

Récapitulatif Complet — Chapitre 1 + Chapitre 2



Chapitre 1 — Introduction à la Cybersécurité



Objectif

Comprendre **pourquoi** on protège les données, **contre qui**, et **comment**.



Types de données



Données personnelles

- Identité : nom, adresse, âge, photos
- Santé, école, finances, emploi
- Identité en ligne (réseaux sociaux, comptes)



Risques : vol d'identité, fraude, réputation



Données d'entreprise

- Données transactionnelles (achats, opérations)
- Données financières
- Propriété intellectuelle (brevets, plans)
- Données *IoT & Big Data*



Risques : perte financière, espionnage industriel, sabotage

Menaces

Source	Exemples
Criminels	Vol d'argent, phishing, ransomware
Entreprises	Collecte et vente de données
Gouvernements	Surveillance
Menaces internes	Employés négligents / malveillants
Menaces externes	Hackers, malwares, attaques réseau



Modèle fondamental : Triade CIA

Principe	Objectif	Exemples
Confidentialité	Empêcher accès non autorisé	Chiffrement, contrôle accès
Intégrité	Empêcher modification non autorisée	Hash, signatures, contrôle accès
Disponibilité	Assurer accès aux services	Backups, mises à jour, redondance



Moyens de protection

- **Technologie** : pare-feux, antivirus, IDS, chiffrement
- **Processus** : politiques, gestion accès, plan urgence
- **Formation** : sensibilisation utilisateurs

⚠️ Conséquences d'attaques

- Perte financière
 - Perte de confiance & réputation
 - Fuite de données
 - Sabotage / vandalisme
 - Amendes légales
-

🔒 Chapitre 2 — Techniques de Cryptographie Classique

🎯 Objectif

Comprendre **évolution du chiffrement** des méthodes anciennes vers modernes.

🏛️ Évolution historique

Période	Méthodes	Objectif
Antiquité	Scytale, Polybe, César	Cacher ou remplacer lettres
Moyen-Âge	Vigenère, analyse fréquentielle	Niveaux plus élevés de sécurité
XXe siècle	Enigma, Bombes	Crypto mécanisée & guerre
Moderne	DES, AES, RSA	Crypto mathématique avancée
Futur	Post-quantique	Résister ordinateurs quantiques

Méthodes classiques du fichier

Méthode	Type	Description
Scytale	Stéganographie	Cacher le message
Carré de Polybe	Substitution par coordonnées	2 chiffres par lettre
César	Substitution mono	Décalage alphabet
Mono-alphabetique	Substitution fixe	Une permutation unique
Analyse fréquentielle	Cryptanalyse	Casser substitution
Vigenère	Substitution poly	Clé répétée, alphabets multiples
Rail Fence	Transposition	Zigzag puis lecture lignes
Transposition colonnes	Transposition	Permutation colonnes
Enigma	Machine rotors	Substitution dynamique

Formules importantes (César)

$$C = (P + k) \mod 26 \quad (\text{chiffrement})$$

$$P = (C - k) \mod 26 \quad (\text{déchiffrement})$$



Concepts modernes introduits

Algorithme	Type	Caractéristiques
DES	Symétrique	Clé 56 bits (faible)
AES	Symétrique	Standard actuel 128/192/256 bits
RSA	Asymétrique	Clé publique/privée



Crypto quantique

- Menace : algorithme de Shor peut casser RSA/ECC
 - Solution : algorithmes **post-quantiques**
-



Synthèse finale

La cybersécurité protège les systèmes et données contre des attaques diverses, tandis que la cryptographie permet de garantir la confidentialité, l'intégrité et la disponibilité des informations grâce à des techniques de chiffrement évoluées depuis l'Antiquité jusqu'aux algorithmes modernes.

Carte mentale express

Cybersécurité

- └─ Données : perso / entreprise
- └─ Menaces : internes / externes
- └─ Triade CIA : Confidentialité - Intégrité - Disponibilité
 - └─ Protection : tech / politiques / formation

Cryptographie

- └─ Antiquité : César, Polybe, Scytale
- └─ Moyen-Âge : Vigenère, analyse fréquentielle
- └─ WWII : Enigma, Bombes
- └─ Moderne : DES, AES, RSA
- └─ Futur : post-quantique