# **Another method (PubKeyAlgo) Normal Login:**

The user accesses the website.

The user is given challenge and nonce.

The user responds with the encrypted challenge + nonce + timestamp and unencrypted username, seed pin, and seed string range (A range within which the actual seed string lies in).

The server using the seed pin, the range, the pin and the pattern to recreate the encryption key which is then used to decrypt the encrypted challenge, nonce and timestamp to further validate the key.

The key is then used for secure communication, or it can be used to send out a new shared key which could be much stronger. The middleman doesn’t have the pin and pattern to recreate the key.

# **Registration Process:**

The user once again re-logins to the site with the pin and pattern. And after logging in, the user has to immediately change the pin and pattern combination for security reasons.

The server using the seed pin, and the range calculates the pin and pattern to decrypt the encrypted challenge to validate the decryption key works, and then sends an email/SMS to the user to re-login to the server. Calculating pin and pattern is very time consuming process.

The user responds with the encrypted challenge + nonce + timestamp and unencrypted username, seed pin, and seed string range (A range within which the actual seed string lies in).

The user is given a challenge string with nonce and timestamp.

The user accesses the website.