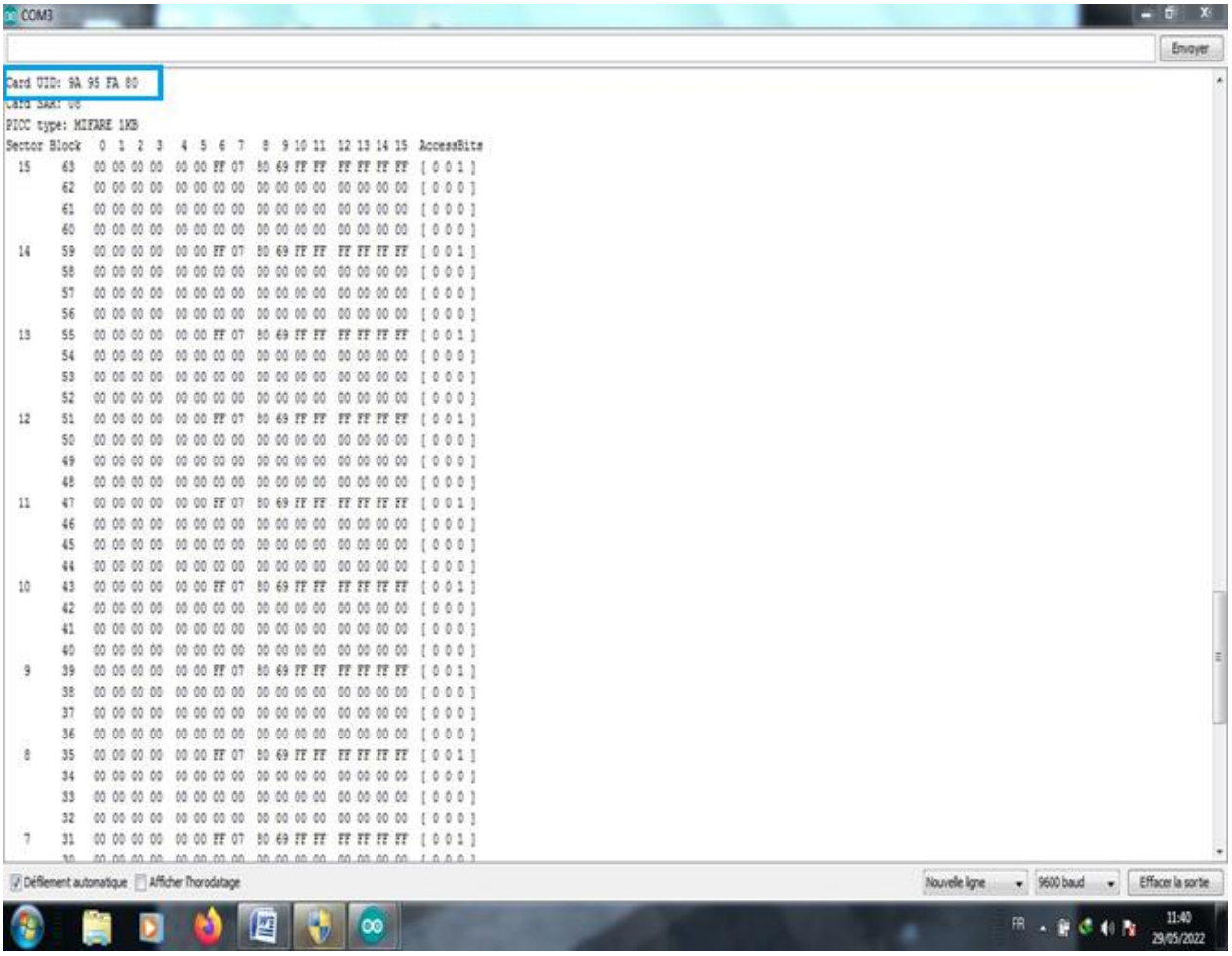


Figure III - 12: Récupération d'identifiant de la clé

La figure ci-dessus montre le résultat de présentation de la clé au lecteur. On peut voir ce résultat sur le moniteur série d'Arduino.
Le code UID en hexadécimale associé à la clé est :9A 95 FA 80

III.7. Partie expérimentale

Pour le besoin de nos différents tests on a simulé, le code UID de la carte comme valide et le code UID de la clé non valide.

III.7.1. Conception d'un système de contrôle d'accès à base d'un lecteur RFID

III.7.1.1. Schéma de câblage

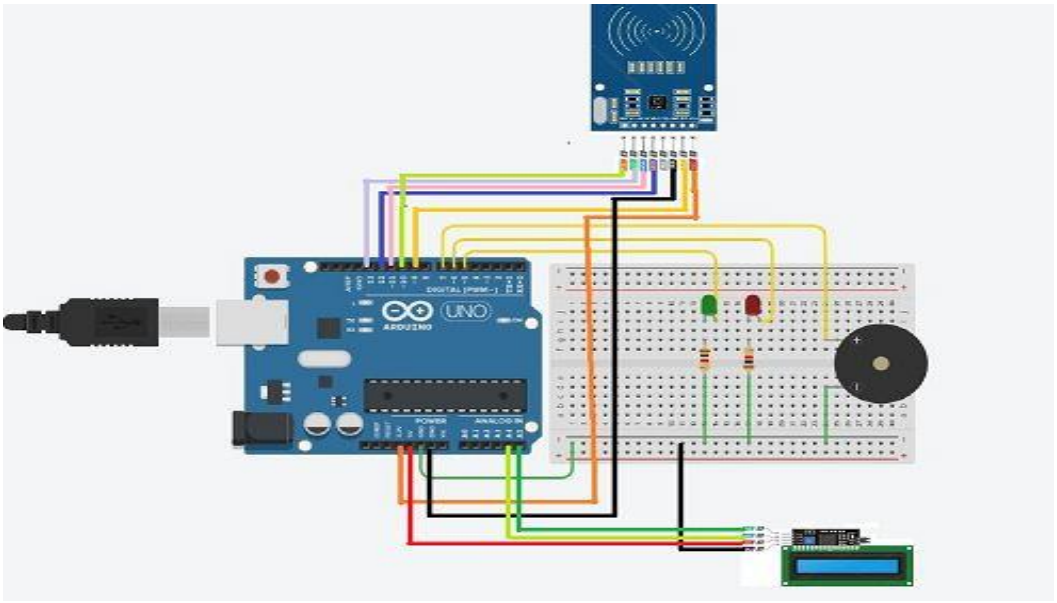


Figure III - 13: Raccordement du lecteur RFID -Arduino-afficheur LCD I2C

III.7.1.2. Programme de fonctionnement du système de contrôle d'accès avec lecteur RFID

Ci-dessous le programme de fonctionnement du système de contrôle d'accès avec lecteur RFID

```
#include <MFRC522.h>
#include <LiquidCrystal_I2C.h>
#include <SPI.h>
#include <Wire.h>
LiquidCrystal_I2C lcd(0x27, 16, 2);
MFRC522 mfrc522(10, 9); // MFRC522 mfrc522(SS_PIN, RST_PIN)
int greenLed =5;
int redLed = 6;
int RELAY = 8;
int BUZZER = 7;
int sda = A4;
int scl = A5;
String cardUID = "57 79 81 4B";  // String to store UID of card. Change it with your tag's UID
boolean RFIDMode = true; // boolean to change modes
int i = 0;  // Variable used for counter
void setup() {
  // Arduino Pin configuration
 pinMode(BUZZER, OUTPUT);
 pinMode(RELAY, OUTPUT);
 pinMode(redLed, OUTPUT);
  pinMode(greenLed, OUTPUT);
  pinMode(SDA, INPUT_PULLUP);
  pinMode(SCL, INPUT_PULLUP);
  digitalWrite(RELAY,HIGH);
  lcd.init();
  lcd.init();
```

```
  lcd.backlight();
  SPI.begin();      // Init SPI bus
  mfrc522.PCD_Init();   // Init MFRC522
  lcd.clear(); // Clear LCD screen
}
void loop() {
  // System will first look for mode
  if (RFIDMode == true){
    lcd.setCursor(1, 0);
    lcd.print("   Door Locked ");
    lcd.setCursor(0, 1);
    lcd.print(" Scan Your card ");
    // Look for new cards
    if ( ! mfrc522.PICC_IsNewCardPresent()) {
      return;
    }
    // Select one of the cards
    if ( ! mfrc522.PICC_ReadCardSerial()) {
      return;
    }

    //Reading from the card
    String card = "";
    for (byte j = 0; j < mfrc522.uid.size; j++)
    {
      card.concat(String(mfrc522.uid.uidByte[j] < 0x10 ? " 0" : " "));
      card.concat(String(mfrc522.uid.uidByte[j], HEX));
    }
    card.toUpperCase();

    //Checking the card
    if (card.substring(1) == cardUID)
    {
      // If UID of card is matched.
      lcd.clear();
      lcd.print("ACCEPTED");
      digitalWrite(greenLed, HIGH);
       digitalWrite(RELAY, LOW);
      delay(3000);
      digitalWrite(greenLed, LOW);
      digitalWrite(RELAY, HIGH);
      lcd.clear();
          }
    else
    {
      // If UID of card is not matched.
      lcd.clear();
      lcd.setCursor(3, 0);
      lcd.print("Wrong card Shown");
      lcd.setCursor(1, 1);
      lcd.print("Access Denied");
      digitalWrite(redLed, HIGH);
      digitalWrite(BUZZER, HIGH);
      delay(3000);
      digitalWrite(redLed, LOW);
      digitalWrite(BUZZER, LOW);
        lcd.clear();
   }
    }
  }
```

III.7.1.3. Test de notre système avec le lecteur RFID

Nous avons testé le montage avec le lecteur RFID sur notre maquette, et le résultat est représenté sur la figure suivante :

Figure III - 14: Test du montage avec lecteur RFID

III.7.2. Conception d'un système de contrôle d'accès à base d'un clavier matriciel (mot de passe)

III.7.2.1. Schéma de câblage

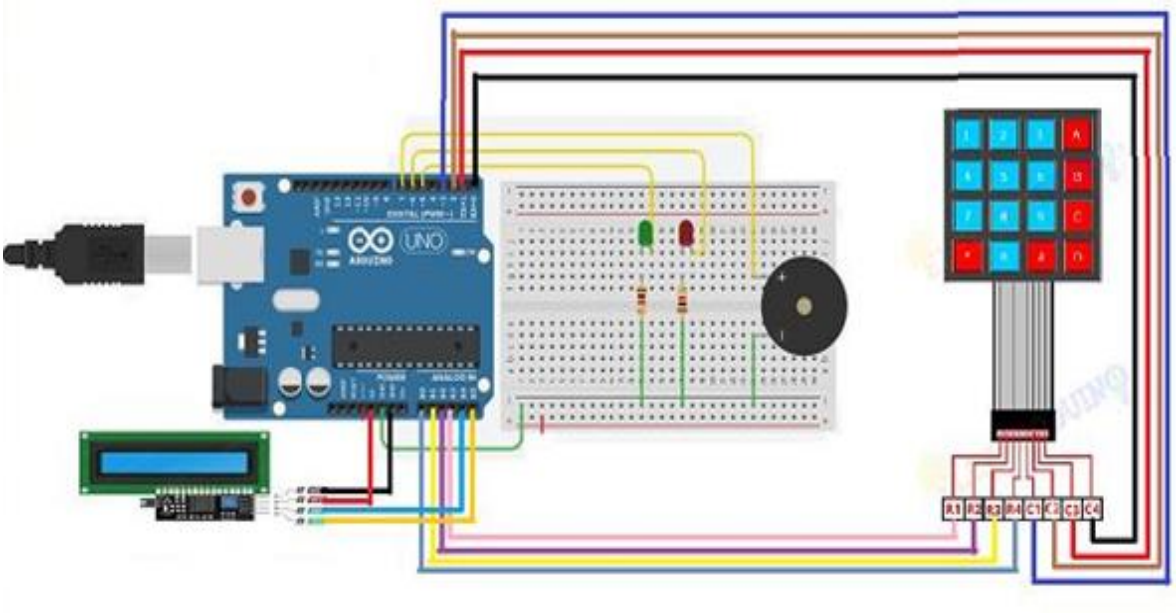


Figure III - 15: Raccordement du clavier matriciel - Arduino-afficheur LCD I2C

III.7.2.2. Programme de fonctionnement du système de contrôle d'accès avec clavier matriciel

Ci-dessous le programme de fonctionnement du système de contrôle d'accès avec clavier matriciel

```
#include <LiquidCrystal_I2C.h>
#include <Keypad.h>
#include <SPI.h>
#include <Wire.h>
LiquidCrystal_I2C lcd(0x27, 16, 2);
// Initialize Pins for led's, servo and buzzer
// Blue LED is connected to 5V
int greenLed =5;
int redLed = 6;
int RELAY = 8;
int BUZZER = 7;
int sda = A4;
int scl = A5;
char initial_password[4] = {'1', '2', '3', '4'};  // Variable to store initial password
String cardUID = "57 79 81 4B";  // String to store UID of card. Change it with your tag's UID
char password[4];   // Variable to store users password
char key_pressed = 0; // Variable to store incoming keys
int i = 0;  // Variable used for counter
// defining how many rows and columns our keypad have
const byte rows = 4;
const byte columns = 4;
// Keypad pin map
char hexaKeys[rows][columns] = {
  {'1', '2', '3', 'A'},
  {'4', '5', '6', 'B'},
  {'7', '8', '9', 'C'},
  {'*', '0', '#', 'D'}
};
// Initializing pins for keypad
byte row_pins[rows] = {A3, A2, A1, A0};
byte column_pins[columns] = {3,2,1,0};
// Create instance for keypad
Keypad keypad_key = Keypad( makeKeymap(hexaKeys), row_pins, column_pins, rows, columns);
void setup() {
  // Arduino Pin configuration
```

```
  pinMode(BUZZER, OUTPUT);
  pinMode(RELAY, OUTPUT);
  pinMode(redLed, OUTPUT);
  pinMode(greenLed, OUTPUT);
  pinMode(SDA, INPUT_PULLUP);
  pinMode(SCL, INPUT_PULLUP);
   digitalWrite(RELAY,HIGH);
    lcd.init();
  lcd.init();
  lcd.backlight();
  SPI.begin();      // Init SPI bus
  lcd.clear(); // Clear LCD screen
}
void loop() {
  // System will first look for mode
     lcd.print("Enter Password:");
     lcd.setCursor(1, 0);
    key_pressed = keypad_key.getKey(); // Storing keys
    if (key_pressed)
    {
     password[i++] = key_pressed; // Storing in password variable
     lcd.print("*");
    }
    if (i == 4) // If 4 keys are completed
    {
     delay(200);
     if (!(strncmp(password, initial_password, 4))) // If password is matched
     {
       lcd.clear();
       lcd.print("Pass Accepted");
       digitalWrite(greenLed, HIGH);
       digitalWrite(RELAY, LOW);
       delay(3000);
       digitalWrite(greenLed, LOW);
       digitalWrite(RELAY,HIGH);
       lcd.clear();
       i = 0;
           }
     else    // If password is not matched
     {
```

```
      lcd.clear();
      lcd.print("Wrong Password");
      digitalWrite(redLed, HIGH);
      digitalWrite(BUZZER, HIGH);
      delay(3000);
      digitalWrite(redLed, LOW);
      digitalWrite(BUZZER, LOW);
      lcd.clear();
      i = 0;
          }
   }
}
```

III.7.2.3. Test de notre système avec le clavier matriciel

Nous avons testé le montage avec le clavier matriciel sur notre maquette, et le résultat est représenté sur la figure suivante :

Figure III - 16: Test du montage avec clavier matriciel

III.7.3. Conception d'un système contrôle d'accès combiné à base d'un lecteur RFID et d'un clavier matriciel

III.7.3.1. Schéma de câblage

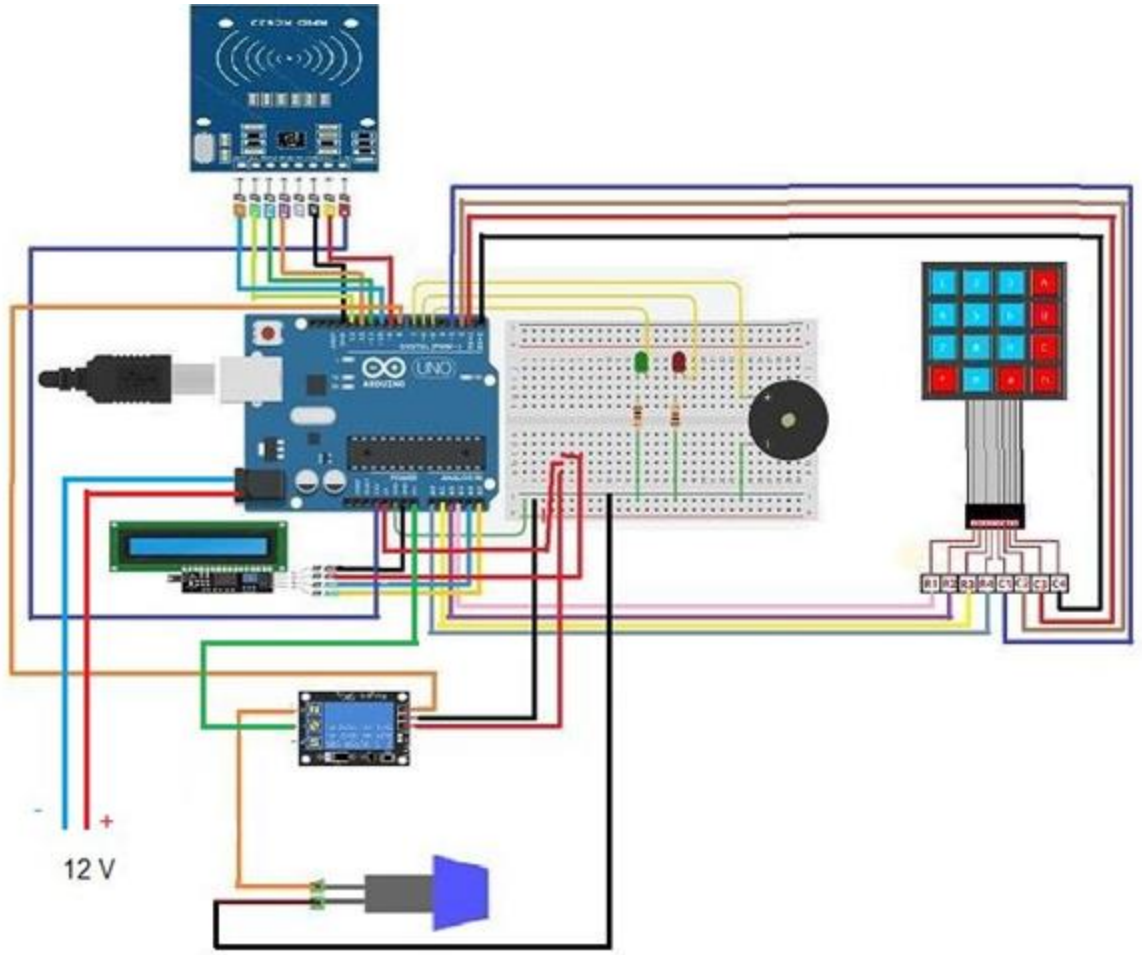


Figure III - 17: Raccordement des différents composants du système

III.7.3.2. Programme de fonctionnement du système de contrôle d'accès combine RFID-Mot de passe

Le programme ci-dessous illustrent le programme IDE Arduino fonctionnel à notre projet **<<système de control d'accès combiné à base de lecteur RFID et du clavier matriciel>>.**

```
#include <MFRC522.h>
#include <LiquidCrystal_I2C.h>
#include <Keypad.h>
#include <SPI.h>
#include <Wire.h>
LiquidCrystal_I2C lcd(0x27, 16, 2);
MFRC522 mfrc522(10, 9); // MFRC522 mfrc522(SS_PIN, RST_PIN)
int greenLed =5;
int redLed = 6;
int RELAY = 8;
int BUZZER = 7;
```

```
int sda = A4;
int scl = A5;
char initial_password[4] = {'1', '2', '3', '4'};  // Variable to store initial password
String cardUID = "57 79 81 4B";  // String to store UID of card. Change it with your tag's UID
char password[4];   // Variable to store users password
boolean RFIDMode = true; // boolean to change modes
char key_pressed = 0; // Variable to store incoming keys
int i = 0;  // Variable used for counter
const byte rows = 4;
const byte columns = 4;

// Keypad pin map
char hexaKeys[rows][columns] = {
  {'1', '2', '3', 'A'},
  {'4', '5', '6', 'B'},
  {'7', '8', '9', 'C'},
  {'*', '0', '#', 'D'}
};
// Initializing pins for keypad
byte row_pins[rows] = {A3, A2, A1, A0};
byte column_pins[columns] = {3,2,1,0};
// Create instance for keypad
Keypad keypad_key = Keypad( makeKeymap(hexaKeys), row_pins, column_pins, rows, columns);
void setup() {
  // Arduino Pin configuration
  pinMode(BUZZER, OUTPUT);
  pinMode(RELAY, OUTPUT);
  pinMode(redLed, OUTPUT);
  pinMode(greenLed, OUTPUT);
  pinMode(SDA, INPUT_PULLUP);
  pinMode(SCL, INPUT_PULLUP);
  digitalWrite(RELAY,HIGH);

   lcd.init();
  lcd.init();
  lcd.backlight();
  SPI.begin();      // Init SPI bus
  mfrc522.PCD_Init();   // Init MFRC522
  lcd.clear(); // Clear LCD screen
}
void loop() {
  // System will first look for mode
  if (RFIDMode == true){
    lcd.setCursor(1, 0);
    lcd.print("   Door Locked ");
    lcd.setCursor(0, 1);
    lcd.print(" Scan Your card ");
    // Look for new cards
    if ( ! mfrc522.PICC_IsNewCardPresent()) {
      return;
    }
    // Select one of the cards
    if ( ! mfrc522.PICC_ReadCardSerial()) {
      return;
    }
    //Reading from the card
    String card = "";
    for (byte j = 0; j < mfrc522.uid.size; j++)
    {
      card.concat(String(mfrc522.uid.uidByte[j] < 0x10 ? " 0" : " "));
```

```
    card.concat(String(mfrc522.uid.uidByte[j], HEX));
  }
  card.toUpperCase();
  //Checking the card
  if (card.substring(1) == cardUID)
  {
    // If UID of card is matched.
   lcd.clear();
    lcd.print("card Matched");
    digitalWrite(greenLed, HIGH);
    delay(3000);
    digitalWrite(greenLed, LOW);
    lcd.clear();
    lcd.print("Enter Password");
    lcd.setCursor(1, 1);
    RFIDMode = false; // Make RFID mode false
       }
  else
  {
    // If UID of card is not matched.
    lcd.clear();
    lcd.setCursor(3, 0);
    lcd.print("Wrong card Shown");
    lcd.setCursor(1, 1);
    lcd.print("Access Denied");
    digitalWrite(redLed, HIGH);
    digitalWrite(BUZZER, HIGH);
    delay(3000);
    digitalWrite(redLed, LOW);
    digitalWrite(BUZZER, LOW);
    lcd.clear();
  }
}
// If RFID mode is false, it will look for keys from keypad
if (RFIDMode == false) {
  key_pressed = keypad_key.getKey(); // Storing keys
  if (key_pressed)
  {
    password[i++] = key_pressed; // Storing in password variable
    lcd.print("*");
  }
  if (i == 4) // If 4 keys are completed
  {
    delay(200);
    if (!(strncmp(password, initial_password, 4))) // If password is matched
    {
      lcd.clear();
      lcd.print("Pass Accepted");
      digitalWrite(greenLed, HIGH);
      digitalWrite(RELAY, LOW);
      delay(3000);
      digitalWrite(greenLed, LOW);
      digitalWrite(RELAY,HIGH);
      lcd.clear();
      i = 0;
      RFIDMode = true; // Make RFID mode true
    }
    else    // If password is not matched
    {
      lcd.clear();
```

```
      lcd.print("Wrong Password");
      digitalWrite(redLed, HIGH);
      digitalWrite(BUZZER, HIGH);
      delay(3000);
      digitalWrite(redLed, LOW);
      digitalWrite(BUZZER, LOW);
      lcd.clear();
      i = 0;
      RFIDMode = true;  // Make RFID mode true
    }
  }
}
```

III.7.3.3. Test de notre système par la combinaison du lecteur RFID et du clavier matriciel

Le branchement des composants sur bread bord est illustré par la figure suivante :

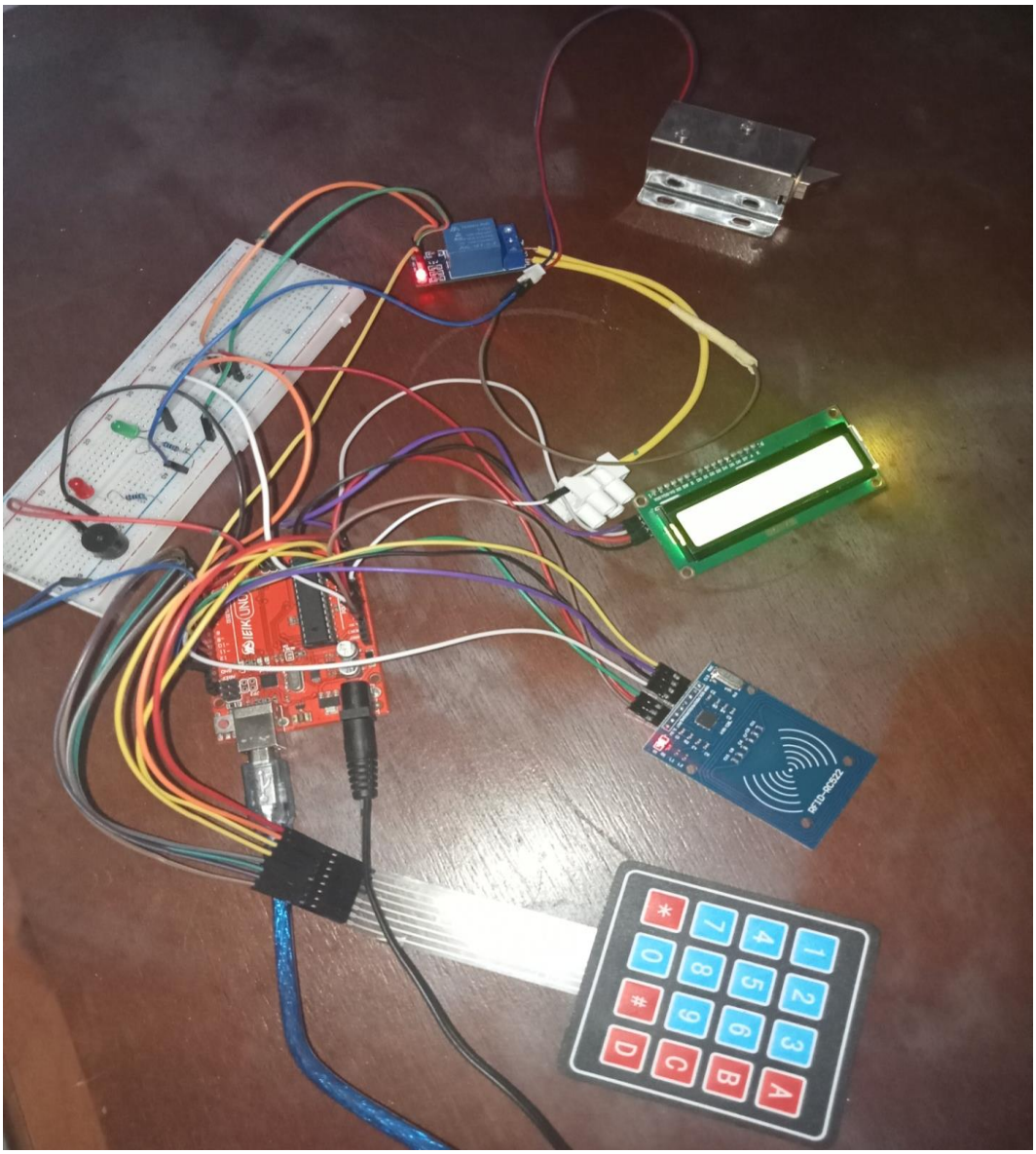


Figure III - 18: Raccordement des composants de notre système sur bread bord

Vue extérieure

Vue intérieure

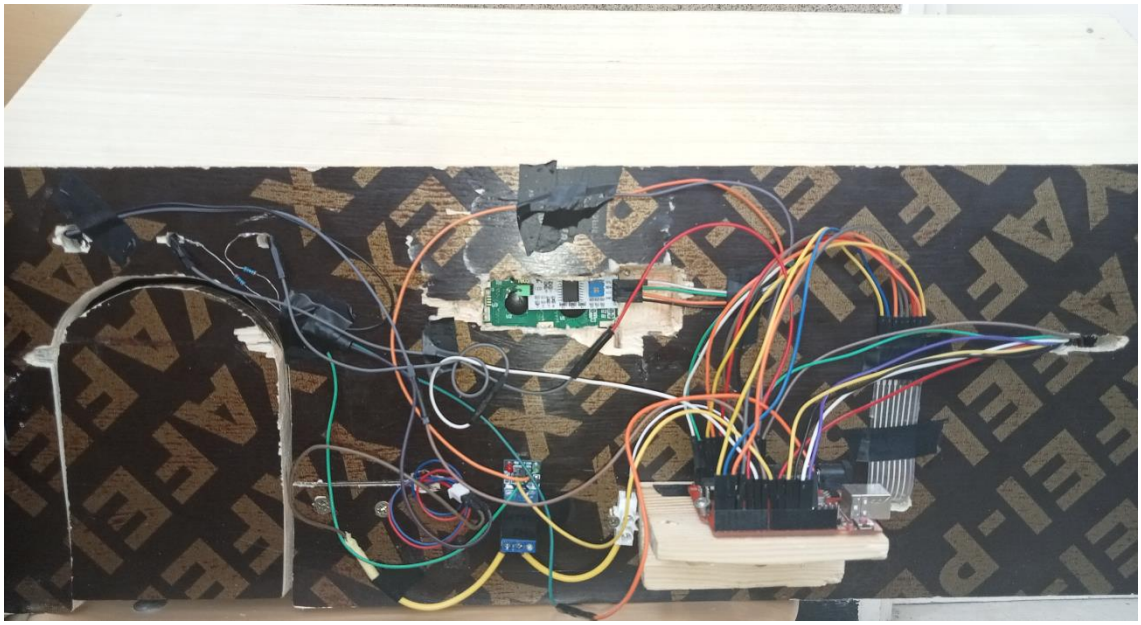


Figure III - 19: Raccordement des composants de notre système sur maquette

III.8. Conclusion

Au cours de ce de dernier chapitre, nous avons décrit les étapes de réalisation et de test de notre système. En premier lieu, nous avons présenté les outils de développement utilisés ainsi que les configurations matérielles et les raccordements nécessaire, ensuite, dans la deuxième partie, nous avons présenté les trois tests qu'on a réalisés.

Comme nous l'avons mentionné, notre système offre une flexibilité et dispose de différentes fonctionnalités nécessaires pour gérer un système de contrôle d'accès sécurisé. En obtenant les résultats attendus, on peut conclure que le système mis en place répond bien au besoin de contrôle d'accès combiné d'un lecteur RFID et clavier matriciel (mot de passe).

CONCLUSION GENERALE ET PERSPECTIVES

L'objectif du présent travail étant de concevoir et de développer un système permettant de contrôler l'accès à des zones particulières. L'utilisation de nouvelles technologies d'identification rend l'échange d'informations plus rapide, notamment l'identification par radiofréquence (RFID) qui permet le contrôle d'accès et assure une meilleure traçabilité.

Ce projet permet de fournir une méthode pratique de marquage des individus. En utilisant des bases de données en temps réel, ces derniers sont mieux organisés et mieux exploités en termes de sondage, sécurité, calcul divers.

Ce système est également convivial car la manipulation et la récupération des données peuvent se faire via des interfaces physiques faciles à utiliser.

Au terme de ce travail élaboré dans le cadre de notre projet de fin d'études, nous considérons que ce projet nous a été bénéfique vu qu'il nous a permis de consolider nos connaissances vers le développement d'un système embarqué qui sera utile dans le domaine de contrôle d'accès.

En effet., comme toute autre technologie de l'information, la RFID n'est pas à l'abri de risques de sécurité qui ont une incidence sur l'intégrité des systèmes, leur disponibilité et leur confidentialité, notre contribution réside à l'ajout d'un clavier matriciel pour renforcer la sécurité et la fiabilité de ce système.

Perspectives

Pour la suite de ce travail, nous avons comme perspectives : l'amélioration du matériel utilisé notamment le remplacement de la carte Arduino Uno par une Arduino Nano qui se caractérise par ses petites dimensions et un faible coût. L'utilisation de la carte RFID et les empreintes digitales en même temps pour renforcer la sécurité. Contrôler l'accès par rapport à des jours et des horaires bien précis.
A long terme la combinaison de la RFID avec d'autres technologies laisse entrevoir d'intéressantes perspectives. Les technologies de communication et les capteurs permettront de suivre à distance les conditions ambiantes (par exemple, température, pression) dans des secteurs tels que la santé et l'environnement.

BIBLIOGRAPHIES

BIBLIOGARPHIES

[1] : https://rfid.ooreka.fr/comprendre/systeme-rfid.

[2]: Klaus Finkenzeller. RFID Handbook: Fundamentals and applications in Contactless Smart Cards and identification. Deuxième Edition, John Wiley et Sons, Ltd., England. ISBN 0-470-84402-7.

[3] : Eric Schuler et Jean-François PILLOU, Article, de www.arvensys.com.

[4] : CNRFID, De l'innovation au déploiement de solution RFID et NFC, le centre national de référence

[5] : Pattabhiraman Krishna et David Husak. RFID INFRASTRUCTURE. IEEE Communications Magazine. Volume :45, Issue :9, pages 4-10. Septembre 2007.

[6] : Rafael Antonio Quiroz Moreno, << Solutions novatrices pour l'amélioration du taux de lecture de tags RFID UHF dans des environnements complexes>>, mémoire pour obtenir le grade de docteur de l'Université Paris-Est, Spécialité : Électronique. 4 mars 2014

[7] : Jean de françoi, RFID (Radio Frequency Identification, septembre 2015

[8] : Noyel Mélanie Pisaneschi Thomas, Mise en place d'un système RFID pour une entreprise de panneaux laqués haute finition, Rapport de fin d'études, 2010 / 2011

[9] : Yves Saint-Oyant et Jonathan Brisart. La norme RFID. Thèse de Master IAGL. Université de sciences et technologie. Lille1. 2010.

[10]: https://rfid.ooreka.fr/comprendre/etiquette-rfid

[11] : Imad BELKACEM, << Analyse des données d'un système RFID en vue de sa sureté de fonctionnement>>, diplôme de Magistère en informatique, Option : Ingénierie des données et des connaissances, Université Es-Senia ORAN.

[12]: http://www.centrenational-rfid.com/classification-des-tags-rfid-article-19-fr-ruid 17.html

[13]: L'identification par radiofréquence Document réalisé par le collège Utilisateurs du CNRFID

[14]: http://www.journaldunet.com/solutions/systemes-reseaux/dossier/rfid-10-applicationsqui-
montent/rfid-10-applications-qui-montent.shtml

[15] : RFID'' Identification par radiofréquence'', Orientation de L'OCDE, Sécurité de l'information et protection de la vie privée, Application, Impacts et initiatives nationale, Réunion Ministérielle de l'OCDE, le futur de l'économie, Internet. Seoul, Corée, 17 et 18 juin 2008.

[16] : https://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&cad=rja&uact=8&ved=0ahUKEwig35jD393SAhXGPBQKHQtQDh8QFgg8MAk&url=http%3A%2F%2Fformationmasterss3.e-monsite.com%2Fmedias%2Ffiles%2F121-1--1.docx&usg=AFQjCNGCF5LvhQW8C5RzYPyvOuWsIrexiQ&bvm=bv.149760088, d . d24.

[17] : Nicolas G., Goeffrey L., 2015. Arduino Apprendre à développer pour créer des objets intelligents.

[18] : KRAMA A., GOUGUI A., 2015. « Étude et réalisation d'une carte de contrôle par Arduino via le système Androïde », mémoire Master Académique, Université Kasdi Merbah Ouargla.

[19] : http://www.techmania.fr/arduino/Decouverte_arduino.pdf

[20] : //perso-laris.univ-angers.fr/~cottenceau/ArduinoCottenceau1112.pdf

[21] : ARDUINO1.pdf

[22] : http://perso-laris.univ-angers.fr/~cottenceau/ArduinoCottenceau1112.pdf Consulté le

[23] : https://www.aurel32.net/elec/lcd.php

[24] : https://fr.scribd.com/doc/35887890/Les-Afficheurs-LCD

[25] : https://fr.wikipedia.org/wiki/Relais_%C3%A9lectrom%C3%A9canique

[26] : http://gilles.berthome.free.fr/02-Syntheses/F_Transmision_info/Synthese_relais.pdf

[27] : https://www.sonelec-musique.com/electronique_theorie_buzzers.html

[28] : RFID : Contrôle d'accès par badge avec Arduino – RC522, FPGA | Arduino | Matlab | Cours @ www.electronique-mixte.fr

[29] : Tassadit CHAFA, Nacera OTMANI, 2016. « Contrôle d'accès à base de la technologie RFID », mémoire Master académique en informatique, Université Mouloud MAMMERI de TIZI-OUZOU.

[30] : Astalaseven, Eskimon et Olyte,2012. Arduino pour bien commencer en electronique et en programmation.