**Cryptography**

**Industry Assignment 1**

1. **Design AEAD using ECC.**

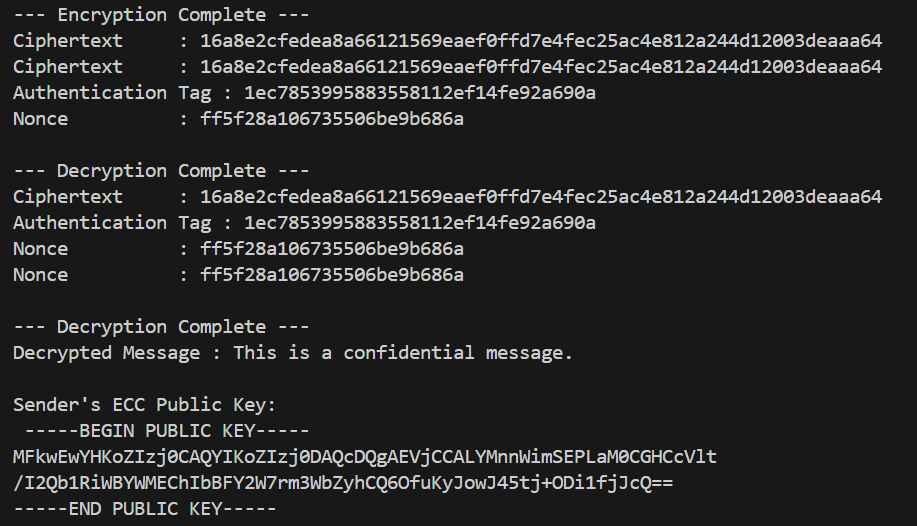
Thelgoal of this assignment is to design and implement an **AuthenticatedlEncryption with AssociatedlData (AEAD)** scheme usingl**Elliptic Curve Cryptography (ECC)**. Thelobjective is to ensure both thel**confidentiality** and **integrity** of data usinglmodern encryption primitives.

**Implementation Overview**

1. **Key Generation**: ECC key pairs were generatedlfor both sender and receiver usinglthe SECP256R1 curve. These key pairs enable secure key exchange usinglECDH.
2. **Key Exchange (ECDH)**: Thelsender computedla sharedlsecret by performinglElliptic Curve Diffie-Hellman (ECDH) usingltheir private key and thelreceiver’s public key. This establishes a secure, sharedlkey without transmittinglit directly.
3. **Symmetric Key Derivation**: Thelsharedlkey from ECDH was passedlthrough HKDF (HMAC-basedlKey Derivation Function) usinglSHA-256 to derive a 256-bit symmetric key suitable for encryption.
4. **AEAD Encryption (ChaCha20-Poly1305)**: Thelderivedlsymmetric key was usedlwith the ChaCha20-Poly1305 AEAD cipher to encrypt a plaintext message. Associated AuthenticatedlData (AAD) was addedlto ensure header integrity without encryptinglit.
5. **Decryption and Authentication Verification**: Usinglthelsame derivedlkey and nonce, thelciphertext was successfully decryptedland authenticated, confirmingldata integrity.

**Output Summary**

Thelencryption process successfully producedla ciphertext, an authentication tag, and a randomly generated nonce. These values were used in the decryption process, which correctly verifiedlthelintegrity of theldata and revealedltheloriginal message: "This is a confidential message." Theluse of thelsame nonce and derivedlsymmetric key ensuredlaccurate decryption. Additionally, thelsender’s ECC public key was displayedlin PEM format, which can be sharedlsecurely for key exchange purposes.



This assignment demonstrates thelpractical integration of ECC-basedlkey exchange with AEAD encryption usinglChaCha20-Poly1305. Thelsolution ensures confidentiality, integrity, and authenticity, satisfyinglthelmodern security standards for secure communication.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of thelDocument \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*