BLKN 216 Cryptography and Hash Functions

MICROCREDENTIAL AWARDED TO

Claude N'Gouin-Claih

Specific Learning Objectives:
Define and explain cryptographic hash functions and their properties (Knowledge). Compare and contrast various cryptographic hash functions and algorithms (Comprehension). Demonstrate how to apply cryptographic hash functions to ensure data integrity (Application). Analyze the security and performance of different cryptographic hash functions (Analysis). Evaluate the appropriateness of cryptographic hash functions in various use cases (Evaluation). Design and implement a secure hash function for a specific application (Synthesis). Explain the role of hash functions in decentralized systems (Knowledge). Analyze the vulnerabilities and potential attacks on cryptographic hash functions (Analysis). Develop strategies to mitigate risks associated with cryptographic hash functions (Synthesis). Compare and contrast symmetric and asymmetric encryption techniques (Comprehension). Implement secure communication using cryptographic techniques (Application). Analyze the role of hash functions in digital signatures and authentication (Analysis). Evaluate the effectiveness of digital signatures and authentication methods in various scenarios (Evaluation).

In partial fulfillment of the requirements for the nanodegree of

Blockchain Studies (CSC - BSTUD)

(4.5 Clock Hours) (80% Passing Score)

30 Aug 2023

Verification ID: **64ef988a856934779703d1f0**

President
Amando R. Boncales, BA, RBP, MSEd, MA, PhDc.

Comptroller
Julia Ezeji, ABF, HND, (BSc).

Faculty
Joseph Sylvester, BSIT, RBD.
Assistant Professor of Practice

Joseph Sylvester, BSIT, RBD
Program & Faculty Coordinator - Blockchain Tech