Flow Diagrams

Client Side

Server Side

Sender: Writing

Check Encryption Box → Display Question & Answer Form → Send Button Pressed → Check user input: 1 "To" destinatary, others → Generate Message Random AES Key, Encrypt the message body but don't replace it. → AJAX – JSON send: 1.To Address -E-mail 2.Question 3. Passphrase (canonical) 4.- AES Key →

1.- Generate and Insert into Message Table:
a. Message ID
b. Check User table for PGP Keys (generate if none)
c. Question & Answer (Passphrase)
d. Message AES Key

2.- Cryptography Operations
a. ELGAMAL: AES KEY + Public Key.
b. AES Encrypt Private PGP key with Passphrase.

3.- Return the message id (link)

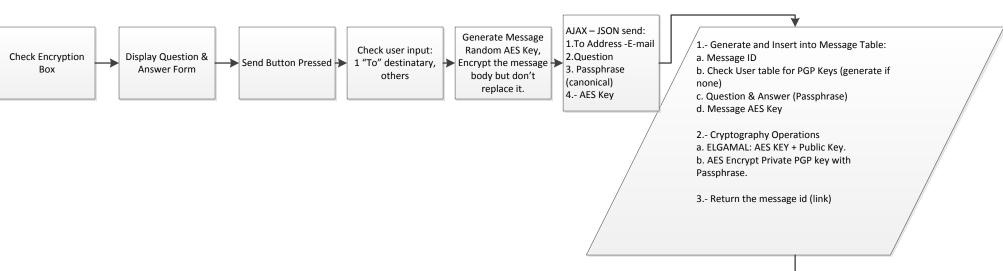Replace the actual body text, with the encrypted stored and add a message like this:

To decrypt this safe message go to:
Www.safegmail.com/w2898hdz
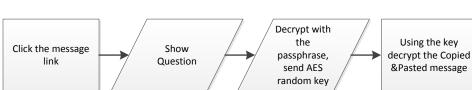You should copy & paste this entire message.
-----Encrypted Message------
luahsdfaishz0281812120012830oijafaj
ludsasaafaishz0pf812120012830oijafaj
luahsdfaishz0281548912001830oiaafaj
luahsdfaishz02818121gszzxX2830oijafaj
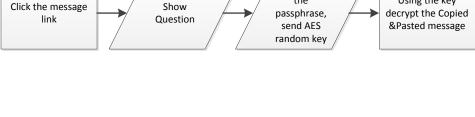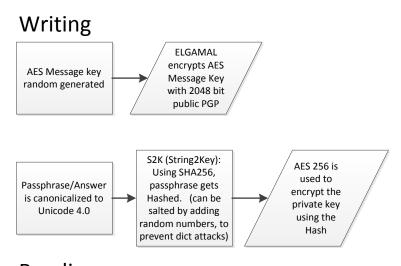---- End of encrypted message-

Receiver: Reading

Click the message link → Show Question → Decrypt with the passphrase, send AES random key → Using the key decrypt the Copied &Pasted message

Writing

AES Message key random generated → ELGAMAL encrypts AES Message Key with 2048 bit public PGP

Passphrase/Answer is canonicalized to Unicode 4.0 → S2K (String2Key): Using SHA256, passphrase gets Hashed. (can be salted by adding random numbers, to prevent dict attacks) → AES 256 is used to encrypt the private key using the Hash

Reading

Reader Passphrase/ Answer is canonicalized to Unicode 4.0 → AES 256 is used to unencrypt the private key → ELGAMAL decrypts AES Message Key with 2048 bit private PGP → Message is obtained and send to browser client