# BLKN 215 Applied Cryptography: Private & Public Keys And Digital Signature

**MICROCREDENTIAL AWARDED TO**

# Isiaka Latifat

Specific Learning Objectives:
Define the key concepts and principles of applied cryptography. Differentiate between symmetric and asymmetric encryption techniques. Generate secure public and private key pairs using appropriate algorithms. Explain the process of distributing and managing public and private keys. Implement digital signatures to ensure the authenticity and integrity of data. Verify the validity of digital signatures in various applications. Describe the role of cryptography in cryptocurrencies and blockchain technology. Identify potential security threats and vulnerabilities in cryptographic systems. Apply appropriate mitigation techniques to enhance the security of cryptographic systems. Evaluate the strengths and weaknesses of different cryptographic algorithms. Choose the most suitable public or private key for a specific use case. Assess the trade-offs between security, performance, and usability in cryptographic systems. Discuss the ethical considerations of using cryptography in various contexts. Collaborate effectively with others to design, implement, and evaluate cryptographic solutions. Communicate complex cryptographic concepts clearly and concisely, both orally and in writing.

**In partial fulfillment of the requirements for the nanodegree of**

Blockchain Studies (CSC - BSTUD)

(4.5 Clock Hours) (80% Passing Score)

26 Sep 2023

**Verification ID:** **651340b24f5df43c610ad506**

**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.
Assistant Professor of Practice