Encrypted File Storage Encrypted File Read

Cipher = EAES (Plaintext, K) K = ERSA (Ksecure, RSAprivate)

Ksecure = ERSA (K, RSApublic) Plaintext = EAES (Cipher, K)

K: AES doc key

Ksecure: Secure AES doc key

RSApublic: RSA public key

RSAprivate: RSA private key

Encrypted File Sharing Encrypted Shared File Reading

K = ERSA (Ksecure, RSAprivate\_A) K = ERSA (Ksharing, RSAprivate\_B)

Ksharing = ERSA (K, RSApublic\_B) Plaintext = EAES (Cipher, K)

K: AES doc key

Ksecure: Secure AES doc key

Ksharing: AES doc key to share

RSApublic\_A: RSA public key of Alice

RSAprivate\_A: RSA private key of Alice

RSApublic\_B: RSA public key of Bob

RSAprivate\_B: RSA private key of Bob