TP 2 : Protection d'un Flux de Données IIoT

Nom : _____

Prénom : _____

Note : /20

Durée : 3H

AAVs Évalués

- **AAV 2:** Utiliser une bibliothèque pour appliquer un schéma de chiffrement authentifié léger afin de protéger un flux de données dans un scénario IIoT.

Évaluation

Partie 1 : Qualité du Code (6 pts)

1.1. Implémentation Fonctionnelle

Maîtrisé (3 pts)	Acquis (2 pts)	Passable (1 pts)	Non Acquis (0 pts)
Le code est parfaitement fonctionnel, exécute tous les scénarios (nominal, corruption ciphertext, corruption AD) sans erreur et produit les résultats attendus.	Le code est fonctionnel pour le cas nominal, mais présente des erreurs mineures dans l'un des scénarios d'expérimentation, ou une fonction est incomplète.	Le code contient des erreurs significatives qui empêchent l'exécution complète d'un ou plusieurs scénarios. La logique de base est présente mais incorrectement implémentée.	Le code est absent, non fonctionnel, ou ne répond pas du tout à la demande.

Commentaires :

1.2. Robustesse et Bonnes Pratiques

Maîtrisé (3 pts)	Acquis (2 pts)	Passable (1 pts)	Non Acquis (0 pts)
Le code est exemplaire : la gestion d'erreur (try/except) est correctement implémentée, les types de données (bytes, str, dict) sont manipulés sans erreur, le code est clair, commenté et suit les conventions PEP8.	Le code est fonctionnel, mais manque de robustesse. La gestion d'erreur est présente mais imparfaite, ou des conversions de types sont maladroites. Le code est peu ou pas commenté.	Le code ne gère aucune erreur (pas de try/except), les manipulations de types sont incorrectes, rendant le code fragile. Le style est très peu soigné.	Absence totale de bonnes pratiques. Le code est illisible et difficile à maintenir.

Commentaires :

Partie 2 : Analyse Théorique et Expérimentale (10 pts)

2.1. Compréhension du Fonctionnement de l'AEAD

Maîtrisé (4 pts)	Acquis (3 pts)	Passable (1.5 pts)	Non Acquis (0 pts)
Les réponses sont précises, détaillées et justifiées.	Les réponses sont correctes mais superficielles.	L'étudiant montre une confusion sur au moins un des concepts clés.	Les réponses sont absentes ou incorrectes.

Commentaires :

2.2. Analyse des Propriétés de Sécurité

Maîtrisé (4 pts)	Acquis (3 pts)	Passable (1.5 pts)	Non Acquis (0 pts)
L'analyse des expériences est excellente. L'étudiant explique clairement que l'échec est dû à la non-correspondance du tag, et extrapole le rôle des AD pour lier le ciphertext à son contexte, en donnant un autre exemple pertinent et bien argumenté.	L'analyse est correcte. L'étudiant constate que les tests échouent comme prévu et explique correctement le rôle des AD dans le scénario du TP, mais l'exemple supplémentaire est faible ou manque de pertinence.	L'analyse est très limitée. L'étudiant se contente de constater l'échec des tests sans expliquer pourquoi le mécanisme AEAD a permis de détecter l'altération.	Aucune analyse des résultats n'est fournie, ou l'interprétation est fautive.

Commentaires :

2.3. Analyse des Limites du Schéma

Maîtrisé (2 pts)	Acquis (1 pts)	Passable (0.5 pts)	Non Acquis (0 pts)
La réponse est complète et précise.	La réponse est partiellement correcte.	L'étudiant mentionne le problème mais ne propose aucune solution viable.	La question n'est pas traitée ou la réponse est incorrecte.

Commentaires :

Partie 3 : Qualité du Compte Rendu (4 pts)

3.1. Clarté et Structure

Maîtrisé (2 pts)	Acquis (1.5 pts)	Passable (0.5 pts)	Non Acquis (0 pts)
Le rapport est très bien structuré, facile à lire. Toutes les sections demandées sont présentes. Le tableau de résultats est clair, complet et met en évidence les conclusions des expériences.	Le rapport est globalement bien structuré, mais pourrait être plus clair. Il manque des éléments mineurs, ou le tableau de résultats est présent mais peu lisible ou incomplet.	Le rapport est désorganisé, difficile à suivre. Des sections importantes sont manquantes. Le tableau de résultats est absent.	Le rapport est absent ou inexploitable.

Commentaires :

3.2. Rigueur et Précision de la Rédaction

Maîtrisé (2 pts)	Acquis (1.5 pts)	Passable (0.5 pts)	Non Acquis (0 pts)
La rédaction est professionnelle et rigoureuse. Le vocabulaire cryptographique (nonce, tag, AEAD, intégrité, confidentialité) est utilisé à bon escient et sans ambiguïté.	La rédaction est correcte, mais présente quelques imprécisions terminologiques ou des phrases manquant de clarté.	La rédaction est négligée, avec de nombreuses fautes ou un usage incorrect et répété de la terminologie technique.	La qualité de la rédaction rend le rapport incompréhensible.

Commentaires :