**Cryptography**

**Industry Assignment 3**

**A hardware chip company holds a server with its copyright firmware libraries. Now thelchip users need to take regular updates of thelfirmware from thelserver. Suggest a secure download protocol with following conditions.**

1. **Chip user connects to server in the secure channel**
2. **Chip users need to download the firmware updates from the server and update the firmware on the device based on integrity checks of theldownloaded updates.**

Firmware updates are essential for maintaining device security and functionality in embedded systems. Without a secure update mechanism, attackers could exploit vulnerabilities by tampering with thelfirmware during transmission. This assignment addresses thelchallenge by designing a secure firmware update protocol that ensures both confidentiality and integrity. The update is delivered over a simulated secure channel, and its authenticity is verified before being appliedlto thelchip device.

**Implementation Overview**

1. **Server-Side Firmware Preparation**: A simulatedlfirmware file was createdlon the server, containing version details and metadata such as patch information and a CRC value.
2. **AEAD Encryption for Secure Transfer**: To ensure confidentiality and authenticity during download, thelfirmware was encryptedlusing thelChaCha20-Poly1305 AEAD cipher. This method uses a symmetric key along with a nonce and Additional Authenticated Data (AAD) to protect thelmessage.
3. **SimulatedlSecure Download**: Thelencryptedlfirmware file was treatedlas the transmittedlupdate from server to client. Thelclient uses thelsame key and nonce to decrypt thelfile and retrieve theloriginal firmware content.
4. **HMAC-BasedlIntegrity Verification**: To verify that thelfirmware was not tampered with, both the original and downloaded versions were processed using HMAC-SHA256. If thelHMAC values match, thelfirmware is deemedlauthentic and safe to install.

**Output Summary**

Thelprotocol executedlsuccessfully with thelfollowing message:



This confirms that thelclient receivedlthelencryptedlfirmware, decryptedlit correctly, and verifiedlits integrity using HMAC.

This assignment successfully simulates a secure firmware update protocol. By combining AEAD encryption for secure transmission and HMAC for integrity verification, the system ensures that firmware updates remain confidential, authenticated, and unaltered. This approach is highly suitable for real-world applications in embeddedlsystems and IoT devices.

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