

MASTER CYBERSÉCURITÉ



DIPLÔME NATIONAL

niveau de diplôme

Grade de Master (Bac+5)

durée

2 années

lieu-x de formation

Caen

crédit ECTS

120

CONTACT

Université de Caen Normandie
UFR des Sciences
Esplanade de la Paix · CS 14032
· 14032 Caen Cedex 5

ufr-sciences.unicaen.fr/

Le master de cybersécurité propose une formation de deux ans niveau bac + 5 en sécurité informatique, qui permet de découvrir et d'approfondir tous les aspects de la sécurité informatique.

Cette formation est co-accréditée entre l'université de Caen Normandie et l'ENSICAen

MÉTIERIS VISÉS

Tous les métiers proposés dans le [panorama des métiers de la CyberSécurité](#) de l'ANSSI

COMPÉTENCES ACQUISES

- Apprendre le hacking éthique à travers des enseignements orientés vers la sécurité défensive et offensive et des projets basés sur des CTF et des plateformes variés.
- Gérer et piloter la sécurité d'un système d'information sous tous ses aspects (matériel, système, réseau, web, logiciel, information, cloud)
- Connaître les aspects pluridisciplinaires de la cybersécurité, notamment les aspects sociétaux, droit, vie privée et gestion de la sécurité.
- Maîtriser et appliquer les aspects techniques avancés de la sécurité informatique, comme la programmation sécurisée, la biométrie, les blockchains et la forensique.
- Comprendre les aspects théoriques avancés de la cybersécurité, notamment la cryptographie, la cryptanalyse et l'informatique quantique.

POURSUITE D'ÉTUDES

La poursuite d'étude est possible dans le cadre d'une thèse. Notamment au sein du laboratoire [GREYC](#) (UMR CNRS 6072) dans le cadre du Campus Normandie Cyber.

PRINCIPAUX ENSEIGNEMENTS

Au cours des deux ans de formations, le master contient quatre groupes de 5 UE pour tous les étudiants (Formation initiale et Formation par apprentissage) où chaque UE possède un volume horaire de 40h avec de nombreux travaux pratiques et de challenges de sécurité à réaliser :

Cryptographie

- Mathématiques pour la cryptographie
- Cryptographie
- Cryptographie et cryptanalyse avancée
- Cryptographie post-quantique
- Parallélisme et cryptanalyse quantique

Aspects pluridisciplinaires de la Sécurité informatique

- Anglais et communication
- Aspects économique et sociaux pour la sécurité
- Anglais scientifique et communication
- Droit pour la sécurité et la vie privée
- Gestion de la sécurité

Sécurité d'un système d'information

- Sécurité informatique
- Sécurité système et logicielle
- Sécurité web et réseaux
- Sécurité défensive/offensive
- Sécurité IoT, cloud et blockchain

Fondements Informatique de la sécurité

- Programmation C/C++ sécurisée
- Linux avancé
- Transmission de l'information
- Forensique
- Biométrie

Le master contient aussi 2 UE de 50h pour les étudiants en formation initiale seulement:

- Hacking éthique
- Hacking avancé

Deux stages de 4 à 6 mois chacun en fin de chaque année complètent la formation.

ADMISSION · INSCRIPTION

NIVEAU DE RECRUTEMENT

Bac+3

CONDITIONS D'ACCÈS

L'accès à la première année de master est sélectif, les critères d'admission et de capacité d'accueil sont définis par l'université.

Diplômes conseillés : Licence Informatique, Licence Mathématique, BUT Informatique.

Les excellentes candidatures venant d'autres formations Bac+3 (Licences, BUT) seront considérées.

Modalités de sélection : Examen sur dossier (qualité du cursus antérieur, motivation(s) et CV).

PROCÉDURE D'INSCRIPTION : CANDIDATURE

Année universitaire 2024/2025

En formation initiale ou en alternance, les candidatures en première année de master se font sur la plateforme nationale de candidature monmaster.gouv.fr du 26 février au 24 mars 2024 (phase principale) et du 25 juin au 31 juillet 2024 (phase complémentaire, en cas de places vacantes).

Vous souhaitez reprendre des études en formation continue, faire valider une expérience professionnelle pour être admis en master ou vous relevez de la procédure Études en France, consultez dès à présent la plateforme [eCandidat](#) pour prendre connaissance des différents calendriers de dépôts de candidatures.