**Synthèse algorithmique – Séance 6 et 7**

*Quelques questions reprises du Test Wooclap*

Quel est le but principal de l'algorithme Minimax dans les jeux à somme nulle à deux joueurs ?

* Maximiser les gains potentiels du joueur en cours.

Quelle est la principale caractéristique de l'algorithme de Backtracking ?

* Il explore séquentiellement les différentes possibilités, en abandonnant une branche dès qu'elle devient non prometteuse.

Quelle méthode est souvent préférée pour représenter les graphes denses où la plupart des arêtes possibles sont présentes ?

* Matrice d'adjacence

Quelle est la principale caractéristique de l'algorithme de Kruskal pour trouver un arbre couvrant de poids minimum dans un graphe pondéré ?

* Il utilise une approche gloutonne en sélectionnant à chaque étape l'arête de poids minimum.

Quel inconvénient majeur rencontre-t-on lorsque l'algorithme Minimax est appliqué à des jeux présentant un grand nombre de possibilités ?

* Il est limité par la profondeur de recherche maximale.

Dans le contexte de la recherche d'itinéraire, quelle est la principale caractéristique de l'algorithme A\* ?

* L'algorithme A\* utilise une fonction d'évaluation heuristique pour guider la recherche vers la solution.

**Chiffrement**

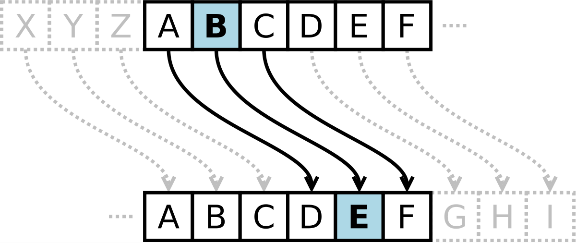
*Chiffrement ?*

* C’est quoi ?
  + Le chiffrement est une technique de cryptographie utilisée pour sécuriser des données en les rendant illisibles pour toute personne qui n'a pas la clé de déchiffrement correspondante. Cela permet de transmettre des informations de manière privée et sécurisée à un destinataire, de sorte que seul celui-ci puisse les comprendre.
* Objectifs principaux
  + Confidentialité : Le chiffrement assure que seules les personnes autorisées peuvent comprendre les données, les protégeant ainsi contre l'accès non autorisé.
  + Intégrité : Il garantit que les données restent inchangées et complètes pendant la transmission, évitant toute altération non autorisée ou toute perte de contenu.
  + Authenticité : Le chiffrement permet de vérifier que le message provient bien de la personne prétendant l'avoir envoyé, assurant ainsi la confiance dans l'identité de l'expéditeur et l'origine du message.

*Technique de base*

* Substitution
  + Cesar
* Transposition
* Par blocs
  + DES, AES
* Par flux
  + RC4

*César*

Le code César consiste à substituer une lettre par une autre un plus loin dans l'alphabet, c'est-à-dire qu'une lettre est toujours remplacée par la même lettre et que l'on applique le même décalage à toutes les lettres, cela rend très simple le décode d'un message puisqu'il y a 25 décalages possibles.

*Vigenère*

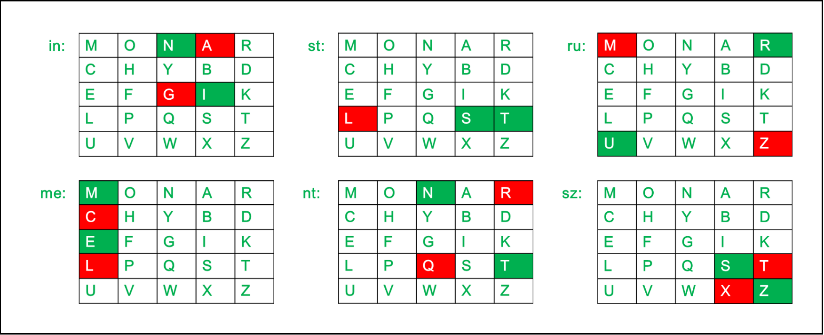
Le chiffre de Vigenère est une méthode de chiffrement manuel datant du 16ème siècle. Il s’agit d’une méthode de substitution polyalphabétique monographique. Le texte est décomposé en caractères simples et substitué en utilisant la clé ainsi que le carré de Vigenère.

*Playfair*

Le chiffrement de Playfair consiste en plusieurs étapes :

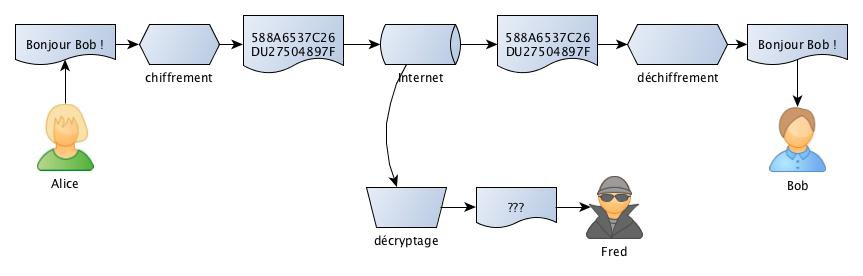
1. Création d'une grille 5x5 contenant toutes les lettres de l'alphabet, dans un ordre désordonné.
2. Génération de la clé de chiffrement à partir d'un mot-clé choisi.
3. Transformation du texte en clair en paires de lettres (bigrammes).
4. Application de règles de substitution pour chiffrer chaque paire de lettres en utilisant la grille et la clé.
5. Déchiffrement en utilisant le même processus, mais en sens inverse.

Cela permet de créer un texte chiffré qui est plus difficile à décrypter sans la clé de déchiffrement.



*Différence entre décryptage et déchiffrage*

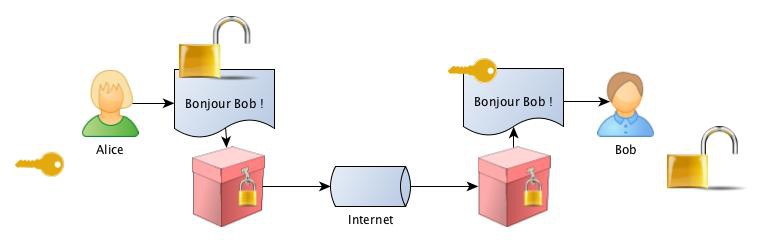
La différence entre décryptage et déchiffrage réside dans la nature des codes ou des langages impliqués. Le décryptage concerne généralement la conversion de codes secrets ou chiffrés en un format compréhensible en utilisant des techniques avancées telles que la cryptanalyse. D'autre part, le déchiffrage se réfère généralement à la traduction de codes simples ou de langages peu complexes en utilisant des méthodes plus directes et moins sophistiquées.

**

*Chiffrement symétrique*

Le chiffrement symétrique est un système où une seule clé est utilisée pour chiffrer et déchiffrer des données. Voici quelques points clés :

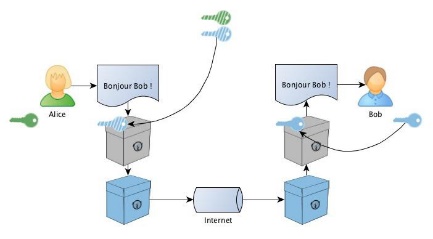
1. Utilisation d'une seule clé secrète pour chiffrer et déchiffrer les données .
2. Rapidité et efficacité pour chiffrer de grandes quantités de données .
3. Nécessite un accord préalable sur une clé secrète commune entre l'émetteur et le destinataire ou son transfert sécurisé .
4. Peut utiliser un chiffrement par flux ou par bloc, selon la taille des données à chiffrer .
5. Exemples d'algorithmes symétriques courants : AES, Blowfish, DES, Triple DES, Serpent .

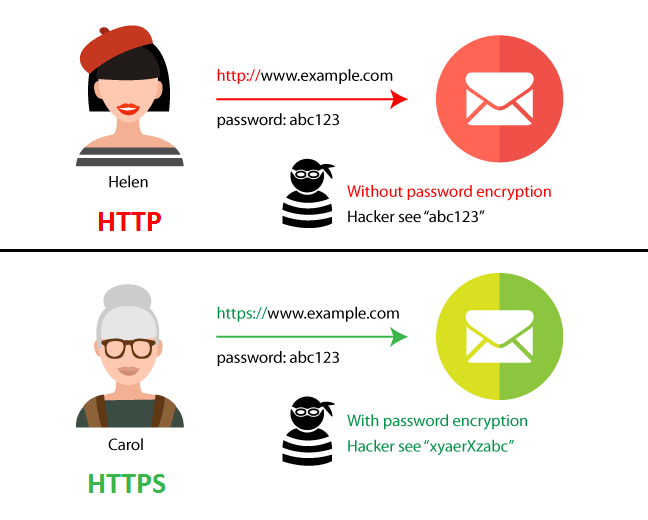
**Le chiffrement symétrique est largement utilisé dans la protection des données et la sécurisation des communications.

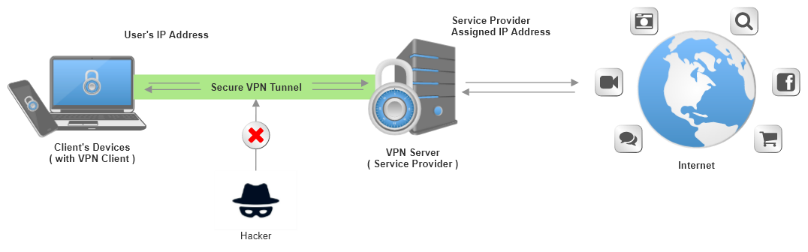
*Chiffrement asymétrique*

Explication simple des points clés du chiffrement asymétrique :

1. **Clé publique :** C'est comme une boîte aux lettres publique où tout le monde peut déposer des messages. C'est utilisé pour chiffrer les données avant de les envoyer.
2. **Clé privée :** C'est comme la clé de la boîte aux lettres, que seul le propriétaire possède. Cette clé est utilisée pour déchiffrer les données reçues, chiffrées avec la clé publique correspondante.

**Ces deux clés travaillent ensemble pour sécuriser les communications. Quand vous envoyez un message à quelqu'un, vous utilisez leur clé publique pour le chiffrer. Ils peuvent alors utiliser leur clé privée pour le déchiffrer et le lire. Cela garantit que seul le destinataire prévu peut accéder aux données

*Utilité dans la vie courante*



**Chiffrement symétrique**

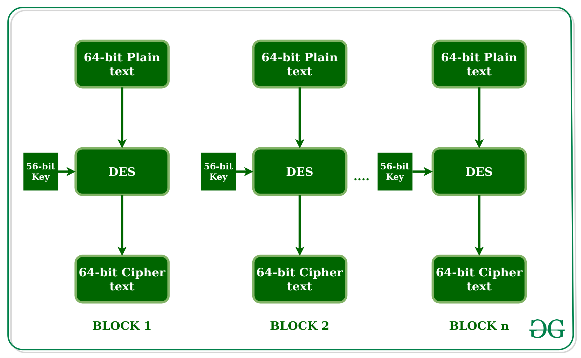
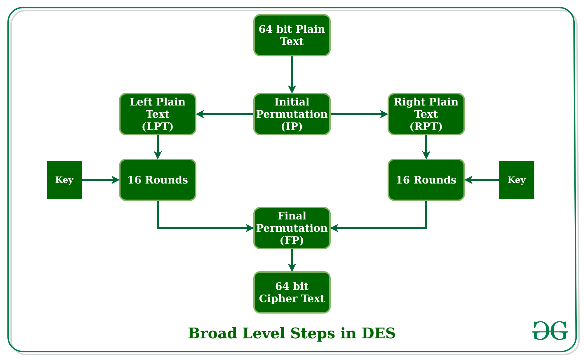
*Algorithmes*

* DES (Data Encryption Standard)
* 3DES (Triple DES)
* AES (Advanced Encryption Standard)
* Blowfish
* Twofish

*DES*

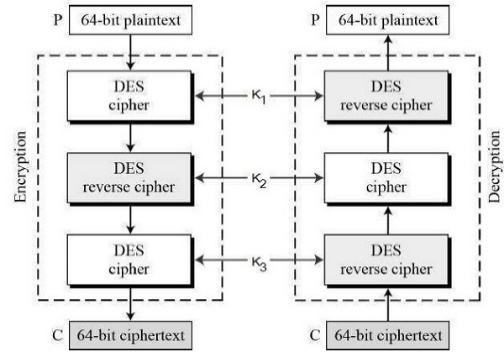
Le Data Encryption Standard (DES) est un algorithme de chiffrement symétrique utilisant des clés de 56 bits. Il transforme un bloc de 64 bits en un autre bloc de 64 bits. Les étapes de son fonctionnement incluent la manipulation de clés individuelles de 56 bits et la transformation des blocs de données.

1. Clé initiale : Le DES utilise une clé de 64 bits, mais avant de commencer le processus, chaque 8e bit de la clé est supprimé, produisant ainsi une clé de 56 bits.
2. Schéma de Feistel : Le DES est basé sur le schéma de Feistel, où le bloc de texte en clair de 64 bits est transformé en un autre bloc de 64 bits. Il effectue 16 tours d’opérations, mélangeant les bits à chaque étape.
3. Permutations initiale et finale : Avant le premier tour, le bloc de texte en clair subit une permutation initiale (IP). Ensuite, après les 16 tours, une permutation finale (FP) est appliquée au bloc combiné pour produire le texte chiffré de 64 bits.



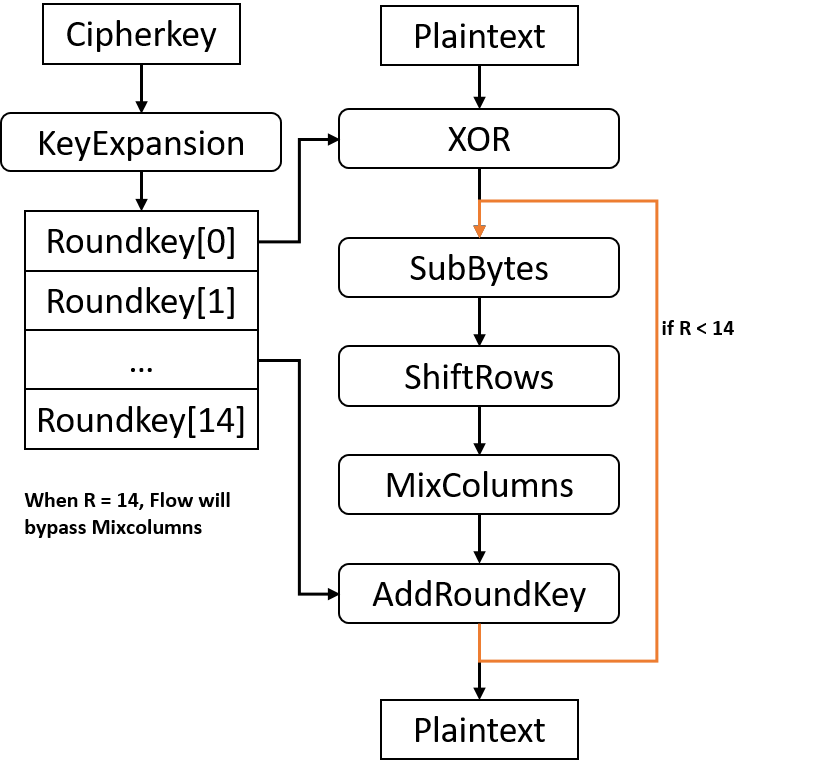
*3DES*

Le Triple DES (3DES) fonctionne en appliquant l’algorithme DES trois fois à chaque bloc de données. Voici comment cela se passe :

1. Chiffrement :
   * Le 3DES prend un bloc de données de 64 bits.
   * Il utilise trois clés distinctes (généralement de 112 bits ou 168 bits au total).
   * Pour chaque bloc, il effectue les étapes suivantes :
     + Chiffre le bloc avec la première clé DES.
     + Déchiffre le résultat avec la deuxième clé DES.
     + Chiffre à nouveau le résultat avec la troisième clé DES.
     + **Le résultat final est le texte chiffré.
2. Déchiffrement :
   * Pour déchiffrer, le processus est inversé :
   * Déchiffre le texte chiffré avec la troisième clé DES.
   * Chiffre le résultat avec la deuxième clé DES.
   * Déchiffre à nouveau le résultat avec la première clé DES.
   * Le résultat final est le bloc de données d’origine.

*AES*

L’algorithme AES (Advanced Encryption Standard) fonctionne de manière robuste et sécurisée pour le chiffrement des données. Voici un aperçu de son fonctionnement :

1. Entrée : L’AES prend en entrée un bloc de 128 bits (soit 16 octets) et une clé de 128, 192 ou 256 bits.
2. Substitution : Les octets d’entrée sont permutés selon une table prédéfinie appelée SubBytes. Cette étape remplace chaque octet par un autre octet spécifique.
3. Permutation : Les octets sont ensuite placés dans une matrice de 4x4 éléments appelée State Array.
4. Rotation : Les lignes de la matrice subissent une rotation vers la droite.
5. Mélange : Une opération de mélange (appelée MixColumns) est effectuée sur les colonnes de la matrice.
6. Ajout de clé : La clé est combinée avec le bloc de données à l’aide d’une opération XOR (ou exclusif).
7. **Répétition : Les étapes de substitution, permutation, rotation, mélange et ajout de clé sont répétées plusieurs fois (10, 12 ou 14 tours, en fonction de la longueur de la clé).
8. Sortie : Le résultat final est le bloc de données chiffré.

L’AES a remplacé le DES (Data Encryption Standard) obsolète et est largement utilisé pour sécuriser les communications, les fichiers et les données sensibles. Sa force réside dans sa capacité à résister aux attaques cryptographiques modernes

*Modes de chiffrement*

* ECB (Electronic Codebook)

Divise les données en blocs de taille fixe.

Vulnérable aux attaques de type dictionnaire car des blocs identiques sont chiffrés de la même manière.

* CBC (Cipher Block Chaining)

Bloc de données combiné avec le précédent.

Cela rend l'attaque de type dictionnaire plus difficile.

* CTR (Counter)
* OFB (Output Feedback)

*Problèmes courants*

* Echange de clés
* Distribution des clés
* Rotation des clés

*Solutions*

* Chiffrement de clé
* PKI (Public Key Infrastructure) : la PKI est un système de chiffrement asymétrique qui permet d'authentifier et de sécuriser les communications électroniques. La PKI utilise des certificats numériques pour vérifier l'identité des parties et assurer l'intégrité des données.
* Gestion de clés centralisée : les organisations peuvent utiliser des systèmes de gestion de clés centralisés pour gérer les clés de chiffrement. Ces systèmes peuvent faciliter l'échange, la distribution et la rotation des clés.

*Vulnérabilités*

* Brute force

Le brute force est une méthode de piratage qui utilise l’essai et l’erreur pour craquer des mots de passe, des identifiants de connexion et des clés de chiffrement. C’est une tactique simple mais fiable pour accéder illégalement à des comptes individuels et aux systèmes et réseaux d’organisations.

* Attaque par dictionnaire

Utilisation d’une liste de mots courants. Cette attaque peut être efficace pour des clés courtes ou faibles.

* Attaque par analyse différentielle

Analyse des différences entre les textes clairs et les textes chiffrés pour trouver des patterns ou des vulnérabilités dans le chiffrement.

* Attaque par force brute en temps réel

Attaque interceptant le message chiffré et essayant de déchiffrer le message en temps réel en utilisant différentes clés jusqu'à ce que le message chiffré soit déchiffré avec succès

*Améliorer la sécurité*

* Augmentation de la longueur de la clé
* Utilisation de clés aléatoires
* Utilisation de modes de chiffrement plus sûrs
* Utilisation de clés unique

*Utilisation*

* Chiffrement de fichiers
* Chiffrement de disques
* Chiffrement de bases de données
* Chiffrement de communications
* Chiffrement de courrier électronique

**Chiffrement asymétrique**

*Rappel*

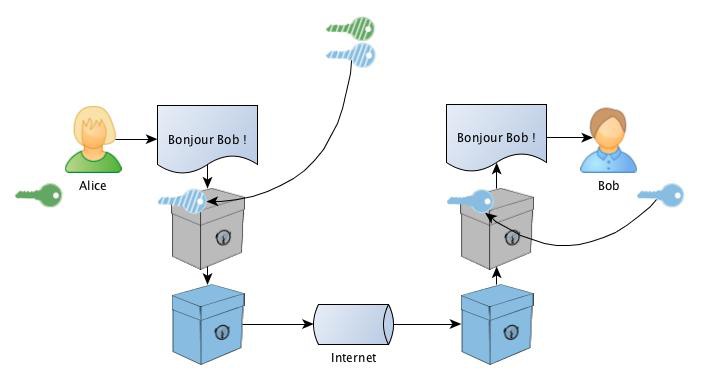
* Un chiffrement asymétrique va utiliser un couple de clés :

Une clé publique *p*

Une clé privée *s*

* La clé publique va permettre de chiffrer le message alors que la clé privée permettra de le déchiffrer
* Il y a donc une fonction de chiffrement f et une fonction de déchiffrement g :

*Principe*



*Algorithmes*

* RSA
* Chiffrement El Gamal ( Juste connaitre le nom )
* Chiffrement de Merkle-Hellman ( juste connaitre le nom )

*RSA*

RSA a été décrit en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman

1. Clés RSA :
   * Le chiffrement RSA utilise une paire de clés : une clé publique et une clé privée.
   * La clé publique est accessible à tous et sert à chiffrer les données.
   * La clé privée est connue uniquement de la personne (par exemple, Alice) qui souhaite recevoir des données confidentielles. Elle permet de déchiffrer ces données.
   * Alice peut également utiliser sa clé privée pour signer des données qu’elle envoie, et la clé publique permet à ses correspondants de vérifier la signature.
2. Fonctionnement :
   * Le chiffrement RSA repose sur des congruences et le petit théorème de Fermat appliqués aux entiers.
   * Tous les calculs se font modulo un nombre entier n, qui est le produit de deux nombres premiers.
   * Les messages clairs et chiffrés sont des entiers inférieurs à n.
   * Les opérations de chiffrement et de déchiffrement consistent à élever le message à une certaine puissance modulo n (c’est l’opération d’exponentiation modulaire).

1. Utilisation :
   * Le chiffrement RSA est souvent utilisé pour communiquer une clé de chiffrement symétrique. Bob peut envoyer à Alice une clé de chiffrement symétrique, qui permet ensuite d’échanger des données de manière confidentielle.

* Rivest Shamir Adleman (RSA) est basé sur la difficulté de factoriser de grands nombres entiers en facteur premier.
* On peut définir le RSA avec les informations suivantes :

La clé publique

La clé privée

La fonction de chiffrement :

La fonction de déchiffrement :

*Comment ?*

* Pour générer une clé RSA :

On choisit 2 nombres premiers distincts et

On calcule le module de chiffrement

On calcule l’indicatrice d’Euler :

On choisit un nombre premier premier avec

On calcule le nombre entier

*Pourquoi ?*

* Il est rapide de calculer le
* Il est difficile de calculer sur base de dans un temps raisonnable

*Attaques*

1. Brute force sur p & q : Une méthode consistant à tester toutes les combinaisons possibles de valeurs pour les paramètres p et q dans un algorithme de cryptographie à clé publique, souvent utilisée pour casser les clés RSA.

2. Attaque de Wiener : Une attaque cryptanalytique visant à retrouver la clé privée dans un système de cryptographie à clé publique basé sur le chiffrement RSA en exploitant une approximation de fractions continues.

3. Attaque de Håstad : Une attaque qui exploite le théorème de Håstad pour récupérer des informations secrètes à partir de plusieurs chiffrés qui ont été chiffrés avec la même clé publique mais avec des messages différents.

4. Time attack : Une attaque visant à déterminer des informations sensibles, telles que des clés de chiffrement, en analysant le temps de traitement requis par un système lorsqu'il traite différentes données.

5. Adaptive chosen ciphertext attack : Une attaque où un attaquant a la capacité d'obtenir des chiffrés correspondant à des textes clairs de son choix et d'observer les réponses du système, ce qui lui permet de déduire des informations sur la clé de chiffrement ou de déchiffrer des messages chiffrés.

**RegEX**

* Une expression régulière est une chaîne de caractères qui décrit un ensemble de chaînes de caractères.
* Exemple :

\b[A-Za-z0-9.\_%+-][+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}\b](mailto:+@[A-Za-z0-9.-]+\.%5bA-Za-z%5d%7b2,%7d\b)

*Les ensembles*

* Représenté par des [ ]

[a-z] : les lettres minuscules

[0-9] : les chiffres

[&é"'(è\_çà)=] : les caractères spéciaux (à compléter au besoin)

[^a] : ce qui n’est PAS dans mon ensemble

* Cas particuliers :

[aei-ou] : a, e, tout ce qui se trouve entre i et o, u.

*Raccourcis d’ensembles*

* \w : lettres + chiffres + \_
* \d : chiffres
* \s : caractères blancs
* . : n’importe quel caractère (\. pour détecter le point)
* Chaque raccourci en majuscule donne la négation

*Les opérateurs*

* a|b : les a OU les b
* Opérateurs de quantité :

? : 0 ou 1 élément

\* : 0 ou plusieurs éléments

+ : au moins 1 élément

{n,m} : un nombre défini d’éléments

* Exemple :

\b\w{4,6}\b : les mots de 4 à 6 caractères

*Syntaxe*

\b[A-Za-z0-9.\_%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}\b

* \b : début ou fin d’un mot
* [A-Za-z0-9.\_%+-]+ : 1 ou plusieurs caractères parmi ceux dans les crochets
* \. : le point avec le \ pour l’échapper
* {2,} : 2 caractères au moins parmi les précédents

*Ressources*

* Regex101.com
* Regexr.com
* Rexegg.com