PDF Carrier Test Document
Purpose: This is a test document for the PDF Carrier secure file encryption syst
em.
Project: PDF Carrier - Secure File Encryption System
This cryptography course project demonstrates advanced encryption concepts inclu
ding:
■ Hybrid encryption (RSA + AES + ChaCha20)
■ Multi-layer security (defense in depth)
■ Kerckhoffs's Principle (algorithm transparency)
■ Perfect forward secrecy
■ Authenticated encryption with HMAC
Encryption Algorithms Used:
Algorithm
Type
Key Size
Purpose
AES-256-GCM
Symmetric
256 bits
Layer 1 encryption
ChaCha20-Poly1305
Symmetric
256 bits
Layer 2 encryption
RSA-OAEP
Asymmetric
4096 bits
Key encapsulation
HMAC-SHA256
MAC
256 bits
Integrity verification
Security Features:
1. Multi-layer Encryption: Sequential application of 2 encryption algorithms pro
vides defense in depth.
2. Random Algorithm Selection: System randomly chooses which algorithms to use f
or each
encryption.
3. Authenticated Encryption: Both AES-GCM and ChaCha20-Poly1305 provide built-in
authentication.
4. HMAC Verification: Additional integrity check detects any tampering.
5. Perfect Forward Secrecy: Unique keys generated for each encryption session.
6. Kerckhoffs's Principle: Algorithm metadata stored in file header (not secret)
.
How to Test:

1. Encrypt: Upload this PDF to the encryption page
2. Download: Save both the encrypted file and key file
3. Decrypt: Upload both files to the decryption page
4. Verify: Compare the decrypted PDF with this original

Expected Result: The decrypted file should be identical to this original documen
t.

Generated on: 2025-10-26 22:10:47

Document ID: TEST-PDF-20251026221047