Université Abou Bekr Belkaid
Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Université Abou Bekr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

# Mémoire de fin d'étude

***Pour l'obtention du Diplôme de Master en Informatique***
***Option : Réseaux et Systèmes Distribués***

# Thème

*Développement d'une application de cryptage des Stream Vidéo capturé par webcam en basant sur le modèle client/serveur*

*Réalisé par :*

*Mr MOULAI Mohamed Tareq*

*Mr ZERROUKI Mohamed Wanis*

*Devant le jury composé de :*

*Président : Mr BENAMAR Abdelkarim*

*Examinateur : Mr MANA Mohamed*

*Encadreur : Mr BENAISSA Samir Mohamed*

# Sommaire

# *Liste des figures*

## Chapitre 1



## Chapitre 2



## Chapitre 3



## Chapitre 4

**Chapitre 5**

# *Liste des tableaux*

# *Remerciements*

"وَعَسَىٰ أَن تَكْرَهُوا شَيْئًا وَهُوَ خَيْرٌ لَّكُمْ"

Tout d'abord, je voudrais mentionner les difficultés que nous avons rencontrées dans la préparation de ce projet de fin d'études après l'apparition du virus de la corona en Algérie et la déclaration de l'état d'urgence :

-ne pas rencontrer le professeur encadreur-Ne pas rencontrer de collègue

-Fermeture des universités et des bibliothèques et manque d'accès aux références et aux livres

-Difficulté à communiquer sur les réseaux sociaux

Mais cela ne nous a pas empêchés de remettre en question et de nous efforcer de préparer et d'obtenir le diplôme de fin d'étude.

Et je tiens à exprimer ma gratitude la plus sincère pour **DIEU TOUT PUISSANT** sans l'aide duquel ce mémoire n'aurait pas eu lieu.

Je tiens à remercier **BENAISSA MOHAMMED** qui a bien voulu m'encadrer, me conseiller, me guider et me confier ce travail.

A Messieurs les membres de jury que nous remercions de l'intérêt qu'ils ont bien voulu apporter à notre travail par sa lecture et sa discussion.

# *Dédicaces*

A nos très chers parents, source de vie, d'amour et d'affection

A nos chers frères et sœurs, source de joie et de bonheur

A toute la famille ZERROUKI et MOULAI, source d'espoir et de motivation

A tous nos chers amis

A vous cher lecteur

# *Introduction*

Les entreprises du monde entier détiennent une quantité énorme de données informatiques concernant leurs clients, leurs partenaires, leurs prestataires. Il est parfois difficile de savoir comment toutes ces informations, qui ont pour certaines un haut degré de confidentialité, peuvent être utilisées. Et que l'on soit en Europe ou aux États-Unis peut tout changer quant au cadre légal et aux obligations concernant ces données.

163 zettaoctets (soit 163 milliards de téraoctets), c'est le volume de données informatiques que la population mondiale sera amenée à stocker d'ici 2025. Il existe plusieurs types de données informatiques, comme les données personnelles par exemple. D'après l'article 2 de la loi « **Informatique et libertés** », constitue une donnée à caractère personnel, toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Une personne est identifiable, par exemple, lorsqu'un fichier comporte des informations permettant de la reconnaître (ex : nom, prénom, n° de téléphone, photographie, n° d'immatriculation, adresse IP, éléments biométriques comme l'empreinte digitale etc). Au sein d'une entreprise, la création et le traitement de ces données sont théoriquement soumis à des obligations destinées à **protéger la vie privée des personnes et les libertés individuelles**.

Le cryptage vidéo est le processus consistant à masquer les données en les convertissant d'une forme à une autre. De nos jours, il y a une croissance rapide des techniques multimédias, où toutes les informations peuvent être partagées via le réseau / Internet. Tout en partageant données / informations de l'expéditeur au récepteur, une perte de données peut se produire entre les deux pendant le transfert. Donc, afin de fournir sécuriser transmission, le cryptage doit être effectué avant de transférer les données / informations au récepteur.

La réduction / perte de données peut être réduit par le processus de cryptage. Les données chiffrées peuvent être déchiffrées au niveau du récepteur en utilisant la clé secrète chiffrement. La sécurité est requise pour la vidéo pendant la transmission car dans l'enseignement à distance, les informations transférées ne doivent pas être variées. Le cryptage est nécessaire pour une transmission de bonne qualité et sécurisée. Les deux types d'algorithmes de chiffrement sont symétriques cryptographies à clé et cryptographie à clé asymétrique.

Le processus de cryptage vidéo utilise l'algorithme AES modifié et le processus de brouillage pour une transmission sécurisée. Ici la vidéo la qualité est maintenue après décryptage au niveau du récepteur.

Notre mémoire est structurée comme suite :

**Chapitre 1 :** Introduction aux architectures client/serveur.

**Chapitre 2 :** Les techniques et les algorithmes de chiffrement a clé publique et a clé secrète

**Chapitre 3 :** Méthode de Cryptage En RC4

**Chapitre 4 :** Études générales sur la vidéo

**Chapitre 5 :** Application

*Chapitre 1*

# Introduction aux architectures client/serveur

# Chapitre 1 : Introduction aux architectures client/serveur

## 1. Introduction

Une architecture client-serveur (figure 1) divise une application en deux parties, « client » et « serveur ». Une telle application est implémentée sur un réseau informatique, qui connecte le client au serveur. La partie serveur de cette architecture fournit la fonctionnalité centrale : c'est-à-dire que n'importe quel nombre de clients peuvent se connecter au serveur et demander qu'il exécute une tâche. Le serveur accepte ces demandes, exécute la tâche requise et renvoie les résultats au client, le cas échéant. [1]


Figure 1 Simple client–server application

## 2. Évolution

### A. Ordinateur central

Dès ses débuts, le modèle de gestion des données par ordinateur était basé sur l'utilisation de terminaux distants, qui étaient connectés directement à un ordinateur central. Ledit ordinateur central était chargé de fournir des services caractérisés en ce que chaque service n'était fourni qu'à un groupe exclusif d'utilisateurs.

### B. Ordinateurs dédiés

C'est l'époque où chaque service utilisait son propre ordinateur qui permettait aux utilisateurs de ce service de se connecter directement. Ceci est une conséquence de l'apparition de petits ordinateurs conviviaux, moins chers et plus puissants que les ordinateurs conventionnels.

### C. Connexion gratuite

Il y a plus de 10 ans, les ordinateurs de bureau sont apparus de manière massive. Cela a permis à une partie appréciable de la charge de travail de calcul à la fois au niveau du calcul et de la présentation d'être exécutée à partir du bureau de l'utilisateur. Dans de nombreux cas, l'utilisateur obtient les informations dont il a besoin à partir d'un ordinateur de service. Ces ordinateurs de bureau se connectent aux ordinateurs de service à l'aide d'un logiciel qui permet l'émulation d'un

certain type de terminal. Dans d'autres cas, les informations leur sont transmises à l'aide de ressources magnétiques ou par transcription.

D. Calcul via des réseaux

C'est l'ère qui est basée sur le concept de réseaux informatiques, dans lequel les informations résident dans un ou plusieurs ordinateurs, les utilisateurs de ces informations utilisent des ordinateurs pour travailler et tous sont connectés les uns aux autres. Cela permet à tous les utilisateurs d'accéder aux informations de tous les ordinateurs pendant que les différents systèmes échangent des informations.

E. Architecture client-serveur

Dans cette architecture, l'ordinateur de chacun des utilisateurs, appelé client, produit une demande d'information à partir de n'importe lequel des ordinateurs qui fournissent des informations, appelés serveurs, ces derniers répondent à la demande du client qui les a produites. Les clients et les serveurs peuvent être connectés à un réseau local ou à un réseau étendu, tel que celui qui peut être implémenté dans une entreprise ou à un réseau mondial tel qu'Internet. Selon ce modèle, chaque utilisateur est libre d'obtenir à tout moment les informations dont il a besoin auprès d'une ou plusieurs sources locales ou distantes et de les traiter selon les besoins. Différents serveurs peuvent également échanger des informations au sein de cette architecture.

## 3. Composants du système

**Client :**

C'est celui qui initie une demande de service. L'exigence initiale peut être convertie en plusieurs exigences de travail via des réseaux LAN ou WAN. L'emplacement des données ou des applications est complètement transparent pour le client.

**Serveur** :

Il s'agit de toute ressource informatique dédiée à répondre aux besoins des clients. Les serveurs peuvent être connectés aux clients via des réseaux LAN ou WAN, pour fournir plusieurs services aux clients et aux citoyens tels que l'impression, l'accès aux bases de données, la télécopie , le traitement des images , etc.

Les serveurs peuvent effectuer des tâches simples (cas du serveur de jour qui renvoie une réponse) ou des tâches complexes (cas du serveur FTP dans lequel des opérations doivent être effectuées avant de renvoyer une réponse). Les serveurs simples traitent une demande à la fois (ils sont séquentiels ou interactifs), ils ne vérifient donc pas si une autre demande est arrivée avant d'envoyer la réponse de la précédente.

Les plus complexes fonctionnent avec des requêtes simultanées même lorsqu'une seule requête met longtemps à être servie (dans le cas du serveur FTP qui doit copier un fichier sur une autre machine). Ils sont complexes car ils ont des exigences élevées en matière de protection et d'autorisation. Ils peuvent lire les fichiers système, rester en ligne et accéder aux données protégées et aux fichiers utilisateur. Vous ne pouvez pas répondre aveuglément aux demandes des clients, vous devez renforcer les politiques d'accès et de protection du système. Les serveurs se composent généralement de deux parties :

- ✓ Programme ou processus responsable de l'acceptation de nouvelles demandes : enseignant ou parent.
- ✓ Programmes ou processus qui doivent gérer des demandes individuelles : esclaves ou enfants.[13] [14]

## 4. Tâche du programme maître

- Ouvrez un port local bien connu auquel les clients peuvent accéder.
- Attendez les demandes des clients.
- Choisissez un port local pour les demandes qui arrivent pour informer le client du nouveau port (inutile dans la plupart des cas).
- Démarrez un programme esclave ou un processus enfant qui assiste la demande sur le port local (l'esclave lorsqu'il a fini de traiter une demande ne reste pas en attente des autres).
- Retour à l'attente des demandes pendant que les esclaves traitent simultanément les demandes précédentes. [2]

## 5. Classification des serveurs

- Serveurs sans état (stateless) Figure 2.
- Serveurs avec état (stateful) Figure 3.
- Serveurs simultanés [15]

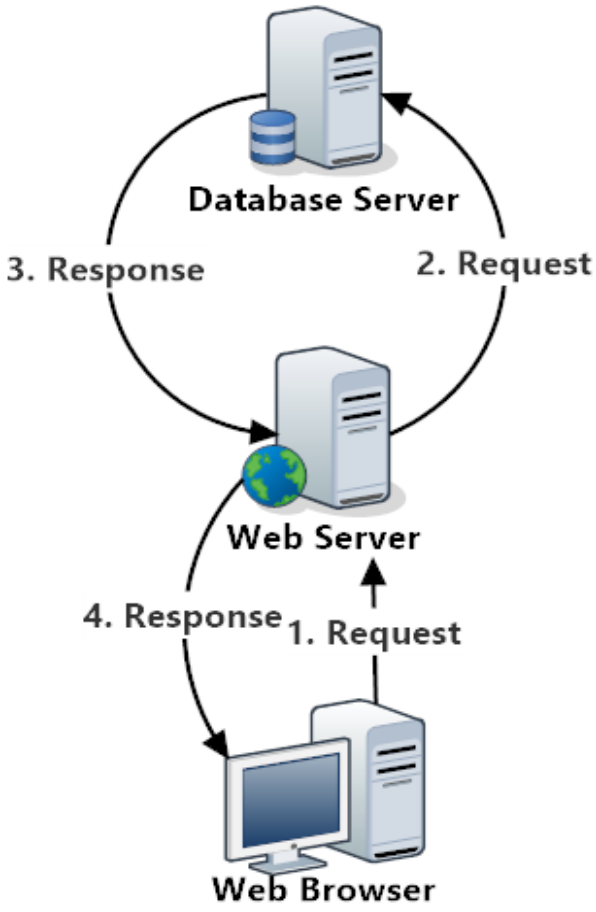



Figure 2 Schéma de serveur sans état

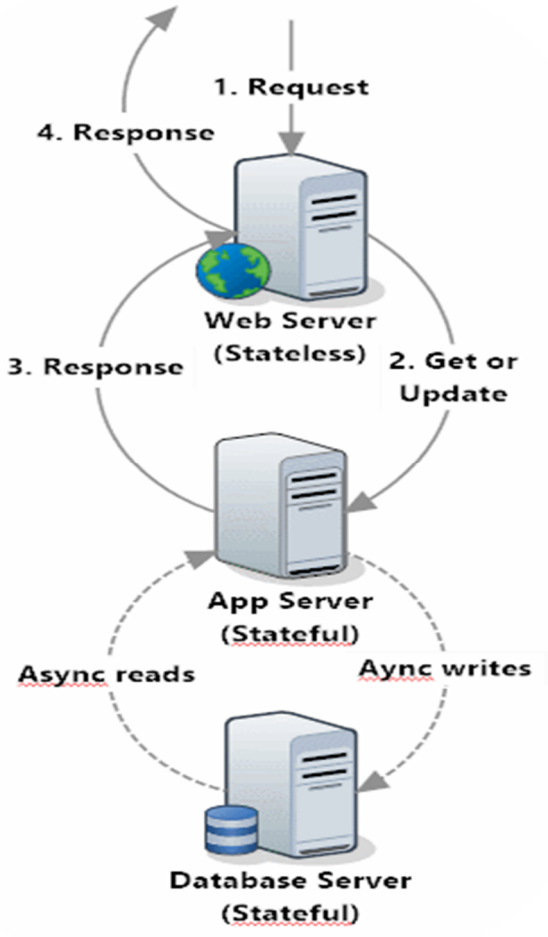



Figure 3 Schéma de serveur avec état

## 6. Caractéristiques de l'architecture client-serveur

- Combinaison d'un client qui interagit avec l'utilisateur et d'un serveur qui interagit avec les ressources à partager. Le processus client fournit l'interface entre l'utilisateur et le reste du système. Le processus serveur agit comme un moteur logiciel qui gère les ressources partagées telles que les bases de données, les imprimantes, les modems, etc.
- Les tâches client et serveur ont des exigences différentes en ce qui concerne les ressources informatiques telles que la vitesse du processeur, la mémoire, la vitesse et les capacités du disque et des périphériques d'entrée-sortie.
- Une relation est établie entre différents processus, qui peuvent être exécutés sur la même machine ou sur différentes machines réparties sur le réseau.
- Il existe une distinction claire des fonctions basées sur le concept de "service", qui est établi entre les clients et les serveurs.
- La relation établie peut être plusieurs à un, dans laquelle un serveur peut servir de nombreux clients, régulant leur accès aux ressources partagées.

- Les clients correspondent aux processus actifs dans la mesure où ce sont eux qui font les demandes de service. Ces derniers sont de nature passive, car ils attendent les demandes des clients.
- Il n'y a pas d'autre relation entre les clients et les serveurs que celle établie par l'échange de messages entre les deux. Le message est le mécanisme de demande et de livraison des demandes de service.
- L'environnement est hétérogène. La plate-forme matérielle et les systèmes d'exploitation client et serveur ne sont pas toujours les mêmes. Précisément l'un des principaux avantages de cette architecture est la possibilité de connecter clients et serveurs quelles que soient leurs plateformes.
- Le concept d'évolutivité horizontale et verticale est applicable à tout système client-serveur. L'évolutivité horizontale vous permet d'ajouter des postes de travail plus actifs sans affecter de manière significative les performances. L'évolutivité verticale vous permet d'améliorer les caractéristiques du serveur ou d'ajouter plusieurs serveurs.

## 7. Avantages du schéma client-serveur

Existence de plates-formes matérielle de plus en plus bon marché. Ceci constitue à son tour l'un des avantages les plus palpables de ce schéma, la possibilité d'utiliser des machines beaucoup moins chères que celles requises par une solution centralisée, basée sur de grands systèmes (mainframes). De plus, des composants, matériels et logiciels, de différents fabricants peuvent être utilisés, ce qui contribue considérablement à la réduction des coûts et favorise la flexibilité dans la mise en œuvre et la mise à jour des solutions.

- Il facilite l'intégration entre différents systèmes et partage des informations, ce qui permet par exemple d'utiliser des machines existantes mais en utilisant des interfaces conviviales. De cette façon, les PC peuvent être intégrés à des systèmes moyens et grands, sans que tout le monde n'utilise le même système d'exploitation.
- En favorisant l'utilisation d'interfaces graphiques interactives, les systèmes construits dans le cadre de ce schéma ont une interface utilisateur plus grande et plus intuitive. Dans l'utilisation des interfaces utilisateur graphique, elle présente l'avantage, par rapport à une interface centralisée, qu'il n'est pas toujours nécessaire de transmettre des informations graphiques sur le réseau car elles peuvent résider chez le client, ce qui permet une meilleure utilisation de la bande passante du Web.
- La structure intrinsèquement modulaire facilite également l'intégration des nouveaux techniques et la croissance de l'infrastructure informatique, favorisant ainsi l'évolutivité des solutions.
- Il contribue également à apporter aux différents services d'une organisation des solutions locale, mais permettant l'intégration des informations.

## 8. Désavantages

La maintenance des systèmes est plus difficile car elle implique l'interaction de différentes parties du matériel et des logiciels, distribués par différents fournisseurs, ce qui rend difficile le diagnostic des pannes.

Il dispose de très peu d'outils pour gérer et ajuster les performances des systèmes.

Il est important que les clients et les serveurs utilisent le même mécanisme (par exemple des sockets ou RPC), ce qui implique que vous devez avoir des mécanismes généraux qui existent sur différentes plateformes.

Vous devez avoir des stratégies pour gérer les erreurs et maintenir la cohérence des données.

Les performances (performances), des problèmes de ce style peuvent apparaître par des encombrements dans le réseau, des difficultés de trafic de données, etc. [3]

## 9. Conclusion

Dans ce chapitre, nous avons présentés une introduction générale du modèle client-serveur et leur utilité dans le réseau informatique. Ce modèle client/serveur est la base de toutes les applications développer dans le monde des systèmes distribués. Plus, nous avons indiqués l'importance de la notion de protocoles, ports et sockets pour simplifier l'implémentation des applications client/serveur dans l'Internet. [b1]

*Chapitre 2*

# Les techniques et les algorithmes de chiffrement a clé publique et a clé secrète

# Chapitre 2 : Les techniques et les algorithmes de chiffrement a clé publique et a clé secrète

## 2.1 Introduction

Le but de la cryptographie est de protéger les données transmises en présence probable d'un adversaire. Comme le montre la figure 2.1, une transformation cryptographique des données est une procédure par laquelle les données en clair sont déguisées ou chiffrées, ce qui entraîne un texte modifié, appelé texte chiffré, qui ne révèle pas l'entrée d'origine. Le texte chiffré peut être transformé en sens inverse par un destinataire désigné afin que le texte en clair d'origine puisse être récupéré.

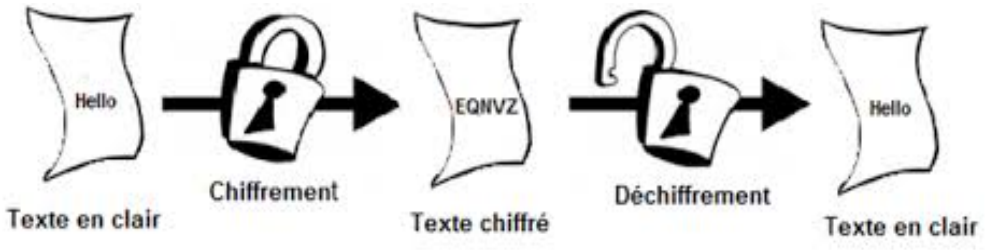



Figure 2.1. Le processus de chiffrement et de déchiffrement

La cryptographie joue un rôle essentiel dans :

Authentification : Ce processus pour prouver l'identité d'une entité peut être basé sur quelque chose que vous savez, comme un mot de passe, quelque chose que vous avez, comme une clé ou une carte de chiffrement, quelque chose que vous êtes, comme les mesures biométriques, y compris les scans rétiniens ou la reconnaissance vocale, ou toute combinaison de ceux-ci.

Confidentialité : des données. Avec cette propriété, aucune information n'est mise à disposition ou divulguée à des individus, entités ou processus non autorisés. Lorsque deux ou plusieurs parties sont impliquées dans une communication, le but de la confidentialité est de garantir que seules ces parties peuvent comprendre les données échangées. La confidentialité est garantie par le cryptage.

Intégrité des données : Cette propriété fait référence aux données qui n'ont pas été modifiées, détruites ou perdues de manière non autorisée ou accidentelle. Le besoin d'intégrité des données est particulièrement évident si les données sont transmises sur un réseau non sécurisé, comme Internet, où une attaque de l'homme du milieu peut facilement être montée. L'intégrité est renforcée par des fonctions mathématiques appliquées au message transmis.

Non-répudiation : La répudiation est le refus par l'une des entités impliquées dans une communication d'avoir participé à tout ou partie de la communication. La non-répudiation est une protection contre la répudiation et peut être de deux types.

- La non-répudiation avec la preuve d'origine fournit au destinataire des données des preuves qui prouvent l'origine des données et protège ainsi le destinataire contre une tentative de l'expéditeur de refuser faussement l'envoi des données. Son but est de prouver qu'une

transaction particulière a eu lieu, en établissant la responsabilité des informations sur un événement ou une action particulière envers son entité d'origine.

- La non-répudiation avec la preuve de réception fournit à l'expéditeur des données des preuves prouvant que les données ont été reçues telles qu'adressées et protège ainsi l'expéditeur contre une tentative du destinataire de nier faussement la réception des données.

Pour les lecteurs qui peuvent se sentir intimidés par le jargon mathématique associé à la cryptographie, nous avons essayé d'expliquer les mathématiques associées à la cryptographie de manière claire et simple. Notre intention est de démystifier les concepts et les termes entourant la cryptographie.[4]

## 2.2 Définition de la cryptographie

. Un cryptosystème est un tuple (P, C, K, E, D) satisfaisant aux propriétés suivantes :

P est l'ensemble (fini) de textes en clair ;

C'est l'ensemble (fini) de textes chiffrés ;

3. K est l'ensemble (fini) de clés ;

4. E = {Ek: k ∈ K} est une famille de fonctions de chiffrement Ek: P → C;

5. D = {Dk: k ∈ K} est une famille de fonctions de déchiffrement Dk: C → P;

6. Pour tout e ∈ K il existe un d ∈ K tel que nous avons

$$Dd\,(Ee\,(p)) = p \text{ pour tous les textes en clair } p \in P.$$

Dans bon nombre des descriptions ci-dessous, deux parties communicantes seront appelées Alice et Bob, il s'agit de la nomenclature commune dans le domaine de la cryptographie et de la littérature pour faciliter l'identification des parties communicantes. S'il y a une troisième et une quatrième partie à la communication, elles seront appelées respectivement Carol et Dave. Une partie malveillante est appelée Mallory, une écoute indiscrète comme Ève et une tierce partie de confiance comme Trent. Figure 2.2

Enfin, la cryptographie est la plus étroitement associée au développement et à la création des algorithmes mathématiques utilisés pour crypter et déchiffrer les messages, tandis que la cryptanalyse est la science de l'analyse et de la rupture des schémas de cryptage. La cryptologie est le terme générique se référant à la vaste étude de l'écriture secrète, et englobe à la fois la cryptographie et la cryptanalyse.

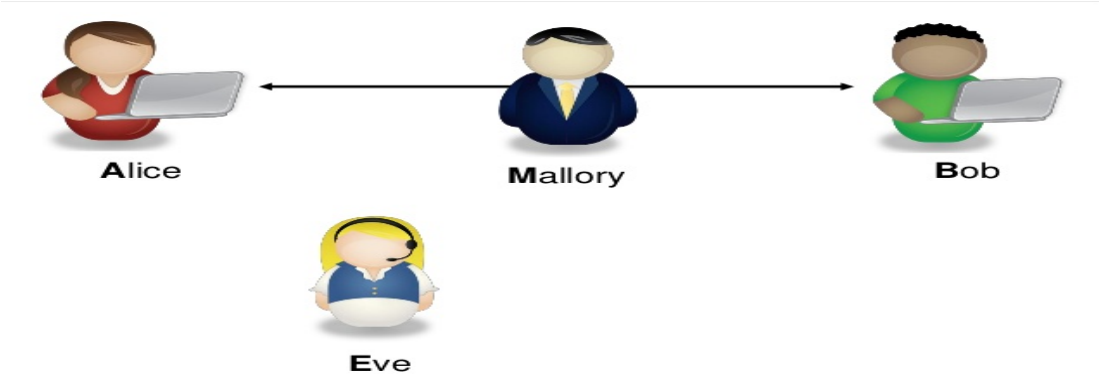



Figure 2.2 : modèle de cryptage

## 2.3 Mécanisme de la cryptographie

Le processus de chiffrement et de déchiffrement est le principal mécanisme qui fonctionne et guide le flux de données. La cryptographie a deux modes appelés clé publique et clé secrète. La clé est généralement définie comme l'information secrète qui doit être transférée sur le réseau. L'utilisation d'une clé secrète est parfois connue sous le nom de clé symétrique et celle d'une clé asymétrique est connue sous le nom de clé publique. Le fonctionnement de la clé secrète est vraiment simple. Les informations d'origine sont transformées en contenu crypté à l'aide de la clé secrète, puis à l'aide d'une autre clé secrète, elles sont à nouveau transformées en une forme lisible. Le fonctionnement de la clé publique est un peu différent. Dans la transformation asymétrique, la clé privée ou secrète est utilisée pour transformer les données originales sous forme chiffrée, puis à l'autre extrémité la clé publique est utilisée pour reconvertir les données en données déchiffrées. La clé publique fournit une transformation lente des données et peut-être utilisée pour convertir une petite quantité de données.

**2.3.1 Chiffres symétriques :** un type de chiffrement utilisé pour le chiffrement des données et rendu l'objet illisible pour l'autre en utilisant le même ou le type identique de clé algorithmique pour chiffrer ou déchiffrer les données requises est appelé chiffrement symétrique. Les clés qui sont utilisées par les systèmes ayant des chiffrements symétriques peuvent partager ces clés avec les modules de déchiffrement, c'est-à-dire qu'elles sont également appelées chiffrements symétriques partagés. Les performances de travail des chiffres symétriques sont bien plus rapides que celles des chiffres asymétriques. Ainsi, les chiffres symétriques sont le meilleur moyen de protéger les informations privées ou personnelles.

**2.3.2 Chiffres asymétriques :** un autre type de chiffrement important à l'aide d'ID de chiffrement est le chiffrement asymétrique, il est assez similaire à celui des chiffrements symétriques mais la seule différence entre le chiffrement symétrique et asymétrique est que la clé utilisée pour le chiffrement et le déchiffrement ne sont pas identiques. Ainsi, il existe deux formes différentes de clés utilisées dans le processus, l'une est appelée clé publique et l'autre est privée. Les utilisateurs peuvent utiliser la clé publique localement pour le partage tandis que la clé privée est la clé secrète. Les systèmes sont appelés asymétriques car lorsque les utilisateurs utilisent ce chiffre pour transmettre du texte, il utilise donc la clé publique pour chiffrer et le récepteur utilise la clé privée pour déchiffrer, c'est pourquoi le système est appelé ainsi.

## 2.4 Types d'algorithme cryptographique :

Il existe plusieurs façons de classer les algorithmes cryptographiques. Aux fins du présent document, elles seront classées en fonction du nombre de clés utilisées pour le chiffrement et le déchiffrement, et définies en fonction de leur application et de leur utilisation. Les trois types d'algorithmes qui seront discutés sont :

Cryptographie à clé secrète (SKC) : utilise une seule clé pour le chiffrement et le déchiffrement, également appelé cryptage symétrique. Principalement utilisé pour la vie privée et la confidentialité.

Cryptographie à clé publique (PKC) : utilise une clé pour le chiffrement et une autre pour le déchiffrement, également appelé cryptage asymétrique. Principalement utilisé pour l'authentification, la non-répudiation et l'échange de clés.

Fonctions de hachage : utilise une transformation mathématique pour « crypter » irréversiblement les informations, fournissant une empreinte numérique. Principalement utilisé pour l'intégrité des messages.

**2.4.1 Cryptographie à clé secrète :** [b2] [b3] [b4] Les méthodes de cryptographie à clé secrète utilisent une seule clé pour le chiffrement et le déchiffrement. Comme le montre la figure 1 A, l'expéditeur utilise la clé pour crypter le texte en clair et envoie le texte chiffré au récepteur. Le destinataire applique la même clé pour déchiffrer le message et récupérer le texte en clair. Étant donné qu'une seule clé est utilisée pour les deux fonctions, la cryptographie à clé secrète est également appelée cryptage symétrique (Figure 2.3).

Avec cette forme de cryptographie, il est évident que la clé doit être connue à la fois de l'expéditeur et du destinataire, c'est en fait le secret. La plus grande difficulté avec cette approche, bien sûr, est la distribution de la clé (plus à ce sujet plus tard dans la discussion sur la cryptographie à clé publique).

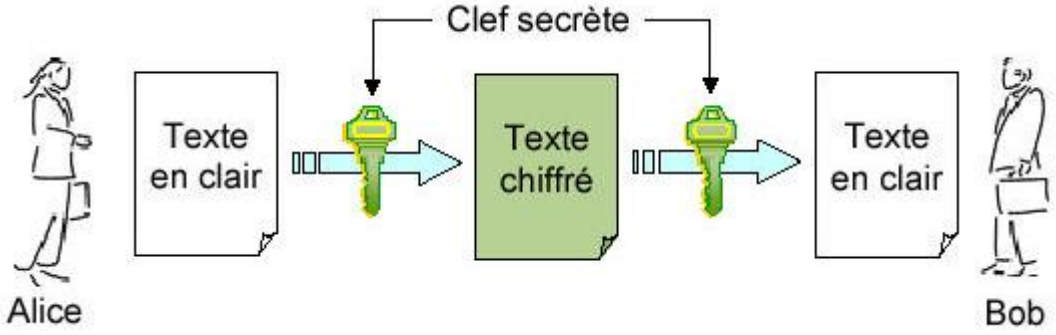



Figure 2.3 : Cryptographie à clé secrète

Les algorithmes de cryptographie à clé secrète utilisés aujourd'hui - ou, du moins, importants aujourd'hui même s'ils ne sont pas utilisés - comprennent :

**Data Encryption Standard (DES):** est un chiffrement par bloc à clé symétrique publié par le National Institute of Standards and Technology (NIST).

DES est une implémentation d'un chiffrement Feistel. Il utilise une structure Feistel 16 rondes. La taille de bloc est de 64 bits. Bien que la longueur de la clé soit de 64 bits, DES a une longueur de clé effective de 56 bits, car 8 des 64 bits de la clé ne sont pas utilisés par l'algorithme de chiffrement (fonctionnent uniquement comme des bits de contrôle).

**Advanced Encryption Standard (AES) :** est un chiffre itératif plutôt que Feistel. Il est basé sur un « réseau de substitution-permutation ». Il comprend une série d'opérations liées, dont certaines impliquent le remplacement d'entrée par des sorties spécifiques (substitutions) et d'autres impliquent un brassage de bits (permutations).

**Algorithme international de chiffrement des données (IDEA) :** cryptosystème à clé secrète écrit par Xuejia Lai et James Massey, en 1992 et breveté par Ascom, un chiffrement de bloc SKC 64 bits à l'aide d'une clé 128 bits. Également disponible à l'international.

Chiffres Rivest (alias Code de Ron): Nommé pour Ron Rivest, une série d'algorithmes SKC.

**RC1 :** conçu sur papier mais jamais implémenté.

**RC2 :** un chiffrement par blocs de 64 bits utilisant des clés de tailles variables conçues pour remplacer DES. Son code n'a pas été rendu public, bien que de nombreuses entreprises aient autorisé le RC2 à être utilisé dans leurs produits.

**RC3 :** trouvé cassable pendant le développement.

**RC4 :** un chiffrement de flux utilisant des clés de tailles variables, il est largement utilisé dans les produits de cryptographie commerciales. (L'algorithme utilisé dans notre application)

**RC5 :** un chiffrement par bloc prenant en charge une variété de taille de blocs (32, 64 ou 128 bits), de tailles de clé et de nombre de chiffrements passe sur les données.

**RC6 :** chiffrement par blocs de 128 bits basés surs, et une amélioration par rapport à RC5, RC6 était l'un des algorithmes AES Round 2.

3.2. Cryptographie à clé publique

**2.4.2 La cryptographie à clé publique :** est considérée comme le nouveau développement le plus important de la cryptographie au cours des 300 à 400 dernières années. Le PKC moderne a été décrit pour la première fois par le professeur Martin Hellman de l'Université de Stanford et l'étudiant diplômé Whitfield Diffie en 1976. Leur article décrivait un système de cryptage à deux clés dans lequel deux parties pouvaient s'engager dans une communication sécurisée sur un canal de communication non sécurisé sans avoir à partager une clé secrète (Figure 2.4 ).

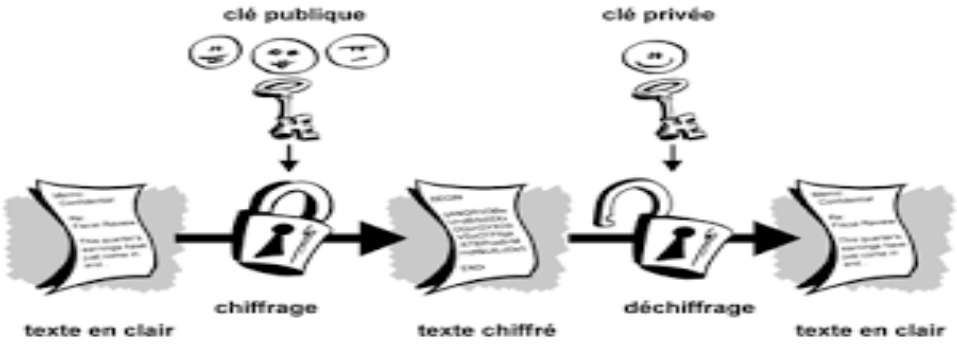



Figure 2.4 : Cryptographie à clé publique

Les PKC utilisés aujourd'hui pour l'échange de clés ou les signatures numériques comprennent :

**RSA :** est un algorithme de cryptage, utilisé pour transmettre en toute sécurité des messages sur Internet. Il est basé sur le principe qu'il est facile de multiplier de grands nombres, mais la factorisation de grands nombres est très difficile. Par exemple, il est facile de vérifier que 31 et 37 se multiplient à 1147, mais essayer de trouver les facteurs de 1147 est un processus beaucoup plus long.

**Diffie-Hellman :** après la publication de l'algorithme RSA, Diffie et Hellman ont mis au point leurs propres algorithmes. Diffie-Hellman est utilisé uniquement pour l'échange de clés à clé secrète, et non pour l'authentification ou les signatures numériques.

**Algorithme de signature numérique (DSA) :** l'algorithme spécifié dans la norme de signature numérique (DSS) du NIST, offre une capacité de signature numérique pour l'authentification des messages.

**Normes de cryptographie à clé publique (PKCS) :** un ensemble de normes et de directives interopérables pour la cryptographie à clé publique, conçu par RSA Data Security Inc.

**2.4.3 Fonctions de hachage :** Les fonctions de hachage, également appelées résumer de messages et cryptage unidirectionnel, sont des algorithmes qui, essentiellement, n'utilisent aucune clé. Au lieu de cela, une valeur de hachage de longueur fixe est calculée sur la base du texte en clair, ce qui rend impossible la récupération du contenu ou de la longueur du texte en clair. Les algorithmes de hachage sont généralement utilisés pour fournir une empreinte numérique du contenu d'un fichier, souvent utilisé pour s'assurer que le fichier n'a pas été modifié par un intrus ou un virus. Les fonctions de hachage sont également couramment utilisées par de nombreux systèmes d'exploitation pour crypter les mots de passe. Les fonctions de hachage fournissent donc un mécanisme pour garantir l'intégrité d'un fichier. (Figure 2.5)

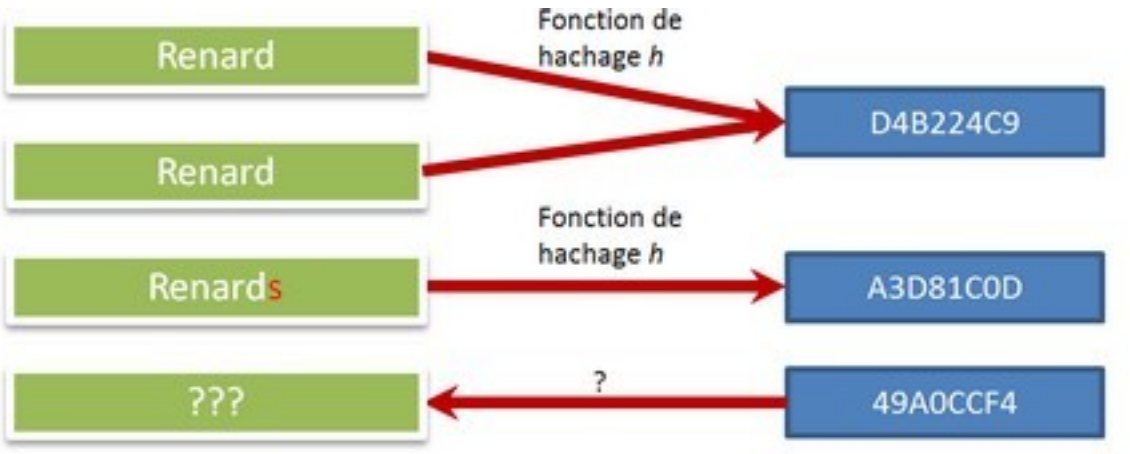



Figure 2.5 Exemple d'une fonction de hachage

Les algorithmes de hachage couramment utilisés aujourd'hui incluent :

**Algorithmes message digest (MD):** une série d'algorithmes orientés octets qui produisent une valeur de hachage de 128 bits à partir d'un message de longueur arbitraire.

**Secure Hash Algorithme (SHA) :** algorithme pour le secure hash standard (SHS) du NIST.

**RIPEMD :** une série de résumés de messages provenant initialement du projet RIPE (RACE Integrity Primitif évaluation). RIPEMD-160 a été conçu par Hans Dobbertin, Antoon Bosselaers et Bart Preneel, et optimisé pour les processeurs 32 bits pour remplacer les fonctions de hachage 128 bits alors en vigueur. Les autres versions incluent RIPEMD-256, RIPEMD-320 et RIPEMD-128.

**Ed2k :** nommés pour le réseau E'onkey2000 (ed2 K), le hachage ed2k est un hachage racine d'une liste de hachage MD4 d'un fichier donné. Un hachage racine est utilisé sur les réseaux de transferts de fichiers peer-to-peer, où un fichier est divisé en morceaux, chaque bloc a son propre hachage MD4 qui lui est associé et le serveur conserve un fichier qui contient la liste de hachage de tous les blocs. Le hachage racine est le hachage du fichier de liste de hachage.

## 2.5 La multiplicité des techniques de cryptage :

Alors, pourquoi existe-t-il autant de types différents de schémas cryptographiques ? Pourquoi ne pouvons-nous pas faire tout ce dont nous avons besoin avec un seul ?

La réponse est que chaque schéma est optimisé pour certaines applications cryptographiques spécifiques. Les fonctions de hachage, par exemple, sont bien adaptées pour garantir l'intégrité des données car toute modification apportée au contenu d'un message entraînera le récepteur à calculer une valeur de hachage différente de celle placée dans la transmission par l'expéditeur. Comme il est hautement improbable que deux messages différents produisent la même valeur de hachage, l'intégrité des données est assurée avec un degré de confiance élevé. (Figure 2.6)

La cryptographie à clé secrète, d'autre part, est parfaitement adaptée au cryptage des messages, assurant ainsi l'intimité et la confidentialité. L'expéditeur peut générer une clé de session par

message pour crypter le message, le récepteur, bien sûr, a besoin de la même clé de session pour déchiffrer le message.

L'échange de clés, bien sûr, est une application clé de la cryptographie à clé publique (sans jeu de mots). Les schémas asymétriques peuvent également être utilisés pour la non-répudiation et l'authentification des utilisateurs, si le destinataire peut obtenir la clé de session chiffrée avec la clé privée de l'expéditeur, alors seul cet expéditeur aurait pu envoyer le message. La cryptographie à clé publique pourrait, en théorie, également être utilisée pour crypter des messages, bien que cela soit rarement fait car les valeurs de cryptographie à clé secrète peuvent généralement être calculées environ 1000 fois plus rapidement que les valeurs de cryptographie à clé publique.

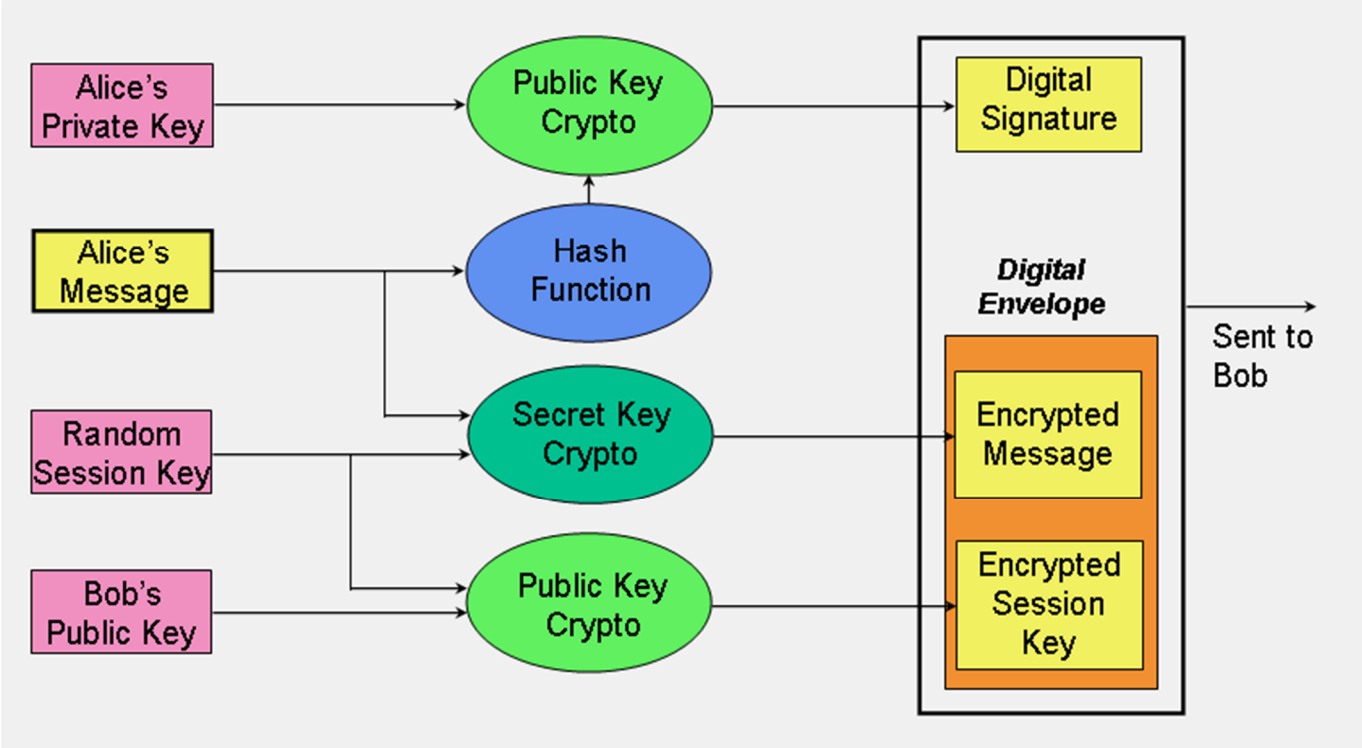



Figure 2.6 : Utilisation des trois techniques cryptographiques pour une communication sécurisée.

Actuellement, les systèmes cryptographiques sont divisés en deux principaux domaines d'étude :

La cryptographie symétrique et asymétrique. Alors que le cryptage symétrique est souvent utilisé comme synonyme de cryptographie symétrique, la cryptographie asymétrique englobe deux utilisations principales : le cryptage asymétrique et les signatures numériques.

Par conséquent, nous pouvons représenter les deux groupes comme suit:

- Cryptographie à clé symétrique

  Cryptage symétrique

- Cryptographie asymétrique (ou cryptographie à clé publique)

  Cryptage asymétrique (ou cryptage à clé publique)

  Signatures numériques (peuvent ou non inclure le cryptage) [5]

**2.6 Cryptage symétrique vs asymétrique :** Le chiffrement ou les algorithmes de chiffrement se répartissent souvent en deux catégories, le chiffrement symétrique et asymétrique. La différence fondamentale entre ces deux méthodes de chiffrement réside dans le fait que les algorithmes de chiffrement symétriques utilisent une seule clé, tandis que les algorithmes de chiffrement asymétriques utilisent deux clés différentes mais liées. Cette distinction, bien qu'elle soit simple en apparence, explique les différences fonctionnelles entre les deux types de techniques de chiffrement et la façon dont elles sont utilisées.

**2.7 Avantages et inconvénients :** Les deux types de cryptage ont des avantages et des inconvénients comparatifs. Les algorithmes de chiffrement symétrique sont beaucoup plus rapides et nécessitent moins de puissance de calcul, mais leur principale faiblesse est la distribution des clés. Étant donné que la même clé est utilisée pour crypter et décrypter les informations, elles doivent être distribuées à tous ceux qui ont besoin d'accéder aux données, qui, logiquement, comportent une série de risques de sécurité (comme expliqués ci-dessus). En revanche, le chiffrement asymétrique résout le problème de la distribution des clés en utilisant des clés publiques pour le chiffrement et des clés privées pour le déchiffrement. Cependant, le compromis est que les systèmes de chiffrement asymétriques sont beaucoup plus lents que symétriques et nécessitent beaucoup plus de puissance de calcul en raison de la longueur plus longue de leurs clés.

### 2.8 Cryptanalyse :

La cryptanalyse est le processus d'étude des systèmes cryptographiques pour rechercher des faiblesses ou des fuites d'informations. La cryptanalyse est généralement considérée comme explorant les faiblesses des mathématiques sous-jacentes d'un système cryptographique, mais elle comprend également la recherche de faiblesses dans la mise en œuvre, telles que les attaques par canal latéral ou les entrées d'entropie faibles.

### 2.9 Niveaux d'attaque d'un système de cryptage :

Le chiffrement des données ne sera jamais une solution 100% sécurisée pour tous nos besoins de sécurité. La technique évolue continuellement pour produire des systèmes / algorithmes de cryptage plus sûrs et donc comme des techniques d'attaquant. Il existe principalement trois façons d'attaquer les systèmes de chiffrement :

- Trouver les clés cryptographiques (par exemple Brute Force et enregistreurs de frappe)
- Cryptanalyse (attaquant l'algorithme de cryptage lui-même)
- Une attaque basée sur le système, donc nous attaquons le logiciel qui implémente l'algorithme de chiffrement [6]

## 2.10 Conclusion

La cryptographie est un domaine particulièrement intéressant en raison de la quantité de travail qui est, par nécessité, effectuée en secret. L'ironie est que le secret n'est pas la clé de la bonté d'un algorithme cryptographique. Quelle que soit la théorie mathématique derrière un algorithme, les meilleurs algorithmes sont ceux qui sont bien connus et bien documentés car ils sont également bien testés et bien étudiés ! En fait, le temps est le seul véritable test de bonnes cryptographies, tout schéma cryptographique qui reste en service année après année est très probablement bon. La force de la cryptographie réside dans le choix (et la gestion) des clés, les touches plus longues résisteront mieux à l'attaque que les touches plus courtes.

*Chapitre 3*

# Méthode de Cryptage En RC4

# Chapitre 3 : Méthode de Cryptage En RC4

## 3.1 Introduction

Les problèmes de sécurité sont l'un des aspects les plus importants d'un système d'information. Données ou informations ne seront plus utiles si des personnes non autorisées ont volé les données ou informations. Le niveau de sécurité doit être en outre renforcé. Le fichier est une donnée importante qui contient des informations à échanger. Le dossier doit avoir un bon système de protection de sécurité pour être dans la livraison de l'archive ne fuit pas. Compte tenu de là l'utilisation des technologies de l'information dans tous les aspects tels que l'éducation, le gouvernement, l'industrie et autres, la sécurité des données doit être correctement prise en compte. Le système utilisé pour sécuriser les données est la cryptographie. Beaucoup des techniques cryptographiques peuvent être appliquées aux informations qui seront protégées, dont l'un est RC4.

## 3.2 Présentation

Rivest Cipher 4 : RC4 est un type de chiffrement de flux. Il traite les données d'unité ou d'entrée en même temps. L'unité ou les données sont un octet ou même parfois bits. De cette façon, le chiffrement ou le déchiffrement peut être mis en œuvre sur la longueur de la variable. Cet algorithme n'a pas à attendre une certaine quantité de données avant d'être traité ou à ajouter des données supplémentaires.
octets à chiffrer. L'exemple est RC4 comme le montre la figure 3.1

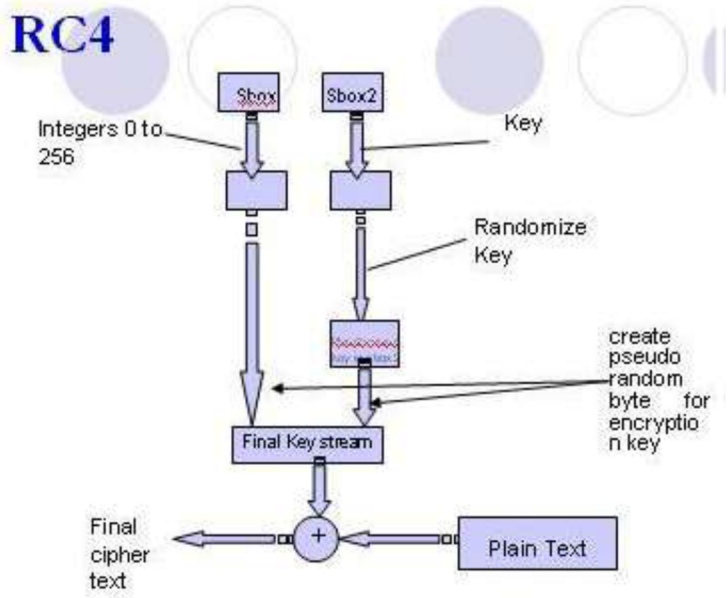



Figure 3.1 RC4 Algorithme

RC4 est un flux de chiffrement symétrique propriétaire créé par RSA Data Security, Inc. La distribution est initiée à partir d'un code source qui serait RC4 et publié anonymement en 1994. L'algorithme publié est très synonyme de l'implémentation du RC4 sur le produit officiel. RC4 est largement utilisé dans de multiples applications et est couramment exprimé très sûr. La génération

de clés RC4 est divisée en plusieurs étapes. La figure 2 décrit les étapes de la RC4. S-Box l'initialisation consiste à organiser le mot de passe occupé pour être le tableau d'octets. Pendant ce temps, la permutation est de faire le nouveau tableau d'octets aussi longtemps que le texte en clair disponible. La nouvelle clé sera cryptée dans le texte en clair. Il génère le texte chiffré.

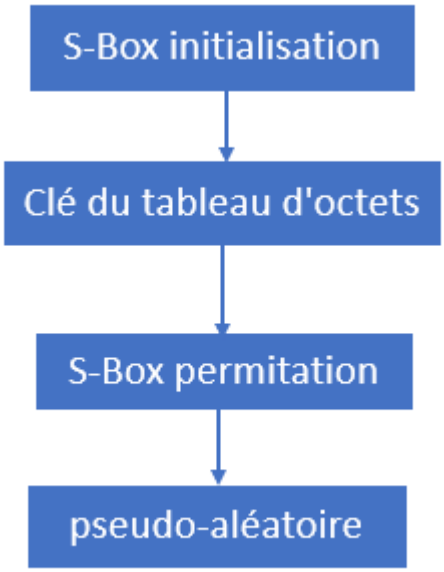



Figure 3.2 RC4 étapes

En cryptographie RC4, cet algorithme a une S-Box, S [0], S [1], ..., S [255], qui contient une permutation de là les nombres 0 à 255 où la permutation est une touche de fonction K, avec une longueur effective. La figure 3 décrit la génération de la S-Box.

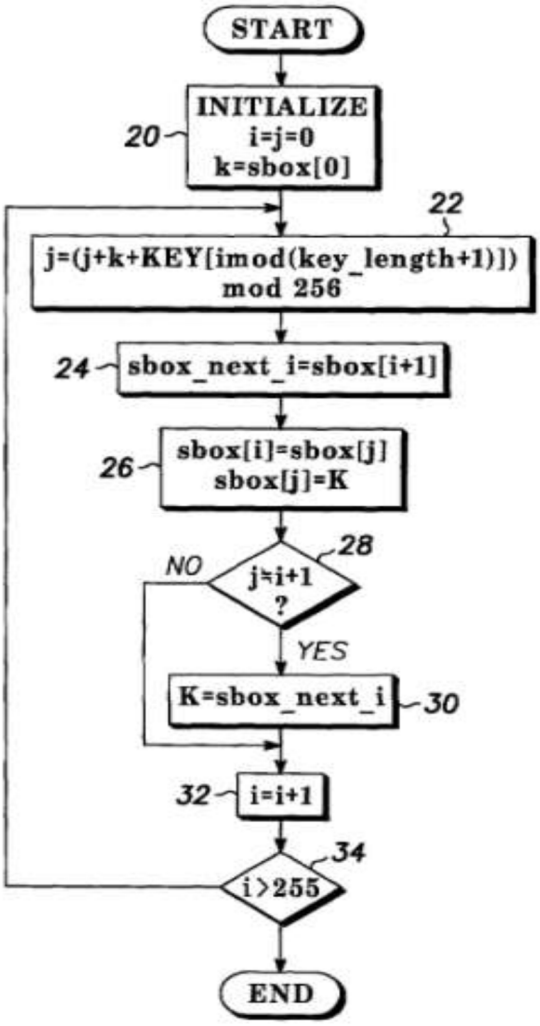



Figure 3.3 Générateur S-Box

La composition de la S-Box sur le même RC4 peut se produire. Cette disposition a abouti à des algorithmes sont vulnérables. Cela se produit parce que la valeur du même pseudo-aléatoire est souvent augmentée à plusieurs reprises, cela se produit parce que la clé utilisateur est répétée pour remplir un tableau de 256 octets. Bien que cette méthode permette l'utilisation d'atteindre 256 octets, personne n'utilise une telle longueur. Si l'utilisateur occupe une longueur de clé de huit octets, il sera répété 16 fois pour remplir le tableau d'octets. Le chiffrement RC4 est le processus XOR entre les octets de données et le flux d'octets pseudo-aléatoires généré à partir de la clé, alors l'attaquant sera en mesure de déterminer certains des messages d'origine en exécutant l'octet Processus XOR sur les deux ensembles d'octets de chiffrement lorsque certains octets de texte en clairs inconnus. Par exemple, « A » a réussi à intercepter deux messages différents chiffrés à l'aide d'un chiffrement de flux algorithme utilisant la même clé. "A" effectue XOR au processus de texte chiffré est pris avec succès pour éliminer l'influence des séries clés. Si le "A" a réussi à trouver le texte en clair de l'un des messages cryptés, alors "A" obtiendra facilement un autre message en clair sans connaître la clé.

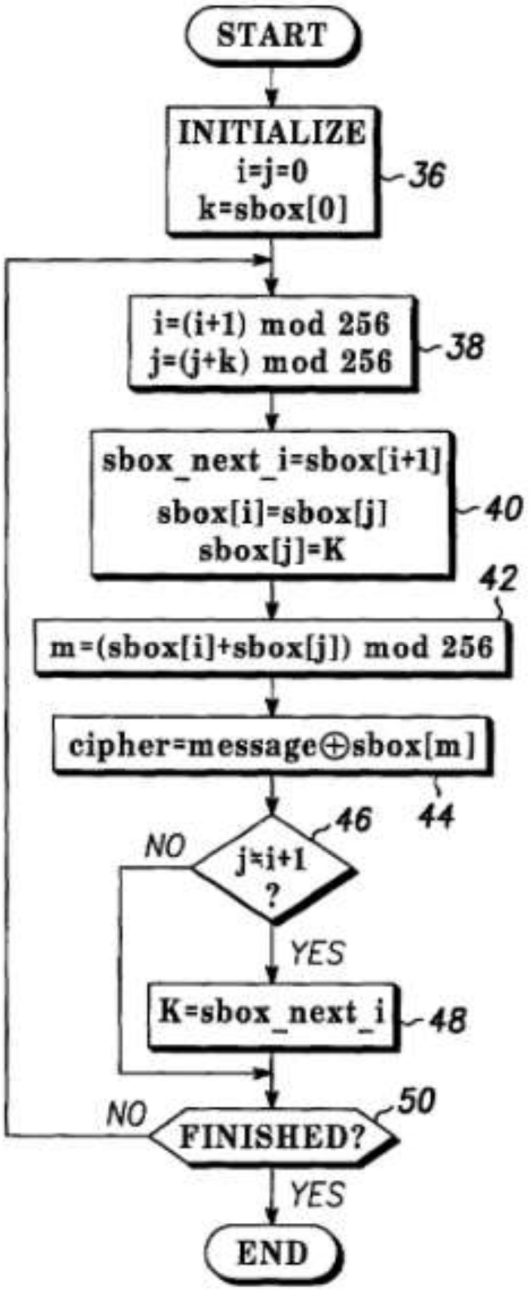



Figure 3.4 Processus de cryptage

L'algorithme RC4 comportes deux phases, la génération de clés et le chiffrement. La génération de clés est la première étape et le plus difficile dans cet algorithme. La clé de chiffrement est utilisée pour générer un chiffrement variable qui utilise deux tableaux, état et clés, et les résultats des opérations de fusion. Cette opération de fusion consiste à échanger, modulo et autres formules. Le fonctionnement de modulo est le processus qui produit la valeur résiduelle des actions. Pour exemple, 11 divisé par 4 est 2 avec le reste de la division est 3, si 7 modulo 4, il produira 3. La variable émerge du processus de génération de clés de chiffrement sera effectuée XOR avec le texte en clair pour produire texte crypté.

```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap values of S[i] and S[j]
    K := S[(S[i] + S[j]) mod 256]
    output K
endwhile
```

XOR est une opération logique qui compare deux bits binaires. Si la différence vaut, elle produira une valeur de 1. Si les deux bits sont égaux, le résultat est 0. Le destinataire déchiffrera alors le message en cliquant sur XOR de retour avec la même clé qui a généré le message à partir de texte brut. La figure 4 décrit le cryptage processus.

**3.3 Méthodologie :** RC4 génère le flux de clé pseudo-aléatoire. Tout comme un chiffrement de flux, il peut être utilisé pour le chiffrement par la combinaison du texte en clair à l'aide de XOR tandis que le déchiffrement se fait également de la même manière. Ce processus est similaire au chiffrement Vernam sauf le bit généré pseudo-aléatoire. Pour générer le flux de clés, le chiffrement utilisant un secret état interne qui se compose de deux parties :

1. une permutation de tous les 256 octets ASCII.

2. Deux index à huit bits, "i" et "j".

Une permutation est initialisée avec une clé de longueur variable, généralement entre 40 et 256 bits, en utilisant l'algorithme de programmation des clés. En outre, le flux binaire généré à l'aide d'algorithme de génération pseudo-aléatoire (PRGA). Plus précisément, RC4 fonctionne avec les étapes suivantes :

**Effectuer l'initialisation de S :** Comment ça marche S-box initialisation algorithme RC4 qui d'abord, S [0], S [1], ..., S [255], avec les nombres 0 à 255. Premièrement, la variable S sera remplie de nombre de 0 à 255 dans la séquence S [0] = 0, S [1] = 1, ..., S [255] = 255. Ensuite, initialisez un autre tableau, par exemple, le tableau K d'une longueur de 256. Le contenu du tableau K avec un clé qui est répété jusqu'à ce que l'ensemble du tableau K [0], K [1], ..., K [255] soit rempli. Le processus d'initialisation de la S-Box s'écrit suivi :

**Keystream** La recherche de valeurs Keystream se fait en échangeant à nouveau entre les éléments S, mais une valeur S stockée dans le K qui est ensuite utilisé comme flux de clés. Plus de détails peuvent être vus dans le pseudo-code suivant. [7]

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i
    mod keylength]) mod 256
    swap values of S[i] and
S[j]
endfor
```

### 3.4 résultat et discussion

Cette section décrit l'utilisation de l'algorithme RC4. Supposons que la clé est « THIS IS THE GOOD KEY ». Table 1 montre l'octet et l'index de la clé fournie.

**Table1 Key**

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| 84 | 72 | 73 | 32 | 32 | 73 | 83 | 32 | 84 | 72 |
| **T** | **H** | **I** | **S** | | **I** | **S** | | **T** | **H** |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 69 | 32 | 71 | 79 | 79 | 68 | 32 | 75 | 69 | 89 |
| **E** | | **G** | **O** | **O** | **D** | | **K** | **E** | **Y** |

À partir de la clé générée ci-dessus, les valeurs de la S-Box peuvent être déterminées en utilisant la formule précédente. Tableau 2 affiche la valeur S-Box de la clé précédente.

Table2S-Box values

| S-BOX GENERATOR | | | | | | | |
|---|---|---|---|---|---|---|---|
| 95 | 157 | 19 | 213 | 92 | 176 | 9 | 22 |
| 140 | 236 | 30 | 82 | 11 | 62 | 207 | 179 |
| 239 | 63 | 50 | 232 | 106 | 199 | 38 | 225 |
| 200 | 42 | 151 | 210 | 66 | 118 | 25 | 206 |
| 33 | 100 | 152 | 125 | 39 | 172 | 48 | 149 |
| 6 | 15 | 183 | 53 | 129 | 247 | 136 | 216 |
| 24 | 153 | 208 | 171 | 224 | 156 | 57 | 80 |
| 178 | 137 | 181 | 31 | 133 | 211 | 111 | 169 |
| 35 | 201 | 79 | 56 | 26 | 131 | 89 | 68 |
| 28 | 217 | 186 | 209 | 103 | 196 | 168 | 191 |
| 69 | 112 | 164 | 139 | 240 | 21 | 194 | 114 |
| 55 | 20 | 76 | 142 | 159 | 124 | 174 | 231 |
| 205 | 173 | 78 | 113 | 158 | 37 | 233 | 128 |
| 188 | 195 | 60 | 175 | 192 | 189 | 107 | 138 |
| 190 | 245 | 250 | 96 | 23 | 12 | 4 | 237 |
| 146 | 154 | 243 | 36 | 184 | 248 | 244 | 147 |
| 230 | 1 | 116 | 215 | 141 | 228 | 185 | 61 |
| 204 | 160 | 46 | 177 | 91 | 241 | 166 | 70 |
| 162 | 5 | 64 | 212 | 41 | 122 | 83 | 235 |
| 202 | 67 | 49 | 145 | 90 | 219 | 34 | 234 |
| 87 | 7 | 119 | 81 | 29 | 75 | 97 | 0 |
| 3 | 246 | 8 | 249 | 167 | 44 | 32 | 14 |
| 135 | 163 | 182 | 58 | 155 | 85 | 123 | 99 |
| 17 | 197 | 27 | 229 | 226 | 252 | 214 | 101 |
| 221 | 134 | 117 | 148 | 47 | 180 | 193 | 255 |
| 242 | 45 | 161 | 86 | 2 | 254 | 73 | 115 |
| 150 | 251 | 104 | 143 | 54 | 40 | 16 | 43 |
| 10 | 71 | 13 | 109 | 88 | 105 | 222 | 110 |
| 130 | 144 | 108 | 59 | 198 | 51 | 102 | 84 |
| 170 | 187 | 98 | 253 | 218 | 165 | 121 | 132 |
| 220 | 77 | 238 | 65 | 72 | 18 | 94 | 52 |
| 203 | 126 | 223 | 93 | 127 | 74 | 120 | 227 |

La clé est prête à être utilisée pour l'instant. Par exemple, le texte en clair est «NO ONE CAN SAVE FROM DEATH».

A. **Le chiffrement :** par exemple, dessinez le premier caractère du texte en clair. Le caractère est « N ». Le convertir en nombre d'octets, il en résulte 78 au format décimal.

Réglez également la première valeur de i et j sur zéro (i = 0, j = 0). Enfin, effectuez le calcul pour générer le « K » valeur

i = (i + 1) mod 256
= 1
j = (j + S[i]) mod 256
= 0 + 157
= 157
S[i] = S [1] = 157

S[j] = S [157] = 219 Après on permutons
S[i] = S [1] = 219
S[j] = S [157] = 157
t = (S[i] + S[j]) mod 256
= (219 + 157) mod 256
= 120
K = S[t]
= S [120]
= 146

La valeur « K » a été déterminée. Il sera utilisé pour convertir le texte en clair en texte chiffré en utilisant l'opération XOR.

La valeur suivante est l'octet de texte chiffré du premier caractère de texte en clair.

CT = CT ⊕ K
= 78⊕146
= 220

Le tableau 3 montre le résultat complet du texte chiffré. Le texte chiffré généré est

Ü~å•ð/|¯£bÌHebôÂ“qÔj±Lÿ¶Í”.

**Table 3**Encryption result

| ENCRYPTION PROCESS | | | | | |
|---|---|---|---|---|---|
| NO | PT | | K | CT | |
| 1 | N | 78 | 146 | 220 | Ü |
| 2 | O | 79 | 49 | 126 | ~ |
| 3 | | 32 | 197 | 229 | å |
| 4 | O | 79 | 218 | 149 | • |
| 5 | N | 78 | 85 | 27 | |
| 6 | E | 69 | 181 | 240 | ð |
| 7 | | 32 | 15 | 47 | / |
| 8 | C | 67 | 63 | 124 | \| |
| 9 | A | 65 | 238 | 175 | ¯ |
| 10 | N | 78 | 237 | 163 | £ |
| 11 | | 32 | 66 | 98 | b |
| 12 | S | 83 | 159 | 204 | Ì |
| 13 | A | 65 | 9 | 72 | H |
| 14 | V | 86 | 51 | 101 | e |
| 15 | E | 69 | 39 | 98 | b |
| 16 | | 32 | 212 | 244 | ô |
| 17 | F | 70 | 132 | 194 | Â |
| 18 | R | 82 | 193 | 147 | “ |
| 19 | O | 79 | 62 | 113 | q |
| 20 | M | 77 | 153 | 212 | Ô |
| 21 | | 32 | 74 | 106 | j |
| 22 | D | 68 | 245 | 177 | ± |
| 23 | E | 69 | 9 | 76 | L |
| 24 | A | 65 | 190 | 255 | ÿ |
| 25 | T | 84 | 226 | 182 | ¶ |
| 26 | H | 72 | 133 | 205 | Í |

## B. Le décryptage :

Du texte chiffré “Ü~å•ð/|¯£bÌHebôÂ“qÔj±Lÿ¶Í” , le premier caractère est «Ü». Le convertir en nombre d'octets, il en résulte 220 au format décimal.

Définissez la première valeur de i et j sur zéro (i = 0, j = 0). Enfin, effectuez le calcul similaire au calcul précédent pour générer la valeur « K ».

i = (i + 1) mod 256
= 1
j = (j + S[i]) mod 256
= 0 + 157
= 157
S[i] = S [1] = 157
S[j] = S [157] = 219 Après on permutons
S[i] = S [1] = 219
S[j] = S [157] = 157
t = (S[i] + S[j]) mod 256
= (219 + 157) mod 256
= 120
K = S[t]
= S [120]
= 146

La valeur « K » a été déterminée. Il sera utilisé pour reconvertir le texte chiffré en texte clair à l'aide de XOR également.

La valeur suivante est l'octet de texte en clair du premier caractère de texte chiffré.

PT = CT ⊕ K
= 220 ⊕ 146
= 78

**Table 4** Decryption result

| DECRYPTION PROCESS | | | | | |
|---|---|---|---|---|---|
| NO | CT | | K | PT | |
| 1 | Ü | 220 | 146 | 78 | N |
| 2 | ~ | 126 | 49 | 79 | O |
| 3 | å | 229 | 197 | 32 | |
| 4 | • | 149 | 218 | 79 | O |
| 5 | | 27 | 85 | 78 | N |
| 6 | ð | 240 | 181 | 69 | E |
| 7 | / | 47 | 15 | 32 | |
| 8 | \| | 124 | 63 | 67 | C |
| 9 | ¯ | 175 | 238 | 65 | A |
| 10 | £ | 163 | 237 | 78 | N |
| 11 | b | 98 | 66 | 32 | |
| 12 | Ì | 204 | 159 | 83 | S |
| 13 | H | 72 | 9 | 65 | A |
| 14 | e | 101 | 51 | 86 | V |
| 15 | b | 98 | 39 | 69 | E |
| 16 | ô | 244 | 212 | 32 | |
| 17 | Â | 194 | 132 | 70 | F |
| 18 | “ | 147 | 193 | 82 | R |
| 19 | q | 113 | 62 | 79 | O |
| 20 | Ô | 212 | 153 | 77 | M |
| 21 | j | 106 | 74 | 32 | |
| 22 | ± | 177 | 245 | 68 | D |
| 23 | L | 76 | 9 | 69 | E |
| 24 | ÿ | 255 | 190 | 65 | A |
| 25 | ¶ | 182 | 226 | 84 | T |
| 26 | Í | 205 | 133 | 72 | H |

Le tableau 4 montre le résultat complet du texte en clair. Le texte en clair est « PERSONNE NE PEUT ÉPARGNER DE LA MORT ». [b5] [17]

## 3.5 Conclusion

RC4 est un algorithme intéressant, bien qu'il ne soit pas possible de casser systématiquement un système de cryptage arbitraire basé sur RC4, il existe de nombreux points où il peut échouer et probablement tous ne sont pas connus.

il est donc préférable de guérir en santé et de mettre en œuvre des algorithmes dans lesquels tant d'échecs ne sont pas connus, en particulier compte tenu du fait que le déploiement des mises à jour de La sécurité des systèmes informatiques est souvent en retard de plusieurs années. [8]

*Chapitre 4*

# Études générales sur la vidéo

# Chapitre 4 : Études générales sur la vidéo

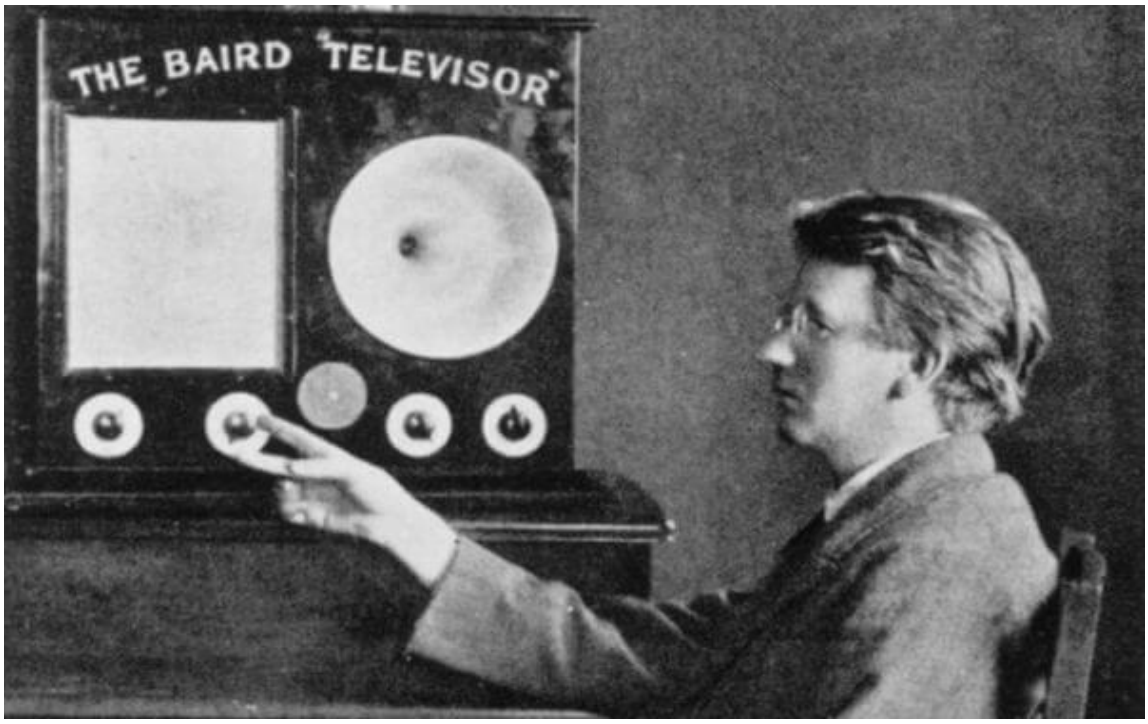
## 4.1 Historique

L'histoire de la vidéo est très curieuse. Nous sommes tellement habitués à appuyer sur un bouton et à regarder des images enregistrées à l'ordinateur ou la télévision que nous n'accordons pas d'importance à cette merveille de la technique.

L'inventeur de la vidéo était l'ingénieur écossais John Logie Baird en 1928. Il réalise les premiers enregistrements ou enregistrements sur un disque utilisé par les radiogrammes, de soixante-dix-huit tours par minute, qu'il visionne sur sa "Télévision Baird" avec une définition de 30 lignes.

En fait, les premiers pas ont été faits par le Russe Vladimir Kozmich Zvorykin, qui en 1923 a inventé un système d'enregistrement rudimentaire et qui n'a pas très bien fonctionné. John Logie a pendant plusieurs années modifié et perfectionné ce système pour y parvenir.

Mais la première démonstration d'un enregistrement vidéo a eu lieu en 1951 aux États-Unis aux mains de Mincom, filiale du puissant 3M / Scotch. Trois ans plus tard, le premier magnétoscope est construit, à l'initiative de la firme RCA.[9]




L'inventeur vidéo John Logie Baird

## 4.2 Introduction

**Définition 1 :** programme, film ou autres produit visuel contenant des images animées, avec ou sans son, enregistrées et sauvegardées numériquement ou sur cassette vidéo

**Définition 2 :**

Source multimédia visuelle qui combine une séquence d'images pour former une image animée. La vidéo transmet un signal à un écran et traite l'ordre dans lequel les captures d'écran doivent être affichées. Les vidéos ont généralement des composants audios qui correspondent aux images affichées à l'écran. [10]

### 4.3 Le signal vidéo

Une image est formée par la lumière incidente sur un support photosensible après avoir traversé l'objectif d'un appareil photo. Ce support photosensible peut être un film photographique ou un support électronique. Les supports photochimiques traditionnels utilisés en photographie et cinéma depuis leur origine sont remplacés dans presque tous les cas par des capteurs photoélectriques du type CCD (Charged-Coupled Device) ou CMOS (Complementary Metal Oxide Semiconductor) qui utilisent les nouveaux appareils photo pour la photographie, la vidéo et cinéma numérique. Figure 4.1

Ces appareils électroniques sont chargés d'attribuer une valeur de tension électrique qui correspond au niveau de luminosité ou à la couleur de chacun des points (pixels) qui composent l'image et convertissent ensuite ces impulsions électriques en valeurs binaires qui peuvent être stockées sur un support numérique. [b9]

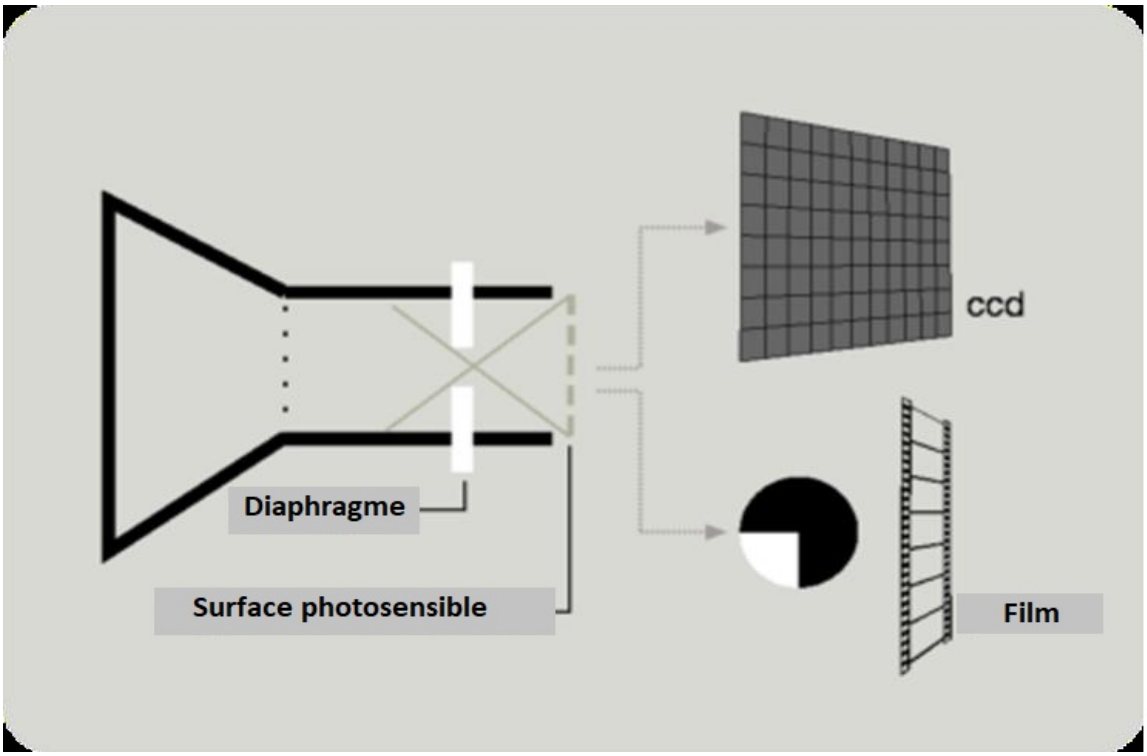



Figure 4.1 Formation de l'image sur différents supports.

**Formation d'images sur les capteurs CCD :**

Il existe deux zones dans le périphérique de capture d'image CCD : zone photoactive et la zone de transmission.

Dans la zone photoactive, les condensateurs accumulent une charge électrique proportionnelle à l'intensité de la lumière qu'ils reçoivent à ce pixel particulier. Un circuit de commande (zone de

transmission) il permet à chaque condensateur de transmettre cette charge, en mesurant sa tension et en la codant pour être stockée en mémoire numérique. Et ce processus est répété pour chacun des pixels de l'image et autant de fois par seconde que requis par le système vidéo avec lequel elle est enregistrée.

Les caméras, avec leurs dispositifs CCD, analysent les trois composantes de couleur de l'image : vert, bleu et rouge (en abrégé "RGB", de l'anglais Rouge, Vert, Bleu). À partir de ces composants, les cellules photoélectriques sont capables d'enregistrer n'importe quelle couleur visible avec toutes ses nuances. Pour décomposer une image en ses canaux de couleur RVB, des filtres de couleur appelés prismes dichroïques sont utilisés. Ainsi, les caméras professionnelles ont trois CCD et se consacreront chacune à numériser chaque composante couleur de l'image.

Cependant, la plupart des caméras fabriquées utilisent un seul CCD utilisant la technologie de masque de Bayer, qui fournit un cadre pour chaque carré de quatre pixels, avec un pixel enregistrant la lumière rouge, une autre lumière bleue et deux pixels. Réservé à la lumière verte (tout comme elle se produit dans l'œil humain, qui est plus sensible à la lumière verte qu'aux couleurs rouges ou bleues). Figure 4.2

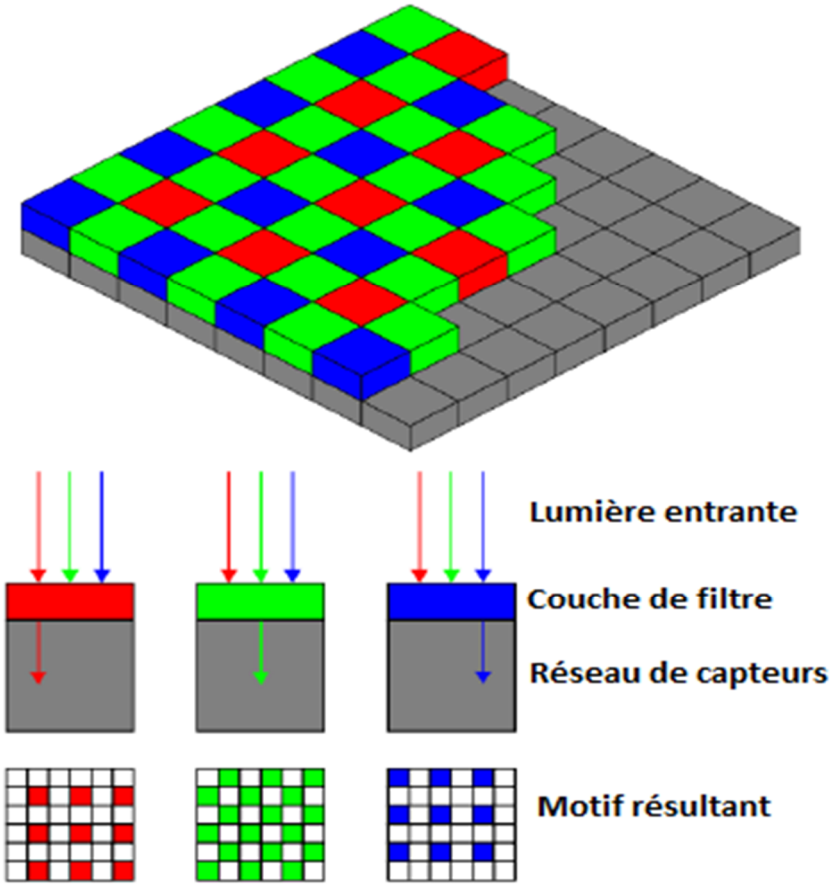



Figure 4.2 Structure d'un CCD Bayer.

Le résultat final avec l'utilisation d'un seul CCD est donc plus favorable aux informations de luminosité qu'aux informations de couleur. Par conséquent, une meilleure qualité est obtenue en utilisant des caméras avec trois capteurs CCD capables d'analyser séparément les trois sources de couleurs primaires (RVB). Pour numériser l'image avec trois capteurs, le prisme dichroïque sépare les composantes rouge, verte et bleue et trois signaux indépendants sont codés, contenant chacun

les informations de couleur correspondant à chacun des pixels de l'image. Ces systèmes sont plus chers que ceux basés sur des masques de couleur sur un seul CCD et le signal numérique résultant est plus grand car il contient les informations de couleur complètes de tous les pixels.

La résolution, ou le degré de détail avec lequel la photographie reproduit le sujet capturé, dépendra du nombre de cellules photoélectriques du CCD. Plus le nombre de pixels est élevé, plus la résolution est élevée.

**Formation d'image dans les capteurs CMOS** La technologie du capteur CMOS (Oxyde métallique semi-conducteur complémentaire) est basé, comme le capteur CCD, sur l'accumulation une charge électrique pour chaque pixel qui varie en relation directe

Avec l'intensité de la lumière reçue par le capteur. Contrairement au CCD, le CMOS numérise les informations reçues pixel par pixel. Étant donné que le processus de numérisation se produit sur le pixel lui-même, les capteurs CMOS éliminent les effets indésirables tels que la propagation de la lumière aux pixels adjacents, ont une vitesse de réponse plus élevée pour les mêmes conditions d'éclairage et consomment moins. Au contraire, ils présentent une qualité d'image inférieure à celle des CCD pour les mêmes conditions d'éclairage, ils nécessitent donc généralement un minimum d'éclairage pour donner une réponse optimale.

**L'interopérabilité :** Une fois les images encodées dans un signal électrique, les informations peuvent être stockées, dans des appareils analogiques ou numériques, ou transmises par un réseau de télécommunications et présentées dans les différents appareils pour recevoir et reproduire des images en mouvement.

Pour garantir la compatibilité des équipements de capture, d'enregistrement, de transmission et de réception d'images, il a fallu dès le début de la télévision établir des normes technologiques internationales. Grâce à ces normes techniques, les différents modèles de télévision utilisés dans le monde ont été établis, spécifiant des aspects tels que la résolution d'image, la fréquence d'images par seconde ou les processus de numérisation.

**Résolution spatiale :** La résolution est la quantité d'informations numérisées par le capteur et détermine la capacité de l'image à reproduire les détails. La résolution spatiale est appelée le nombre total de pixels qui composent l'image, bien que le nombre de pixels horizontaux et verticaux soit généralement indiqué. Plus la résolution spatiale est élevée, meilleure est la qualité de l'image. Donc, quand on se réfère à une image de 1 920 pixels horizontaux par 1 080 verticales sont devant une image de 2 073 600 pixels de résolution spatiale. C'est ce qui, sur le marché national de la photographie, s'exprime par simplicité en résolution de 2 mégapixels. Mais dans l'industrie vidéo professionnelle et La postproduction utilise généralement la forme 1920x1080 la plus précise.

Pour les résolutions plus élevées utilisées dans le cinéma numérique, une autre façon est généralement utilisée pour indiquer la résolution spatiale : pour le format 1 :85, l'abréviation 2K est utilisée pour la résolution 1998x1080 et 4K pour 3996x2160.

Fréquence d'images La fréquence d'images est le nombre d'images par seconde présentées pour créer l'illusion du mouvement. Au cinéma, une fréquence de 24 images par seconde (fps) est

traditionnellement utilisée pour la capture, mais en projection, chaque image est présentée deux fois afin d'atteindre une fréquence de projection de 48 fps et d'éviter l'effet de scintillement.

Dans les environnements de vidéo et d'animation numériques, nous trouvons différentes fréquences d'images pour s'adapter aux différentes normes techniques ou caractéristiques du projet. Aux États-Unis, 30 images par seconde sont généralement utilisées et en Europe, 25 images par seconde pour une meilleure compatibilité avec la fréquence de l'énergie électrique utilisée dans ces zones géographiques.

## Fréquence d'images

La fréquence d'images est le nombre d'images par seconde présentées pour créer l'illusion du mouvement. Au cinéma, une fréquence de 24 images par seconde (fps) est traditionnellement utilisée pour la capture, mais en projection, chaque image est présentée deux fois afin d'atteindre une fréquence de projection de 48 fps et d'éviter l'effet de scintillement.

Dans les environnements de vidéo et d'animation numériques, nous trouvons différentes fréquences d'images pour s'adapter aux différentes normes techniques ou caractéristiques du projet. Aux États-Unis, 30 images par seconde sont généralement utilisées et en Europe, 25 images par seconde pour une meilleure compatibilité avec la fréquence de l'énergie électrique utilisée dans ces zones géographiques.

## Numérisation d'images

Dans les premiers temps de la télévision, afin d'augmenter la fréquence de présentation des images et d'éviter la perception d'un effet de scintillement, les normes techniques ont établi la division de chaque image ou image [Cadre] dans deux domaines [champ], la première composée des lignes impaires de l'image et la seconde des lignes paires. C'est ce qu'on a appelé un balayage entrelacé. Plus tard, avec l'avènement des systèmes informatiques, une autre norme a été définie pour l'exploration d'images consistant en un balayage continu, ligne après ligne, de toute la surface du cadre ou du cadre. C'est ce qu'on a appelé l'exploration progressive. Dans les paragraphes suivants, nous nous attarderons plus en détail sur chacune de ces deux modalités d'exploration d'images.

## Numérisation entrelacée

La technique vidéo entrelacée divise chaque image ou image [Cadre] dans deux domaines [champ] améliorant ainsi la perception du mouvement. La vitesse de balayage dans la norme européenne de télévision couleur PAL est de 25 images par seconde et donc de 50 champs par seconde.

À ses débuts, le balayage entrelacé a été implanté dans la télévision analogique précisément pour augmenter la fréquence d'exposition, car l'effet de scintillement est très perceptible à un taux de 25 images par seconde et disparaît complètement à 50. Cet effet sensoriel est produit par persistance rétinienne, c'est-à-dire la permanence des images dans la rétine de l'œil, ce qui facilite, dans le système de perception visuelle, l'illusion du mouvement.

Pour éviter le scintillement et assurer une perception continue des mouvements, la norme de télévision européenne a choisi d'augmenter le taux d'apparition à 50 images par seconde par balayage entrelacé.

Actuellement, les téléviseurs augmentent la fréquence d'exposition des images à 100 par seconde (téléviseurs à 100 Hz), répétant chaque image deux fois, obtenant ainsi une plus grande stabilité de la luminosité de chaque pixel. Figure 4.3

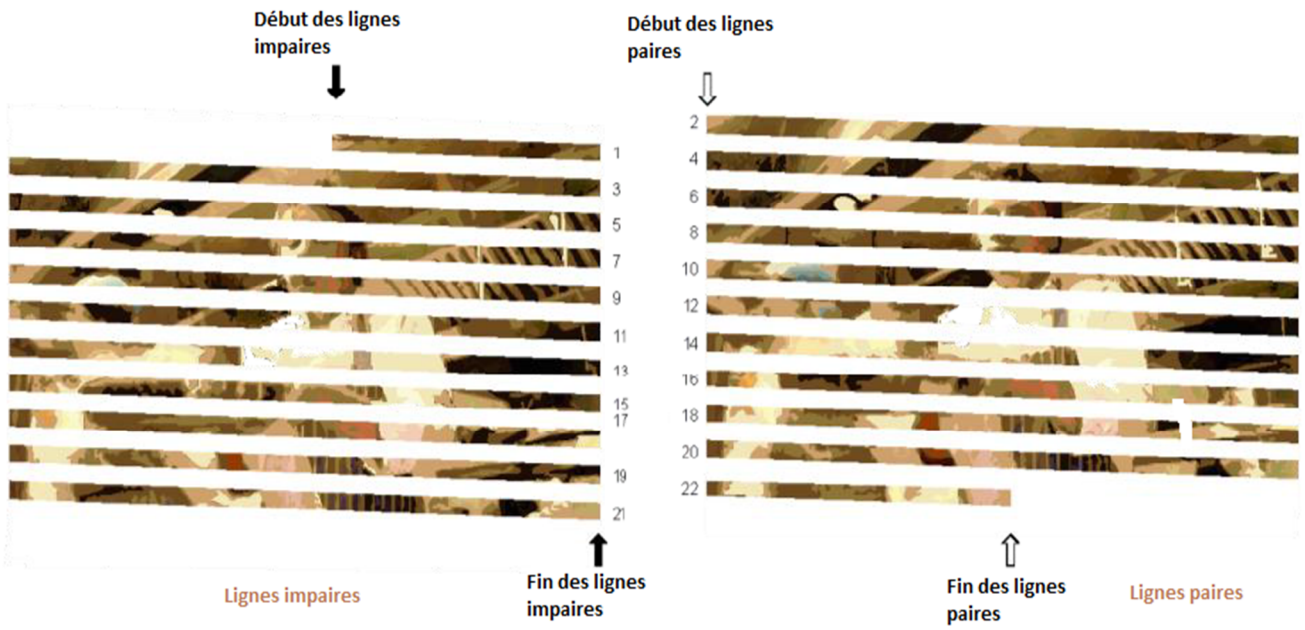



Figure 4.3 Direction du faisceau lors de la lecture des lignes d'image sur l'écran de la télévision à tube.

**Exploration progressive :** Le balayage progressif consiste en un balayage séquentiel de chaque ligne de l'image. L'effet de scintillement est compensé en utilisant une fréquence de balayage de 50 ou 100 Hz sur l'équipement d'affichage.

Les écrans d'ordinateur et la plupart des écrans LCD ou plasma haute définition utilisent un balayage progressif. Par conséquent, on peut affirmer que les environnements numériques ont largement adopté le système de balayage progressif. L'augmentation des dispositifs de visualisation basés sur le balayage progressif permet à l'ensemble du processus d'acquisition, de traitement, de transmission et de reproduction du signal de se faire avec le même système de balayage, ce qui évite les effets dérivés de la conversion entrelacée à la conversion progressive.

L'un des inconvénients du balayage progressif est qu'il nécessite plus de bande passante que la bande passante entrelacée pour la transmission du signal. C'est pourquoi les nouvelles normes de télévision haute définition continuent de considérer l'option de balayage entrelacé comme c'est le cas avec le format HDTV 1080i. D'autre part, comme nous l'avons vu précédemment, le système de balayage entrelacé PAL décompose le mouvement en 50 champs par seconde, réalisant ainsi une plus grande fluidité dans la représentation du mouvement qu'avec le système progressif à 25 images par seconde.

Lorsqu'un dispositif de surveillance à balayage progressif reçoit un signal entrelacé, il doit passer de l'entrelacer au progressif via un processus de conversion.

Les applications de montage vidéo et de post-production nous permettent de travailler avec les deux formes d'exploration, et bien que nous utilisions une vidéo avec les images explorées en entrelacement, nous pourrons la voir sur l'écran de l'ordinateur grâce à la conversion effectuée par le joueur lui-même.

**La proportion pixel :** Les pixels sont les plus petits éléments unitaires qui composent l'image numérique. Le système de télévision couleur PAL européen, que nous verrons plus loin dans ce chapitre (voir page 17), compte 625 lignes (576 lignes actives) et 720 pixels par ligne (702 pixels actifs). C'est pourquoi nous disons qu'une trame de télévision PAL de définition standard a une résolution de 702 x 576 pixels.

Le rapport de pixels, ou son rapport d'aspect, décrit la taille de sa hauteur par rapport à sa largeur. De nombreuses images numériques ont des pixels carrés. Cependant, le rapport hauteur / largeur en pixels des images vidéo varie selon les normes techniques de la télévision.

Pour calculer le rapport d'un pixel de télévision PAL de définition standard, nous divisons les 576 lignes par les 702 pixels actifs par ligne et le multiplions par le rapport d'aspect de la trame, 4/3. On obtient ainsi que le rapport hauteur / largeur du pixel dans l'image PAL soit de 1 094, alors qu'en NTSC il est de 0,9 (525/702 * 4/3). C'est-à-dire qu'en PAL, l'aspect pixel est plus large que haut et l'aspect pixel en NTSC est plus élevé que large. Dans certains formats vidéo panoramiques, le rapport L / H en pixels est encore plus large. Les ordinateurs utilisent à la place des pixels carrés par défaut.

Si nous voulons incorporer un graphique généré par ordinateur dans une édition vidéo, nous devons le créer avec le rapport d'aspect final du format vidéo, sinon il apparaîtra déformé. Par exemple, un cercle créé avec un pixel carré (rapport 1: 1) dans un flux vidéo NTSC sera compressé latéralement et dans un flux vidéo PAL, il sera étiré latéralement. Figure 4.4

Figure 4.4 Aspect qui présenterait un cercle créé avec un rapport d'aspect de 1 : 1 (ordinateurs) et affiché dans une configuration d'affichage pour le système PAL

(1094 : 1), à gauche, et dans une configuration d'affichage pour le système NTSC (0,9: 1), à droite.

Les programmes de création et d'édition d'images tels que Photoshop vous permettent de configurer le rapport hauteur / largeur des pixels pour s'adapter au format final dans lequel le graphique sera utilisé et éviter ces déformations. Par exemple, si vous affichez l'image d'une balle avec le rapport d'aspect en pixels défini pour PAL Panoramic dans Photoshop, elle sera compressée latéralement. Cependant, si l'option d'affichage avec le rapport d'aspect d'origine est activée, l'image est mise à l'échelle en laissant la circonférence parfaite sans la déformation ovale.

Il en va de même pour les programmes de montage vidéo. Une fois le fichier importé dans le dossier du projet, le programme d'édition ne reconnaît pas toujours l'aspect pixel du fichier vidéo, il doit donc être indiqué au programme. Pour découvrir quel aspect de pixel le fichier à, vous pouvez vérifier les caractéristiques du fichier, afin que vous puissiez ajuster le fichier et le projet vidéo avec les mêmes caractéristiques d'aspect de pixel.

Actuellement, la tendance des nouvelles normes de télévision et de vidéo haute définition est l'utilisation du pixel carré. Il est courant en post-production lorsque nous devons incorporer des matériaux avec d'autres formats pour effectuer une conversion précédente afin de travailler avec des pixels carrés.

Couleur dans les systèmes de codage de télévision et de luminance et de chrominance :

Comment la couleur est-elle reproduite à la télévision ? La couleur d'une image est synthétisée dans ses trois composantes chromatiques fondamentales : le rouge, le vert et le bleu.

Le système de mélange de couleurs utilisé est l'additif, qui peut former du blanc et le reste des couleurs visibles à l'œil humain à partir des couleurs primaires de la lumière (rouge, vert et bleu). Figure 5.5

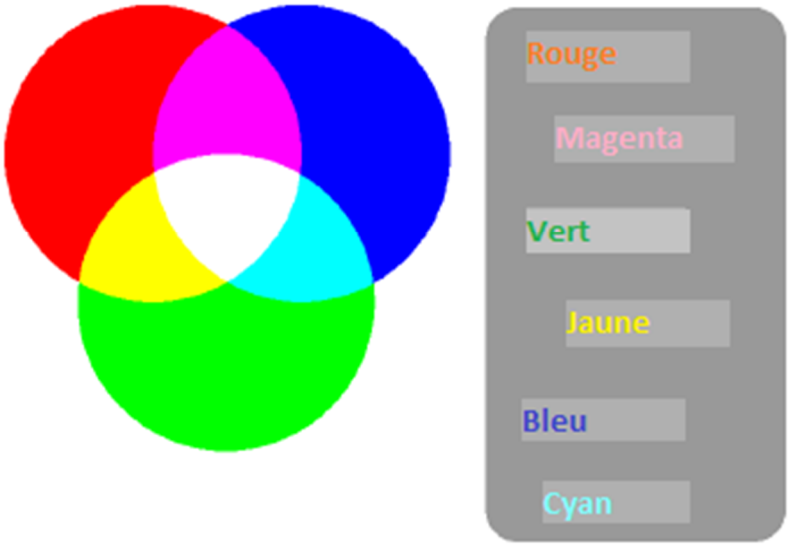



Figure 5.5 Mélange de couleurs additif : à partir des trois couleurs primaires de la lumière, le blanc et le reste des couleurs du spectre visible sont obtenus.

Les informations sur la luminosité et la couleur collectées par les pixels des caméras photographiques et vidéo doivent être codées de manière standardisée afin d'être ensuite interprétées par les différents dispositifs de stockage et de reproduction.

## Profondeur de couleur (profondeur de bits)

Chaque pixel peut être codé avec un nombre variable de bits. Le bit est l'unité minimale de codage binaire que seul peut avoir deux états : un ou zéro. Par conséquent, si seulement nous avons un peu pour décrire un pixel, nous pouvons l'utiliser pour indiquer s'il est blanc (1) ou noir (0). Si nous en avons plusieurs bits pour décrire un pixel, nous pouvons l'utiliser pour exprimer toute une gamme de niveaux de gris et l'utilisation de plusieurs bits pour chaque composante de couleur RVB nous permettra d'atteindre la précision des couleurs requise par une image photographique. Le nombre de bits utilisés pour chaque composant de la couleur est connu comme la profondeur de couleur ou la profondeur de bits (profondeur de bits des composants). Plus grande profondeur de couleur (plus de bits informations par pixel) signifie plus de couleurs disponibles représentation des couleurs plus précise. La profondeur de couleur la plus courante est de 8 bits par canal, c'est-à-dire une image 24 bits (8 bits pour la composante rouge, 8 pour le vert et 8 pour le bleu). C'est ce qu'on appelle aussi vraie couleur (True color) car c'est la résolution de couleur qui il est nécessaire pour une image de qualité photographique.

Pour les éléments graphiques composés de tons directs. Je pourrais utiliser une profondeur de couleur inférieure, mais 24 bits sont assez pour couvrir la capacité de perception de l'œil humain. Pour des applications de haute qualité telles que le cinéma numérique où certains outils de post-production peuvent être utilisés profondeur de couleur la plus élevée : 10 bits, 16 bits et même 32 bits par canal pour les images HDRI (High Dynamic Range) qui contiennent plus d'informations de brillance et de couleur que vous ne pouvez œil humain sur un moniteur numérique.

**Signal vidéo composite** Le signal vidéo composite est le signal vidéo analogique qui est utilisé pour la télévision dans les processus d'enregistrement, de diffusion et reproduction. Grâce à un seul câble coaxial, ils sont transportés les signaux de luminance, de chrominance et de signal synchronisme. En traitant toutes les informations ensemble, une certaine perte de signal, provoquant l'image finale couleurs et définition d'image de moins bonne qualité que nous obtiendrions avec un signal composant ou un signal RGB. Ce type de signal, malgré sa qualité inférieure, est le signal analogique sur le marché intérieur, grâce à sa simplicité de connexion et pour offrir une qualité d'image acceptable pour un réglage à domicile des écrans de résolution la norme. Le connecteur le plus courant pour transporter le signal vidéo composé est un RCA jaune (Figure 4.6), qui va généralement accompagner de deux autres connecteurs, rouge et blanc, qui portent le signal audio stéréo.

Figure 4.6 Connecteur RCA pour signal vidéo composite.

### Signal vidéo S-Vidéo

Le S-Vidéo, (vidéo séparée) est un système de transmission vidéo analogique qui code la luminance et la couleur séparément. Il a été créé pour offrir une meilleure qualité que la vidéo composite la sphère domestique. Il se compose de deux signaux : Y pour la luminance et C pour couleur, d'où l'abréviation Y. / C. Le signale Y porter les informations de luminance, c'est-à-dire vidéo en noir et blanc, tandis que C rend compte des valeurs de couleur. Le connecteur le plus utilisé pour le signal S-Vidéo est du type Mini-DIN à 4 broches (Figure 4.7). Les mini-DIN 7 sont également courantes broches.

Figure 4.7 Connecteur S-Vidéo.

## Signal vidéo composante

La séparation des informations de luminance et de chrominance pour utilisations professionnelles a été spécifié dans le soi-disant signal vidéo par composants qui est une adaptation du signal RGB. Sa fonction est respectant au maximum les niveaux de qualité obtenus à partir des caméras, indépendamment des limitations de bande passante typique de la transmission télévisée. C'est donc un type de signal utilisé dans les environnements de production professionnels et éventuellement dans un équipement de lecture vidéo élevé qualité.

Le triple signal vidéo appartenant aux couleurs rouge, vert et bleu, fourni par le dispositif de capture d'image, doit être transformé en un signal qui, d'une part, est compatible avec la télévision en noir et blanc et qui d'autre part n'occupe pas une largeur de bande supérieure au signal RGB d'origine. À votre destination finale, que ce soit un écran d'accueil ou un moniteur professionnel, ce sera nécessaire pour le reconvertir au signal RGB d'origine sans perte de qualité.

Les trois signaux correspondant au rouge, Vert et Bleu de l'image se transforment en trois autres qui représentent, d'une part, la luminance de l'image, c'est-à-dire l'image dans des tons de gris, et qui sont représentés par la lettre Y; et de l'autre, les deux sont obtenus signaux qui transportent les informations de couleur, appelés composants de la couleur R-Y et B-Y, comme nous le verrons continuation. Nous nous référons généralement à la vidéo par composants comme Y, $C_B$, $C_R$ ou comme Y, U, V. Figure 4.8


Figure 4.8 connecteur pour signal vidéo composant.

### Signal vidéo RGB

Dans la norme RGB, un canal séparé est utilisé pour chaque composante couleur. C'est le format naturel des deux équipes absorption et reproduction. (Figure 4.9)

Dans ce type de signal, la luminance ou la luminosité ne concerne pas indépendamment mais dépendra de l'intensité de chaque l'une des couleurs primaires.

Cette intensité dans le codage numérique 8 bits reste représentée en 256 valeurs différentes (de 0 à 255) pour chacune de couleurs primaires telles que le rouge pur correspondra (255, 0, 0) ; vert pur à : (0, 255, 0) ; et le bleu pur : (0, 0, 255). En conséquence, la cible (qui aime nous avons vu est la somme totale des trois couleurs primaires dans le système additif) sera représentée comme (255, 255, 255) et le noir comme (0, 0, 0).

Pour exprimer les couleurs de manière plus simple, codage hexadécimal, tel que F est la valeur maximale et 0 au minimum, laissant l'intensité de la couleur primaire représentée par des paires: FF0000 = rouge; 00FF00 = vert; 0000FF = bleu; FFFFFF = blanc; 000000 = noir. Le signal RGB utilise généralement des connexions avec SCART, BNC, RCA (avec un connecteur pour chaque couleur) ou avec un VGA.

Figure 4.9 Connecteur pour signal vidéo RGB.

## 4.4 Normes vidéo numériques

### Radiodiffusion numérique

L'arrivée de la télévision numérique a entraîné un tel changement aussi important que le passage du noir et blanc à la couleur. Non seulement contribué des images de meilleure qualité, il a

également ouvert des portes à des services tels que la réception mobile de télévision, interactivité, télévision à la demande ou services multimédias.

En Europe, le consortium DVB (Digital Video Broadcasting) a été responsable de l'élaboration des différentes normes la radiodiffusion numérique au début des années 90. Normes les plus utilisés actuellement sont le DVB-S, pour les transmissions par satellite ; DVB-C, pour les transmissions par câble ; et DVB-T pour les émissions de télévision numérique terrestre [b7] [b8].

### Encodage binaire et sous-échantillonnage des couleurs

La télévision numérique code le signal de manière binaire. Cette permet de reproduire une image identique à l'original à la fin d'une chaîne de transmission, sans aucune perte et sans incorporation de bruit. Mais pour réduire la bande passante requise pour la transmission d'une technique de codage appelée sous-échantillonnage des couleurs.

Le sous-échantillonnage des couleurs est un système de codage ce qui réduit les informations de chrominance du signal en profitant ce que la vision humaine est plus sensible à la luminosité qu'à la couleur. La norme pour les applications vidéo numériques professionnelles est le sous-échantillonnage 4: 2: 2, qui définit 4 échantillons pour la luminance (Y) et seulement deux échantillons pour chacun des signaux de différence de couleur (U et V). Tous les pixels portent informations de luminance, mais seulement un sur deux portes l'information sur les couleurs. Cette norme est utilisée pour la transmission de la télévision numérique et la perte d'informations sur les couleurs n'est pas perceptible.

### Haute définition (HD)

La télévision numérique a permis la mise en œuvre de normes de vidéo avec une résolution plus élevée que la norme de télévision PAL et NTSC. La haute définition prend en charge des résolutions plus élevées qu'anciens systèmes vidéo, avec des résolutions de 1280 × 720 et 1920 × 1080 pixels. Les grands réseaux de télévision américains et européens diffusent actuellement dans des formats haute définition 1080i (i = entrelacer] et 720p (p = progressif).Cependant, de nouvelles normes de compression comme le codec H264 réduits considérablement la bande passante nécessaire, donc tout présuppose une plus grande utilisation de 1080p avec numérisation progressif, même à des vitesses de 50 ou 60 images par seconde, particulièrement utile lors d'événements sportifs.

### Comité consultatif international des radiocommunications (CCIR)

Le CCIR est l'un des anciens organes de l'UIT (Union Télécommunications Association) qui a déterminé la norme d'exploration, de modulation et de transmission du signal de télévision en 1945.

### DVB (Digital Video Broadcasting)

La DVB est un organisme chargé de réglementer et de proposer les procédures de transmission des signaux de télévisions numériques compatibles. Il est composé de plus de 220 institutions et entreprises dans le monde et normes. Les propositions ont été largement acceptées en Europe et presque tous les continents, à l'exception des États-Unis et du Japon où ils coexistent avec d'autres systèmes propriétaires. [b6]

### 4.4 Formats vidéo numériques :

Comme pour les documents texte, les photographies ou les fichiers audio, la vidéo au format numérique est disponible dans différents formats ou extensions.

Lorsque nous parlons de formats vidéo, nous pouvons faire référence à plusieurs choses. Les plus courants, les formats physiques dans lesquels nous avons accès à un film, une série ou un documentaire. En ce sens, nous trouvons actuellement des DVD et des Blu-Ray, bien que certains d'entre nous gardent toujours dans un vieux placard VHS et peut-être certains Betacam.

Mais un deuxième sens où sens des formats vidéo fait référence à leur codage, car dans la vidéo numérique, comme avec un programme informatique, tout fichier est écrit dans un code spécifique. Dans les vidéos, le code influence la qualité de l'image, la qualité du son, qu'il inclut ou non des sous-titres et, surtout, la relation entre la qualité et la taille du fichier.

Ainsi, nous consommons actuellement du contenu audiovisuel numérique via des disques physiques (DVD, Blu-Ray), en streaming et via IPTV (télévision sur Internet), mais nous traitons également des fichiers vidéo numériques, notamment pour les contenus que nous générons nous-mêmes. Ensuite, nous passerons en revue les formats vidéo numériques les plus courants que nous pouvons trouver, quelle est leur origine et quels avantages ils offrent. Je m'excuse d'avance pour le charabia d'acronymes.


## Avi

Nous commençons par le format le plus populaire que nous trouverons. Les fichiers vidéo avec une extension .AVI proviennent d'un format sorti en 1992 et sont si populaires qu'ils sont lus par la plupart des téléviseurs intelligents, lecteurs DVD / Blu-Ray, consoles de jeux et systèmes d'exploitation.AVI est un acronyme pour Audio Video interleave et peu de gens savent qu'il a été créé par Microsoft comme alternative numérique sans dépendre d'un format physique comme le DVD alors populaire. Parmi ses avantages, il permet d'inclure plusieurs canaux audio et contenus hébergés générés avec différents codecs (AC3 ou MP3 pour l'audio, Divx ou Xvid pour la vidéo), ce qui peut être un avantage mais aussi un inconvénient selon les joueurs.

## MP4

MP4 ou MPEG-4 est l'un des formats les plus modernes, sorti en 1998 en tant que norme pour la lecture vidéo et audio dans un seul fichier numérique.MPEG est l'acronyme de Moving Pictures Experts groupes, le groupe d'experts qui a établi des normes numériques audio et vidéo et qui a été formé par deux organisations internationales, l'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale).En résumé, les formats MPEG et MPEG-2 ont été publiés respectivement en 1993 et .1995 en tant que normes pour le codage audio et vidéo numérique. Pour nous comprendre, tout DVD propose son contenu audiovisuel en MPEG-2 .MP4 prend également en charge plusieurs canaux audios, mais il a l'avantage de permettre plus de qualité d'image et de son dans un fichier plus léger, car il compresse mieux les données. Apple, par exemple, parie sur ce format et ses dérivés pour son contenu ITunes. Liés à MP4, nous pouvons trouver M4V (vidéo) ou M4A (audio).[16]

## MKV

Le format vidéo MKV est un format ouvert, gratuit à payer des redevances, et dont le nom complet est Matroska, comme les poupées russes traditionnelles. MKV est sorti fin 2002 et est devenu populaire grâce au fait qu'au sein d'un même fichier MKV, nous pouvons stocker, avec le canal audio, plusieurs canaux ou pistes audio et plusieurs pistes de sous- titres. Comme MP4, il offre une très bonne qualité audio et vidéo dans un petit espace. Et comme curiosité, le format WebM qui vous permet d'intégrer des vidéos en ligne via HTML, s'inspire de Matroska.

## FLV

Le format FLV où flash Video a été créé par Macromedia, puis acquis par Adobe. Ce format se trouve généralement sous la forme d'une extension FLV ou SWF.Comme les autres contenus Flash, les vidéos FLV sont destinées à être lues en ligne à partir du navigateur via adobe flash Player. Comme nous l'avons vu dans un article précédent, Flash cessera de se développer en 2020, bien que nous trouvions toujours des pages qui l'utilisent.

## MOV

J'ai déjà dit qu'Apple parie actuellement sur MP4 (et AAC) pour fournir du contenu multimédia. Mais son format vedette pendant de nombreuses années était MOV.MOV, de QuickTime Movie, est aussi appelé QuickTime file Format, et aujourd'hui c'est toujours le format par défaut pour QuickTime, le lecteur vidéo MacOs. Ce format peut également être trouvé dans de nombreuses caméras vidéo numériques, car il offre une très bonne qualité d'image et un son non compressé.

## WMV

De nombreux utilisateurs de Windows des années 90 et 00 se souviendront des formats WMV et WMVA, le premier pour la vidéo et le second pour l'audio.WMV a été lancé en 1999 et est l'acronyme de Windows Media Video, créé par Microsoft pour offrir la meilleure qualité vidéo possible via le streaming. Le format a connu une certaine popularité, en partie grâce à Windows media Player, le lecteur Windows par défaut pendant de nombreuses années et qui disparaîtra dans la dernière mise à jour de Windows 10. Bien qu'il n'offre pas une très bonne qualité, WMV

permettait de transmettre des vidéos en petits fichiers, ce qui était très pratique avec les connexions Internet de l'époque.[11]

## 4.5 Conclusion

Dans ce chapitre, nous avons défini ce que signifie le mot « vidéo », l'histoire et l'inventaire d'une première vidéo, Avec cela, je pense que nous couvrons toutes les sections

La technologie vidéo a d'abord été développée pour les systèmes de télévision , mais a évolué en de nombreux formats pour permettre l'enregistrement vidéo par les consommateurs et peut également être visionnée sur Internet.

*Chapitre 5*

# Cryptage de flux vidéo

# Chapitre 5 : Cryptage de flux vidéo

## 5.1 Introduction

Dans ce chapitre, nous présentons une application qui cryptera et sécurisera les flux vidéo par un modèle client / serveur. Nous avons établi une comparaison sur la qualité et la vitesse de l'opération de cryptage et de transmission. Nous utilisons l'algorithme de cryptage RC4. . Nous avons utilisé un ordinateur Intel (R) Core (TM) i3 ou i5 cadencé à 1,70 GHz avec 4,00 Go de RAM et un système d'exploitation Windows 10.

## 5.2 Présentation de l'application

### Langage de programmation :

Le langage choisi pour la réalisation de notre application est "Microsoft Visual c ++ / basic studio 2019"

Visual Basic est un langage de programmation et un environnement de développement créés par Microsoft. Il s'agit d'une extension du langage de programmation BASIC qui combine les fonctions et commandes BASIC avec des commandes visuelles.

Visual Basic fournit une interface graphique utilisateur qui permet au développeur de faire glisser et déposer des objets dans le programme ainsi que d'écrire manuellement le code du programme.

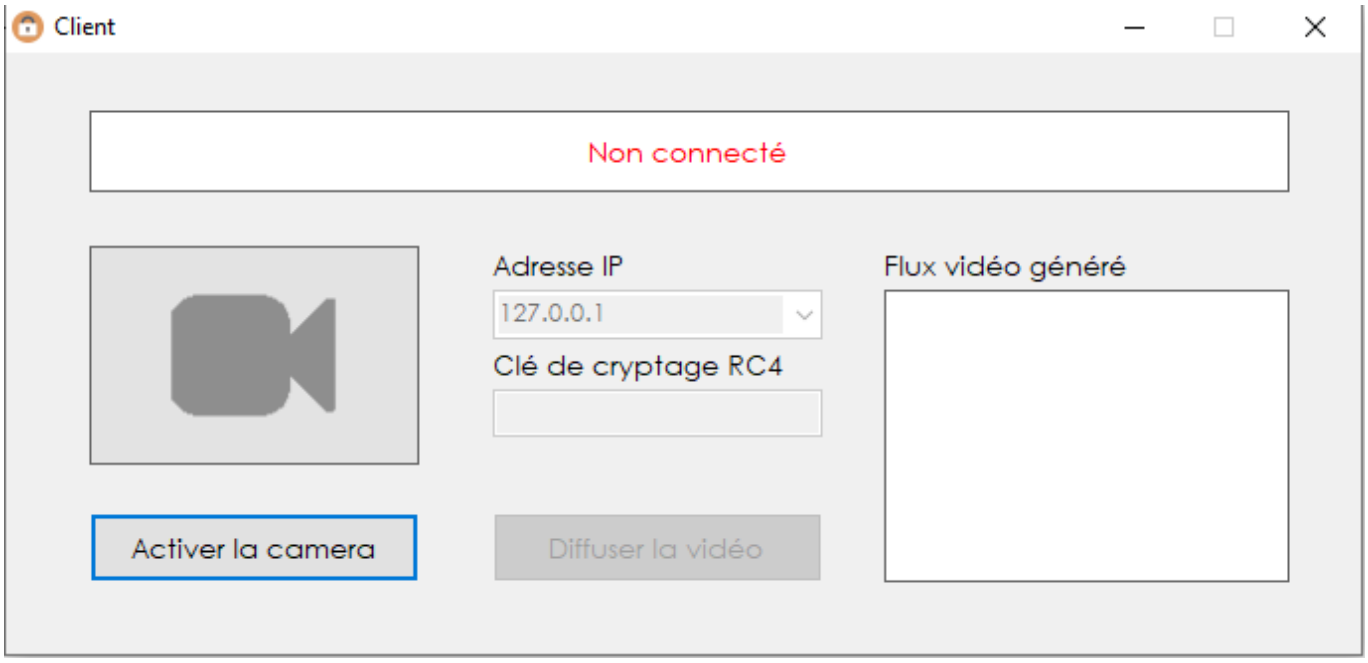
Visual Basic, également appelé «VB », est conçu pour rendre le développement logiciel simple et efficace, tout en étant suffisamment puissant pour créer des programmes avancés. Par exemple, le langage Visual Basic est conçu pour être « lisible par l'homme », ce qui signifie que le code source peut être compris sans nécessiter beaucoup de commentaires. [12]

### L'interface de l'application

- **Client :**

La fenêtre d'interface de notre client est illustrée ci-dessus dans la figure :

Figure 5.1 : interface de Client




**Le menu de programme :**

**Le Button Diffuser :** permet d'établir une connexion avec l'adresse IP entré

**Le Button Activer la cam :** permet d'ouvrir la cam dans interface de programme

- **Serveur**

La fenêtre d'interface de notre client est illustrée ci-dessus dans la figure :

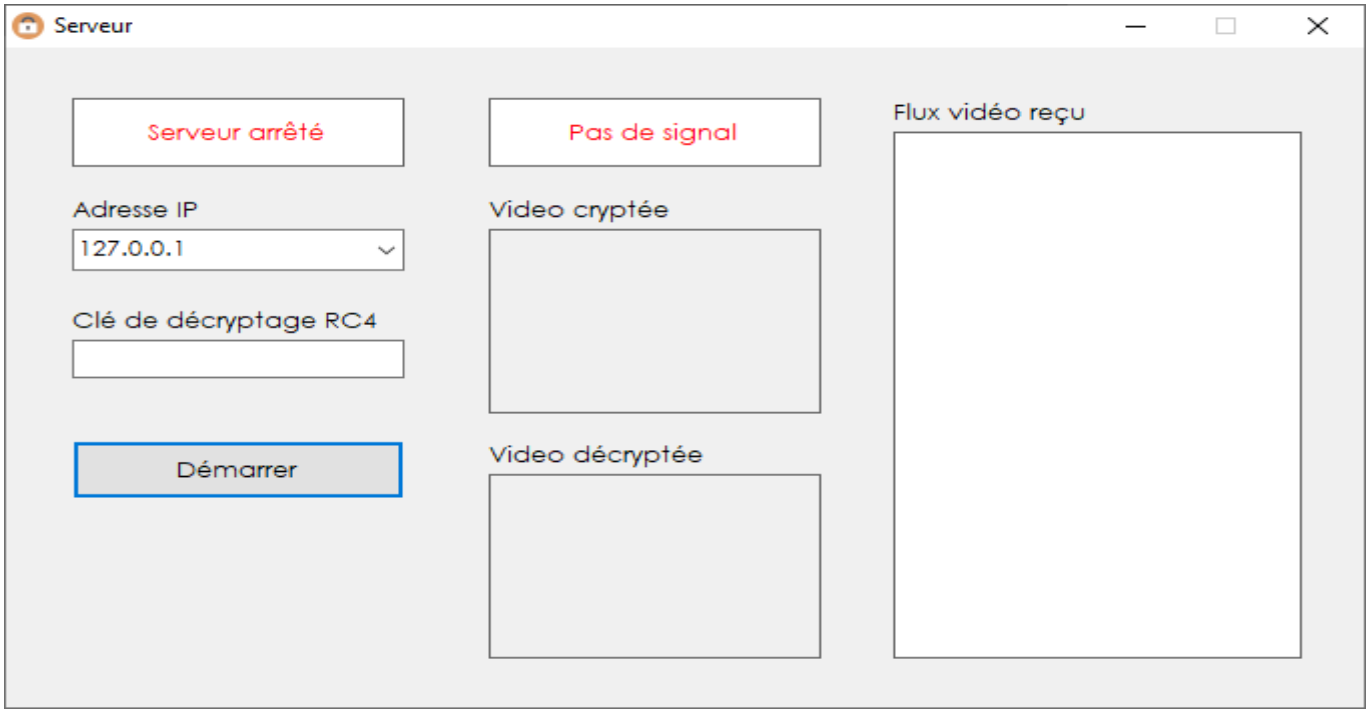
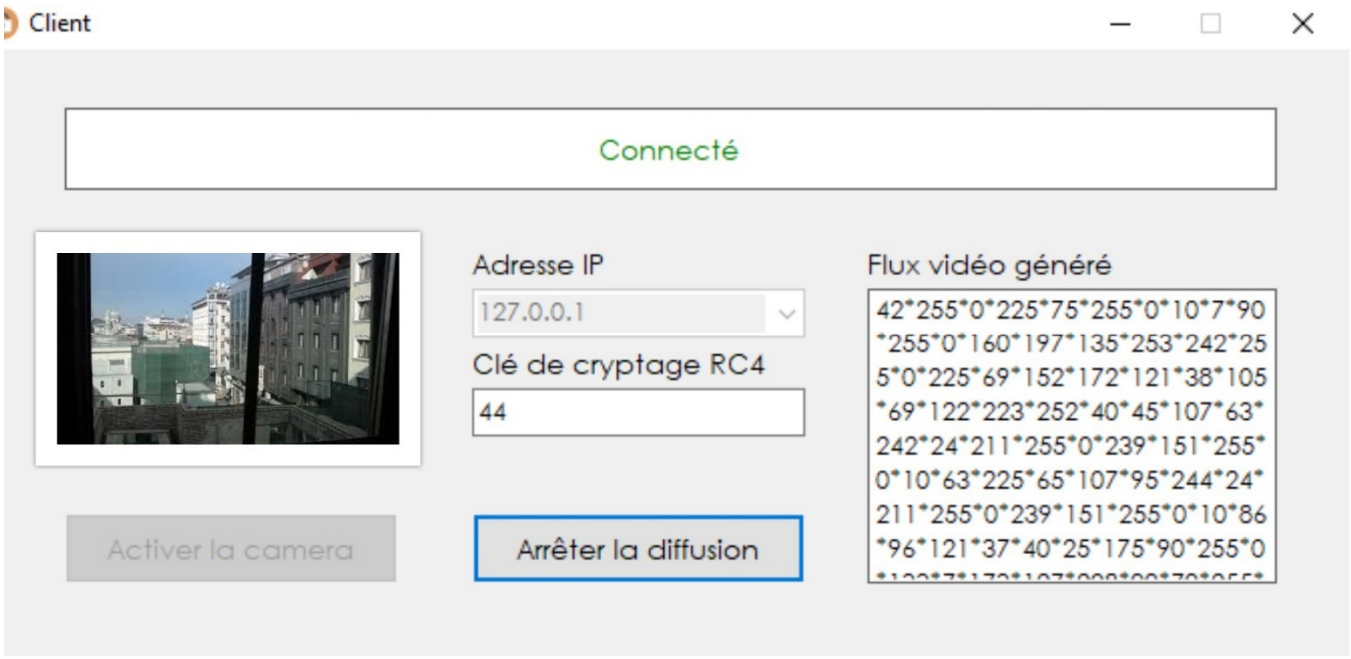



Figure 5.2 : interface de Serveur

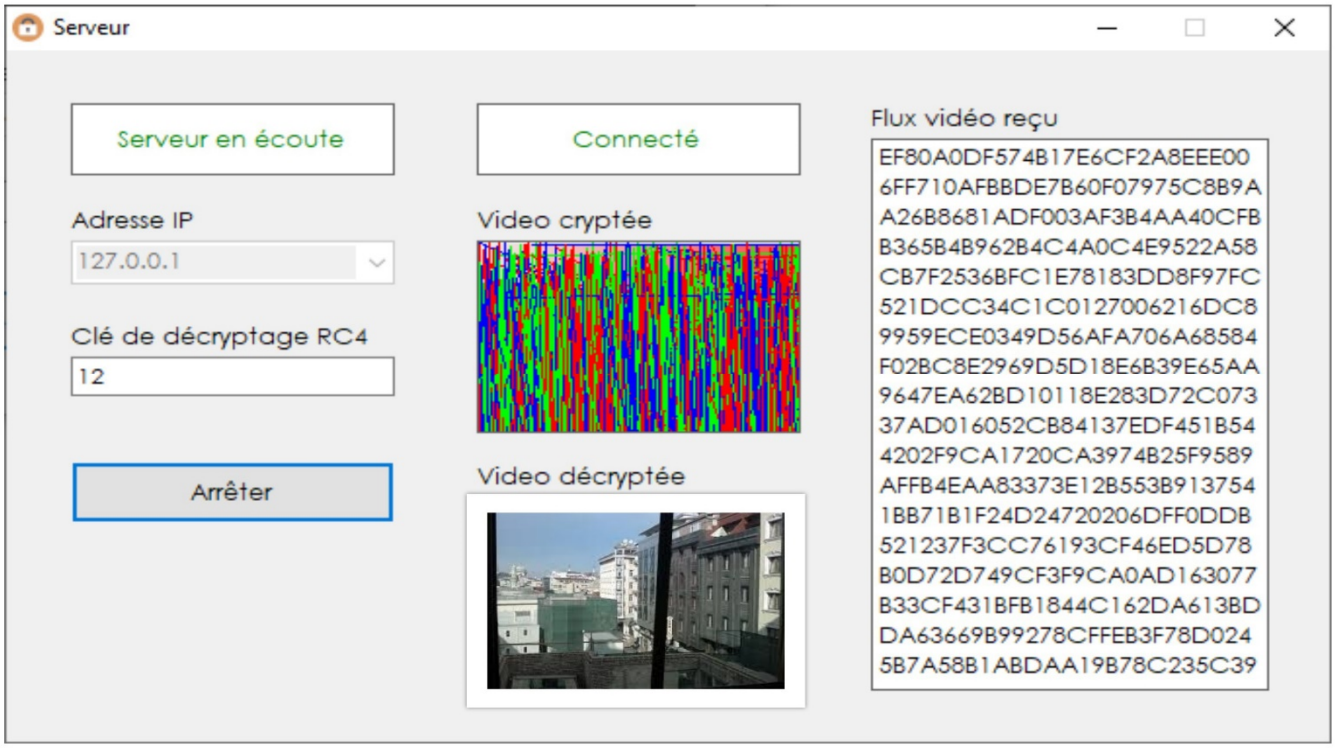
## 5.3 Les résultats obtenus

### Vidéo en couleur

### Client :




### Serveur :



### Trame vidéo sans cryptage :

61*79*235*93*199*252*42*93*107*63*241*251*167*255*0*223*79*255*0*196*210*255*0*194*166*214*255*0*231*250*195*254*250*127*254*38*165*97*42*246*39*218*35*131*44*72*168*203*115*142*213*223*159*132*154*217*255*0*151*237*63*254*250*127*254*38*147*254*21*30*181*255*0*63*218*127*253*244*255*0*252*77*90*195*84*236*39*52*31*8*206*124*75*121*255*0*94*103*255*0*67*90*43*166*240*63*129*245*15*12*106*211*221*221*220*91*75*28*150*230*32*34*102*36*29*202*123*129*199*6*138*244*40*197*198*9*51*38*238*207*255*217

### Trame vidéo crypté :

A20D6545813AD4B07352B8609CF2551AB3E064685AEBA665659173E6CD1D351C2C359D63973DB7C26B08104ED18AB128313E94B140507DC96ABB8890E5B825FFB4B188CB7191ACA2AD370E7791F498154C413DB248D4A8E3D5CC45404A6CC989B44AA69BD649878D16366A5DD6AEEE264E26556AF54DE3DB4C2E171331F1F6115DBA41AA08E5EEEB2BA136A1B9A65BBE2F2DB444274C5BA112F77E8D7EA0AA8EA91858EC8902D87DC5E8C740BAC6E75DB4D8BF14A415560FCBD38B068860EB7591F556EE00FB71CE42D76E4F71D5E8282BD57B14C02E61C6C7E661DF42408DCABD3FB8933E263F4746ADF167E1566F3C2FF4F462D1D6B3924E

### Remarque :

- Le temp de chiffrement est chargé par le changement de vidéo
- Le temp de transmission est chargé aussi par le changement vidéo et aussi la qualité de réseau entre le client et serveur
  dans le cas de local réseau le temps de transmission et de 240 millisecondes
- Le temp de Déchiffrement dans serveur est le même que le client
- Le temp pour afficher une image dans serveur et de 530 millisecondes [b10] [b11] [b12]

### Vidéo Noir et Blanc

- Le temp de chiffrement est chargé par le changement de vidéo
- Le temp de transmission est chargé aussi par le changement vidéo et aussi la qualité de réseau entre le client et serveur
  dans le cas de local réseau le temps de transmission et de 95 millisecondes

- Le temp de Déchiffrement dans serveur est le même que le client
- Le temp pour afficher une image dans serveur et de 215 millisecondes

**Résultats obtenus :**

La taille de vidéo augmente quand les couleurs est bien définit

Donc la taille de trame augment quand la qualité d'image et plus haut

## 5.4 Conclusion

Notre objectif est d'assurer la sécurité des flux vidéo échangés dans une architecture client et serveur à l'aide d'un algorithme de cryptage RC4 qui maintient les performances et l'efficacité de l'opération de cryptage. Les critères de performance sont déterminés sur les temps de transmission et la longueur de trame cryptée. [b13] [b14] [b15]

# Conclusion Générale

La sécurisation des informations est la protection des systèmes informatiques et les informations contre les dommages, le vol et l'utilisation non autorisée. Il s'agit du processus de prévention et de détection de l'utilisation non autorisée de votre système informatique.

Dans ce cas, il est nécessaire de recourir à des algorithmes de chiffrement des données.

La cryptographie informatique professionnelle est une solution, elle fait référence à des techniques sécurisées d'information et de communication dérivées de concepts mathématiques et d'un ensemble de calculs basés sur des règles appelées algorithmes, pour transformer les messages de manière difficile à déchiffrer.

Au cours de cette Mémoire, nous avons étudié et implémenté la transmission de vidéo dans une architecture Client / Serveur avec cryptage des flux par l'algorithme RC4.

Les critères de comparaison des cas dans le chiffrement de la qualité d'image sont les suivants :

- La vitesse et le temps de l'opération de chiffrement à l'aide des algorithmes RC4 étudiés dans notre projet de fin d'étude.
- La qualité et les performances de l'opération de chiffrement.

Notre objectif principal est de garantir une connexion à distance sécurisée et authentifiée. Pour la transmission de flux vidéo, cette solution est utilisée dans divers domaines commerciaux. Dans la perspective de nos travaux, nous souhaitons une étude comparative sur la qualité du cryptage des transmissions vidéo avec d'autres algorithmes cryptographiques tels que DES et AES

## Résumé

Parce que la communication est au cœur de l'activité humaine dans tous les domaines de la vie, les systèmes de télécommunications ont un impact significatif sur la société, car ils ont permis la communication multimodale (y compris l'audio, la vidéo et le texte). D'un point à un autre à tout moment, à condition que l'infrastructure appropriée existe.

Cryptographie utilisée pour dissimuler des informations, cette science devient maintenant un domaine très important en informatique. L'objectif principal de notre projet est d'assurer que le cryptage des flux vidéo capturés par une webcam soit transmis sur un réseau de communication. Nous sommes intéressés par une architecture client-serveur utilisant un algorithme de chiffrement à clé publique RC4.



**Mot-clé :** serveur, client, RC4, vidéo, image, statefull, stateless, clé publique, clé privée.



## ملخص

نظرًا لأن الاتصال هو قلب النشاط البشري في جميع مجالات الحياة ، فإن أنظمة الاتصالات السلكية واللاسلكية لها تأثير كبير على المجتمع ، حيث أنها أتاحت الاتصالات متعددة الوسائط (بما في ذلك الصوت والفيديو و نص). أشر إلى نقطة في أي وقت ، بشرط وجود البنية التحتية المناسبة.

يستخدم التشفير لإخفاء المعلومات ، وأصبح هذا العلم الآن مجالًا مهمًا للغاية في علوم الكمبيوتر. الهدف الرئيسي لمشروعنا هو ضمان نقل تشفير تدفقات الفيديو الملتقطة بواسطة كاميرا الويب عبر شبكة اتصالات. نحن مهتمون ببنية خادم العميل باستخدام خوارزمية تشفير المفتاح العام RC4.



## Abstract

Because communication is at the heart of human activity in all areas of life, telecommunications systems have a significant impact on society, as they have enabled multimodal communication (including audio, video and text). From one point to another at any time, provided the appropriate infrastructure exists.

Cryptography used to hide information, this science is now becoming a very important field in computer science. The main objective of our project is to ensure that the encryption of video streams captured by a webcam is transmitted over a communication network. We are interested in a client-server architecture using an RC4 public key encryption algorithm.

# Bibliographies


[b1] E.V.A., UCI. Coferencia#5 Modelo Cliente-Servidor. Teleinformática II.

[b2] B. Gadanayak, C. Pradhan, and U. C. Dey. “Comparative study of different encryption techniques on MP3 compression,” Int. J. Comput. Appl., vol. 26, no. 3, 28-31, 2011.

[b3] R. Gnanajeyaraman, K. Prasadh, and Ramar, "Audio encryption using higher dimensional chaotic map,"International Journal of Recent Trends in Engineering, vol. 1, pp. 103-107, 2009.

[b4] M. Kaur and S. Kaur, "Survey of Various Encryption Techniques for Audio Data," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, pp. 1314-1317, 2014.

[b5] Isnar Sumartono - An Overview of the RC4 Algorithm

[b6] La señal de vídeo Autores: Manuel Armenteros Gallardo y Francisco Utray Delgado

[b7] Digital Video Broadcasting Proyect (DVB). Normas de Televisión Digital. Disponible en Machado, T. B. (Ed.). (2003). Televisión Digital (2 ed.): I. G. Afanias. Colección Beta. Temas audiovisuales.

[b8] Brinkmann, Ron (2008), The art and science of digital composing (Third edition). Morgan Kaufman.

[b9] Machado, TB (Ed.). (2003). Télévision numérique ( 2 éd.): IG Afanias. Collection Bêta. Thèmes audiovisuels.

[b10] Rupali N. Hole, Megha Kolhekar, "Robust Video Encryption and Decryption using Selective Encryption," International Conference on Nascent Technologies in the Engineering Field, 2017

[b11] A. Kirthanaa, N.Mathan, T.Vino, "Improved perceptual video Encryption and Decryption using S-Transform," International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2015

[b12] Dhananjay M. Dumbere, Nitin J. Janwe, "Video Encryption using AES algorithm," International Conference on Current Trends in Engineering and Technology, IEEE Conference, July 8, 2014

[b13] Ms. Pooja Deshmukh, Ms. Vaishali Kolhe, "Modified AES Based Algorithm for MPEG Video Encryption," ICICES2014

[b14] Obaida M. Al-Hazaimeh, Nouh Alhindawi, 3Nesreen A. Otoum, "A Novel Video Encryption algorithm-Based on Speaker Voice as the Public Key,"IEEE, 2014

[b15] Nazar AL-Hayani, Naseer Al-Jawad, Sabah Jassim, "Simultaneous video compression and encryption for real-time secure transmission," 8th International Symposium on Image and Signal Processing and Analysis (ISPA 2013).

# Reference

## Reference site web


[1] - https://www.open.edu/openlearn/science-maths-technology/introduction-web-applications-architecture/content-section-1.1

[2] https://www.monografias.com/trabajos24/arquitectura-cliente-servidor/arquitectura-cliente-servidor.shtml#qcliente

[3] http://www.moct.gov.sy/ICTSandards/en/15/2_Annex_2_Software_Architecture_Issues.htm

[4] https://www.informit.com/articles/article.aspx?p=170808#:~:text=The%20purpose%20of%20cryptography%20is,not%20reveal%20the%20original%20input.

[5] https://www.garykessler.net/library/crypto.html

[6] https://academy.binance.com/es/security/symmetric-vs-asymmetric-encryption

[7] https://www.garykessler.net/library/crypto.html#rc4

[8] http://rufian.eu/Cifrado_RC4/

[9] https://curiosfera-historia.com/historia-del-video-inventor/

[10] https://www.dictionary.com/browse/video

[11] https://blogthinkbig.com/los-formatos-de-video-digital-como-diferenciarlos

[12] https://techterms.com/definition/visualbasic#:~:text=Visual%20Basic%20is%20a%20programming,and%20commands%20with%20visual%20controls.

[13] https://www.supinfo.com/articles/single/2519-architecture-client-serve

[14] http://www.yannvidal.com/wordpress/pdf/kit2survie.pdf

[15] http://ecariou.perso.univ-pau.fr/cours/web/cours-architecture-par6.pdf

[16] http://dspace.univ-tlemcen.dz/bitstream/112/1046/10/chapitre4.pdf.

[17] https://www.youtube.com/watch?v=kfdvlaOD1ig&ab_channel=MohamedAsaad