

CLAIMS

1. A data security system supporting access to encrypted data by a user, the system comprising:
 - a public computer server being arranged to store the encrypted data as ciphertext;
 - a public database provided on the public computer server, the public computer server being arranged to store: a public decryption key for partially decrypting the ciphertext to yield a partially decrypted ciphertext; an attribute set arranged to regulate use of the public decryption key; and a user identifier to be associated with the user, and wherein the partial decrypting of the ciphertext is only permitted if the user identifier is stored in the public database;
 - a private computer server;
 - a private database provided on the private computer server, the private computer server being arranged to store: the user identifier; and a first private decryption key for partially decrypting the partially decrypted ciphertext to yield an intermediate decrypted ciphertext, and wherein the decrypting of the partially decrypted ciphertext is only permitted if the user identifier is stored in the private database; and
 - user equipment associated with the user, the user equipment arranged to store a second private decryption key for fully decrypting the intermediate decrypted ciphertext to yield unencrypted data.
2. A data security system as claimed in claim 1, further comprising a key generation program being arranged to generate cryptographic keys including the public decryption key, the first private decryption key, and the second private decryption key.
3. A data security system as claimed in claim 2, wherein the key generation program is arranged to simultaneously amend the public decryption key and user identifier in the public database, and to amend the first private decryption key and user identifier in the private database.
4. A data security system as claimed in claim 2 or 3, wherein the key generation program is arranged to simultaneously delete the public decryption key and user

identifier in the public database, and to delete the first private decryption key and user identifier in the private database.

5. A data security system as claimed in any one of claims 1 to 4, wherein the second private decryption key is unable to decrypt the ciphertext or to decrypt the partially decrypted ciphertext.
6. A data security system as claimed in any one of claims 1 to 5, wherein the public computer server is at least one of a public cloud server, an unsecured publically accessible personal computer, and an unsecured publically accessible mobile device.
7. A method for operating a data security system to support access to encrypted data by a user, the user associated a user identifier, the method comprising the steps of:
 - providing the encrypted data as ciphertext on a public computer server;
 - providing a public decryption key, the public decryption key associated with the user identifier;
 - partially decrypting the ciphertext on the public computer server using the public decryption key to yield a partially decrypted ciphertext, wherein the public decryption key is associated with an attribute set arranged to regulate use of the public decryption key, and wherein the step of partially decrypting the ciphertext is only performed if the public decryption key is associated with the user identifier;
 - transmitting the partially decrypted ciphertext to a private computer server;
 - providing a first private decryption key to the private computer server, the first private decryption key associated with the user identifier;
 - partially decrypting the partially decrypted ciphertext on the private computer server using the first private decryption key to yield an intermediate decrypted ciphertext, and wherein the step of partially decrypting the partially decrypted ciphertext is only performed if the first private decryption key is associated with the user identifier; and
 - transmitting the intermediate decrypted ciphertext to user equipment associated with the user, the user equipment having a second private decryption key; and
 - fully decrypting the intermediate decrypted ciphertext by the user using the second private decryption key to yield unencrypted data.

8. A method as claimed in claim 7, wherein the public computer server is a public cloud server, an unsecured publically accessible personal computer or an unsecured publically accessible mobile device.
- 5 9. A method as claimed in claim 7 or 8, wherein the step of partially decrypting the ciphertext to yield a partially decrypted ciphertext, comprises decrypting the ciphertext to a substantial extent whereby each of the subsequent steps of decrypting the partially decrypted ciphertext and decrypting the intermediate decrypted ciphertext, respectively comprise performing only minimal computations.
- 10 10. A method as claimed in claim 9, wherein the minimal computations comprise performing only one exponential operation.
11. A method as claimed in any one of claims 7 to 10, further comprising a step of amending the public decryption key and user identifier on the public computer server, and amending the first private decryption key and user identifier on the private computer server.
- 15 12. A method as claimed in any one of claims 7 to 11, further comprising a step of deleting the public decryption key and user identifier from the public computer server, and deleting the first private decryption key and user identifier from the private computer server.