Claims

1. System for protecting messages, comprising:
    a. A sending and receiving clients
    b. 2 pairs of always-available private and public key (transport pair and user pair)

    Where transport pair is used to generate ephemeral (temporary) transport key and all messages are encrypted by sender with receiver's user pair public key and ephemeral key (respecting this order) and receiver decrypts message with ephemeral key and user private key.
2. The system of claim 1, where user private key is password-protected, and all messages are stored on receiving client until private key is available for decryption.
3. The system of claim 2, where messages are extended with header, which is only encrypted using ephemeral key, and contains information, if the message encrypted should be persisted and if user should be notified about it.
4. The system of claim 3, where unused bits in header are randomized.
5. The system of claim 3, where packets with fixed payload size are extended with meaningless random bits.
6. The system of claim 1, where packets may be delivered using P2P networking or may be stored in RAM of a server, before they are taken from it by receiver, and protocol is extended with message "delivered".
7. Method for protecting messages, comprising:
    a. A sending and receiving clients
    b. 2 pairs of always-available private and public key (transport pair and user pair)

    Where transport pair is used to generate ephemeral (temporary) transport key and all messages are encrypted by sender with receiver's user pair public key and ephemeral key (respecting this order) and receiver decrypts message with ephemeral key and user private key.
8. The method of claim 7, where user private key is password-protected, and all messages are stored on receiving client until private key is available for decryption.

9. The method of claim 8, where messages are extended with header, which is only encrypted using ephemeral key, and contains information, if the message encrypted should be persisted and if user should be notified about it.
10. The method of claim 9, where unused bits in header are randomized.
11. The method of claim 9, where packets with fixed payload size are extended with meaningless random bits.
12. The method of claim 7, where packets may be delivered using P2P networking or may be stored in RAM of a server, before they are taken from it by receiver, and protocol is extended with message “delivered”.