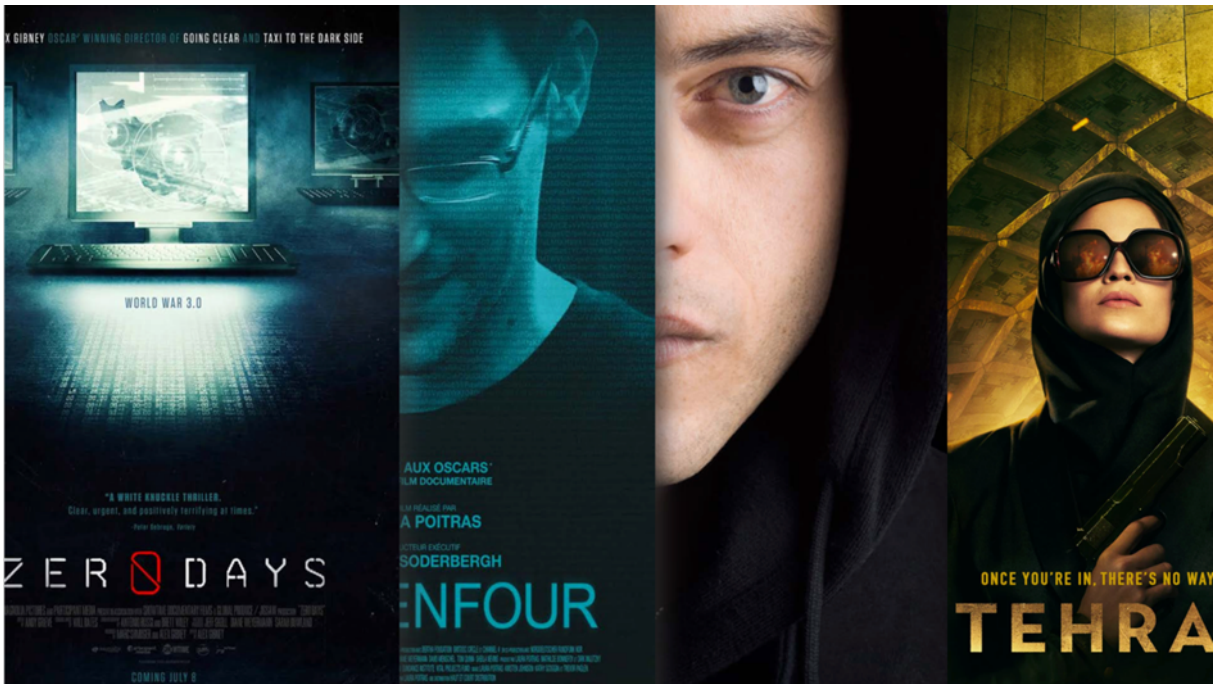
SYLLABUS DE COURS 2022-2023

Année :	*2023*
Formation :	*S2*
Titre du cours :	*CRYPTOGRAPHIE*
Langue :	*Français*
Professeur :	LEGER-DERVILLE Benoit
Volume horaire présentiel :	*7h (3,5 h + 3,5 h)*
Travail personnel :	*1,5 h*
ECTS :	

Cryptographie



Prérequis ***(que doivent-ils savoir en arrivant en 1ere année ?)***

1. **Aucun** savoir théorique ni pratique.
2. Venir avec sa CNIe (Carte Nationale d'Identité électronique) et/ou son Passeport.

3. Installer sur son smarphone une application de lecteur RFID de titre électronique
Par exemple :
https://play.google.com/store/apps/details?id=com.ariadnext.passportreader
https://apps.apple.com/fr/app/passport-nfc-reader/id1571930268
4. Avoir vu ou revu les films/documentaires suivants avant le cours magistral n°1 :

- **The Imitation Game** (2014) - https://www.imdb.com/title/tt2084970/
- **Zero Days** (2016) - https://www.imdb.com/title/tt5446858/

Description du cours

La cryptographie ne se contente plus d'assurer la confidentialité des secrets, elle détient désormais le pouvoir d'empêcher de **cloner des passeports** (*ou pas*), de garantir la solidité technique du **Bitcoin** et de rendre le chiffrement du ransomware **WannaCry** invincible. Mais attention, maîtriser ces compétences requiert l'apprentissage des cinq (5) fondamentaux cryptographiques de ce cours ! Les temps des vieilles « méthodes » de chiffrement de César, Mary Stuart, Vigenère et Enigma sont révolus, place à la cryptographie asymétrique et aux assemblages maitrisés. Préparez-vous à plonger dans la magie d'un des piliers de la cybersécurité.

Objectifs pédagogiques

Compréhension de l'apport fondamental et innovant de la **cryptographie asymétrique**. Puis appréhension des assemblages cryptographiques complexes utilisant les 5 briques fondamentales.

La cryptographie asymétrique est une compétence clé :) pour assurer la protection des données dans tous les environnements numériques actuels. Sa connaissance permet de garantir la maîtrise des assemblages cryptographiques complexes qui sont au cœur de tous les systèmes numériques avancés.

Connaissances acquises :

À la fin des deux cours, les étudiants doivent pouvoir citer et expliquer le rôle des 5 briques cryptographiques modernes que sont les principes :

- Du chiffrement symétrique ;
- Des protocoles d'établissement de clés ;
- De la cryptographie à clé publique ou asymétrique ;
- Des fonctions de hachage ;
- Des générateurs de nombres pseudo-aléatoires.

Évaluation :

1. Participation active aux cours et aux ateliers pédagogiques.
2. Réussir l'atelier/jeu en TD (travaux dirigés).

Pédagogie :

n° 1 Cours Magistral :

Apprentissage progressif de l'utilisation des 5 briques essentielles de la cryptographie dans les assemblages complexes que sont :

- Les titres d'identité sécurisés tels que les passeports et la CNIe
- La sécurité du Bitcoin

- Les indispensables VPN - TLS - PGP
- Les messageries Signal, WhatsApp, Olvid, Telegram et Berty
- Les méchants ransomwares
- Le CEV des factures EDF
- La signature électronique sécurisée

n° 2 Ateliers / Jeux :

Atelier/Jeu n° 1 : « **Attaque-moi si tu peux !** » - Jeu de chiffrement et de déchiffrement.
Se joue à 10 étudiants : 3 États-majors - 3 Commandos et 4 Ennemis.

« Pendant l'opération militaire, un bureau d'état-major et un groupe commando étaient en communication constante pour coordonner leurs actions. Cependant, ils étaient conscients que leurs messages étaient susceptibles d'être interceptés et écoutés par l'ennemi.

Pour protéger leur communication, ils ont décidé d'utiliser l'établissement de clé Diffie-Hellman pour chiffrer leurs messages. Grâce à cette méthode, ils pouvaient échanger des clés de chiffrement sans que l'ennemi puisse les intercepter.

Cependant, l'ennemi était rusé et avait réussi à se placer en tant qu'homme du milieu, ce qui signifie qu'il était capable de voir tous les messages échangés entre le bureau d'état-major et le groupe commando.

Pour contourner cette menace, ils ont décidé d'utiliser des techniques de brouillage pour rendre leurs messages incompréhensibles pour l'ennemi. Ils ont également changé régulièrement leurs clés de chiffrement pour rendre la tâche de l'ennemi plus difficile.

Grâce à leur persévérance et à leur ingéniosité, le bureau d'état-major et le groupe commando ont réussi à maintenir leur communication secrète et à coordonner avec succès leurs actions sur le terrain. »

Atelier/Jeu n° 2 : « **WannaCry nightmare** » - Puzzle cryptographique.
Se joue à 5 étudiants.

« En 2017, le monde a été frappé par une attaque de ransomware sans précédent appelée WannaCry, qui a infecté des centaines de milliers d'ordinateurs dans plus de 150 pays. Le ransomware était particulièrement dangereux, car il utilisait un ***assemblage cryptographique*** *redoutablement efficace pour chiffrer les fichiers des victimes, rendant ainsi la récupération des données impossible sans la clé de déchiffrement correcte.* ***Sauras-tu le reconstruire ?*** *»*

Mini CV de l'intervenant + 1 photo HD :

Benoit LEGER-DERVILLE est un expert cybersécurité, ingénieur diplômé de l'ESIEA et de Telecom ParisTech (MS-SSIR). Il est certifié CISSP, ISO 27001, SANS SEC542 et SANS SEC660, ainsi que responsable d'Audit LSTI certifié eIDAS, PASSI, PVID, MIE et habilité ANSSI. Il est expert cybersécurité auprès des assurances et a conduit de nombreuses missions d'audit de sécurité et de mise en place de PSSI et de SMSI de type ISO 27001 pour différentes structures du domaine de l'administration publique (Passeport Biométrique et CNIe), des finances et de l'industrie. Il est également enseignant à l'EPITA, responsable du cours sur la signature électronique sécurisée, ainsi que membre du jury des soutenances d'ingénieurs Cybersécurité. Enfin, il a animé un workshop sur la cryptographie pour l'École 42 et donné des conférences sur la sécurité du Bitcoin et de la Blockchain à Genève et Luxembourg pour Bloomberg.

Verbatim de l'intervenant :
"Do not implement crypo yourself !"

Besoins logistiques :
Salle permettant de répartir 8 ateliers cryptographiques simultanés : 4x10 + 4x5 = 60 étudiants.

Programmation des séances

Séances	Objectif	Thème général et contenu
1 - 19 juin 2023	**Cours Magistral - Les 5 briques**	**Théorie et illustrations**
2 - 20 juin 2023	**8 Ateliers/Jeux en simultané** **Jeu n°1 : 4 x 10 étudiants** **Jeu n°2 : 4 x 5 étudiants**	**Assemblage et réflexions cryptographiques**

GPT-4 :
*Q était le génie de la cryptographie au sein de l'organisation de James Bond. Il était le gardien des secrets les plus précieux de l'agence, et il avait développé une combinaison de cinq cryptosystèmes pour protéger les informations les plus sensibles. Il avait utilisé la **cryptographie symétrique** pour verrouiller les informations secrètes, la **cryptographie asymétrique** pour protéger les communications secrètes, des **générateurs de nombres pseudo-aléatoires** pour brouiller les pistes des ennemis, des **protocoles d'échange de clés** pour éviter les interceptions, et des **fonctions de hachage** pour garantir que les données n'étaient pas altérées. Cette combinaison de technologies de pointe avait permis à Q de protéger les secrets les plus précieux de l'agence, des plans de missiles aux identités de ses agents les plus importants. Grâce à Q et à sa combinaison de briques cryptographiques, James Bond avait été en mesure de remplir ses missions les plus dangereuses et de sauver le monde à maintes reprises.*

Bibliographie :

- Serious Cryptography - A Practical Introduction to Modern Encryption - by Jean-Philippe Aumasson
- Protocols for Authentication and Key Establishment - Colin Boyd , Anish Mathuria , Douglas Stebila
- Mooc - Coursera - Stanford University - Cryptographie I - Dan Boneh
- Mooc - Coursera - University of Maryland - Cryptographie - Jonathan Katz
- ANSSI - Guides - https://www.ssi.gouv.fr/guide/mecanismes-cryptographiques/
- ANSSI - Cours de Cryptologie
- ANSSI - Annexes B du RGS
- Histoire des codes secrets - de Simon Singh

Date de révision : Avril 2023