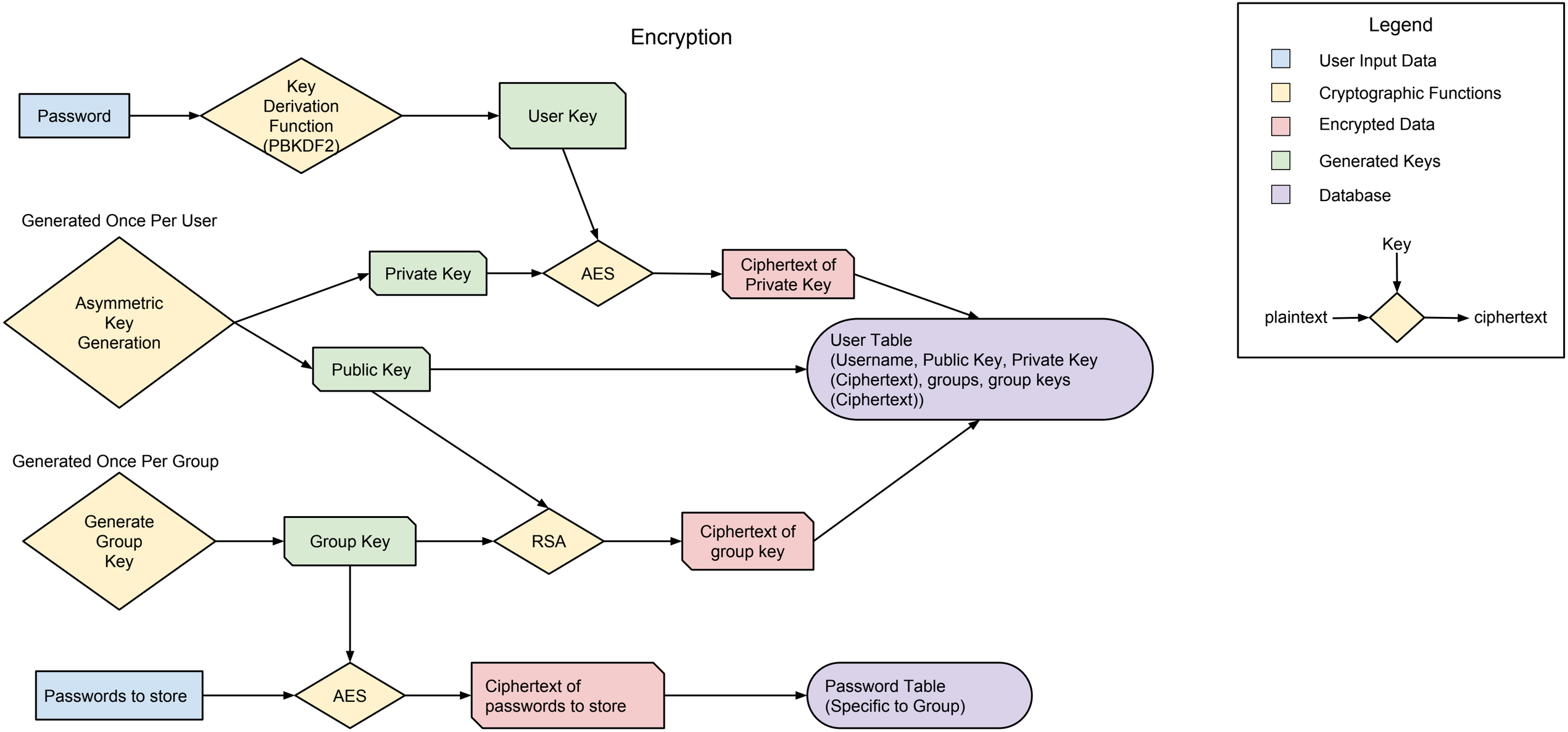
Encryption
Password
Key Derivation Function (PBKDF2)
User Key
Generated Once Per User
Asymmetric Key Generation
Private Key
AES
Ciphertext of Private Key
Public Key
User Table (Username, Public Key, Private Key (Ciphertext), groups, group keys (Ciphertext))
Generated Once Per Group
Generate Group Key
Group Key
RSA
Ciphertext of group key
Passwords to store
AES
Ciphertext of passwords to store
Password Table (Specific to Group)
Legend
User Input Data
Cryptographic Functions
Encrypted Data
Generated Keys
Database
Key
plaintext
ciphertext