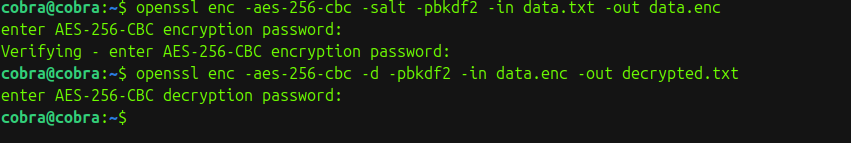
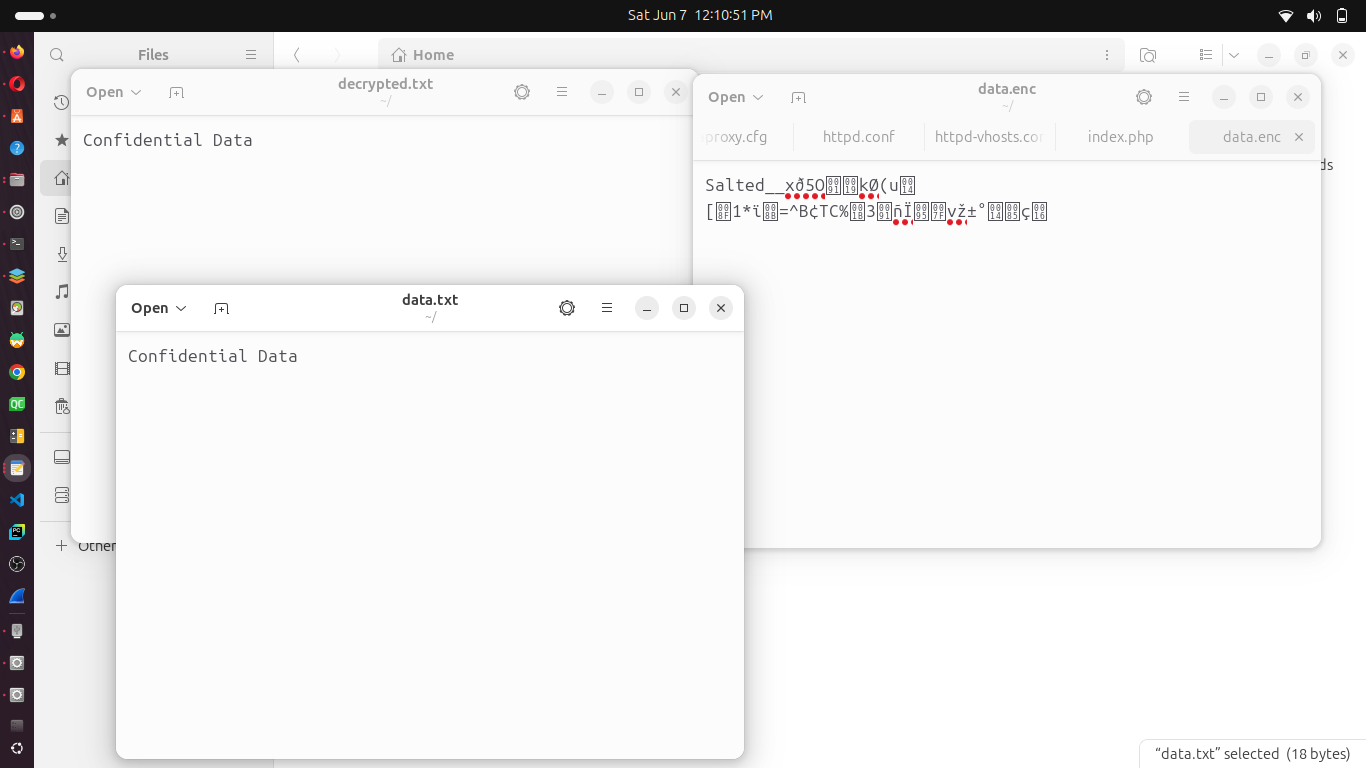
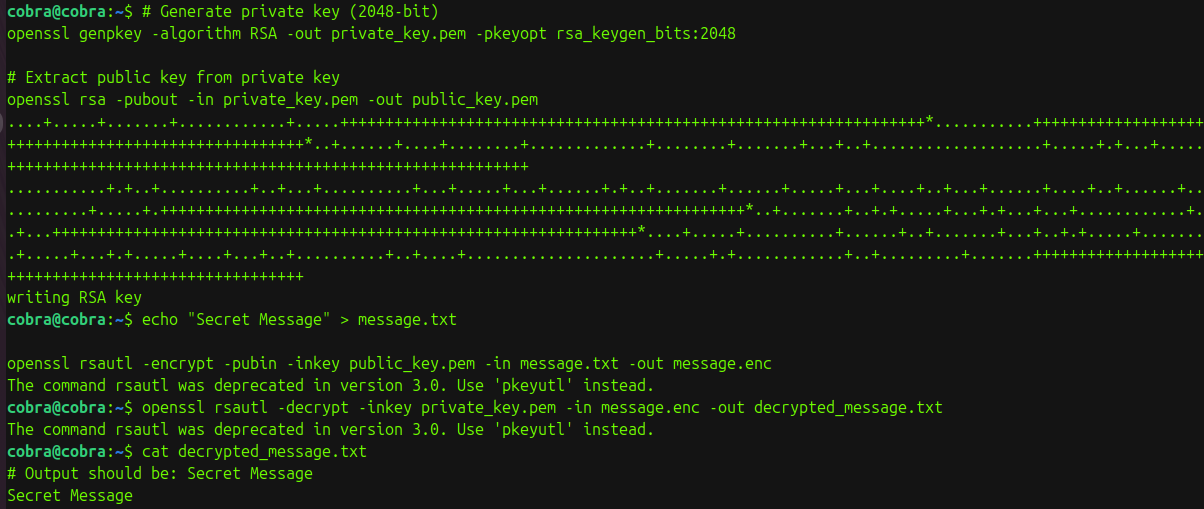
# **Section A: Encryption**

**1. Symmetric Encryption with OpenSSL**

## Objective: Encrypt and decrypt files using AES-256 encryption.

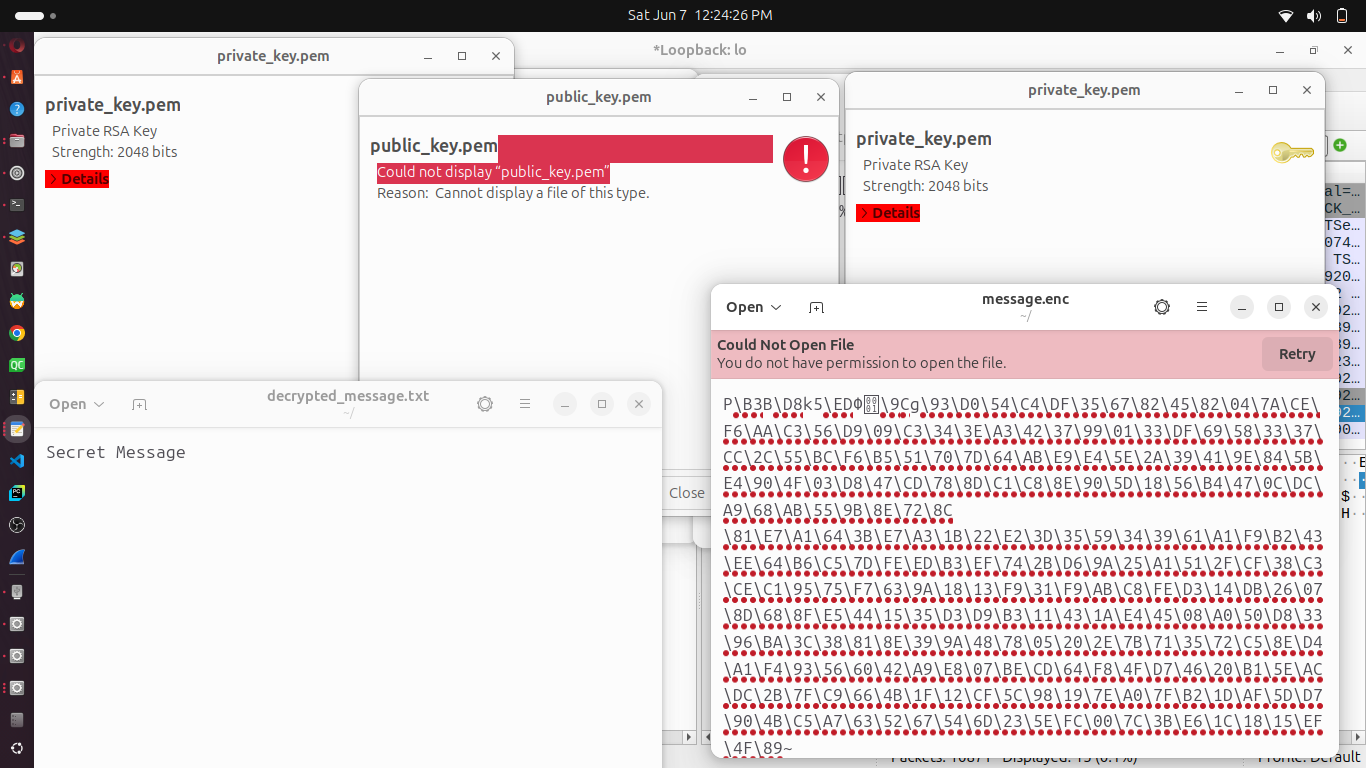


**2. Asymmetric Encryption (Optional: RSA with Python or OpenSSL)**



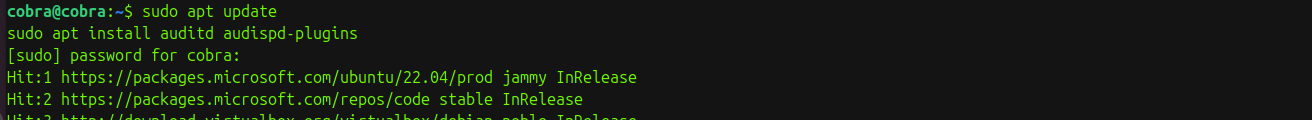
**rsa\_encrypt\_decrypt.py:**

|  |
| --- |
| from cryptography.hazmat.primitives.asymmetric import rsa, padding  from cryptography.hazmat.primitives import serialization, hashes  # Generate RSA private key  private\_key = rsa.generate\_private\_key(public\_exponent=65537, key\_size=2048)  # Get public key from private key  public\_key = private\_key.public\_key()  # Message to encrypt  message = b"Secret Message"  # Encrypt with public key  ciphertext = public\_key.encrypt(  message,  padding.OAEP(  mgf=padding.MGF1(algorithm=hashes.SHA256()),  algorithm=hashes.SHA256(),  label=None )  )print("Encrypted message:", ciphertext)# Decrypt with private key  plaintext = private\_key.decrypt(  ciphertext,  padding.OAEP(  mgf=padding.MGF1(algorithm=hashes.SHA256()),  algorithm=hashes.SHA256(),  label=None))  print("Decrypted message:", plaintext.decode()) |

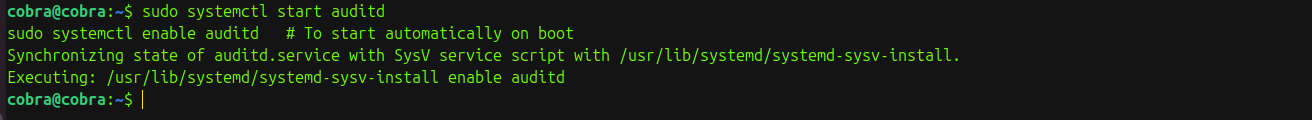


# **Section B: Audit Logging on Linux Using auditd:**

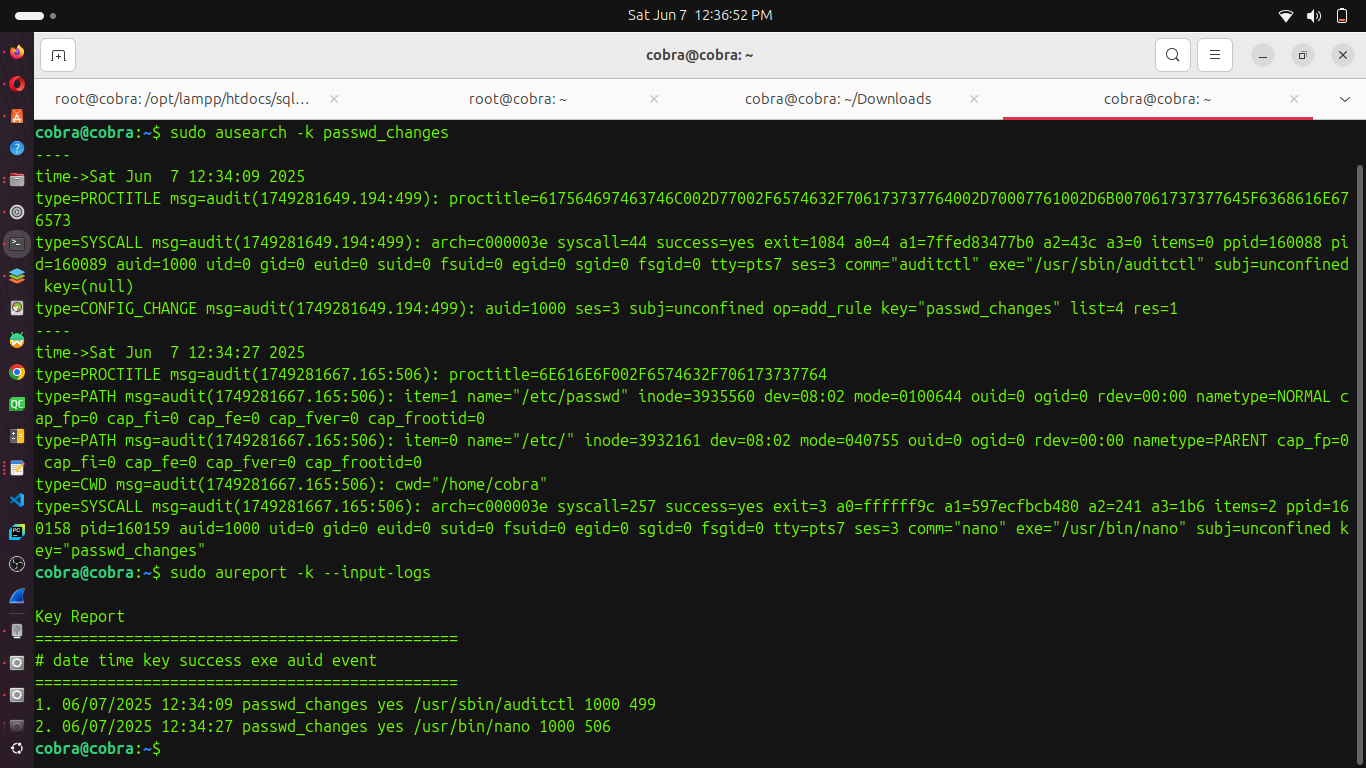
1. **Install auditd:**



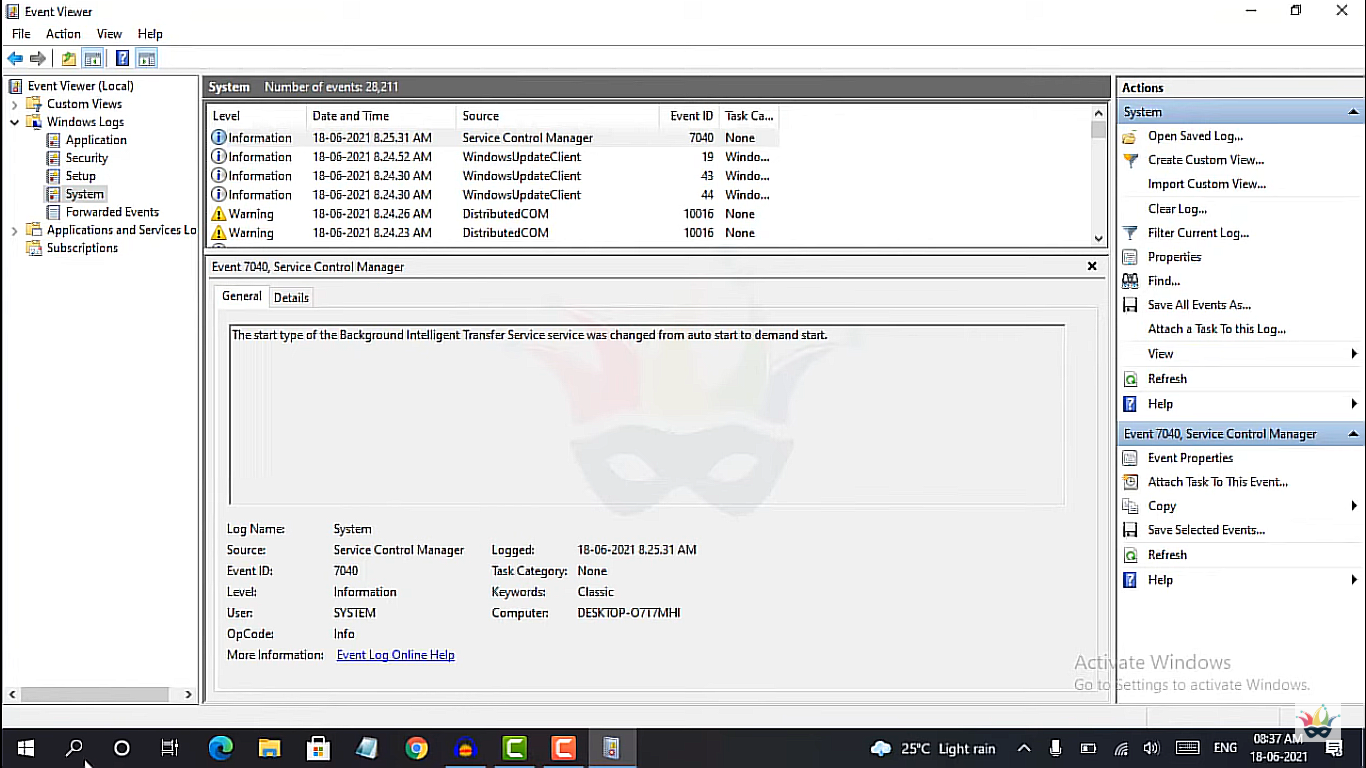
1. **Start the service**:



1. **Audit Logs(Add a rule to monitor ,Trigger an event,Search logs):**



1. **Windows: Viewing Logs in Event Viewer**



# **Section C: Compliance Check (Discussion/Reflection)**

1. - Relevant standards: GDPR, HIPAA, ISO 27001 all mandate encryption and audit logging for sensitive data.
2. - Encryption ensures confidentiality and integrity; audit logs help with incident investigation and accountability.
3. - Best practices: use encryption at rest and in transit, regularly review logs, restrict access to logs, and use tamper-evident logging systems.

**Assessment Questions – Sample Answers**

Q: What are the advantages and limitations of symmetric vs. asymmetric encryption?

A: Symmetric is faster and suitable for large data but requires secure key sharing; asymmetric is secure for key exchange but slower.

Q: What information can audit logs provide in the event of a security breach?

A: They show who accessed what, when, from where, and what actions were taken, helping trace unauthorized activity.

Q: Which compliance standards mandate encryption and logging?

A: GDPR, HIPAA, PCI DSS, and ISO 27001 are examples.

Q: How would you secure audit logs against tampering?

A: By using write-once storage, access controls, log encryption, and centralized logging servers.