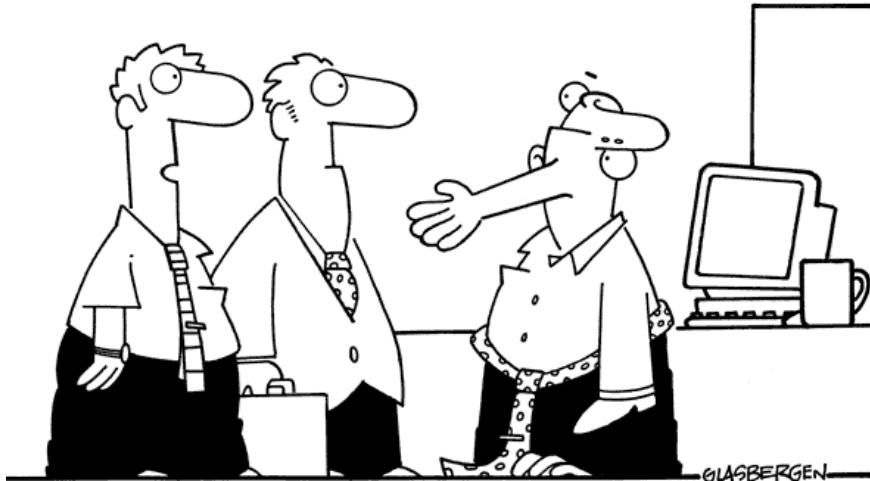


Sécurité informatique

INF36207

Martin Arsenault, ing., MBA, MGP
Janvier 2026

Copyright 2002 by Randy Glasbergen.
www.glasbergen.com



"That's our CIO. He's encrypted for security purposes."





Activités de la soirée!

- Mot de Bienvenue!
- Fonctionnement en vidéoconférence
- Qui suis-je et comment me rejoindre ?
- Organisation de mes déplacements
- Revue du plan de cours
- Théorie :
 - Qu'est-ce que la sécurité informatique?
 - Qu'est-ce qu'une attaque informatique?
 - Qui sont les attaquants?
 - Qu'est-ce qui motive les attaquants?
 - Cybercriminalité, cyberterrorisme, et « hacktivisme » : mythes et réalités.
 - Stratégies de défense.



Fonctionnement en vidéoconférence

- Quelques consignes pour s'assurer que tout le monde entend bien et comprend bien :
 - Les micros ne fonctionnent pas et ne discriminent pas les bruits comme le font nos oreilles → Attention aux bruits de chaises, mouvements, manipulations d'objets : Tous les bruits sont captés par les micros.
 - Si à distance vous voulez parler, lever la main ou appeler mon nom.
 - Je ne peux pas distribuer les documents en mains propres sur les 2 sites, je vais les déposer sur Moodle, idéalement, ayez avec vous votre ordinateur pour les récupérer lors de nos sessions de cours.
- 1 ou 2 responsables par site pour aider au démarrage de la salle lorsque je suis sur l'autre site.
 - Ouverture/fermeture du canon et des téléviseurs + Ajustement des caméras

PREFERABLE DE NE PAS MANGER VOS CHIPS EN CLASSE OU DE DISCUTER AVEC VOS VOISINS PENDANT LE COURS !!! 😊



Tour de table

PRÉNOM ET NOM

VOTRE PARCOURS PROFESSIONNEL, S'IL Y A LIEU

VOTRE PROGRAMME
AUQUEL VOUS ÊTEZ
INSCRIT

VOTRE EXPÉRIENCE
AVEC LA SÉCURITÉ
INFORMATIQUE

VOTRE AVANCEMENT
DANS LE PROGRAMME

VOS ATTENTES SUR LE COURS

VOTRE FILLE
DE VOTRE MÈRE, VOTRE
VIE DE NAISSANCE, LA
MARQUE DE VOTRE
MÈRE VOUS

LE NOM DE JEUNE FILLE
DE VOTRE MÈRE, VOTRE
VIE DE NAISSANCE, LA
MARQUE DE VOTRE
MÈRE VOUS



Qui suis-je ?

Pour me contacter
martin_arsenault@uqar.ca

- Formations :
 - Génie électrique spécialisé en télécom (ÉTS 2000)
 - Maîtrise en gestion de projet – Profil professionnel (UQAR 2010)
 - Maîtrise en administration des affaires – MBA exécutif pour cadre en exercice (UQAM 2017)
 - Plusieurs autres sur le plan professionnel : VoIP, Réseau, Linux, Sécurité, etc.
- Poste actuel : Directeur du service des ressources informationnelles au Centre de services scolaire des Phares
 - Responsable : Informatique, bibliothèques, archives et gestion documentaire et les conseillers pédagogiques soutenant les RI
- Sur le marché depuis 25 ans dans le domaine des TI, de la sécurité et des télécoms
- Expériences sur le marché du travail : Nortel Network, Vidéotron Télécom, Cégep de Rimouski, UQAR, Cogeco Câble, Télécommunication de l'est, CSPQ, Telus et CSSDP;
- Principalement sur des postes :
 - Ingénieurs / Analystes de système et de réseau
 - Coordination et Direction

Revue du plan de cours

UQAR Université du Québec à Rimouski
Département de mathématiques, informatique et de génie

PLAN DE COURS
SESSION HIVER 2026

SIGLE : INF36207
TITRE : Sécurité informatique
GROUPE : MS
HORAIRE DES COURS : Lundi 19h15 à 22h05
DÉBUT / FIN : 12 janvier au 27 avril 2026
LOCAL : Campus de Rimouski J-455 / Campus de Lévis 2059
CHARGÉ DE COURS : Martin Arsenault, ing., MBA, MGP
martin_arsenault@uqr.ca
COMMIS RESPONSABLE : Cathy Morin
cathy_morin@uqr.ca

DESCRIPTION DU COURS SELON L'ANNUAIRE

Objectifs : Connaitre les problèmes liés à la sécurité des systèmes informatiques et s'initier aux différentes techniques de détection des attaques et de protection des systèmes et de leurs données.

Contenu : Historique, Cibles probables et courantes, Vulnérabilités et types d'attaques, Sécurité dans les systèmes d'exploitation, Sécurité dans les bases de données, Sécurité dans les réseaux, Sécurité dans les logiciels, Cryptographie et cryptanalyse.

Insertion du cours dans le programme : Ce cours est disponible dans différents programmes offerts à l'UQAR dont le programme court de 1^{er} cycle en informatique appliquée, de même que le certificat, la majeure et le baccalauréat en informatique. Ce cours reprend des éléments d'autres cours (notamment la réalisation de programmes robustes et des notions de téléinformatique) pour permettre à l'étudiant de bien comprendre (du point de vue des attaques comme des programmeurs et des administrateurs de systèmes) les failles de sécurité possibles tout en l'outillant sur des techniques et des méthodes permettant une prévention, une détection et une remédiation efficaces.

Préalables :

- INF14107 – Architecture des systèmes informatiques
- INF15107 – Bases de données
- INF26207 – Téléinformatique

Évaluations

Évaluations	
informatique? Qu'est-ce qu'une clé qui motive les activismes? : mythes et	
renseignements personnels: analyse de risque et son Responsabilités légales.	
giques (authentification, (confidentialité, (intimité. Sécurité physique.	Énoncé TP#1
ité et anonymisation, niveau le produit? Est-ce sociale.	
gements simples es. Cryptanalyse des	
z de chiffrement ffs publiques/privées. iques. Stéganographie. tique. Politiques de	
o. Protocoles de du pare-feu. Règles de l'accès. Filtrage par la Capture de trafic et sécurité pour les	Remise du TP#1 Énoncé TP#2
	Examen intra
ics informatiques. t. scripts, SNMP, attaques réseau.	
sabilité et TACACS, LDAP et	Remise du TP#2 Énoncé TP#3
la propriété des DRM. Casser les systèmes. Groupes, accès, es USB, Bluetooth, thème d'exploitation.	
lles de WEP/WPA. ne architecture sans que a grande dentale et nommées.	
les. Injection de ces spécifiques su	
nux, Windows	
	Remise du TP#3 Examen final
assaire et approprié, après en avoir précisément	
est pas sécuritaire de réaliser les déplacements.	

Épreuves

Épreuves	Pondérations
ratique #1	15%
ratique #2	15%
ratique #3	20%
ntre	25%
inal	25%
	100%

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Évaluations	
incontré de trois heures chaque semaine en classe comportant des leçons ux pratiques, exercices, analyses de situations et études de cas. Étant donné entre Lévis et Rimouski, l'enseignant se déplacera entre les sites en fonction tions météorologiques. L'horaire des déplacements est présenté dans le	
ent prévus. Ils seront en équipe de 3 ou 4 personnes au maximum, au choix et se réserve le droit d'assigner les équipes pour certains travaux, s'il le juge t indiquées dans le calendrier des rencontres et les sujets des travaux seront nibilité des énoncés.	
in total de 50 %.	
total de 50 %.	
ours est répartie ainsi :	
Épreuves	Pondérations
ratique #1	15%
ratique #2	15%
ratique #3	20%
ntre	25%
inal	25%
	100%

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
A+	73% - 77%	C+
A	70% - 73%	C
A-	66% - 70%	C-
B+	62% - 66%	D+
B	60% - 62%	D
B-	< 60%	E

Évaluations

Cotes	Notes	Cotes
-------	-------	-------

Revue du plan de cours

- Objectifs :
 - Connaître les problèmes liés à la sécurité des systèmes informatiques et s'initier aux différentes techniques de détection des attaques et de protection des systèmes et de leurs données.
- Contenu :
 - Historique. Cibles probables et courantes. Vulnérabilités et types d'attaques. Sécurité dans les systèmes d'exploitation. Sécurité dans les bases de données, Sécurité dans les réseaux. Sécurité dans les logiciels. Cryptographie et cryptanalyse.

Insertion du cours dans le programme

- Ce cours est disponible dans différents programmes offerts à l'UQAR dont le programme court de 1^{er} cycle en informatique appliquée, de même que le certificat, la majeure et le baccalauréat en informatique. Ce cours reprend des éléments d'autres cours (notamment la réalisation de programmes robustes et des notions de téléinformatique) pour permettre à l'étudiant de bien comprendre (du point de vue des attaquants comme des programmeurs et des administrateurs de systèmes) les failles de sécurité possibles tout en l'outillant sur des techniques et des méthodes permettant une prévention et une remédiation efficaces.
- Préalables :
 - INF14107 – Architecture des systèmes informatiques
 - INF15107 – Bases de données
 - INF26207 – Téléinformatique

Mise en contexte du cours

- À la base de la sécurité informatique, on retrouve des **outils technologiques permettant d'assurer la sécurité des systèmes et des réseaux de même que la protection de données**. On retrouve également des **principes qui dictent les bonnes pratiques assurant une sécurité accrue des systèmes et des infrastructures**. Ce cours portera principalement sur les **aspects technologiques de la sécurité informatique** (réseaux, systèmes, outils, failles, protocoles, cryptographie, etc.) tout en abordant les différents **enjeux sociaux liés à la problématique de la sécurité informatique** (sensibilisation des acteurs sur les risques, déontologie, « hacktivisme », pirates, fraude, protection de la vie privée et confidentialité des données personnelles, etc.).
- De plus en plus de **systèmes et d'objets sont connectés à des réseaux privés et publics et assurent des fonctions de transmission, de traitement ou d'entreposage de données** pour eux-mêmes ou au nom de tiers systèmes. Ces systèmes et objets reliés sont souvent la **cible d'attaques de toutes sortes**. L'étudiant qui œuvra avec ces systèmes devra s'assurer de **comprendre la nature des attaques possibles et les risques qui s'y rattachent**. Il devra en tenir compte dans le but d'en assurer leur sécurité afin de garantir la disponibilité, l'intégrité et la confidentialité du système et des données qu'il comporte.
- Dans l'ère dans laquelle nous évoluons, où la **sensibilité du public à la sécurité et à la protection des renseignements personnels est hautement élevée**, il est essentiel que l'étudiant puisse évaluer la **portée de ses actions et ses responsabilités quant à son apport sur la sécurisation des systèmes** qu'il sera appelé à exploiter et/ou développer. Dans cette optique, les aspects légaux liés à la sécurité informatique seront également abordés.

Objectifs spécifiques du cours :

- Connaître la **terminologie** de base;
- Connaître les **enjeux** et les **domaines** de la sécurité informatique, distinguer les aspects **politiques et légaux** des aspects **technologiques**, et comprendre comment ils **s'influencent mutuellement**;
- Comprendre comment les **enjeux changent à cause des technologies** qui évoluent sans cesse;
- Comprendre les problèmes principaux de la sécurité, soit **l'authentification**, **l'autorisation**, **la confidentialité**, **l'intégrité**, **la disponibilité**, **l'imputabilité** et **la non-réputation**;
- Comprendre la structure des **protocoles de communication** et comment le réseau interagit avec les applications;
- Comprendre la **nature de certaines attaques** (injection de données malicieuses, déni de service, etc.);
- Se familiariser avec les techniques de **codage et de décodage de données sécurisées**;
- Se familiariser avec les **applications de surveillance et d'analyse de réseau**;
- Se familiariser avec les technologies de **sécurisation des réseaux** (réseaux virtuels privés, pare-feu, etc.);
- Se familiariser avec des **outils de pénétration et de tests de réseau**;
- Identifier les **risques** dans un système informatique et proposer/concevoir des **architectures sécurisées**, filaires et/ou mobiles afin **d'atténuer les risques identifiés**;
- Connaitre les **modalités légales en termes de protection des renseignements personnels**;
- Comprendre la **catégorisation des actifs informationnels** et les processus de mise en place de **plans de relève** appropriés assurant la **continuité des affaires**.

Calendrier des rencontres

#	Dates	Descriptions	Évaluations
1	12 janvier	Présentation du cours. Qu'est-ce que la sécurité informatique? Qu'est-ce qu'une attaque informatique? Qui sont les attaquants? Qu'est-ce qui motive les attaquants? Cybercriminalité, cyberterrorisme et « hacktivisme » : mythes et réalités. Stratégies de défense.	
2	19 janvier	Aspects légaux et lois en vigueur sur la protection des renseignements personnels. Actifs informationnels : catégorisation et inventaire. Analyse de risque et son importance. Plan de relève et continuité des affaires. Responsabilités légales. Aspects déontologiques.	
3	26 janvier	Les rôles de la sécurité informatique. Aspects technologiques (authentification, autorisation, disponibilité, intégrité) et aspects sociaux (confidentialité, imputabilité, non-répudiation). Technologies et algorithmes. Sécurité physique. Sensibilisation des utilisateurs/usagers.	Énoncé TP#1
4	2 février Enseignant à Lévis*	Enjeux de la sécurité informatique : vie privée, traçabilité et anonymisation. Pérennité des données et les conséquences sociales. Êtes-vous le produit? Est-ce vraiment confidentiel? Sécurité des données et ingénierie sociale.	
5	9 février	Cryptographie (partie #1). Historique. Exemples de chiffrements simples (substitution, transposition, etc.). Systèmes à clefs uniques. Cryptanalyse des systèmes simples.	
6	16 février Enseignant à Lévis*	Cryptographie (partie #2). Principes de base des systèmes de chiffrement modernes. Partages de secrets communs, systèmes à clefs publiques/privées. Cryptanalyse des systèmes complexes. Signatures numériques. Stéganographie. Futurs de la cryptographie : algorithmes et physique quantique. Politiques de sécurité et mots de passe. Outils de chiffrement.	

Calendrier des rencontres

7	23 février	Sécurité et réseaux (partie #1). Modèle OSI et applications. Protocoles de communication (raw sockets, ICMP, UDP, TCP, etc.). Rôle du pare-feu. Règles de routage, ports, redirections/translation, liste de contrôle d'accès. Filtrage par MAC. Protocoles sécurisés : IPSec, VPN, SSH et tunnels SSH. Capture de trafic et intrusion. Exploration et découverte des réseaux. Outils de sécurité pour les réseaux.	Remise du TP#1 Énoncé TP#2
8	2 mars	Semaine de lecture – Pas de cours	
9	9 mars	----- Examen intra -----	Examen intra
10	16 mars Enseignant à Lévis*	Sécurité et réseaux (partie #2). Nouvelles installations et parcs informatiques. Importance des mises à jour. Gestion de parcs informatiques : scripts, SNMP, Nagios, MDM, Intune. BYOD & réseau d'entreprise. Types d'attaques réseau.	
11	23 mars	Authentification et autorisation. Pourquoi s'authentifier? Traçabilité et imputabilité. Systèmes d'authentification : Kerberos, Radius, TACACS, LDAP et EntraID. Protocoles OAUTH & SAML.	Remise du TP#2 Énoncé TP#3
12	30 mars Enseignant à Lévis*	La sécurisation des contenus (DRM). Enjeu de protection de la propriété intellectuelle et aspect légaux. Études de cas. Mathématiques des DRM. Casser les DRM : stratégies et conséquences. Mécanismes de sécurité des systèmes d'exploitation. Niveaux de Priviléges. Sécurisation des fichiers. Groupes, accès, attributs, et particularités. Restrictions d'accès au matériel (clés USB, Bluetooth, etc.). Sandboxing au niveau des applications, au niveau du système d'exploitation.	
13	6 avril	Congé du lundi de Pâques – Pas de cours	

Calendrier des rencontres

14	13 avril Enseignant à Lévis*	Réseaux sans fil et protocoles. Niveaux de sécurité et vulnérabilités de WEP/WPA. Danger des appareils sans fil pour l'entreprise. Conception d'une architecture sans fil sécurisée. Évolution de la sécurité des réseaux sans-fil. Attaques à grande échelle, déni de service, etc. Botnets et cybercriminalité. Confidentialité et anonymisation. Cybercrime, anonymat et « Web obscur ». Cryptomonnaies.	
15	20 avril	Hacking, cracking et exploitations. Exploitation de failles logicielles. Injection de données malicieuses, injections SQL, HTML, XSS et autres attaques spécifiques au langage de programmation/logiciel. Comment solidifier le code. Systèmes d'exploitation et leurs outils de sécurité intégrés : SELinux, Windows Defender, etc. Systèmes de fichiers. Autres sujets à déterminer.	
16	27 avril	----- Examen final -----	Remise du TP#3 Examen final

* L'enseignant se réserve le droit de modifier le calendrier des rencontres et son contenu, s'il le juge nécessaire et approprié, après en avoir préalablement informé les étudiants.

* : Il est possible que l'enseignant modifie ses déplacements si les conditions météo font en sorte qu'il n'est pas sécuritaire de réaliser les déplacements.

Organisation de mes déplacements Rimouski / Lévis

Sites	Dates
Rimouski	Janvier : 12-19-26 Février : 9-23 Mars : 23 Avril : 20
Lévis	Janvier : ... Février : 2-16 Mars : 16-30 Avril : 13

✿ Sous réserve que les conditions météorologiques permettent des déplacements sécuritaires

Formules pédagogiques

- La formule se compose d'une rencontre de trois heures chaque semaine comportant des leçons magistrales, démonstrations/travaux pratiques, exercices et analyses de mise en situation. Étant donné que le cours sera en vidéoconférence entre Lévis et Rimouski, l'enseignant se déplacera entre les sites en fonction de ses disponibilités et des conditions météorologiques.
- Trois travaux pratiques sont également prévus. Ils seront en équipe de 3 ou 4 personnes au maximum, au choix des étudiants. Toutefois, l'enseignant se réserve le droit d'assigner les équipes pour certains travaux. Les dates de remises sont indiquées dans le calendrier des rencontres et les sujets des travaux seront connus au moment de la mise en disponibilité des énoncés.
- Modalités d'évaluations :
 - Trois travaux pratiques pour un total de 50 %.
 - Deux examens écrits pour un total de 50 %.
- Une absence non justifiée dans les délais prescrits à un examen entraîne une note de 0.
- À moins d'entente avec l'enseignant, tout retard dans le dépôt des travaux pratiques entraînera une perte de 10% par jour de retard sur la note obtenue, et ce, jusqu'à concurrence de 0 après la dixième journée de retard.
- Jusqu'à 10 % des points peuvent être accordés à la qualité du français écrit dans les travaux et les examens.

Dates importantes - Travaux pratiques / Examens

Examens	Date	%	
Intra	9 mars	25	
Final	27 avril	25	
Travaux Pratiques	Date de disponibilité de l'énoncé	Date de remise du Travail Pratique	%
#1 – À déterminer	26 janvier	23 février	15
#2 – À déterminer	23 février	23 mars	15
#3 – À déterminer	23 mars	27 avril	20

100%

Notation proposée

Note	Cote
96% - 100%	A+
92% - 96%	A
88% - 92%	A-
84% - 88%	B+
80% - 84%	B
77% - 80%	B-
73% - 77%	C+
70% - 73%	C
66% - 70%	C-
62% - 66%	D+
60% - 62%	D
< 60%	E

Modalités particulières

Prestation de cours :

Bien que dans un cours régulier la ponctualité et le sérieux des étudiants sont de rigueur, ce principe devient d'une importance capitale dans le cas de la tenue d'un cours par vidéoconférence. Ainsi, dans votre intérêt et dans l'intérêt de vos collègues étudiants présents au cours à vos côtés et à distance, il est demandé de limiter les bruits et les discussions avec les voisins.

Enfin, le mode de prestation du cours demeure tel que défini lors de l'inscription, et ce, pour toutes les séances du trimestre, peu importe les circonstances.

Fermeture d'établissement :

S'il y a fermeture d'un des deux établissements de l'UQAR (Campus de Lévis ou de Rimouski) en raison des intempéries, le cours est annulé sur les deux sites.

- La théorie demeure déposée sur le portail Moodle et l'enseignant revient sur la théorie au cours suivant;
- Les dates de remises des travaux demeurent inchangées et conformes au plan de cours original.

Si des ajustements complémentaires sont nécessaires, l'enseignant diffusera un message dans la section « Annonces » du portail Moodle du cours dans les plus brefs délais afin d'informer les étudiants.

Plagiat :

Le plagiat ne sera pas toléré. Vous devrez toujours citer correctement vos sources (livres, articles, collègues, sites Web, etc.). Tout étudiant suspecté de plagiat verra son cas traité selon les modalités en vigueur du [Règlement 5 : Régime des études de premier cycle](#) de l'UQAR.

Modalités particulières

Infractions relatives aux études :

L'Université du Québec à Rimouski prône l'intégrité, le respect et l'honnêteté dans les études. Ainsi, l'appropriation et l'utilisation des propos ou de productions d'autrui sans source ni référence sont interdites.

Toute personne étudiante doit respecter le [Règlement 7 : Infractions relatives aux études](#) dans le cadre du présent cours. L'article 9 de ce règlement présente les sanctions possibles à toute infraction.

C'est le Comité de discipline de l'Université du Québec à Rimouski qui a pour mandat de traiter tout dossier qui lui est soumis en conformité avec le [Règlement 7 : Infractions relatives aux études](#).

Consultez-le [ici](#) pour plus d'information.

Appréciation étudiante de l'enseignement :

Soucieuse de valoriser l'enseignement qu'elle offre dans ses murs, l'UQAR rappelle aux personnes étudiantes l'importance de remplir, lors de la période et sur le support prescrit par l'Université, le questionnaire d'« Appréciation étudiante de l'enseignement » du présent cours.

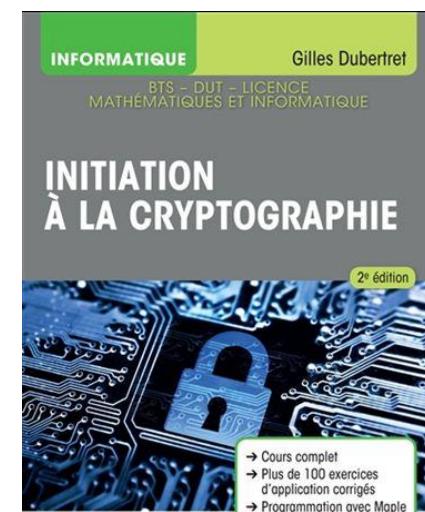
À l'UQAR, hormis les cours offerts en tutorat (TU, 7T, TA, TL), toutes les activités d'enseignement sont appréciées pour les raisons suivantes :

- Améliorer de manière continue la prestation des professeures et professeurs ainsi que des personnes chargées de cours et l'équipe pédagogique;
- Permettre aux personnes étudiantes de donner leur appréciation à propos de l'enseignement qu'elles et qu'ils reçoivent;
- Informer les différentes instances universitaires (conseils de module, comités de programmes, départements, unités départementales, comités d'appréciation, comité de promotion, etc.) chargées d'assurer le suivi administratif auprès des professeures et des professeurs ainsi que des personnes chargées de cours. Prenez note que le suivi administratif n'est assuré que dans le cas des appréciations ayant obtenu un taux de participation égal ou supérieur à 50 %.

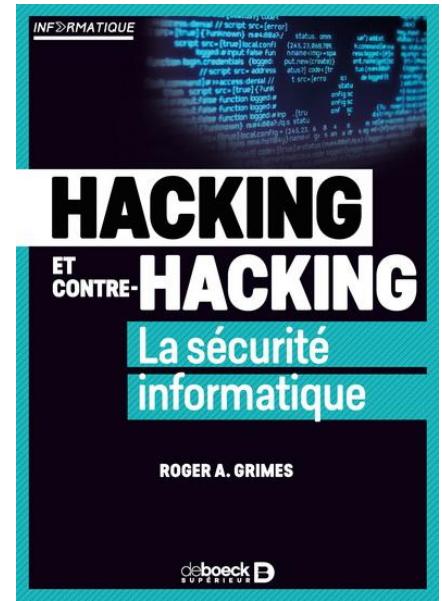
Bibliographie

- Ghernaouti S., *Cybersécurité – Analyser les risques, Mettre en œuvre les solutions*, DUNOD, 7e édition, 2022
- Brooks C., Grow C., Craig P., Short D., *Cybersécurité – Sécurisation des systèmes informatiques*, DeBoeck Supérieur, 2021
- Dubertret G., *Initiation à la cryptographie*, VUIBERT, 2018
- Grimes R. A., *Hacking et contre-hacking – La sécurité informatique*, DeBoeck Supérieur, 2019

Cybersécurité

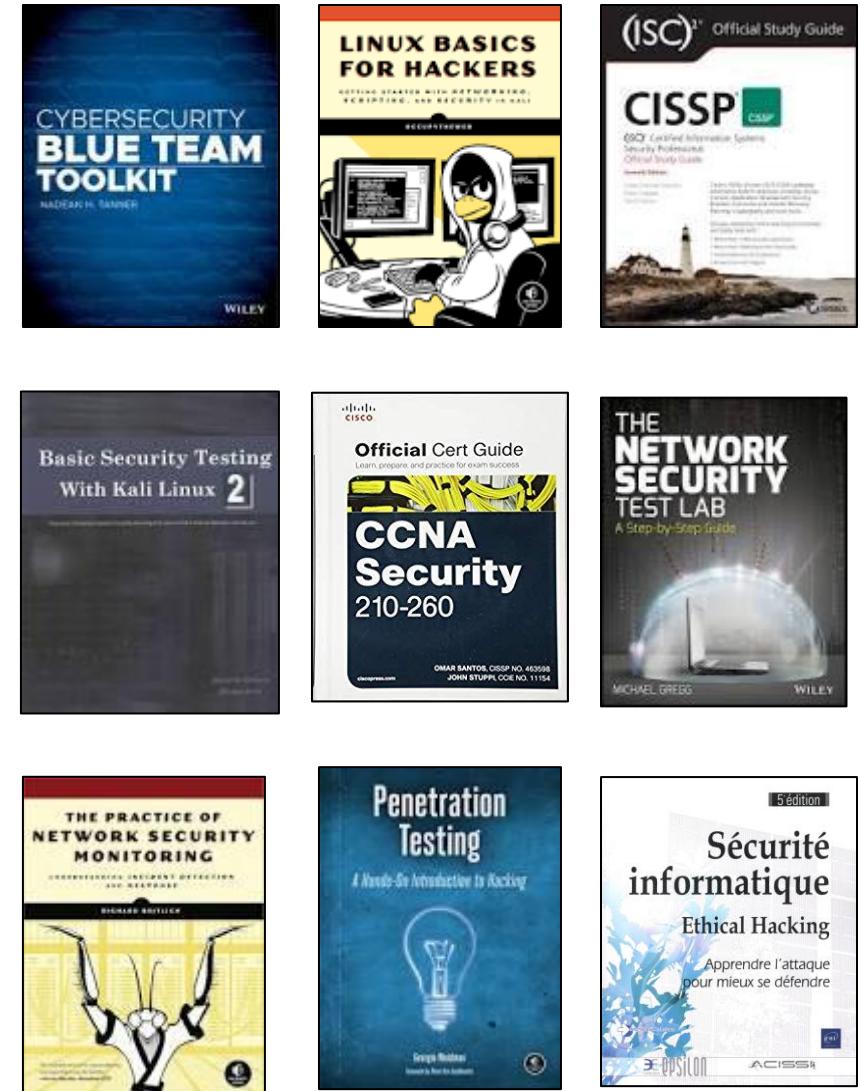


Vuibert



Bibliographie

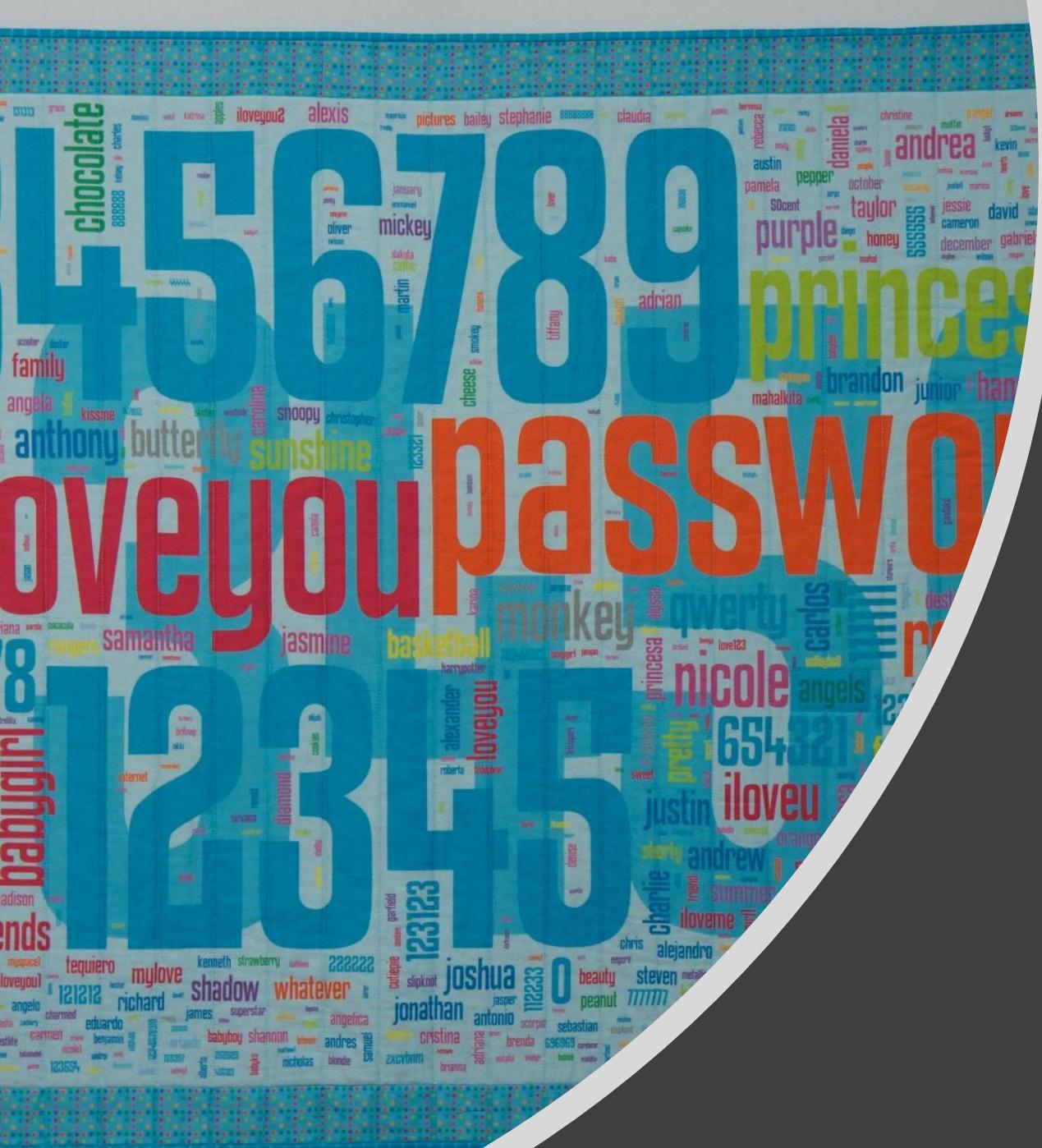
- Tanner N. H., *Cybersecurity Blue Team Toolkit*, WILEY, 2019
- OccupyTheWeb, *Linux Basics for Hackers – Getting started with Networking, Scripting and Security in Kali*, No Starch Press, 2019
- Chapple M., Stewart, J.M., Gibson, D., *Certified Information Systems Security Professional (CISSP) - Official Study Guide*, SYBEX, 8e édition, 2018
- Dieterle D.W., *Basic Security Testing With Kali Linux – Vol 2*, Cyberarms, 2016
- Santos O., Stuppi J., *CCNA Security 210-260 – Official Cert Guide*, CiscoPress, 2015
- Gregg M., *The Network Security Test Lab: A Step-by-Step Guide*, WILEY, 2015
- Bejtlich R., *The practice of network security monitoring : understanding incident detection and response*, No Starch Press, 2013
- Weidman G., *Penetration Testing – A hands-on Introduction to Hacking*, No Starch Press, 2013
- ACCISSI, *Sécurité informatique – Ethical Hacking : apprendre l'attaque pour mieux se défendre*, Éditions ENI, 2009



...et plusieurs autres! Il existe des centaines de livres sur le sujet!



Questions ?



Quel est le mot de passe le plus sécuritaire selon vous ?

Les 12 derniers digits du chiffre PI (π) ?



12 digits, est-ce cassable ??

$\text{Pi} = 3.\underline{141592653589}7932384626433\dots$

Temps nécessaires pour casser un mot de passe

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols	Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly	4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly	5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs	6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	25 secs	1 min	6 mins	7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	5 secs	22 mins	1 hour	8 hours	8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	2 mins	19 hours	3 days	3 weeks	9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	58 mins	1 month	7 months	5 years	10	Instantly	4 mins	3 days	3 weeks	5 months
11	2 secs	1 day	5 years	41 years	400 years	11	Instantly	2 hours	5 months	3 years	34 years
12	25 secs	3 weeks	300 years	2k years	34k years	12	2 secs	2 days	24 years	200 years	3k years
13	4 mins	1 year	16k years	100k years	2m years	13	19 secs	2 months	1k years	12k years	202k years
14	41 mins	51 years	800k years	9m years	200m years	14	3 mins	4 years	64k years	750k years	16m years
15	6 hours	1k years	43m years	600m years	15bn years	15	32 mins	100 years	3m years	46m years	1bn years
16	2 days	34k years	2bn years	37bn years	1tn years	16	5 hours	3k years	173m years	3bn years	92bn years
17	4 weeks	800k years	100bn years	2tn years	93tn years	17	2 days	69k years	9bn years	179bn years	7tn years
18	9 months	23m years	61tm years	100tn years	7qd years	18	3 weeks	2m years	467bn years	11tn years	438tn years

2020

› Learn about our methodology at hivesystems.io/password

2021

› Learn about our methodology at hivesystems.io/password

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	1 secs
9	Instantly	Instantly	4 secs	21 secs	1 mins
10	Instantly	Instantly	4 mins	22 mins	1 hours
11	Instantly	6 secs	3 hours	22 hours	4 days
12	Instantly	2 mins	7 days	2 months	8 months
13	Instantly	1 hours	12 months	10 years	47 years
14	Instantly	1 days	52 years	608 years	3k years
15	2 secs	4 weeks	2k years	37k years	232k years
16	15 secs	2 years	140k years	2m years	16m years
17	3 mins	56 years	7m years	144m years	1bn years
18	26 mins	1k years	378m years	8bn years	79bn years

2023

› Learn how we made this table at hivesystems.io/password

Disons-nous les vraies affaires !!

- Quel type de Hash est-il utilisé ?
- Quel hardware a été utilisé ?
- Est-ce que l'information est fiable ?

2020 hardware: 1 x RTX 2080 + password hash: MD5

2021 hardware: 8 x A100 + password hash: MD5

2023 hardware: 12 x RTX 4090 + password hash: MD5

Hachage MD5

Extrait d'un thread sur le forum de Hashcat :

```
Short Benchmark for the RTX 4090
CUDA API (CUDA 11.8)
=====
* Device #1: NVIDIA GeForce RTX 4090, 23867/24252 MB, 128MCU

Benchmark relevant options:
=====
* --optimized-kernel-enable
* --workload-profile=4

-----
* Hash-Mode 0 (MD5)

-----
Speed.#1.....: 155.9 GH/s (12.99ms) @ Accel:512 Loops:1024 Thr:32 Vec:8
```

- Prenons par exemple un mot de passe composé de 12 chiffres (123456789012) encodé en MD5. Celui-ci peut être craqué très rapidement.
- La nature de l'algorithme MD5 et la faible entropie des mots de passe purement numériques en sont la cause
- Nombre de combinaisons possibles :
 - Un mot de passe de 12 chiffres comporte :
 - $10^{12} = 1\ 000\ 000\ 000\ 000 \rightarrow 1$ trillion de combinaisons
- Vitesse de cassage (par GPU moderne) :
 - Avec des outils comme **Hashcat** (John the Ripper est mieux pour les CPU), une carte graphique haut de gamme (RTX 4090) peut tester environ 200 à 300 milliards de hachages MD5 par seconde.

$$\frac{10^{12}}{300 \times 10^9} = \frac{1\ 000\ 000\ 000\ 000}{300\ 000\ 000\ 000} \approx 3.\overline{33} \text{ secondes}$$

$$\approx 6.414 \text{ secondes}$$

Et ça, c'est le pire cas, où le « dernier » hash calculé est le bon.

complexité et
imprévisibilité

Hachage de mots de passe

Voici une évaluation de la robustesse des 10 algorithmes de hachage, exprimée en pourcentage de leur robustesse et en tenant compte de leur sécurité, leur résistance aux attaques par force brute et leur capacité à ralentir les attaques.

Algorithmes	Robustesse (%)	Justification
Argon2id	98%	Meilleur choix actuel. Résistant aux attaques par GPU/ASIC, coûteux en mémoire et temps.
bcrypt	95%	Très robuste grâce au facteur de coût ajustable et au salage. Légèrement moins performant qu'Argon2 face aux nouvelles attaques.
scrypt	93%	Exigeant en mémoire, efficace contre les attaques par GPU, mais peut être moins sécurisé qu'Argon2 pour certaines implémentations.
PBKDF2	85%	Robuste, mais moins résistant aux attaques par GPU comparé à scrypt ou Argon2. Nécessite un grand nombre d'itérations pour être efficace.
MD5 (avec salage)	40%	Très vulnérable seul. Même avec salage et itérations, il reste obsolète et exposé aux collisions. 

Algorithmes	Robustesse (%)	Justification
SHA-3	82%	Très sécurisé, mais pas spécifiquement conçu pour le hachage de mots de passe. Moins de fonctionnalités intégrées que bcrypt ou Argon2.
Blake2b	80%	Rapide et sécurisé, mais pas optimisé pour ralentir les attaques par force brute sur les mots de passe.
SHA-512/256	75%	Sécurisé, mais nécessite salage et itérations manuelles. Moins efficace pour le hachage direct des mots de passe.
Whirlpool	70%	Sécurisé, mais moins étudié et adopté que SHA-3 ou bcrypt pour les mots de passe.
HMAC (SHA-256)	68%	Sécurisé pour l'authentification, mais pas spécifiquement conçu pour le hachage de mots de passe.

Temps nécessaire en 2024

COMBIEN DE TEMPS FAUT-IL À UN PIRATE POUR TROUVER VOTRE MOT DE PASSE 2024

12 x RTX 4090 | bcrypt

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	3 secs	6 secs	9 secs
5	Immédiat	4 secs	2 mins	6 mins	10 mins
6	Immédiat	2 mins	2 heures	6 heures	12 heures
7	4 secs	50 mins	4 jours	2 semaines	1 mois
8	37 secs	22 heures	8 mois	3 ans	7 ans
9	6 mins	3 semaines	33 ans	161 ans	479 ans
10	1 heure	2 ans	1k ans	9k ans	33k ans
11	10 heures	44 ans	89k ans	618k ans	2M ans
12	4 jours	1k ans	4M ans	38M ans	164M ans
13	1 mois	29k ans	241M ans	2Md ans	11Md ans
14	1 an	766k ans	12Md ans	147Md ans	805Md ans
15	12 ans	19M ans	652Md ans	9Bn ans	56Bn ans
16	119 ans	517M ans	33Bn ans	566Bn ans	3Bd ans
17	1k ans	13Md ans	1Bd ans	35Bd ans	276Bd ans
18	11k ans	350Md ans	91Bd ans	2Tn ans	19Tn ans



› www.hivesystems.com/password

Il est de plus en plus simple de casser un mot de passe avec l'évolution des moyens technologiques : CPU, GPU, Quantique, etc.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years



Hive Systems

Temps nécessaire
en 2025

2020 hardware: 1 x RTX 2080 + password hash: MD5

2022 hardware: 8 x A100 + password hash: MD5

2023 hardware: 12 x RTX 4090 + password hash: MD5

2024 hardware: 12 x RTX 4090 + password hash: bcrypt (1 seule itération)

2025 hardware: 12 x RTX 5090 + password hash: bcrypt (1024 itérations)

Il est de plus en plus simple de casser un mot de passe avec l'évolution des moyens technologiques : CPU, GPU, Quantique, etc.

Time it takes
a hacker to
brute force
your password
in 2025

Hardware: 12 x RTX 5090
Password hash: bcrypt (10)

Read more and download at
hivesystems.com/password

Hachage Bcrypt

- Facteur de coût ajustable (work factor)
 - Le facteur de coût détermine le nombre d'itérations appliquées au processus de hachage. Plus le coût est élevé, plus le hachage prend du temps, ce qui ralentit les attaquants.
 - Exemple : Un coût de 10 signifie que bcrypt effectuera 2^{10} (1024) itérations du processus de hachage.
- Salage automatique (automatic salting)
 - bcrypt génère automatiquement un sel unique (random salt) pour chaque mot de passe haché. Cela empêche les attaques par rainbow tables (tables précalculées).
 - Avantage : Deux mots de passe identiques auront des hachages différents.
- Résistance à la force brute (brute-force resistance)
 - Même avec des GPU puissants, bcrypt reste lent par design, rendant les attaques coûteuses en temps et en énergie.
- Sortie de longueur fixe
 - bcrypt produit un hachage de 60 caractères au format Base64 modifié. Ce hachage contient le facteur de coût, le sel et le hachage proprement dit.

Algorithme	Sécurité	Performance	Salage	Facteur coût
Argon2id	Supérieure	Plus lent que scrypt	Automatique	Oui (mémoire/CPU)
bcrypt	Très élevée	Lent par design	Automatique	Oui
scrypt	Très élevée	Plus lent que bcrypt	Automatique	Oui (mémoire/CPU)
PBKDF2	Élevée	Moyen (selon itération)	Manuel	Oui



Maintenant, passons à la théorie de la soirée...