Craque le code

5e à la 7e année

Actua | 111 Murray Street, Ottawa, ON K1N 5M5 | www.actua.ca | 613 234 4137

Jeunesse · STIM · Innovation
Youth · STEM · Innovation

Craque le code

Conditions d'utilisation

Avant de réaliser cette activité en tout ou en partie, vous reconnaissez et acceptez ce qui suit :

- Il vous appartient de passer en revue toutes les sections du présent document et la documentation connexe ainsi que d'appliquer les consignes de sécurité nécessaires à la protection de toutes les personnes concernées;
- Les mesures précisées à la rubrique « Consignes de sécurité » du présent document ne sont pas exhaustives ni ne remplacent votre propre cadre d'examen de la sécurité;
- Actua n'est pas responsable des dommages attribuables à l'usage du présent contenu;
- Vous pouvez adapter ce document à vos besoins (le remanier, le transformer ou créer du matériel à partir de celui-ci), à condition d'indiquer qu'Actua en est l'auteur original et que vous y avez apporté des changements. Ce contenu ne peut être transmis à de tierces parties sans la permission écrite d'Actua.

À propos d'Actua

Représentant plus de 40 universités et collèges à travers le pays, Actua est le principal réseau de sensibilisation des jeunes aux sciences, à la technologie, à l'ingénierie et aux mathématiques (STIM) au Canada. Chaque année, 350 000 jeunes prennent part à des ateliers pratiques, à des camps et à des projets communautaires inspirants dans plus de 500 localités d'un océan à l'autre. Actua met l'accent sur la participation de jeunes sous-représentés dans le cadre de programmes destinés aux Autochtones, aux filles et aux jeunes femmes, aux jeunes à risque ainsi qu'à ceux vivant dans des communautés nordiques ou éloignées. Pour de plus amples renseignements, consultez notre site web à actua.ca et suivez-nous sur Twitter, Facebook, Instagram et YouTube!

Craque le code

Présentation de l'activité

Dans cette activité, les élèves se familiariseront avec la cryptographie et des méthodes de chiffrement et de déchiffrement efficaces pour la protection des données et des renseignements personnels. Les élèves apprendront aussi à créer des mots de passe forts et mémorisables.

Cette activité fait partie d'une série d'activités basées sur l'éducation cybernétique. La suite comprend : La citoyenneté numérique et toi, La présence en ligne, Cyberdétective, La nétiquette, Craque le code et Sécurise ton réseau. Explorez le Guide pédagogique pour former des jeunes cyberfutés pour apprendre comment vous pouvez introduire l'éducation cybernétique dans votre milieu éducatif.

Activité conçue par Actua, en 2021.

Environnement	Durée	Public cible	Spécifications techniques
En personne	1 heure	5e-7e année (10-13 ans)	Certains exercices nécessitent l'utilisation d'un ordinateur portable ou d'une tablette. Moyennant certaines modifications, on peut regrouper les élèves en équipes de deux ou plus. **Les responsables de l'animation doivent avoir à leur disposition un ordinateur portable, un projecteur, des haut-parleurs et un écran ou un mur vierge pour y faire des projections.** • Projecteur

Environnement	Durée	Public cible	Spécifications techniques
			• Haut-parleurs • Écran ou mur vierge • Ordinateurs portables ou tablettes

Résultats d'apprentissage

À la fin de l'activité, les élèves pourront :

- comprendre le rôle de la cryptographie dans la gestion des renseignements personnels;
- utiliser et expliquer à leur entourage les principales stratégies à appliquer pour créer des mots de passe forts et uniques ainsi que pour protéger ses données personnelles.

OUTILS	COMPÉTENCES	ATTITUDES
Connaissances, ressources et expériences • Cryptographie • Chiffrement • Déchiffrement • Mots de passe forts et uniques	**Compétences numériques et en STIM, et aptitudes essentielles à l'employabilité et à la vie quotidienne** • Comportement sûr et responsable en ligne • Numératie • Jugement critique	**Intelligence numérique, action communautaire et pensée computationnelle** • Gestion des renseignements personnels • Pensée logique • Culture informatique

OUTILS	COMPÉTENCES	ATTITUDES
	• Faculté d'analyse • Résolution de problème	

Logistique (durée, taille du groupe, matériel)

Section	Durée estimée	Taille du groupe	Matériel
Introduction	10 minutes	*Tout le groupe*	**Responsable de l'animation** • Tableau et marqueur **Par élève** • Papier et crayon
1 . Déchiffrer des codes secrets	20 minutes	*Tout le groupe*	**Responsable de l'animation** • The Caesar cipher | Journey into cryptography | Computer Science | Khan Academy (sous-titrage en français)

Section	Durée estimée	Taille du groupe	Matériel
			• Craque le code (présentation) **Par élève** • Papier et crayon
2. Créer des mots de passe	20 minutes	*Individuellement*	**Responsable de l'animation** • #WorldPasswordDay TikTok (en anglais) • Sensibiliser les élèves aux questions de sécurité et de confidentialité sur Internet • Tableau et marqueur **Par élève** • Papier et crayon
Réflexion et récapitulation	10 minutes	*Tout le groupe*	**Responsable de l'animation** • Code Breakers Of Bletchley Park (en anglais)

Consignes de sécurité

Les consignes de sécurité ci-dessous ne sont pas exhaustives. Veillez à passer en revue l'activité et à inspecter l'environnement où elle sera réalisée afin de déterminer si des mesures additionnelles sont requises pour assurer la sécurité des élèves.

Sécurité émotionnelle

Ce projet vise à fournir aux jeunes les outils et les connaissances nécessaires pour comprendre les comportements en ligne et prendre des décisions sécuritaires.

- Tenez compte du fait que les élèves n'ont pas toutes et tous les mêmes expériences et connaissances en matière de pratiques cybersécuritaires, de cybersécurité et de citoyenneté numérique. La présente activité pourrait vous amener à discuter de sujets délicats, comme la cyberintimidation et d'autres cyberrisques. Veuillez préserver en tout temps la sécurité émotionnelle des jeunes et vous reporter à la formation reçue à votre établissement et pour ce projet.
- Orientez la discussion vers les comportements sains et sûrs en ligne et encouragez les jeunes à faire des choix responsables, informés et judicieux.

Sécurité en ligne

Certains volets de cette activité nécessitent l'usage d'appareils connectés à Internet.

- Examinez au préalable les vidéos, les sites web et le matériel prévus afin de vous assurer qu'ils conviennent à vos élèves.
- Au besoin, rappelez aux jeunes de se concentrer sur la tâche à faire et d'utiliser uniquement les liens fournis pour l'activité.
- Donnez l'exemple et encouragez l'adoption de comportements appropriés en ligne (poser des questions et y répondre dans la boîte de clavardage, employer un langage positif et motivant, utiliser les appareils uniquement pour réaliser l'activité, etc.).

Liens avec le programme d'études

Chacune des activités s'aligne avec ces trois aspects du Cadre de référence pancanadien pour l'enseignement de l'informatique :

Ordinateurs et réseaux : Cybersécurité

- L'élève débutant devrait pouvoir définir le concept de cybersécurité et créer des mots de passe sûrs selon des critères d'efficacité. L'élève compétent devrait pouvoir décrire des types courants de cyberattaques et reconnaître le contenu malveillant, appliquer des moyens de prévention et évaluer le rôle joué par les personnes dans la création, la prévention et la réduction de la portée des cyberattaques ainsi que leurs effets sur la population et la société (p. 24).

Données : Gouvernance des données

- L'élève débutant devrait pouvoir nommer des manières dont les activités numériques ou physiques créent des données numériques et régler les paramètres de confidentialité sur des outils numériques couramment utilisés. L'élève compétent devrait pouvoir déterminer qui possède ses données numériques, évaluer les lois et les politiques provinciales et fédérales sur la gouvernance des données et les accords autochtones sur la gouvernance des données et comprendre, ainsi que défendre ses droits par rapport aux données et ceux des autres (p. 26).

Technologie et société : Éthique, sécurité et politique

- L'élève débutant devrait pouvoir décrire des stratégies pour protéger ses renseignements personnels et son identité en ligne. L'élève compétent devrait pouvoir définir et appliquer des principes de base en lien avec les droits d'auteur, expliquer les problèmes liés à la vie privée et évaluer les effets de la cybercriminalité et du piratage sur soi-même et la société (p. 28).

Marche à suivre

Préparation

Section	Préparation

Généralités	• **Préparez l'activité et les mesures d'adaptation requises, s'il y a lieu :**
	  ○ Déterminez votre **mode d'enseignement** et puisez des idées, au besoin, dans les sections Recommandations selon le mode d'enseignement et Possibilités d'adaptation.
	  ○ Même si la **durée estimée** est précisée, il peut être utile de réfléchir au temps que vous voulez consacrer aux différents exercices et aux discussions.
	  ○ La **taille du groupe** indiquée (en équipes de deux ou plus, ou individuellement) n'est qu'une suggestion et peut être adaptée aux besoins de votre classe.
	• **Contenu :**
	  ○ Préparez des **réponses** aux diverses questions de réflexion posées durant l'activité.
	  ○ Examinez les vidéos et le matériel fournis à l'annexe C pour déterminer si leur contenu **convient** à vos élèves.
	• **Matériel :**
	  ○ Vérifiez que votre appareil, l'écran et le projecteur sont bien installés et fonctionnels.
	  ○ Préparez les appareils des élèves.

Introduction	• Écrivez au tableau le message fourni.

Section	Préparation
1. Déchiffrer des codes secrets	• Familiarisez-vous avec les concepts de chiffrement et de déchiffrement et mettez à l'essai chacun des défis (en particulier le défi 1): Craque le code
2. Créer des mots de passe	• Exercez-vous à suivre la séquence de création d'un mot de passe décrite à l'étape 5.

Introduction

1. Écrivez ce message au tableau : « Protégez vos renseignements personnels. »
2. Remettez à tous les élèves un crayon et un papier et demandez-leur d'« encoder » le message. La phrase doit conserver le même sens, mais être impossible à déchiffrer pour une autre personne que celle qui l'a encodée.
    a. ***Remarque :*** Rappelez aux élèves de noter leur code, c'est-à-dire les signes utilisés pour remplacer les lettres. Il peut s'agir par exemple de symboles, d'émojis, de chiffres ou d'autres lettres.
3. Expliquez-leur que cet exercice constitue un exemple de chiffrement ou de « cryptage » (l'art d'écrire des codes). Le déchiffrement, c'est donc l'art de déchiffrer des codes, ou ce qu'on appelle aussi parfois « décryptage », « craquage » ou « cassage » de codes. Les jeunes auront l'occasion d'explorer davantage le chiffrement et le déchiffrement dans le prochain exercice.

1. Déchiffrer des codes secrets

1. **Quels types de renseignements souhaiteriez-vous garder secrets (confidentiels) sur Internet?**
    a. **Réponses possibles :** mots de passe (pour les appareils mobiles, les médias sociaux, les plateformes de jeux, etc.), photos de famille, conversations avec des amis, documents utilisés pour l'école ou le travail, lieux de vacances, boutiques fréquentées, dossier médical, etc.

        i. Tous vos renseignements personnels, en particulier les données permettant de vous identifier, devraient rester confidentiels : nom et prénom, âge, adresse courriel, numéro de téléphone, photos de vous, etc.

2. Annoncez aux jeunes qu'elles et ils vont maintenant déchiffrer des messages à l'aide du chiffre de César. Montrez-leur cette vidéo : The Caesar cipher | Journey into cryptography | Computer Science | Khan Academy (sous-titrée en français) (Khan Academy, 0:00-**1:03**)
3. Affichez cette présentation : Craque le code (voir les Notes de présentation pour les détails). Remettez aux jeunes du papier et un crayon pour la réalisation du Défi 1; si vos élèves ont besoin d'un plus grand défi, passez à l'un des suivants.
    a. Cet exercice a pour but de montrer que plus un message est difficile à déchiffrer, mieux il protège les renseignements personnels et les données sensibles. C'est pourquoi, par exemple, les comptes munis d'un mot de passe fort et unique sont plus difficiles à pirater.

2. Créer des mots de passe

L'opération de chiffrement (comme celle réalisée dans l'exercice précédent) constitue une mesure simple pour augmenter la protection d'un mot de passe pendant qu'il se trouve sur un serveur ou circule sur Internet. En gros, le chiffrement brouille le mot de passe afin de le rendre illisible et/ou inutilisable par des pirates. Cependant, cette protection ne suffit pas; il est tout aussi important d'avoir un mot de passe fort.

1. Montrez cette vidéo #WorldPasswordDay TikTok (OnlineKyne, 0:30, en anglais) créée par Kyne Santos, qui démontre mathématiquement l'importance de créer des mots de passe forts.
2. Voici quelques exemples de questions pour lancer la discussion :
    a. **« À quoi servent les mots de passe? »**
        i. *Réponses possibles :* à protéger nos renseignements personnels, à empêcher les autres d'accéder au contenu de nos appareils ou

de se connecter à nos comptes de jeux en ligne, à protéger les données qui servent à nous identifier en ligne, à éviter que des gens accèdent à nos systèmes (p. ex. Xbox ou Wi-Fi résidentiel).

ii. ***Remarque :*** Pour faciliter la compréhension des élèves qui ne sont pas familiers avec les mots de passe, vous pouvez comparer ceux-ci à un cadenas (pour verrouiller un vélo, un casier, un journal intime, etc.). Comme la clé ou la combinaison d'un cadenas, un mot de passe doit être unique pour assurer une protection efficace.

b. **« Quels types de comptes ou d'appareils ont besoin d'un mot de passe? »**

i. *Réponses possibles :* dossier et courriel scolaires, courriel personnel, compte bancaire en ligne, comptes de jeux, comptes Facebook, Instagram, Snapchat ou TikTok, appareils (téléphone, ordinateur portable ou de bureau, etc.).

c. **« Pourquoi est-ce important d'avoir des mots de passe ou des procédés d'authentification forts et uniques? »**

i. Exemples de procédés d'authentification : lecteur d'empreintes digitales, reconnaissance faciale, accès par NIP, schéma de déverrouillage.

3. Démarrez un remue-méninges en notant au tableau les réponses des élèves à la question suivante : **« Quelles méthodes peuvent servir à créer des mots de passe forts et à protéger nos renseignements personnels? »** (pour en savoir plus, voir l'annexe B, Information documentaire).
4. Montrez cette vidéo : Sensibiliser les élèves aux questions de sécurité et de confidentialité sur Internet (Google for Education, 4:00). Demandez aux jeunes si d'autres stratégies pourraient être ajoutées à la liste.
5. Parcourez les étapes ci-dessous avec les jeunes pour leur montrer comment transformer un mot de passe faible en mot de passe fort (le mot de départ a été choisi au hasard). Écrivez les différentes versions du mot de passe au

tableau et demandez aux jeunes de nommer les changements qui y ont été apportés pour le renforcer.

   a. **trésors (Ceci est le mot de passe faible de départ)**
   b. **Coffre aux** trésors **bien rempli** (+ On en fait une phrase)
   c. **C**offreaux**T**résorsbien**R**empli (+ On colle tous les mots ensemble et on ajoute une lettre majuscule au début de certains mots)
   d. CaTbR (On crée un sigle à partir de la première lettre de chaque mot)
   e. CaTbR**01** (On ajoute un ou des chiffres qu'on va mémoriser)
   f. Ca*****TbR01***** (On ajoute des symboles qu'on va mémoriser)

6. C'est maintenant le tour des élèves! Donnez-leur du papier, un crayon et un mot au hasard, puis demandez-leur de partir de ce dernier pour créer un mot de passe fort à l'aide de la méthode que vous venez de présenter (transformation en phrase, combinaison de lettres majuscules et minuscules, ajout de symboles, etc.).
   a. Exemples : étoile, arbre, mathématiques... Comment peut-on renforcer ces mots de passe?

Réflexion et récapitulation

1. **« Qu'est-ce qu'il faut faire pour protéger ses mots de passe? »**
   a. *Réponses possibles : avoir un mot de passe différent pour chaque compte, toujours se déconnecter (fermer sa session) avant de quitter un site, ne jamais révéler son mot de passe aux autres, ni le noter par écrit, utiliser un gestionnaire de mots de passe, etc.*
2. **Lien avec une profession :** Montrez la vidéo Code Breakers Of Bletchley Park (CBS, *0:00-**1:09**) (en anglais). Cette vidéo souligne le rôle essentiel des femmes durant la Deuxième Guerre mondiale et dans le domaine de la cryptographie en général.
3. Encouragez les élèves à devenir des ambassadrices et des ambassadeurs cyberfutés en transmettant à leur famille et à leurs amis les stratégies apprises durant cette activité.

Recommandations selon le mode d'enseignement

Ce contenu a été conçu pour l'enseignement en personne, mais peut être présenté dans d'autres contextes. Voici des recommandations pour l'enseigner à distance (en ligne) ou dans un environnement « débranché » (avec peu ou pas de support technologique).

À distance (en ligne)	Débranché (peu ou pas de techno)
Généralités	
• Invitez les jeunes à ouvrir leur micro ou à utiliser la boîte de clavardage, à leur convenance. • Utilisez un outil permettant à tous les élèves de participer aux discussions en ligne (Mentimeter, Jamboard, etc). • Notez les liens à fournir aux élèves et copiez-les dans la boîte de clavardage au moment opportun. • Faites appel à des sondages ou à d'autres formes d'interactions en groupe pour faire le point avec les élèves et maintenir leur niveau de motivation.	• Utilisez un tableau pour faire des remue-méninges et noter les idées et réponses des jeunes.
Introduction	

À distance (en ligne)	Débranché (peu ou pas de techno)
• Grossissez la phrase chiffrée à l'écran.	• Pour expliquer les opérations de chiffrement et de déchiffrement, utilisez de l'encre invisible au jus de citron : https://fr.wikihow.com/%C3%A9crire-un-message-%C3%A0-l%E2%80%99encre-invisible#:~:text=Fabriquer%20de%20l'encre%20invisible%20avec%20du%20bicarbonate%20de%20soude,-1&text=Versez%2060%20ml%20de%20bicarbonate,un%20morceau%20de%20papier%20blanc
1. Déchiffrer des codes secrets	
• Sélectionnez l'option Pointeur laser lors de la présentation des diapositives. • L'exercice peut être réalisé tel quel en ligne. Le remue-méninges peut se faire verbalement ou au moyen d'un outil de collaboration (Jamboard, Google Doc, Mentimeter, etc.).	• Au lieu d'afficher la présentation, écrivez un exemple au tableau et notez les défis à relever sur une grande tablette de papier (*voir la présentation*).
2. Créer des mots de passe	

À distance (en ligne)	Débranché (peu ou pas de techno)
• Utilisez les salles de sous-groupe; demandez aux élèves de faire l'exercice individuellement, puis d'écrire leurs mots de passe dans la boîte de clavardage pour voir lequel est le plus fort.	• Faites ce jeu qui permet de mettre à l'épreuve un mot de passe en suivant une série d'instructions verbales : https://curriculum.code.org/csf-19/coursec/2/#powerful-passwords 4 (en anglais)
Réflexion et récapitulation	
• L'exercice peut être réalisé tel quel en ligne. Le remue-méninges peut se faire verbalement ou au moyen d'un outil de collaboration (Jamboard, Google Doc, Mentimeter, etc.).	• L'exercice peut être réalisé tel quel, sans support technologique.

Possibilités d'adaptation

Il est possible d'adapter différents aspects de cette activité (durée, environnement, matériel, taille du groupe ou instructions) pour la rendre plus accessible ou plus complexe. Les **modifications** ci-dessous vous permettront de diminuer le niveau de difficulté de l'activité et les **ajouts,** d'augmenter sa durée ou son niveau de difficulté.

Modifications

GÉNÉRALITÉS

- Sélectionnez l'option de sous-titrage (si disponible) pour la diffusion des vidéos.
- Fournissez une souris aux jeunes pour faciliter l'utilisation de l'ordinateur portable.
- Faites travailler les élèves en équipes de deux ou plus plutôt qu'individuellement.

1. DÉCHIFFRER DES CODES SECRETS

- Concentrez-vous sur les défis 1 et 2 dans la présentation.
- Aidez les élèves en leur fournissant des solutions partielles aux messages chiffrés.
- Donnez plus de temps aux jeunes pour déchiffrer les messages.
- Répartissez les élèves en équipes et remettez à chaque groupe une copie imprimée de l'alphabet.

Ajouts

1. DÉCHIFFRER DES CODES SECRETS

- Activité de chiffrement Simple Encryption (en anglais) créée pour l'Heure de Code.

2. CRÉER DES MOTS DE PASSE

- Invitez les élèves à évaluer la force de leur mot de passe selon les cinq façons proposées par le gouvernement du Canada.
    - Par la suite, demandez-leur si cette évaluation les a incités à apporter des améliorations à leur mot de passe, et, si oui, lesquelles.
- Jeu pour tester la force d'un mot de passe (en anglais) (les jeunes avancent ou reculent d'un certain nombre de pas selon que leur mot de passe correspond ou non au critère énoncé).

- Jeu de déchiffrage de mots de passe de Nova Lab (les élèves devront résoudre un problème d'attaque de virus avant de pouvoir choisir le défi de déchiffrement de mot de passe, qui traite du piratage par essai-erreur ou « attaque par force brute »).
    - ***Remarque*** : Ce jeu est en anglais seulement et fonctionne mieux dans Google Chrome.

RÉFLEXION ET RÉCAPITULATION

- Les élèves peuvent créer une affiche avec Canva afin de faire connaître à leurs amis et à leur famille les stratégies à adopter lorsqu'on interagit avec de nouvelles personnes en ligne. Transmettez-leur ce lien utile https://www.canva.com/fr_fr/affiches/modeles/campagne-affichage/ et explorez vous-même toutes les possibilités de cet outil.
    - Montrez rapidement aux jeunes comment créer et personnaliser un projet dans Canva. Si cela facilite l'activité, sélectionnez vous-même un modèle sur la plateforme plutôt que de laisser ce choix aux élèves ou de les laisser dessiner leur propre affiche.
    - Les élèves peuvent concevoir leur affiche sur papier plutôt que d'utiliser Canva.
    - Si le temps le permet, invitez les élèves à présenter leur affiche à la classe.

Références et remerciements

Binance Academy. (Décembre 2020). *History of Cryptography*. https://academy.binance.com/en/articles/history-of-cryptography

Betterteam. (16 mai 2019). *Mathematician Job Description*. https://www.betterteam.com/mathematician-job-description

CBS. (8 décembre 2008). *Code Breakers Of Bletchley Park* [vidéo]. https://www.youtube.com/watch?v=2458QZmNxRY

Cisco. (s. d.) *What is Multi-Factor Authentication?* https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html

Google. (s. d.) *Créer un mot de passe sécurisé pour un compte plus sûr*. https://support.google.com/accounts/answer/32040?hl=fr#zippy=%2Cmake-your-password-longer-more-memorable

Google for Education. (6 septembre 2017,). *Sensibiliser les élèves aux questions de sécurité et de confidentialité sur Internet* [Vidéo]. https://www.youtube.com/watch?v=l81bevjAr-c&ab_channel=GoogleforEducations

Gouvernement du Canada. (15 janvier 2020). *Votre mot de passe est-il suffisamment robuste? Voici cinq façons de l'évaluer*. https://www.pensezcybersecurite.gc.ca/fr/blogues/votre-mot-de-passe-est-il-suffisamment-robuste-voici-cinq-facons-de-levaluer

Gouvernement du Canada. (s. d.). *Phrases de passe, mots de passe et NIP*. https://www.pensezcybersecurite.gc.ca/fr/securisez-vos-comptes/phrases-de-passe-mots-de-passe-et-nip

Khan Academy. (27 mars 2012). *The Caesar cipher | Journey into cryptography | Computer Science | Khan Academy* [Vidéo sous-titrée en français]. https://www.youtube.com/watch?v=sMOZf4GN3oc

L'Encyclopédie canadienne. (16 juillet 2018). *Transmetteurs en code cri*. https://www.thecanadianencyclopedia.ca/fr/article/cree-code-talkers

MinuteVideos. (30 janvier 2017). *Cryptography and privacy. An easy explanation on how to create a key for encryption* [Vidéo]. https://www.youtube.com/watch?v=MU1Scwxc_RU

National Institute of Standards and Technology. (9 décembre 2019). *Back to basics: Multi-factor authentication (MFA)*. https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication

NordPass. (2021). *Top 200 des mots de passe les plus utilisés*. https://nordpass.com/fr/most-common-passwords-list/

OnlineKyne. (6 mai 2021). *#WorldPasswordDay* [Vidéo]. https://www.tiktok.com/foryou?is_copy_url=1&is_from_webapp=v1&item_id=6959281467310624006#/@onlinekyne/video/6959281467310624006

TechNation Canada. (s. d.) Description des postes. https://lmi.technationcanada.ca/fr-ca/job-descriptions/Cryptographe%2FCryptanalyste

Université d'Ottawa. (2020). *L'importance des mots de passe*. https://ti.uottawa.ca/securite/identite-authentification-vol

Annexes

Annexe A : Liens avec des professions

GENDARMERIE ROYALE DU CANADA : ANALYSTE DE RENSEIGNEMENTS EN CYBERCRIMINALITÉ

- L'analyste de renseignements en cybercriminalité élabore des stratégies pour cerner les types de cybercrimes et les tendances en la matière. Elle ou il utilise cette information pour concevoir des outils de renseignement stratégique et pour fournir son avis lors d'enquêtes criminelles complexes.

SPÉCIALISTE EN CYBERSÉCURITÉ (SPÉCIALISTE EN SÉCURITÉ DE L'INFORMATION)

- La ou le spécialiste en cybersécurité repère les vulnérabilités des systèmes informatiques et des logiciels ainsi que les menaces visant ceux-ci. Elle ou il élabore des mesures de sécurité et des solutions afin de protéger les systèmes contre les cybercrimes tels que le piratage et les logiciels malveillants. Ces mesures et solutions peuvent prendre la forme de technologies ou de processus organisationnels.

ANALYSTE EN CYBERSÉCURITÉ (ANALYSTE EN SÉCURITÉ DE L'INFORMATION)

- L'analyste en cybersécurité surveille les réseaux et les systèmes informatiques d'une entreprise et protège ceux-ci contre les menaces et les brèches informatiques en élaborant et implantant des mesures de sécurité.

CRYPTOGRAPHE

- La ou le cryptographe met au point des systèmes de sécurité qui chiffrent les données à l'aide d'algorithmes et de codes. Elle ou il veille à protéger les données importantes et sensibles (financières, personnelles, d'entreprise, etc.) contre les accès non autorisés.

CRYPTANALYSTE

- La ou le cryptanalyste analyse et déchiffre les messages et les données chiffrés (l'inverse du rôle de la personne cryptographe).

MATHÉMATICIENNE, MATHÉMATICIEN

- La mathématicienne ou le mathématicien emploie des théories et des techniques mathématiques (p. ex. la collecte, l'analyse et la présentation de données) pour résoudre des problèmes pratiques dans divers secteurs, comme le génie, la science, les affaires et l'administration publique.

Annexe B : Information documentaire

CRYPTOGRAPHIE

La cryptographie consiste à transformer un texte écrit en clair en code sécurisé, déchiffrable uniquement par la personne à laquelle il est destiné. Il existe de nombreuses façons de chiffrer un message et la plupart utilisent des formules mathématiques complexes. La cryptographie concerne l'ensemble du processus de sécurisation des communications, qui comprend entre autres les opérations de chiffrement et de déchiffrement.

Exemples d'usages de la cryptographie dans l'histoire

- Égypte (il y a 3 900 ans) : Le remplacement de symboles (la forme la plus primaire de cryptographie) apparaît pour la première fois en Égypte ancienne et en Mésopotamie. Le premier exemple connu de cette pratique a été trouvé dans la tombe d'un noble égyptien.
- Inde ancienne et cité-État grecque de Sparte (dernière période de l'Antiquité) : La cryptographie est largement utilisée pour protéger les renseignements militaires importants.
- Empire romain : Création et usage du chiffre de César, la méthode de chiffrement la plus perfectionnée du monde antique.
- Armée américaine (jusqu'à la fin de la Deuxième Guerre mondiale) : Dans les années 1790, Thomas Jefferson invente un cylindre pour chiffrer et

déchiffrer les messages. Cette méthode est si ingénieuse que l'armée américaine s'en est servi jusqu'à la fin de la Deuxième Guerre mondiale. Durant les deux guerres mondiales, on a fait appel à des transmetteurs en code pour concevoir un système de chiffrement basé sur les langues autochtones. Ces soldats autochtones ont fait appel à leur connaissance de leur langue maternelle pour chiffrer et déchiffrer des renseignements sensibles.

CHIFFREMENT ET DÉCHIFFREMENT

Dans le cadre de la présente activité, le chiffrement consiste à encoder un message afin qu'il soit impossible à lire, sauf par la personne à laquelle il est destiné, et le déchiffrement, à déchiffrer un message afin de le rendre lisible. Il existe de nombreuses formes de chiffrement et la plupart utilisent des formules mathématiques complexes pour protéger les données. Il sera question ici de deux méthodes de chiffrement. Pour en savoir plus, visitez : https://www.w3schools.in/cyber-security/modern-encryption/ (en anglais) ou https://fr.wikipedia.org/wiki/Cryptographie (en français).

Le chiffre de César

Le chiffre de César, nommé d'après le plus célèbre des empereurs romains, constitue la forme la plus simple de chiffrement.

1. Pour *chiffrer* un message, on décale chaque lettre qui le compose d'un nombre déterminé de positions de l'alphabet, vers la droite. Le nombre de positions est fourni par la clé du message.
2. Pour *déchiffrer* ce message, on décale les lettres du même nombre de positions indiqué par la clé, mais vers la gauche.

Exemple : Le message est le prénom « JIM ».

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

Supposons qu'on utilise une clé de 3 pour chiffrer ce message. Chaque lettre sera décalée de trois positions, comme ceci :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

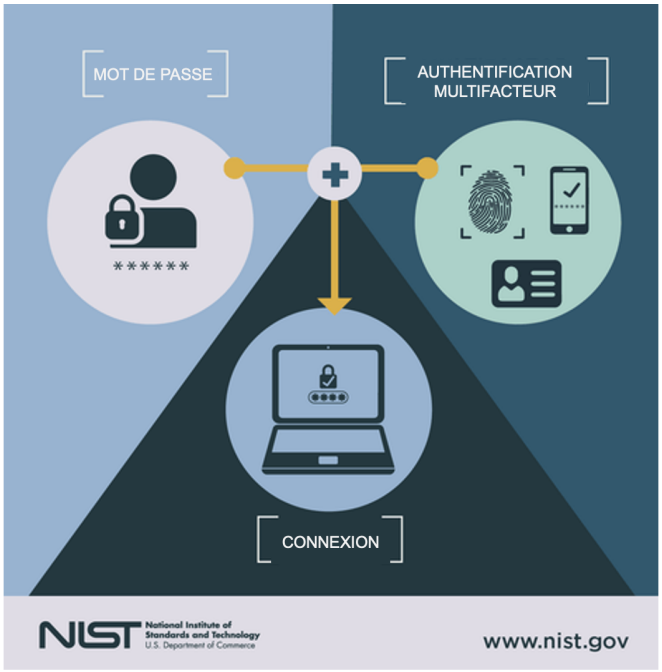
Le message chiffré est « MLP » :

- Le « J » décalé de trois positions devient un « M »;
- Le « I » décalé de trois positions devient un « L »;
- Le « M » décalé de trois positions devient un « P ».

Si vous recevez ce message chiffré avec une clé de 3, il vous suffira de décaler chaque lettre de trois positions vers la gauche pour le déchiffrer. Pour en savoir plus sur le chiffre de César, visitez Caesar Cipher (en anglais) ou le chiffrement par décalage (en français).

BONNES PRATIQUES POUR CRÉER DES MOTS DE PASSE FORTS

- **Lien avec l'informatique :** Pour accroître la protection fournie par les mots de passe forts, on utilise de plus en plus les données biométriques (reconnaissance faciale, vocale, des empreintes digitales et même de l'ADN).
- Utiliser un mot de passe distinct pour chaque compte.
- Plus un mot de passe est long, plus il est efficace (phrases de passe ou secrètes).



- Un mot de passe sûr devrait comprendre au moins huit (8) caractères et comporter des lettres minuscules et majuscules, des chiffres et des symboles.

- Ne pas utiliser de renseignements personnels (date de naissance, nom ou prénom, adresse, etc.).
- Toujours se déconnecter avant de quitter un site, en particulier lorsqu'on utilise un réseau Wi-Fi public ou un ordinateur partagé.
- Éviter d'entrer son mot de passe lorsqu'on utilise une connexion Wi-Fi non sécurisée (p. ex. le Wi-Fi d'un café).
- Ne jamais révéler son mot de passe aux autres ni le noter par écrit.
- Ne pas autoriser un navigateur Internet à enregistrer ses mots de passe.
- S'assurer que personne ne regarde lorsqu'on entre son mot de passe.
- Activer l'authentification à deux facteurs (ou encore mieux, multifacteur).

AUTHENTIFICATION MULTIFACTEUR

Procédure de sécurité qui requiert au moins deux facteurs d'authentification parmi les suivants :

- mémoriel (ce que l'on sait) : un mot de passe ou un code d'accès;
- corporel (ce que l'on est) : des données biométriques, comme l'empreinte digitale ou vocale;
- matériel (ce que l'on possède) : un téléphone ou un jeton.

Exemples d'utilisation :

- Lorsqu'on accède à une boîte de courriel ou à un appareil pour la première fois, on peut nous demander de fournir un mot de passe (facteur mémoriel) et un code spécial envoyé à notre téléphone (facteur matériel).
- Pour accéder à un édifice sécurisé, on peut avoir besoin d'un code (facteur mémoriel) et/ou d'une carte d'accès (facteur matériel).
- Pour ouvrir son appareil, il faut utiliser la fonction d'identification d'empreinte digitale (facteur corporel) et/ou son mot de passe (facteur mémoriel).

Annexe C : Autres ressources

1. DÉCHIFFRER DES CODES SECRETS

Présentation PowerPoint

- Craque le code

Vidéo

- The Caesar cipher | Journey into cryptography | Computer Science | Khan Academy (Khan Academy, 0:00-1:03) (sous-titrée en français)

2. CRÉER DES MOTS DE PASSE

Vidéos

- #WorldPasswordDay TikTok (OnlineKyne, 0:30 s) (en anglais)
- Sensibiliser les élèves aux questions de sécurité et de confidentialité sur Internet (Google for Education, 4:00)

RÉFLEXION ET RÉCAPITULATION

Vidéo

- Code Breakers Of Bletchley Park (CBS, *0:00-1:09) (en anglais)