MODULE #2 | Manipulez l'information
KIT POUR LE DEUXIÈME TEMPS DE RENCONTRE

Image : OpenClassrooms, CC BY 4.0 International.

Le parcours de formation **Class'Code** s'articule autour de 5 modules de formation en ligne (MOOC) et des temps de rencontre (présentiel). Ce document a pour objectif de vous permettre de profiter au mieux de ce **deuxième** temps de rencontre autour du module « **Manipulez l'information** ».

Voilà maintenant trois semaines que vous avez fait vos premiers pas sur le codage de l'information, vous savez comment optimiser votre code et traiter l'information, même la chiffrer !

Comme pour la première séance, nous avons prévu une durée d'environ deux heures, mais la réalité sera variable d'un groupe à l'autre. Libre à vous de la suivre à la lettre, ou de l'aménager en fonction de vos envies, de vos besoins et de vos contraintes. L'important étant de profiter de ce moment pour avancer.

N'hésitez pas, avant la rencontre, à utiliser le PAD mis à disposition sur la page du groupe pour faire remonter vos besoins, choisir les activités qui vous intéressent le plus et vous organiser. Cela vous permettra de profiter au maximum du temps de rencontre sans perdre trop de temps en début de séance.

QUE PRÉPARER AVANT LA SÉANCE ?

Avoir suivi les trois premières semaines du module « Manipulez l'information » sur openclassrooms.fr et être inscrit à un temps de rencontre sur classcode.fr.

Organisation

- Les activités sont prévues pour des groupes de 3 à 20 personnes.
- Faites remonter vos questions, besoins et activités préférées sur le PAD avant la séance.
- Prévoyez de créer des sous-groupes pour faciliter certaines tâches, notamment lors de l'entraide ou des activités débranchées.
- Les temps d'activités sont donnés à titre indicatif, si vous souhaitez tout réaliser durant la séance, nous vous conseillons de désigner un maître du temps qui veillera au respect des horaires. :)

Matériel nécessaire

- Ce kit pédagogique sous forme papier ou électronique.
- Du papier, des stylos ou crayons.
- Des post-it (si possible de plusieurs couleurs).
- Si possible, votre ordinateur portable ou tablette (idéalement il en faut un pour deux).

CONCRÈTEMENT, QUE VA-T-ON FAIRE ?

Pour profiter au maximum de ce temps de rencontre et de votre diversité, nous vous proposons des pistes d'activités qui s'articulent autour de quatre temps pour : se présenter, s'entraider, approfondir et échanger.

Se présenter – env. 15'

Accueil des nouveaux venus et retours sur les semaines écoulées.

S'entraider au codage et programmer ensemble – env. 25'

Ici vous pourrez consacrer un moment à debugger vos programmes ou à réaliser un petit projet collaboratif, comme une sorte de mini *code jam* !

Approfondir – env. 30'

Vous pratiquerez, ensemble, deux activités débranchées. Cela vous permettra d'estimer la mise en pratique de l'activité (des adaptations sont-elles nécessaires, par exemple ?). Dans ce même temps vous reverrez des notions autour du chiffrement.

Échanger – env. 50'

Et après, il va falloir transmettre. Discutez des enjeux en lien avec ce que vous venez d'apprendre, cherchez la meilleure façon d'expliquer ces notions à votre public, répondez collectivement à des questions, partagez vos déroulés.

Et… Vous pouvez lire la suite que lors du temps de rencontre. Néanmoins si vous préférez le faire pour vous préparer, sautez les rubriques « Décryptage » ! :)

MODULE #2 | Manipulez l'information
FEUILLE DE ROUTE

SE PRÉSENTER – env. 15'

Après quelques semaines de travail derrière l'écran, c'est le moment de nous retrouver. Nous nous connaissons déjà tous, ou presque… Si une nouvelle personne se joint à nous, prenons un moment pour l'accueillir. Nous pouvons faire un rapide tour de table de nos impressions depuis le dernier temps de rencontre. Sinon passons directement à la suite !

S'ENTRAIDER AU CODAGE ET PROGRAMMER ENSEMBLE – env. 25'

Coder à plusieurs permet de proposer un travail en équipe, de débrider notre imagination, mais aussi de voir comment chacun et chacune peut avoir des stratégies différentes pour résoudre un même problème, surtout quand il s'agit de codage informatique !

Pour aller plus loin
Si l'un d'entre nous a un projet à coder bien défini (vive la créativité !) et d'autres sont prêts à participer, pourquoi ne pas profiter de cette rencontre pour le démarrer, le partager sur Scratch Studio et le poursuivre même après la fin du module ?

RAPPEL POUR DÉBUGGER

Nouveaux codes, nouveaux bugs. Sans y passer toute la séance - ce serait dommage de ne pas profiter de ce temps de rencontre pour expérimenter et échanger avec les autres sans écran - vous aurez peut-être besoin d'un nouveau regard pour dépasser un blocage. Retrouvez ici les principaux conseils.

- Utiliser le forum de Scratch : scratch.mit.edu/discuss/15/
- Consulter la page « Comment ne pas se faire piéger pendant une animation Scratch ? » : pixees.fr/?p=4252
- Regarder la question de la FAQ facilitateur « Comment aider quelqu'un à trouver une erreur de programmation ? » : pixees.fr/?page_id=8012
- Toujours bloqué ? En dernier recours contacter le bureau d'accueil de Class'Code : pixees.fr/?page_id=42

APPROFONDIR – env. 30'

Lors de notre dernière rencontre nous avons codé l'information et réfléchi aux enjeux liés, comme l'efficacité lors de sa transmission et son « poids » dans la mémoire de la machine. Nous avons essayé d'éviter que ce codage soit connu des autres (les méchants E.T.). Maintenant nous disposons d'éléments autour du chiffrement qui peuvent nous aider à améliorer cet aspect.
Approfondissons la compréhension du chiffrement en informatique avec une activité débranchée ?

LA PROTECTION DE L'INFORMATION …

…OU COMMENT ÉVITER UNE NOUVELLE INVASION DES EXTRATERRESTRES

Nous sommes toujours en 2090 et vous avez sauvé la planète grâce à votre astuce lors de notre dernière rencontre ! Les clefs TLR ont été récupérées, le logiciel installé sur le système des E.T. qui, sans pouvoir s'organiser, ont dû quitter notre planète !

Génial, non ? Mais… vous soupçonnez que certains E.T. espions sont restés sur place pour essayer d'avoir accès au système informatique des humains et préparer une nouvelle invasion.

Pour éviter cela, vous avez pour mission de mettre en place une méthode de transmission de messages à l'épreuve d'espions.

De plus, vous avez trouvé certains messages des E.T. qu'ils ont laissés derrière lors de la fuite. Seriez-vous capables de déchiffrer ces messages secrets ?

Sommes-nous prêts pour accomplir notre mission ? Rendez-vous à la page suivante pour notre activité débranchée.

ACTIVITÉ 1 – PROTÉGEZ L'INFORMATION

Défi

Transmettre une information de sorte qu'elle ne soit comprise que par son destinataire.

Ressources

- Du papier.
- Un stylo (ou crayon, ou…).
- Des post-it (si possible de plusieurs couleurs).

Contexte

- Vous, agents 001 et 002, avez une nouvelle mission : établir un protocole permettant que les messages entre les agents secrets des humains soient transmis de manière sécurisée.
- Vous savez que les E.T. sont capables d'intercepter les messages lorsqu'ils sont en transit, c'est à dire quand ils partent d'un agent vers l'autre.
- Vous disposez de boîtes (assez solides, dans lesquelles vous pouvez placer des objets, des messages...), de cadenas (indestructibles) et de votre astuce.
- Chaque agent dispose de son cadenas et de sa clef, mais pas de celle des autres.

Organisation

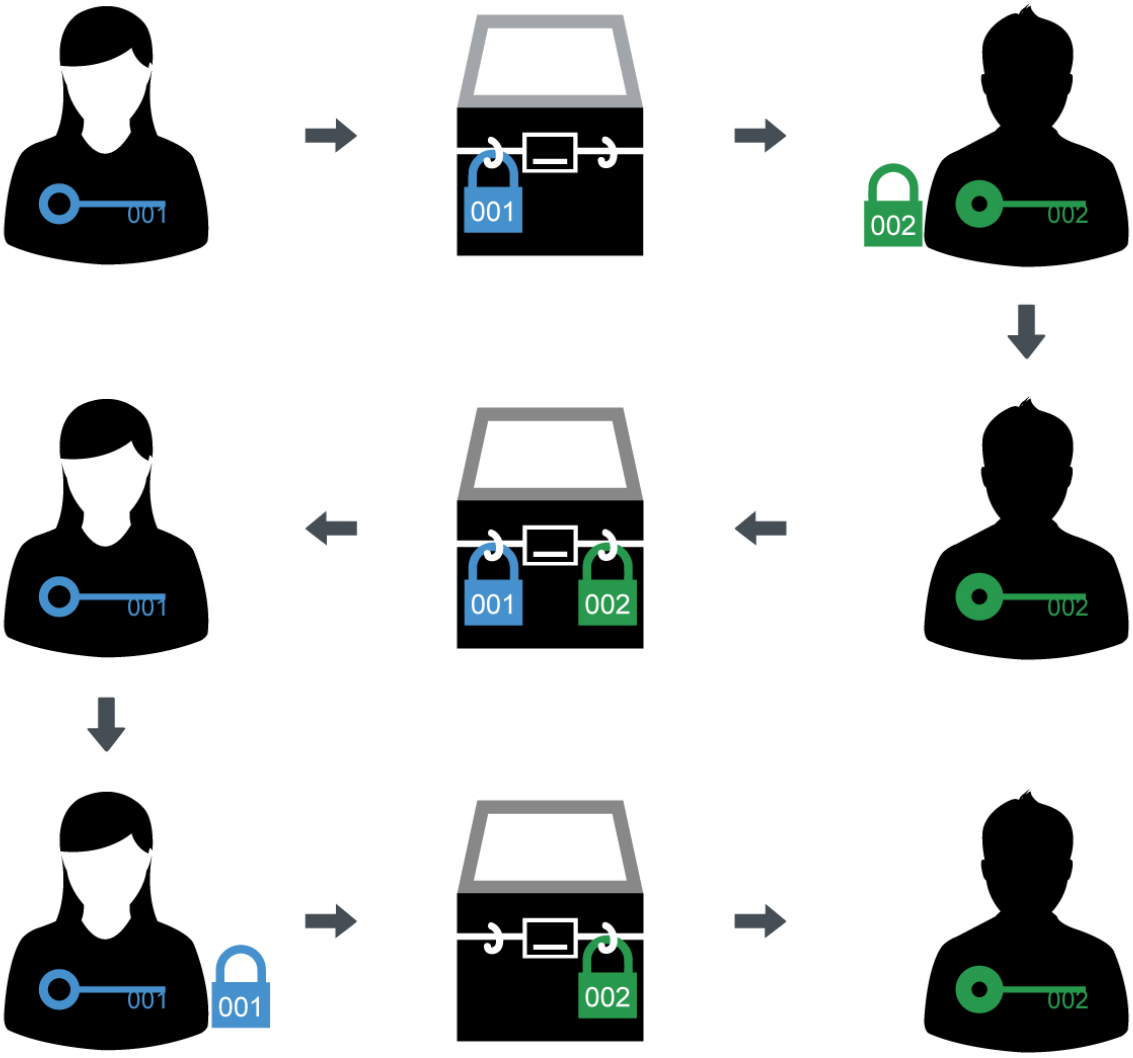
- Répartir les participants en binômes (ou groupes réduits).
- Chacun prend un cadenas et la clef correspondante.
- On ne s'éloigne jamais de sa clef : un E.T. pourrait l'intercepter et avoir accès à tous vos messages !
- L'agent 001 place quelque chose dans la boîte. Un objet important, un message secret, une clef ?
- Gagne l'équipe qui réussit à transmettre le message de l'agent 001 vers l'agent 002 sans qu'il puisse être intercepté par les E.T. espions.

Remarques / points d'attention

- Il est possible de simuler la boîte en pliant le papier du message (un peu d'imagination !).
- Les post-it simulent le cadenas et la clef correspondante (une sorte de code couleur pour se rappeler, ou deux « semi-dessins » dessus qui se complètent). Sinon, un bout de papier avec un dessin/le nom de l'agent fait l'affaire.
- Attention : toute boîte qui transite en étant ouverte risque de voir son contenu volé par les E.T. Et il est impossible de se donner un cadenas directement (si les agents se voyaient directement, ils n'auraient pas besoin des boîtes.
- Par contre, il est tout à fait autorisé de voir la boîte se balader de 001 à 002 plusieurs fois afin de transmettre le message en toute sécurité à l'aide des cadenas. ;)

ACTIVITÉ 1 – PROTÉGEZ L'INFORMATION
DÉCRYPTAGE

Rappel du défi
Transmettre une information de sorte qu'elle ne soit comprise que par son destinataire.



En essayant plusieurs solutions, on voit que 001 va devoir envoyer une boîte, sans doute avec le message secret dedans, fermée par son cadenas. Seulement 002 ne peut pas l'ouvrir, il n'a pas la clef. Par contre il peut rajouter le sien. Sur la boîte doublement verrouillée 001 peut enlever son cadenas, renvoyer à 002 qui ouvre et lit le message.

Décryptage

Voici quelques éléments pour continuer la discussion à propos de cette activité :

1. Et si un E.T. espion se fait passer pour l'agent 002 au début de l'échange, réussit-il à lire le message de l'agent 001 ?
2. Que peut-on changer aux règles ci-dessus pour arriver à empêcher les usurpations d'identité ?
3. Nos clefs et cadenas dans l'activité, ils s'appellent comment dans le monde numérique ?
4. Et ça correspond à quoi exactement le verrouillage d'un « cadenas », dans le monde numérique ?
5. Comment travailler cette activité avec des enfants, selon vous ?

Éléments de réponse

1. Oui, l'E.T. aurait accès au message. Le problème ici c'est que les agents ne partagent aucune information au départ. Et donc tout ce que 002 peut faire, l'E.T. peut l'imiter et 001 ne verra pas la différence. Pour résoudre ce problème il faut que 001 et 002 partagent au moins une information en commun.
2. Si 001 et 002 ont tous les deux la clef du même cadenas ça devient super facile. Cela s'appelle une clef partagée. Sauf que du coup tous les messages envoyés à 001 pourront être lus par 002, même ses messages d'amour pour 003. Pas top, il faudrait une autre solution pour les messages privés de 001. L'autre solution c'est le chiffrement à clef publique, comme dans le système RSA, que nous avons vu en ligne. Pour cela il faut que chacun garde sa clef pour lui, mais donne des copies de son cadenas à tout le monde (ou qu'une personne de confiance les distribue en main propre de sa part). Chaque agent qui veut envoyer un message ferme la boîte avec le cadenas de son interlocuteur, qui sera donc le seul à pouvoir l'ouvrir. Encore une fois 001 et 002 partagent des informations : le cadenas de l'autre.
3. L'équivalent informatique des cadenas et des clefs est ce qu'on appelle une clef en cryptographie (oui, tous les deux sont des clefs). Le cadenas serait une clef de chiffrement, et la clef une clef de déchiffrement. En informatique on ne fait pas la différence. C'est comme si on pouvait fermer la boîte avec une clef, et l'ouvrir avec un cadenas. Et fermer/ouvrir une boîte correspond à l'algorithme de chiffrement/déchiffrement. De plus il y a deux principaux types de chiffrement : symétrique, et asymétrique (ou à clef publique). Le principe du chiffrement asymétrique c'est de disposer de paires de clefs particulières, représentées ici par nos deux clefs/cadenas. Pour rappel (extrait du cours en ligne) :

   U*n algorithme fait en sorte que si on chiffre un message avec une des deux clefs, on peut le déchiffrer avec l'autre clef (mais pas avec la première). Du coup on donne à qui la veut l'une des deux clefs qu'on appelle clef publique, et on garde bien précieusement la deuxième, appelée clef privée. Ensuite si quelqu'un veut vous envoyer un message secret, il le chiffre avec votre clef publique et vous êtes le seul, avec votre clef privée, à pouvoir le déchiffrer. Pour l'image c'est un peu comme si tout le monde pouvait acheter un cadenas avec votre nom dessus, mais seul vous aviez la clef pour l'ouvrir.*

   Pour le chiffrement symétrique par contre, la clef de chiffrement et la clef de déchiffrement sont identiques. On ne peut donc pas donner son cadenas à tout le monde, car on leur permettrait de lire tous nos messages. Donc si on applique l'algorithme de chiffrement une fois avec sa clef, ça rend le message illisible. Si on l'applique une deuxième fois, le message redevient lisible. Ces clefs peuvent être partagées entre deux personnes qui se font confiance, et peuvent ainsi discuter facilement, en s'envoyant des messages toujours chiffrés avec la même clef partagée.

4. Il s'agit bien entendu d'un calcul qui prend le message initial et le transforme avec une formule mathématique qui dépend de la clef (basée par exemple sur des nombres premiers) pour en faire un message crypté.
5. Quelques pistes : soit mettre en place le jeu de manière complètement dirigée, soit leur faire construire eux-mêmes le jeu à partir du dessin ci-dessus, soit découper le dessin et leur demander de retrouver le bon ordre. Ensuite, pourquoi pas leur demander d'expliquer avec leurs propres mots ?

–> Pour retrouver des variations de cette activité, c'est ici :

http://images.math.cnrs.fr/Dis-maman-ou-papa-comment-on-cache-des-secrets-dans-le-monde-numerique

–> Pour faire une vraie boîte, pourquoi pas en origami ?

Voici quelques liens retrouvés sur Internet, à vous de les adapter pour rajouter les cadenas, ou d'en trouver d'autres encore plus intéressants - et n'oubliez pas de les partager avec la communauté Class'Code ! :)

https://www.youtube.com/watch?v=n6Y7P0TvVBk
https://www.youtube.com/watch?v=HvKPOZjVa-c

ACTIVITÉ 2 – RETROUVEZ L'INFORMATION

Défi

Déchiffrer un message à l'aide du chiffre de César (chiffrement par décalage).

Ressources

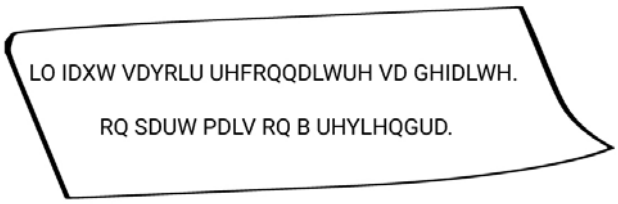
- Du papier (pour réfléchir)
- Un stylo (ou crayon, ou…)
- La roue de César (optionnel, voir ci-dessous)

Contexte

- Quelques bouts de papier avec des messages en français (on ne différencie pas les lettres par rapport aux accents, on garde la ponctuation : les points, les virgules, mais aussi l'apostrophe, par exemple), mais chiffrés, ont été trouvés dans un des campements des E.T.
- Vous savez que les E.T. ne sont pas très doués pour cacher leurs messages et ils ont probablement utilisé un système par décalage, vous le pariez !
- À présent vous avez entre vos mains le message ci-dessous et vous allez essayer de le déchiffrer.

Organisation

- Répartir les participants en binômes (ou groupes réduits).
- Discuter de la meilleure approche (l'analyse fréquentielle ? la longueur des mots ? la force brute ?) pour essayer de trouver la clef : ici, de combien de places on décale les lettres de l'alphabet.
- Décrypter le message !

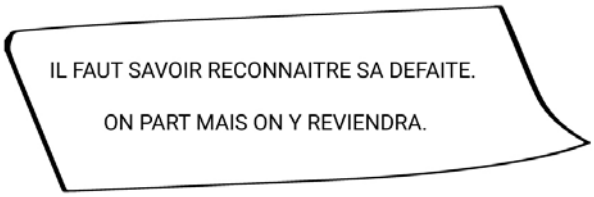


Remarques / points d'attention

- La roue de César facilite la tâche de retrouver la lettre correspondante une fois qu'on a la clef. Retrouvez-la dans l'annexe 2. À vous de décider si le fait de devoir l'assembler prend plus de temps que le fait de faire les correspondances à la main. En tout cas, elle pourra servir quand vous serez en atelier avec les jeunes :)

ACTIVITÉ 2 – RETROUVEZ L'INFORMATION
DÉCRYPTAGE

Rappel du défi
Déchiffrer un message à l'aide du chiffre de César (chiffrement par décalage).



Avez-vous réussi à déchiffrer le message secret ? Comment décrire votre stratégie ?

Décryptage
Voici quelques éléments pour continuer la discussion à propos de cette activité :

1. Quels sont les deux ingrédients d'un chiffrement et comment sont-ils représentés dans cette activité ?
2. Quelle serait, selon vous, la stratégie la plus efficace pour déchiffrer ce message spécifique ?
3. Quelles sont les stratégies d'attaque classiques pour casser ce type de code ?

Éléments de réponse

1. Les deux ingrédients d'un chiffrement sont l'algorithme (ici, décaler les lettres de l'alphabet d'une valeur donnée) et la clef (ici, la valeur du décalage).
2. Si on analyse le texte du message, on remarque qu'il y a un mot composé d'une seule lettre. Bah, en français ce n'est le cas que de deux mots : le « a » (verbe avoir ou préposition - notez qu'on ne distingue pas les lettres accentuées) et le « y » (pronom). Alors c'est simple ! On essaie avec le « a » (clef à 1 pour ce message) et si ça ne marche pas, on essaie avec le « y » (clé à 3 pour ce message). Et voilà !
3. La cryptanalyse dans le cas des chiffrements par décalage est typiquement faite par l'analyse fréquentielle. Pour rappel : on étudie la fréquence d'apparition de chaque lettre dans un texte de référence - dans ce cas un texte en français - et on le compare avec la fréquence d'apparition de chaque lettre dans le texte chiffré. Par exemple, en français, la lettre la plus fréquente est le « e », puis le « s » et le « u ». Cette méthode fonctionne très bien mais c'est moins le cas quand le message est trop court, les fréquences d'apparition peuvent nettement différer de la moyenne, et l'analyse devient plus difficile. C'est notre cas.
   Une autre possibilité est d'utiliser la force brute : ce type de chiffrement nous fait 25 décalages possibles et donc « seulement » 25 possibilités à tester. Pas grave si nous avons du temps ou une machine pour le faire, mais nous sommes plus malins que ça !

ÉCHANGER – env. 50'

Et après, il va falloir transmettre. Discutons des enjeux liés à ce que nous venons d'apprendre, cherchons la meilleure façon d'expliquer ces notions à notre public, répondons collectivement à des questions posées en ligne, partageons nos idées !

Autour des enjeux sociétaux

Dans la dernière semaine en ligne (Partie 3, Chapitre 3), nous avons étudié les bases de données et le fait qu'on laisse des données partout…

Selon vous, quelles sont les conséquences de la collecte et utilisation des données en masse que permet le numérique ?

Autour de la transmission

La dernière activité en ligne (Partie 3, Chapitre 6) propose des activités « clé en main » à mettre en place et adapter selon nos différents contextes d'intervention. Pourquoi ne pas discuter des séquences proposées, ou même en élaborer de nouvelles entre nous ? Partageons-les ensemble pour pouvoir mener des ateliers de qualité ! À partir d'une séquence en particulier, nous pouvons réfléchir sur :

- les points positifs
- les points d'amélioration
- les points d'attention
- l'étendue (quel public ? quelles adaptations nécessaires et possibles ?)
- les besoins en termes de matériel mis à disposition (ordinateur, accès à Internet, etc.)
- le temps minimal pour un bon déroulement

ET ENSUITE…

Vous avez fini le Module #2 de Class'Code, Manipulez l'information ! À l'issue des 3 semaines de formation en ligne et de ces deux temps de rencontre nous faisons le pari que vous serez capables d'animer un atelier sur ce thème avec des jeunes.

C'est maintenant que tout commence ! Vous avez sûrement encore des questions, des doutes, vous allez découvrir de nouvelles situations. Vous pouvez rester en contact et continuer à vous entraider et à échanger sur ces sujets ! Vous faites maintenant partie de la communauté Class'Code.

N'hésitez pas à nous faire part de vos retours et avis : points positifs ou à améliorer, problèmes rencontrés, idées nouvelles, c'est avec vous que nous construisons cette formation.

Envie de poursuivre ? D'autres modules seront bientôt disponibles pour aller plus loin. Ils vous permettront d'animer des ateliers thématiques autour de la robotique ludique et des réseaux. Retrouvez l'ensemble du parcours sur classcode.fr

L'équipe de Class'Code
classcode-accueil@inria.fr

MODULE #2 | Manipulez l'information
ANNEXE 1 – VOCABULAIRE

Cryptographie
La cryptographie est une discipline qui s'attache à protéger les données en les rendant secrètes (on dit : en les chiffrant) avec une clef. La cryptologie est la science qui permet à la fois de protéger les données mais aussi d'analyser le niveau de cette protection (on parle de cryptanalyse).

RSA
Le chiffrement RSA est un algorithme de cryptographie, très utilisé pour échanger des données confidentielles sur Internet. Il est basé sur un mécanisme asymétrique : une clef publique est transmise à la personne qui va transmettre un message pour mélanger son message avec cette clef de façon à ce que le message devienne secret. Le destinataire du message va pouvoir démêler le message de la clef publique avec une deuxième clef, dite privée, qu'il est le seul à détenir et qui est le seul moyen de déchiffrer le message.

Clef de chiffrement
C'est un paramètre qui, avec l'algorithme de chiffrement, permet de chiffrer ou déchiffrer un message. Quand on utilise, pour déchiffrer un message, la même clef qui a permis de le chiffrer, on parle de chiffrement symétrique (cas de notre première activité). Quand les deux clefs sont différentes, on parle de chiffrement asymétrique (cas du système RSA).

Plus de définitions sur pixees.fr

MODULE #2 | Manipulez l'information
ANNEXE 2 – ROUE DE CÉSAR

INSTRUCTIONS

1. Couper les deux cercles
2. Fixer le cercle plus petit sur le plus grand à l'aide du point central
3. Les lettres en vert (grand cercle) sont les lettres de l'alphabet et celles en bleu (petit cercle) sont les lettres du message chiffré
    - pour chiffrer : vert -> bleu
    - pour déchiffrer : bleu -> vert
    - pour changer de clef : faire tourner l'un des deux cercles