

Certificat

Cryptographie Avancée



Certificat Cryptographie Avancée

- » Modalité: en ligne
- » Durée: 6 semaines
- » Qualification: TECH Université Technologique
- » Intensité: 16h/semaine
- » Horaire: à votre rythme
- » Examens: en ligne

Accès au site web: www.techtute.com/fr/informatique/cours/cryptographie-avancee

Sommaire

01

Présentation

page 4

02

Objectifs

page 8

03

Direction de la formation

page 12

04

Structure et contenu

page 16

05

Méthodologie

page 20

06

Diplôme

page 28

01 Présentation

La cryptographie a pris de l'importance ces dernières années. Non seulement c'est une discipline essentielle dans le chiffrement des clés et des données, mais c'est aussi un élément central d'un nouveau domaine technologique en plein essor: *Blockchain*. Par conséquent, les entreprises du secteur numérique et du développement d'applications et d'autres outils informatiques recherchent des spécialistes possédant des compétences avancées en cryptographie. Ainsi, ce programme offre le professionnel un approfondissement complet dans ce domaine, le préparant à répondre aux défis actuels et futurs de la cybersécurité. Tout ça, grâce à une méthodologie d'enseignement en ligne qui vous permettra de combiner votre travail et vos études de manière simple et confortable.



“

La cryptographie est essentielle pour la cybersécurité des entreprises et des administrations. d'entreprises et pour des technologies telles que la Blockchain. Par conséquent, ce programme vous préparera intensivement à progresser professionnellement dans cet important domaine informatique. dans cet important domaine informatique"

L'importance croissante de la cybersécurité a entraîné un essor considérable de la cryptographie. Cette discipline permet de coder, chiffrer et encoder tous types de données, qu'il s'agisse d'informations sensibles de l'entreprise, de transactions ou de clés d'accès. En tant que tel, il est fondamental dans le monde numérique d'aujourd'hui. En outre, l'émergence d'autres domaines tels que la *Blockchain* ou l'intelligence artificielle lui a donné un coup de pouce supplémentaire, ce qui en fait un secteur à forte demande de professionnels spécialisés.

Ce Certificat en Cryptographie Avancée offre donc la possibilité de se plonger dans ce domaine. De se plonger dans ce domaine, en préparant les informaticiens à répondre à tous les défis actuels et futurs dans ce domaine. Tout au long de ce programme, le professionnel se penchera sur des questions telles que la stéganographie et la stéganalyse, la combinaison de chiffrements par blocs, la cryptographie asymétrique et les algorithmes quantiques.

Basé sur un enseignement 100% en ligne, ce Certificat permettra aux informaticiens de progresser professionnellement grâce à son contenu actualisé et à son équipe pédagogique, composée de spécialistes de la cryptographie, au fait des dernières évolutions de ce domaine et de ses nouvelles applications pratiques.

Ce **Certificat en Cryptographie Avancée** contient le programme éducation le plus complet et le plus actuel du marché. Ses principales caractéristiques sont:

- ◆ Le développement d'études de cas présentées par des experts en informatique cybersécurité
- ◆ Les contenus graphiques, schématiques et éminemment pratiques avec lesquels ils sont conçus fournissent des informations scientifiques et sanitaires essentielles à la pratique professionnelle
- ◆ Des exercices où le processus d'auto-évaluation peut être réalisé pour améliorer l'apprentissage.
- ◆ Il met l'accent sur les méthodologies innovantes
- ◆ Leçons théoriques, questions à l'expert, forums de discussion sur des sujets controversés et travail de réflexion individuel
- ◆ La possibilité d'accéder au contenu à partir de n'importe quel appareil fixe ou portable doté d'une connexion internet



Apprenez les dernières applications de la cryptographie grâce à ce Certificat, qui est enseigné selon une méthodologie 100% en ligne"

“

Vous pourrez vous plonger dans les meilleures techniques cryptographiques grâce à de nombreuses ressources multimédias : activités pratiques, résumés multimédias, master classes, etc”

Le corps enseignant du programme englobe des spécialistes réputés dans le domaine et qui apportent à ce programme l'expérience de leur travail, ainsi que des spécialistes reconnus dans de grandes sociétés et des universités prestigieuses.

Grâce à son contenu multimédia développé avec les dernières technologies éducatives, les spécialistes bénéficieront d'un apprentissage situé et contextuel. Ainsi, ils se formeront dans un environnement simulé qui leur permettra d'apprendre en immersion et de s'entraîner dans des situations réelles.

La conception de ce programme est axée sur l'apprentissage par les problèmes, grâce auquel le professionnel doit essayer de résoudre les différentes situations de pratique professionnelle qui se présentent tout au long du programme universitaire. Pour ce faire, l'étudiant sera assisté d'un innovant système de vidéos interactives, créé par des experts reconnus.

Les entreprises technologiques ont besoin d'experts en Cryptographie Avancée et ce Certificat vous préparera à progresser sur le plan professionnel.

Le système d'apprentissage de TECH Le système d'apprentissage de TECH vous permettra de poursuivre développer votre travail professionnel sans interruptions et sans horaires rigides.



“

*Réalisez tous vos objectifs professionnels
en vous spécialisant en cryptographie
avancée grâce à ce Certificat"*

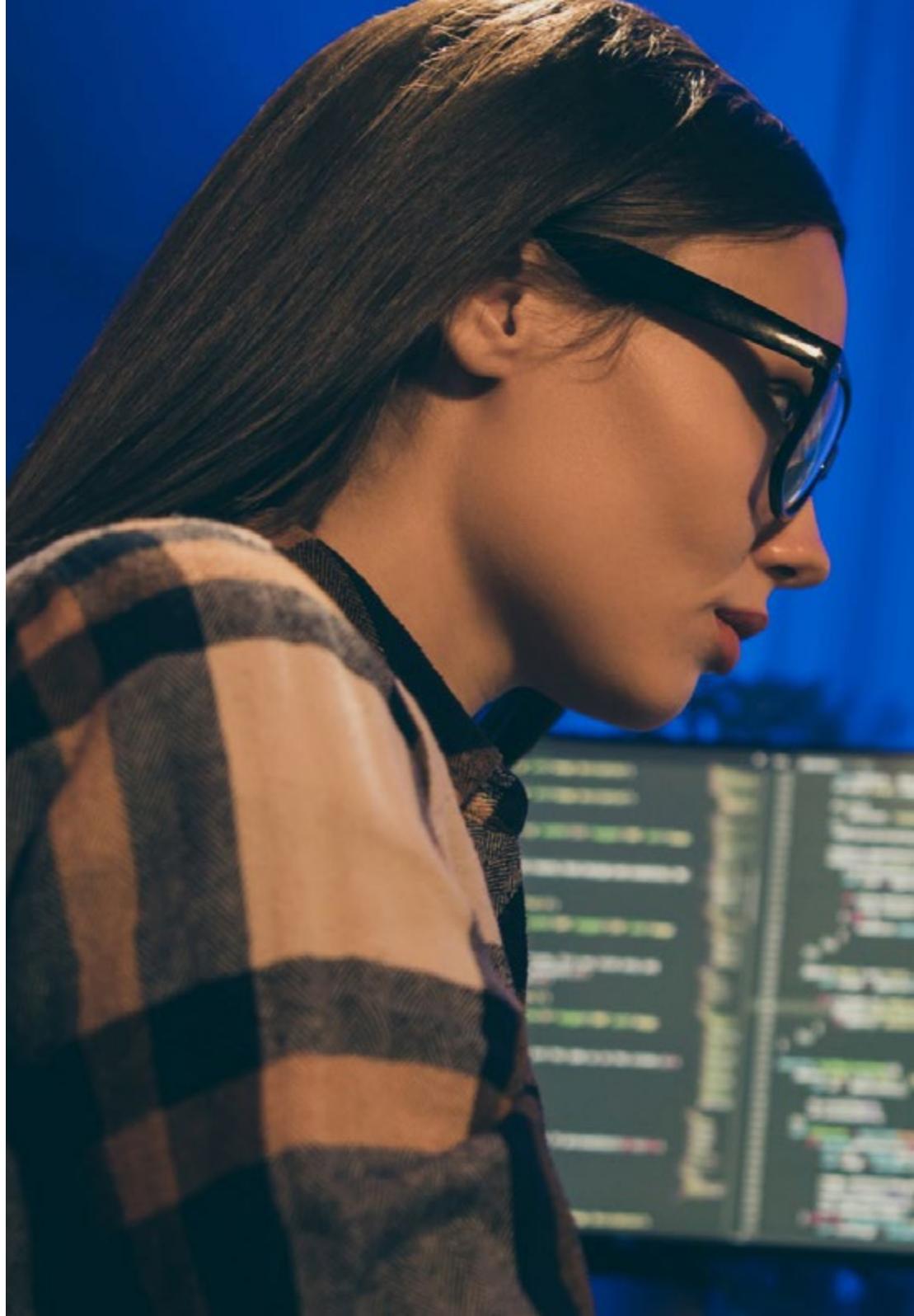


Objectifs généraux

- ◆ Examiner la science de la cryptologie et la relation avec ses branches: cryptographie, cryptanalyse, stéganographie et stégoanalyse
- ◆ Analyser les types de cryptographie en fonction du type d'algorithme et en fonction de son utilisation
- ◆ Compiler les systèmes de gestion des clés
- ◆ Évaluer les différentes applications pratiques
- ◆ Examiner les certificats numériques
- ◆ Examiner l'infrastructure à clé publique (ICP)
- ◆ Analyser les dernières tendances et les derniers défis

“

La cryptographie sera essentielle dans votre future carrière: inscrivez-vous dès maintenant et préparez-vous à saisir des opportunités importantes dans le domaine de la cybersécurité”





Objectifs spécifiques

- ◆ Compiler les opérations fondamentales (XOR, grands nombres, substitution et transposition) et les différents composants (fonctions à sens unique, Hash, générateurs de nombres aléatoires)
- ◆ Analyser les techniques cryptographiques
- ◆ Développer différents algorithmes cryptographiques
- ◆ Démontrer l'utilisation des signatures numériques et leur application dans les certificats numériques
- ◆ Évaluer les systèmes de gestion des clés et l'importance de la longueur des clés cryptographiques
- ◆ Examiner les algorithmes de dérivation de clés
- ◆ Analyser le cycle de vie des clés
- ◆ Évaluer les modes de chiffrement par blocs et de chiffrement par flux
- ◆ Déterminer les générateurs de nombres pseudo-aléatoires
- ◆ Développer des cas réels d'applications cryptographiques, comme Kerberos, PGP ou les cartes à puce
- ◆ Examinez les associations et organismes connexes, tels que l'ISO, le NIST ou le NCSC
- ◆ Déterminer les défis de la cryptographie de l'informatique quantique

03

Direction de la formation

La cryptographie est un domaine très complexe pour lequel vous souhaitez la meilleure préparation possible. L'émergence de nouveaux secteurs technologiques, pour lesquels la cryptographie est un élément de base, a entraîné un essor de ce domaine, dont l'énorme difficulté nécessite l'accompagnement de spécialistes pour en connaître les tenants et les aboutissants.

C'est pourquoi TECH a réuni un corps enseignant très prestigieux qui guidera l'étudiant tout au long du processus d'apprentissage, en veillant à ce que tous les éléments clés de la cryptographie actuelle soient assimilés de manière agile et simple.



“

L'équipe pédagogique de TECH vous guidera pour que les 150 heures d'apprentissage de ce Certificat soient efficaces et vous boostent professionnellement"

Direction



M. Olalla Bonal, Martín

- ♦ Spécialiste technique client Blockchain chez IBM
- ♦ Blockchain Technical Specialist en IBM SPGI
- ♦ Architecte *Blockchain*
- ♦ Architecte d'infrastructure dans le secteur bancaire
- ♦ Gestion de projet et mise en œuvre de solutions en production
- ♦ Technicien en Électronique Numérique
- ♦ Professeur: Formation Hyperledger Fabric pour les entreprises
- ♦ Professeur: Formation Blockchain en entreprise

Professeurs

M. Ortega, Octavio

- ♦ Programmeur d'applications informatiques et développement Web
- ♦ Conception de sites web et d'APPS pour des clients, CRDS pour les recherches menées par l'Instituto de Salud Carlos III, boutiques en ligne, applications Android, etc
- ♦ Professeur de Sécurité Informatique
- ♦ Diplôme de psychologie de l'Universitat Oberta de Catalunya (UOC)
- ♦ Technicien Supérieur Universitaire en Analyse, Conception et Solutions Software
- ♦ Technicien Supérieur Universitaire en Programmation Avancée



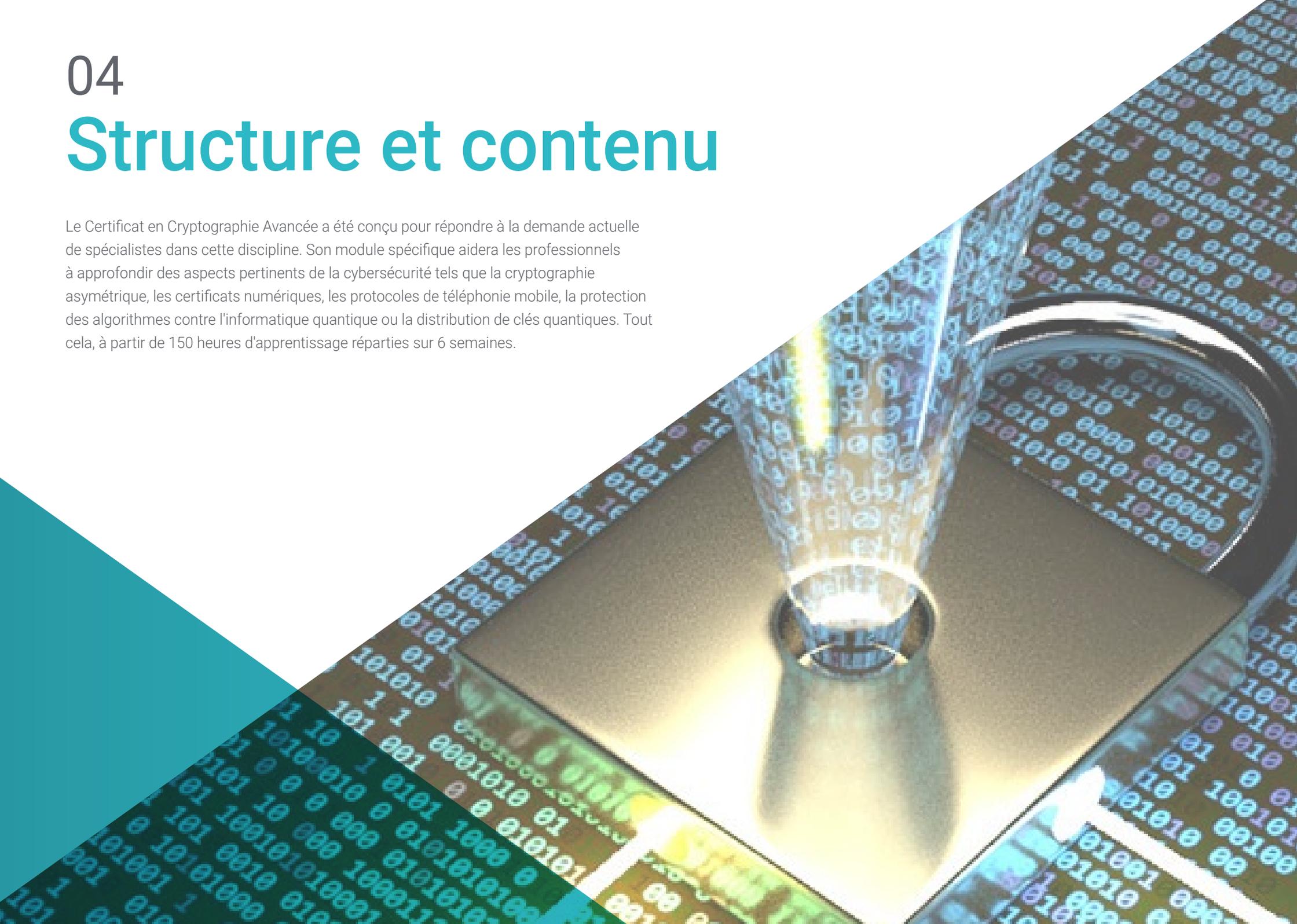
“

Notre équipe pédagogique mettra à votre disposition toutes ses connaissances pour vous permettre de rester au fait des dernières informations dans ce domaine”

04

Structure et contenu

Le Certificat en Cryptographie Avancée a été conçu pour répondre à la demande actuelle de spécialistes dans cette discipline. Son module spécifique aidera les professionnels à approfondir des aspects pertinents de la cybersécurité tels que la cryptographie asymétrique, les certificats numériques, les protocoles de téléphonie mobile, la protection des algorithmes contre l'informatique quantique ou la distribution de clés quantiques. Tout cela, à partir de 150 heures d'apprentissage réparties sur 6 semaines.

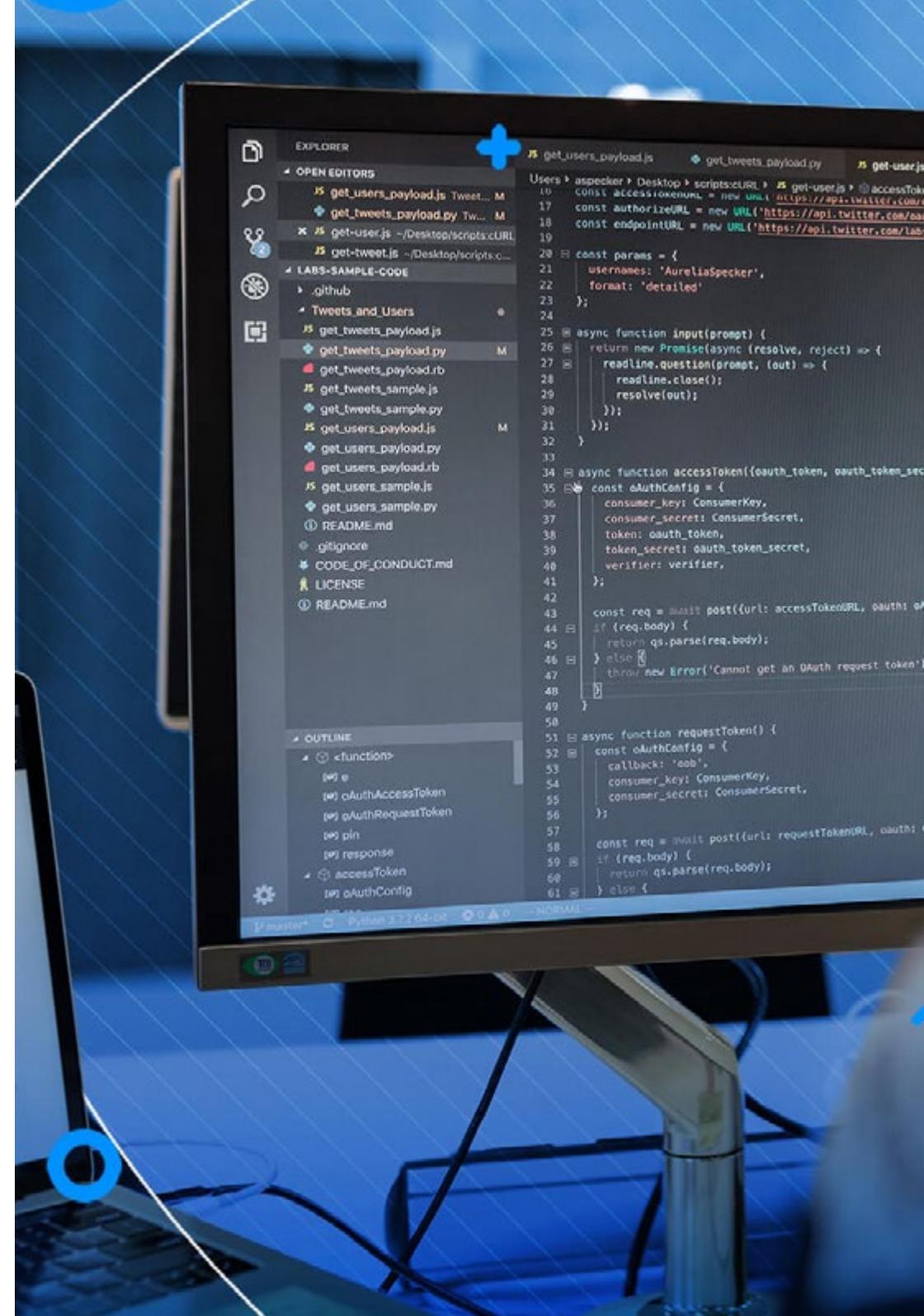


“

Le programme le plus récent en Cryptographie Avancée vous préparera à connaître toutes les clés pour protéger les algorithmes contre l'informatique quantique”

Module 1. Cryptographie en informatique

- 1.1. Cryptographie
 - 1.1.1. Cryptographie
 - 1.1.2. Bases mathématiques
- 1.2. Cryptologie
 - 1.2.1. Cryptologie
 - 1.2.2. Cryptanalyse
 - 1.2.3. Stéganographie et stéganalyse
- 1.3. Protocoles cryptographiques
 - 1.3.1. Blocs de base
 - 1.3.2. Protocoles de base
 - 1.3.3. Protocoles intermédiaires
 - 1.3.4. Protocoles avancés
 - 1.3.5. Protocoles exotériques
- 1.4. Techniques cryptographiques
 - 1.4.1. Longueur de la clé
 - 1.4.2. Manipulation des clés
 - 1.4.3. Types d'algorithmes
 - 1.4.4. Résumé des fonctions. Hash
 - 1.4.5. Générateurs de nombres pseudo-aléatoires
 - 1.4.6. Utilisation d'algorithmes
- 1.5. Cryptographie symétrique
 - 1.5.1. Blocs de chiffrement
 - 1.5.2. DES (*Data Encryption Standard*)
 - 1.5.3. Algorithme RC4
 - 1.5.4. AES (*Advance Encryption Standard*)
 - 1.5.5. Combinaison de chiffrements par blocs
 - 1.5.6. Dérivation de la clé
- 1.6. Cryptographie asymétrique
 - 1.6.1. Diffie-Hellman
 - 1.6.2. DSA (*Digital Signature Algorithm*)
 - 1.6.3. RSA (Rivest, Shamir y Adleman)
 - 1.6.4. Courbe elliptique
 - 1.6.5. Cryptographie asymétrique Typologie



- 1.7. Certificats numériques
 - 1.7.1. Signature numérique
 - 1.7.2. Certificats X509
 - 1.7.3. Infrastructure à clé publique(PKI)
- 1.8. Implémentations
 - 1.8.1. Kerberos
 - 1.8.2. IBM CCA
 - 1.8.3. *Pretty Good Privacy* (PGP)
 - 1.8.4. *ISO Authentication Framework*
 - 1.8.5. SSL et TLS
 - 1.8.6. Cartes à puce dans les moyens de paiement (EMV)
 - 1.8.7. Protocoles de téléphonie mobile
 - 1.8.8. *Blockchain*
- 1.9. Traitement des données en temps réel
 - 1.9.1. Stéganographie
 - 1.9.2. Steganoanalyse
 - 1.9.3. Applications et utilisations
- 1.10. Cryptographie quantique
 - 1.10.1. Algorithmes quantiques
 - 1.10.2. Protection des algorithmes contre l'informatique quantique
 - 1.10.3. Distribution de clés quantiques

“

Ce programme a tout pour plaire: un corps enseignant de haut niveau, une méthodologie flexible qui s'adapte au professionnel et le contenu le plus complet en cryptographie et cybersécurité"

05 Méthodologie

Ce programme de formation offre une manière différente d'apprendre. Notre méthodologie est développée à travers un mode d'apprentissage cyclique: ***le Relearning***.

Ce système d'enseignement est utilisé, par exemple, dans les écoles de médecine les plus prestigieuses du monde et a été considéré comme l'un des plus efficaces par des publications de premier plan telles que le ***New England Journal of Medicine***.





Découvrez Relearning, un système qui renonce à l'apprentissage linéaire conventionnel pour vous emmener à travers des systèmes d'enseignement cycliques: une façon d'apprendre qui s'est avérée extrêmement efficace, en particulier dans les matières qui exigent la mémorisation"

Étude de Cas pour mettre en contexte tout le contenu

Notre programme offre une méthode révolutionnaire de développement des compétences et des connaissances. Notre objectif est de renforcer les compétences dans un contexte changeant, compétitif et hautement exigeant.

“

Avec TECH, vous pouvez expérimenter une manière d'apprendre qui ébranle les fondations des universités traditionnelles du monde entier”



Vous bénéficierez d'un système d'apprentissage basé sur la répétition, avec un enseignement naturel et progressif sur l'ensemble du cursus.



L'étudiant apprendra, par des activités collaboratives et des cas réels, à résoudre des situations complexes dans des environnements commerciaux réels.

Une méthode d'apprentissage innovante et différente

Cette formation TECH est un programme d'enseignement intensif, créé de toutes pièces, qui propose les défis et les décisions les plus exigeants dans ce domaine, tant au niveau national qu'international. Grâce à cette méthodologie, l'épanouissement personnel et professionnel est stimulé, faisant ainsi un pas décisif vers la réussite. La méthode des cas, technique qui constitue la base de ce contenu, permet de suivre la réalité économique, sociale et professionnelle la plus actuelle.

“ Notre programme vous prépare à relever de nouveaux défis dans des environnements incertains et à réussir votre carrière ”

La méthode des cas est le système d'apprentissage le plus largement utilisé dans les meilleures écoles d'informatique du monde depuis qu'elles existent. Développée en 1912 pour que les étudiants en Droit n'apprennent pas seulement le droit sur la base d'un contenu théorique, la méthode des cas consiste à leur présenter des situations réelles complexes afin qu'ils prennent des décisions éclairées et des jugements de valeur sur la manière de les résoudre. En 1924, elle a été établie comme méthode d'enseignement standard à Harvard.

Dans une situation donnée, que doit faire un professionnel? C'est la question à laquelle nous sommes confrontés dans la méthode des cas, une méthode d'apprentissage orientée vers l'action. Tout au long du programme, les étudiants seront confrontés à de multiples cas réels. Ils devront intégrer toutes leurs connaissances, faire des recherches, argumenter et défendre leurs idées et leurs décisions.

Relearning Methodology

TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

Nous enrichissons l'Étude de Cas avec la meilleure méthode d'enseignement 100% en ligne: le Relearning.

En 2019, nous avons obtenu les meilleurs résultats d'apprentissage de toutes les universités en ligne du monde.

À TECH, vous apprendrez avec une méthodologie de pointe conçue pour former les managers du futur. Cette méthode, à la pointe de la pédagogie mondiale, est appelée Relearning.

Notre université est la seule université autorisée à utiliser cette méthode qui a fait ses preuves. En 2019, nous avons réussi à améliorer les niveaux de satisfaction globale de nos étudiants (qualité de l'enseignement, qualité des supports, structure des cours, objectifs...) par rapport aux indicateurs de la meilleure université en ligne.



Dans notre programme, l'apprentissage n'est pas un processus linéaire, mais se déroule en spirale (apprendre, désapprendre, oublier et réapprendre). Par conséquent, chacun de ces éléments est combiné de manière concentrique. Cette méthodologie a permis de former plus de 650.000 diplômés universitaires avec un succès sans précédent dans des domaines aussi divers que la biochimie, la génétique, la chirurgie, le droit international, les compétences en gestion, les sciences du sport, la philosophie, le droit, l'ingénierie, le journalisme, l'histoire, les marchés financiers et les instruments. Tout cela dans un environnement très exigeant, avec un corps étudiant universitaire au profil socio-économique élevé et dont l'âge moyen est de 43,5 ans.

Le Relearning vous permettra d'apprendre avec moins d'efforts et plus de performance, en vous impliquant davantage dans votre formation, en développant un esprit critique, en défendant des arguments et en contrastant les opinions: une équation directe vers le succès.

À partir des dernières preuves scientifiques dans le domaine des neurosciences, non seulement nous savons comment organiser les informations, les idées, les images et les souvenirs, mais nous savons aussi que le lieu et le contexte dans lesquels nous avons appris quelque chose sont fondamentaux pour notre capacité à nous en souvenir et à le stocker dans l'hippocampe, pour le conserver dans notre mémoire à long terme.

De cette manière, et dans ce que l'on appelle Neurocognitive context-dependent e-learning, les différents éléments de notre programme sont reliés au contexte dans lequel le participant développe sa pratique professionnelle.



Ce programme offre le support matériel pédagogique, soigneusement préparé pour les professionnels:



Support d'étude

Tous les contenus didactiques sont créés par les spécialistes qui enseigneront le cours, spécifiquement pour le cours, afin que le développement didactique soit vraiment spécifique et concret.

Ces contenus sont ensuite appliqués au format audiovisuel, pour créer la méthode de travail TECH en ligne. Tout cela, avec les dernières techniques qui offrent des pièces de haute qualité dans chacun des matériaux qui sont mis à la disposition de l'étudiant.



Cours magistraux

Il existe des preuves scientifiques de l'utilité de l'observation par un tiers expert.

La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.



Pratiques en compétences et aptitudes

Les étudiants réaliseront des activités visant à développer des compétences et des aptitudes spécifiques dans chaque domaine. Des activités pratiques et dynamiques pour acquérir et développer les compétences et aptitudes qu'un spécialiste doit développer dans le cadre de la mondialisation dans laquelle nous vivons.



Lectures complémentaires

Articles récents, documents de consensus et directives internationales, entre autres. Dans la bibliothèque virtuelle de TECH, l'étudiant aura accès à tout ce dont il a besoin pour compléter sa formation.





Case studies

Ils réaliseront une sélection des meilleures études de cas choisies spécifiquement pour ce diplôme. Des cas présentés, analysés et tutorés par les meilleurs spécialistes de la scène internationale.



Résumés interactifs

L'équipe TECH présente les contenus de manière attrayante et dynamique dans des pilules multimédia comprenant des audios, des vidéos, des images, des diagrammes et des cartes conceptuelles afin de renforcer les connaissances. Ce système éducatif unique pour la présentation de contenu multimédia a été récompensé par Microsoft en tant que "European Success Story".



Testing & Retesting

Les connaissances de l'étudiant sont périodiquement évaluées et réévaluées tout au long du programme, par le biais d'activités et d'exercices d'évaluation et d'auto-évaluation, afin que l'étudiant puisse vérifier comment il atteint ses objectifs.



06 Diplôme

Le Certificat en Cryptographie Avancée vous garantit, en plus de la formation la plus rigoureuse et la plus actuelle, l'accès à un diplôme universitaire de Certificat délivré par TECH Université Technologique.



“

*Finalisez cette formation avec succès
et recevez votre diplôme sans avoir à
vous soucier des déplacements ou des
démarches administratives”*

Ce **Certificat en Cryptographie Avancée** et de l'Identité Corporative contient le programme le plus complet et le plus actuel du marché.

Après avoir réussi l'évaluation, l'étudiant recevra par courrier postal* avec accusé de réception son correspondant diplôme de **Certificat** délivré par **TECH Université Technologique**.

Le diplôme délivré par **TECH Université Technologique** indiquera la note obtenue lors du **Certificat**, et répond aux exigences communément demandées par les bourses d'emploi, les concours et les commissions d'évaluation des carrières professionnelles.

Diplôme: **Certificat en Cryptographie Avancée**

N.º d'heures Officielles: **150 h.**



*Si l'étudiant souhaite que son diplôme version papier possède l'Apostille de La Haye, TECH EDUCATION fera les démarches nécessaires pour son obtention moyennant un coût supplémentaire.

future

santé confiance personnes

éducation information tuteurs

garantie accréditation enseignement

institutions technologie apprentissage

communauté engagement

service personnalisé innovation

connaissance présent qualité

en ligne formation

développement institutions

classe virtuelle langues

tech université
technologique

Certificat

Cryptographie Avancée

- » Modalité: en ligne
- » Durée: 6 semaines
- » Qualification: TECH Université Technologique
- » Intensité: 16h/semaine
- » Horaire: à votre rythme
- » Examens: en ligne

Certificat

Cryptographie Avancée