Projets cryptographie AP5

I. Introduction :

En complément du cours et des travaux pratiques, vous aurez l'opportunité d'explorer des projets en cryptographie qui viennent compléter et enrichir vos apprentissages en classe. Ces derniers vous permettront de concrétiser les connaissances théoriques via des applications réelles, générant des solutions concrètes et opérationnelles.

Ces projets sont conçus pour être réalisés en équipes de cinq étudiants, favorisant la collaboration, l'échange d'idées et la synergie des compétences. Chaque projet comporte une dimension théorique et une dimension pratique. Bien que des pistes vous soient proposées ci-dessous, vous êtes libres de personnaliser les sujets, à condition de garantir un travail solide et cohérent.

Dans le cadre de suivi des projets, la validation des étapes aura lieu à la fin de chaque séance de cours (10 à 15 minutes). Il est important de noter que ces projets sont structurés pour être menés de manière autonome, manifestant votre capacité d'initiative. Le rôle de l'enseignant consiste à vous conseiller et à orienter vos démarches pour une réussite optimale.

Date des présentations orales	**20/10/2023**
Livrables	1. **Rapport** de projet de 25 à 30 pages en suivant les lignes directrices de rédaction que vous trouverez ci-dessous de ce document. 2. **Présentation** PowerPoint (les diapositives ne sont pas surchargées, la présentation sert de fil conducteur pour faciliter la progression des idées). 3. **Solution** technique si faisable/ vidéo de démonstration.
Nom du dossier	• GX-Intitulé du projet. Zip/.rar où X est le numéro de votre groupe.

II. Objectifs des projets

- Acquérir une compréhension approfondie des concepts fondamentaux de la cryptographie et démontrer leur application pratique.
- Cultiver les compétences en matière d'auto-apprentissage et de prise d'initiative pour une exploration autonome des sujets complexes.
- Transposer les connaissances théoriques acquises en actions tangibles à travers des réalisations pratiques et concrètes.

III. Liste des projets

1. Projet (1) : Mise en place d'un Tunnel VPN sécurisé avec Racoon (IPsec-tools)

a. Description :

Ce projet consiste à créer un canal de communication chiffré entre deux réseaux distincts en utilisant Racoon ; une implémentation open source d'IPsec-tools ; simulant ainsi un scénario réel de sécurisation des échanges entre partenaires ou succursales distantes. En configurant des politiques de sécurité, des clés de chiffrement et des mécanismes d'authentification, vous apprendrez concrètement à établir un tunnel VPN sécurisé, ce qui renforcera vos compétences en sécurisation des données, en gestion des clés et en configuration de protocoles de sécurité.

b. Objectifs :

- Comprendre les principes des réseaux privés virtuels (VPN) et du protocole IPsec.
- Explorer les concepts de chiffrement, d'intégrité et d'authentification dans le contexte d'IPsec.
- Évaluer les avantages et les défis de l'utilisation de Racoon pour sécuriser les communications réseau.
- Acquérir une expérience concrète en matière de gestion des protocoles de sécurité et de sécurisation des communications réseau, en vous préparant à faire face aux enjeux réels de la cybersécurité dans un environnement professionnel.

c. Exemple d’outils à utiliser :

- **Racoon (IPsec-tools)** : L'outil principal pour la mise en place du tunnel VPN sécurisé.
- **Wireshark** : Pour analyser les échanges de données et les protocoles de sécurité.
- **Virtual Machines (VirtualBox, VMware)** : Pour simuler deux réseaux distincts et tester la configuration du tunnel.

2. Projet (2) : Exploration de l'authentification et de l'autorisation avec Kerberos : Concepts et mise en œuvre

a. Description :

Ce projet a pour finalité de vous introduire au système d'authentification et d'autorisation Kerberos, largement utilisé dans les environnements IT pour sécuriser les communications et les accès aux ressources. Vous découvrirez les concepts fondamentaux de Kerberos et apprendrez comment il fonctionne pour garantir l'authenticité et la confidentialité des échanges entre utilisateurs et serveurs. En comprenant les mécanismes de sécurité de Kerberos, vous serez en mesure de mettre en œuvre des solutions d'authentification robustes dans différents contextes.

b. Objectifs :

- Comprendre les principes de base de l'authentification et de l'autorisation.
- Explorer le fonctionnement interne de Kerberos en matière de gestion de tickets et de protocoles de communication.
- Mettre en œuvre un système d'authentification basé sur Kerberos dans un environnement simulé.
- Évaluer les avantages et les limitations de Kerberos en matière de sécurité.

c. Exemple d'outils à utiliser :

- **MIT Kerberos :** L'implémentation de référence de Kerberos, disponible gratuitement, pour mettre en place un environnement de test.
- **Wireshark** : Pour l'analyse des échanges réseau et l'observation des protocoles de Kerberos.
- **Environnement Virtuel (VirtualBox, VMware)** : Pour simuler un réseau d'authentification et de communication entre clients et serveurs (Ubuntu).

3. Projet (3) : Mise en Œuvre de la Sécurité des Communications avec GPG : Chiffrement et Signature Numérique

a. Description :

Le but de ce projet est de vous guider à travers l'utilisation pratique de GPG (GNU Privacy Guard) pour sécuriser les communications en ligne en utilisant le chiffrement et la signature numérique. Vous comprendrez les bases de la cryptographie asymétrique et apprendrez comment GPG peut être utilisé pour protéger la confidentialité et garantir l'authenticité des messages échangés. En explorant GPG, vous serez en mesure de sécuriser vos communications électroniques personnelles et professionnelles.

b. Objectifs :

- Comprendre les concepts fondamentaux de la cryptographie asymétrique et de la sécurité des communications.
- Utiliser GPG pour chiffrer et déchiffrer des messages, assurant ainsi la confidentialité des informations.
- Créer des signatures numériques avec GPG pour prouver l'authenticité et l'intégrité des messages.
- Évaluer les avantages et les limitations de l'utilisation de GPG pour sécuriser les communications.

c. Exemples d'outils à utiliser :

- **GPG (GNU Privacy Guard)** : L'outil principal pour le chiffrement et la signature numérique.
- **Messagerie Électronique** :
  - **Serveur** : Postfix ;
  - **Client de messagerie** : Pour envoyer et recevoir des messages sécurisés (vous pouvez utiliser le client de messagerie Thunderbird)

4. Projet (4) : Transfert Sécurisé de Fichiers avec SFTP

a. Description :

L'objectif de ce projet est de mettre en place un transfert sécurisé de fichiers en utilisant le protocole SFTP (SSH File Transfer Protocol). Vous comprendrez les concepts de base du SFTP et apprendrez comment configurer un environnement pour le transfert sécurisé de fichiers entre des systèmes distants. En implémentant SFTP, vous serez en mesure de sécuriser efficacement les échanges de fichiers sensibles.

b. Objectifs :

- Comprendre les principes des protocoles de transfert de fichiers sécurisés.
- Configurer un serveur SFTP pour permettre le transfert sécurisé de fichiers.
- Utiliser des clients SFTP pour transférer des fichiers en toute sécurité.Expliquer les mécanismes de sécurité et d'authentification intégrés au SFTP.

c. Exemples d’outils à utiliser :

- **Serveur SFTP (par exemple OpenSSH)** : Pour configurer un serveur SFTP sur l'un des systèmes.
- **Clients SFTP (par exemple WinSCP, FileZilla**) : Pour effectuer des transferts sécurisés depuis et vers le serveur SFTP.
- **Environnement Virtuel (VirtualBox, VMware) :** Pour simuler les systèmes distants et tester les transferts.
- **Éditeur de Texte** : Pour la configuration des fichiers de serveur SFTP.
- **Terminal/Console** : Pour l'administration du serveur SFTP et l'exécution des commandes.

5. Projet (5) : Exploration de la Cryptomonnaie et de la Blockchain : Concepts, Transactions et Sécurité (niveau avancé en cryptographie)

a. Description :

Ce projet vise à vous introduire dans le domaine en évolution constante des cryptomonnaies et de la technologie blockchain. L'objectif est de vous familiariser avec les concepts fondamentaux de la cryptomonnaie et de la technologie blockchain, ainsi que d'explorer leur application pratique dans les transactions et la sécurité. En comprenant les mécanismes de fonctionnement de la cryptomonnaie et de la blockchain, vous serez en mesure d'appréhender leurs avantages et leurs défis, tout en acquérant une compréhension solide des protocoles de sécurité et de la protection des données. À travers des activités pratiques et des discussions approfondies, vous développerez une vision globale des opportunités offertes par la cryptomonnaie et la blockchain, ainsi que des préoccupations en matière de sécurité qui les accompagnent.

b. Objectifs :

- Comprendre les bases de la cryptographie et son rôle dans la sécurisation des transactions de cryptomonnaie.
- Examiner les concepts fondamentaux de la cryptomonnaie et de la technologie blockchain.
- Pratiquer la création et la gestion de portefeuilles de cryptomonnaie.
- Simuler des transactions de cryptomonnaie et en comprendre le fonctionnement.
- Analyser les mécanismes de consensus et de preuve utilisés dans les blockchains.
- Explorer les aspects de sécurité liés à la cryptomonnaie et à la protection des données.

c. Concepts techniques à mettre en place :

- **Chiffrement Symétrique et Asymétrique** : Comprendre la différence entre le chiffrement symétrique (utilisant une seule clé pour chiffrer et déchiffrer) et le chiffrement asymétrique (utilisant une paire de clés publique/privée).
- **Clés Publiques et Privées** : Comprendre le concept de paires de clés et comment les clés publiques et privées sont utilisées pour le chiffrement et la signature numérique.
- **Fonctions de Hachage** : Comprendre le fonctionnement des fonctions de hachage pour créer des empreintes uniques à partir de données.
- **Signature Numérique** : Comprendre comment une signature numérique est créée à partir d'un hachage cryptographique et d'une clé privée pour prouver l'authenticité.
- **Preuve de Travail (Proof of Work)** : Avoir une idée de base de la preuve de travail et comment elle est utilisée pour sécuriser les blockchains.
- **Preuve d'Enjeu (Proof of Stake)** : Avoir une idée de base de la preuve d'enjeu comme alternative à la preuve de travail.
- **Courbes Elliptiques** : Comprendre les concepts de base des courbes elliptiques et comment elles sont utilisées dans la cryptographie.
- **Protocoles de Signature à Courbes Elliptiques (ECDSA)** : Comprendre comment ECDSA est utilisé pour créer des signatures numériques dans les blockchains et les cryptomonnaies.
- **Sécurité Cryptographique** : Avoir une compréhension élémentaire des principaux concepts de sécurité cryptographique, y compris la confidentialité, l'intégrité et l'authenticité.
- **Hachage de Mot de Passe :** Comprendre comment les fonctions de hachage de mot de passe sont utilisées pour stocker en toute sécurité les mots de passe.

- **Attaques Cryptographiques Basiques** : Avoir conscience des types d'attaques cryptographiques de base, telles que l'attaque par force brute et l'attaque par dictionnaire

d. Exemples d’outils à utiliser :

- **GPG (GNU Privacy Guard)** : Cet outil de cryptographie open source peut être utilisé pour comprendre et pratiquer les concepts de chiffrement et de signature numérique.
- **Coinbase** (payante) : Cette plateforme de cryptomonnaie en ligne permet la création de portefeuilles et la simulation de transactions avec des cryptomonnaies telles que Bitcoin et Ethereum.
- **Binance** : Une autre plateforme populaire pour la création de portefeuilles et l'exploration de transactions avec diverses cryptomonnaies.
- **Blockchain.info** : Vous pouvez explorer les transactions et les blocs sur la blockchain Bitcoin à l'aide de cet explorateur de blockchain en ligne.
- **Etherscan** : Cet explorateur de blockchain est dédié à la blockchain Ethereum et permet d'explorer les transactions et les contrats intelligents.
- **CryptoSim** : Un simulateur de cryptomonnaie en ligne qui permet de simuler des transactions et de comprendre les mécanismes de consensus.
- **VirtualBox ou VMware** : Pour créer des machines virtuelles avec différents systèmes d'exploitation, afin de tester les outils et les activités du projet dans un environnement isolé.

6. Projet (6) : Gestion Sécurisée des accès à distance avec SSH : configuration, authentification et sécurité

a. Description :

Ce projet vise à établir une gestion sécurisée des accès à distance en utilisant le protocole SSH (Secure Shell). Vous comprendrez les fondamentaux de SSH et apprendrez comment configurer et sécuriser les connexions à distance vers des serveurs. En explorant SSH, vous serez en mesure de garantir l'intégrité et la confidentialité des échanges et des opérations à distance.

b. Objectifs :

- Comprendre les principes de base du protocole SSH et son rôle dans la sécurité des communications.
- Configurer un serveur SSH pour permettre des connexions sécurisées.
- Utiliser des clients SSH pour se connecter à distance à des serveurs.
- Explorer les mécanismes d'authentification et de sécurité de SSH.

c. Exemples d'outils à Utiliser :

- **Serveur SSH (par exemple OpenSSH)** : Pour configurer un serveur SSH sur l'un des systèmes.
- **Clients SSH (par exemple OpenSSH, PuTTY)** : Pour établir des connexions sécurisées à distance.
- **Environnement Virtuel (VirtualBox, VMware)** : Pour simuler un environnement de réseau et tester les connexions.

7. Projet (7) : Contrôle d'Accès Réseau (NAC) avec PacketFence

a. Description :

Ce projet consiste à mettre en œuvre d'une solution de Contrôle d'Accès aux Réseaux (NAC) en utilisant PacketFence. Vous allez concevoir, configurer et déployer une solution de contrôle d'accès qui sécurisera les accès aux réseaux en autorisant uniquement les périphériques et les utilisateurs autorisés. De plus, vous explorerez comment la cryptographie joue un rôle essentiel dans l'authentification et la sécurisation des échanges entre les utilisateurs, les périphériques et les serveurs.

b. Objectifs du Projet :

- Comprendre les concepts et les enjeux du Contrôle d'Accès aux Réseaux (NAC).
- Configurer et déployer PacketFence pour la gestion des accès au réseau.
- Expliquer comment la cryptographie est utilisée pour sécuriser les échanges entre les éléments du réseau.
- Mettre en œuvre des mécanismes de chiffrement et d'authentification pour renforcer la sécurité.

c. Exemples d’outils à utiliser :

- **PacketFence** : Pour la configuration et le déploiement du contrôle d'accès aux réseaux.
- **Wireshark** : Pour analyser les échanges réseau et observer la cryptographie en action.
- **Virtual Machines (VirtualBox, VMware)** : Pour simuler un environnement de réseau et tester la solution.

8. Projet (8) : Sécurité des applications de messagerie instantanée (exemple : Whatsapp)

a. Description du Projet :

Ce projet se concentre sur l'analyse et l'amélioration de la sécurité des applications de messagerie instantanée populaires, telles que WhatsApp. L'objectif principal est d'explorer les vulnérabilités potentielles, de proposer des solutions pour renforcer la sécurité et de sensibiliser aux bonnes pratiques de protection des données personnelles dans ces environnements.

b. Objectifs du Projet :

- Analyse des Vulnérabilités : Examiner en profondeur les vulnérabilités connues ou potentielles dans les applications de messagerie instantanée.
- Chiffrement des Communications : Étudier et évaluer les protocoles de chiffrement utilisés pour sécuriser les messages et les appels.
- Protection des Données Personnelles : Identifier les pratiques de protection des données personnelles mises en place et proposer des améliorations.
- Authentification et Sécurité de Connexion : Examiner les mécanismes d'authentification et les mesures de sécurité liées aux connexions.
- Prévention des Attaques : Proposer des méthodes pour prévenir les attaques courantes telles que l'hameçonnage, le vol d'identité, etc.
- Confidentialité des Groupes : Analyser la sécurité des chats de groupe et proposer des moyens de renforcer la confidentialité.
- Tests de Sécurité : Mettre en place des scénarios de test pour évaluer la sécurité de l'application face aux attaques potentielles.
- Sensibilisation à la Sécurité : Créer des ressources de sensibilisation pour les utilisateurs, afin de les informer sur les risques et les mesures de sécurité à prendre.

c. Exemples d'outils à utiliser :

- **Burp Suite** : Pour effectuer des tests de sécurité sur l'application.
- **Wireshark** : Pour analyser le trafic réseau pour évaluer la sécurité des connexions.
- **Signal Protocol** : Étudiez le protocole de chiffrement Signal utilisé par WhatsApp.
- **Outils de Détection de Malware** : Utilisez des outils comme ClamAV pour détecter les logiciels malveillants.
- **Code Review** : Examinez le code source de l'application pour identifier les failles de sécurité potentielles.

9. Projet (9) : Renforcement de la Sécurité du Système Interbancaire SWIFT : Cryptographie, Authentification et Mesures de Sécurité (niveau avancé en cryptographie)

a. Description :

Ce projet vous plonge dans le monde complexe de la sécurité du système interbancaire SWIFT, utilisé pour les transactions financières internationales. Vous allez explorer comment la cryptographie, l'authentification et diverses mesures de sécurité sont utilisées pour protéger les communications et les transactions sensibles au sein du réseau SWIFT. Vous examinerez également comment les attaques potentielles sont contrées et comment la sécurité est renforcée dans ce contexte critique.

b. Objectifs du Projet :

- Comprendre les défis et les enjeux de sécurité spécifiques au système interbancaire SWIFT.
- Analyser comment la cryptographie est utilisée pour sécuriser les messages et les transactions.
- Expliquer les méthodes d'authentification et les mécanismes de vérification d'identité.
- Mettre en œuvre des mesures de sécurité pour contrer les menaces potentielles.

c. Exemple d'outils à utiliser :

- **Documentation SWIFT** : Pour comprendre les spécificités et les mesures de sécurité mises en place.
- **Wireshark** : Pour analyser les échanges et les messages SWIFT.
- **VirtualBox, VMware** : Pour simuler les transactions et les interactions au sein du réseau SWIFT.
- **Outils de Simulation d'Attaques** (Kali, Metasploit…) : Pour tester la résistance du système face à différentes attaques.

!!! Ce projet vous offrira l'opportunité d'explorer le domaine complexe de la sécurité dans le système interbancaire SWIFT, où vous découvrirez comment la cryptographie et d'autres mesures de sécurité sont déployées pour assurer l'intégrité et la confidentialité des transactions financières internationales.

10. Projet (10) : Exploration de la Cryptographie Post-Quantique basée sur les Fonctions de Hachage : Concepts, Applications et Sécurité (niveau avancé en cryptographie)

a. Description :

Ce projet vous plonge dans le monde de la cryptographie post-quantique, une discipline qui vise à développer des techniques de sécurité capables de résister aux attaques des ordinateurs quantiques. Vous explorerez les concepts fondamentaux de la cryptographie basée sur les fonctions de hachage, qui est l'un des domaines de recherche les plus prometteurs pour la résistance à la puissance de calcul quantique. Vous analyserez les applications potentielles et évaluerez la robustesse de ces techniques contre les attaques classiques et quantiques.

b. Objectifs du Projet :

- Comprendre les défis posés par les ordinateurs quantiques pour la cryptographie traditionnelle.
- Explorer les bases de la cryptographie post-quantique et ses principales approches.
- Examiner comment les fonctions de hachage sont utilisées dans la cryptographie post-quantique.
- Évaluer la sécurité et l'applicabilité des méthodes post-quantiques basées sur les fonctions de hachage.

c. Exemples d'outils à utiliser :

- **Environnement de Programmation (Python, MATLAB, etc**.) : Pour mettre en œuvre et expérimenter les concepts de cryptographie post-quantique.
- **Plateformes de Simulation Quantique (Qiskit, QuTiP, etc.)** : Pour comprendre les aspects quantiques des méthodes.

11. Projet (11) : Vote électronique (vote à distance). (Niveau avancé en cryptographie)

a. Description :

Ce projet vise à concevoir et à mettre en œuvre une solution de vote électronique, particulièrement adaptée aux entreprises et aux collectivités pour leurs processus de décision internes. L'objectif est de créer une application de vote sécurisée, conviviale et évolutive qui permettra aux utilisateurs de participer aux votes à distance, offrant ainsi une alternative moderne aux méthodes de vote traditionnelles.

b. Objectifs du Projet :

- Créer une interface conviviale et ergonomique pour permettre aux utilisateurs de voter électroniquement de manière intuitive (conception).
- Mettre en place des mécanismes de sécurité robustes pour garantir l'intégrité des votes et la confidentialité des choix des utilisateurs.
- Concevoir l'application de manière qu'elle puisse être adaptée aux besoins spécifiques des entreprises et collectivités, en permettant des fonctionnalités évolutives.
- Intégrer des outils d'administration pour permettre aux responsables de gérer les votes, de créer des sondages et de suivre les résultats.
- Mettre en pratique les connaissances en cryptographie en utilisant des méthodes de chiffrement pour sécuriser les données de vote.

c. Exemples d'Outils pour l'Implémentation :

- **Langages de Programmation** : Utilisez des langages comme Python, Java, ou JavaScript pour développer l'application.
- **Frameworks Web** : Choisissez des frameworks web comme Django, Flask, ou Ruby on Rails pour faciliter le développement de l'interface utilisateur et la gestion des données.
- **Chiffrement** : Utilisez des bibliothèques de chiffrement telles que CryptoJS pour sécuriser les données de vote.
- **Base de Données** : Utilisez un système de gestion de base de données comme MySQL ou PostgreSQL pour stocker les informations de vote de manière sécurisée.
- **Authentification** : Implémentez des mécanismes d'authentification robustes en utilisant des bibliothèques telles que OAuth ou JWT.
- **Interfaces Utilisateur** : Utilisez des outils de conception d'interfaces comme React, Angular ou Vue.js pour créer une expérience utilisateur fluide.

Ce projet offre une opportunité d'appliquer des connaissances en **cryptographie**, en **développement logiciel** et en **sécurité des données** pour créer une solution pratique et pertinente.

IV. Autres idées de projets à explorer :

1. Les attaques par collision et les attaques par force brute sur les méthodes de hashage MD5 et SHA1 ;

2. Comparaison entre OpenID Connect et OAuth 2.0 : Renforcement de la Sécurité et de la Gestion des Identités ;

3. Cryptographie légère pour l'internet des objets ;

4. Sécurité des données sensibles dans le cloud avec la cryptographie homomorphe.

V. Éléments à Prendre en Compte lors de la Rédaction du rapport de projet

La structure du rapport de projet devrait être à la fois concise et complète pour refléter vos accomplissements et votre compréhension durant cette courte période. Ci-après une proposition de structure à adopter et adapter selon chaque projet :

1. **Page de Garde :**
   - Nom de l'établissement, du département et du module.
   - Titre du rapport (ex. : " Exploration de la Cryptographie Post-Quantique basée sur les Fonctions de Hachage : Concepts, Applications et Sécurité").
   - Nom complet des étudiants.
   - Nom des enseignants encadrants.
   - Date de la présentation (soutenance).
2. **Résumé :**
   - Un résumé bref mais informatif de vos accomplissements et apprentissages pendant le projet (100 à 150 mots).
3. **Introduction :**
   - Présentation du contexte de la cryptographie et de l'importance de la thématique.
   - Énoncé des objectifs du projet de module et de ce que vous avez cherché à accomplir en un mois.
   - Organisation du rapport (structure).
4. **Chapitre 1 : Cadrage du projet**
   - Choix de thématique : Explication de la thématique spécifique que vous avez explorée dans le domaine de la cryptographie.
   - Objectifs du Projet : Une description claire et concise des objectifs que vous avez fixés pour le projet.
   - Méthodologie : Brève description de l'approche que vous avez utilisée pour atteindre vos objectifs.
   - Planification des activités (gestion de projet, gant, taches/phasage temporel).
5. **Chapitre 2 : Concepts fondamentaux, recherche et apprentissage :**
   - Résumé des connaissances acquises en lien avec la thématique de projet choisie.

- Utilisation des références académiques fiables (à mentionner dans la partie références).

6. **Chapitre 3 : Réalisation et mise en ouvre**
   - Liste des outils, logiciels et technologies utilisés.
   - Explication de la manière dont chaque outil a été utilisé dans le projet.
   - Description des activités spécifiques que vous avez menées pendant la période du projet (ex. : recherche, expérimentation, codage, etc.).
   - Présentation des résultats obtenus et des observations pertinentes dans le contexte de votre projet.
7. **Conclusion générale**
   - Récapitulation des principales réalisations.
   - Réflexion sur ce que vous avez appris, les défis rencontrés et les aspects que vous auriez aimé approfondir.
   - **Perspectives :** Comment vous envisagez de poursuivre vos connaissances et compétences dans la cryptographie.
8. **Références :**
   - Liste des sources académiques et techniques consultées.
9. **Annexes :**
   - Toute information complémentaire pertinente, comme des extraits de code, des captures d'écran des installations, etc.

Cet exemple de structuration offre une approche méthodique pour organiser votre rapport en garantissant la clarté, la cohérence du contenu et l'équilibre des chapitres.