Secure File Transfer Protocol - Complete Security Flow

Alice (Sender)	Server	Bob (Recipient)

1) Register and send RSA public key
[RSA-2048]

3) Register and send RSA public key
[RSA-2048]

HMAC: HMAC-SHA256
RSA: SHA256withRSA
AES: AES-256-GCM

2) Success + session token

4) Success + session token

5) Request Bob's public key

Generate AES-256 symmetric
key and HMAC key

6) Bob's verified public key

7) Encrypt symmetric key with
Bob's public key [RSA/OAEP]
Create transfer request

8) Send file transfer request with
encrypted symmetric key + file metadata

9) Forward request with
unique transfer ID

For each received chunk:
1. Verify Alice's signature
with her public key
2. Verify HMAC integrity
3. Check nonce and sequence numbers
4. Decrypt with symmetric key
5. Write to file

10) Accept transfer request

11) Notify of acceptance

12) Forward encrypted chunks with
digital signature and HMAC

13) Forward to Bob

For each file chunk:
1. Generate nonce with
sequence number
2. Encrypt with AES-256-GCM
3. Add HMAC (integrity)
4. Sign with RSA private key

14) Transfer complete notification

Securely erase ephemeral keys
to ensure Perfect Forward Secrecy

Securely erase ephemeral keys
to ensure Perfect Forward Secrecy

15) Forward completion notice