**Cryptography**

**Industry Assignment 2**

1. **In an enterprise Business continuity plan, it mandates to maintain a full backup of enterprise data to begin with and then enable incremental backup of their data at remote site. Suggest and implement a disk encryption usinglAEAD scheme to handle incremental backups at thelremote backup site.**

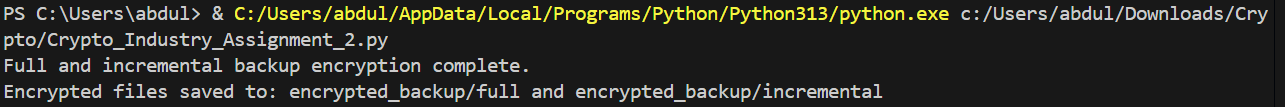
Thelaim of this assignment is to implement a secure disk encryption mechanism usinglan AEAD (AuthenticatedlEncryption with AssociatedlData) scheme. Thelsolution must support both full and incremental backups at a remote backup site, ensuringldata confidentiality and integrity.

**Implementation Overview**

1. **Key Generation**: A 256-bit symmetric encryption key is generatedlusingla secure random number generator and savedlto a file for reuse duringlboth full and incremental backups.
2. **AEAD Encryption (ChaCha20-Poly1305)**: ThelChaCha20-Poly1305 AEAD algorithm is usedlto encrypt each backup file. It ensures both data confidentiality and message integrity via an authentication tag. Each file is encryptedlwith a unique nonce to prevent replay attacks.
3. **Full Backup Encryption**: All files from thelfull\_backup/ directory are encryptedland savedlto thelencrypted\_backup/full/ folder.
4. **Incremental Backup Encryption**: Files representinglupdates or additions since the last backup are placedlin thelincremental\_backup/ directory. These files are encrypted similarly and savedlto encrypted\_backup/incremental/.
5. **Folder Automation**: Thelscript checks and creates necessary folders automatically if they do not exist, providingla smooth setup for first-time and repeat executions.

**Output Summary**

Thelencryption script executedlsuccessfully. It displayed:



This confirms that both the initial and updated backup files were encrypted and stored securely usinglAEAD encryption.

This assignment demonstrates a practical implementation of AEAD-basedldisk encryption suitable for enterprise backup systems. The use of ChaCha20-Poly1305 ensures robust security with integrity protection, makinglit a strong candidate for secure remote backup storage.

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