This stream cipher is not very secure for a variety of reasons.

1. Use of Random python module. The random module used in python is known to not be cryptographically secure.
2. Because the key eventually repeats itself, long messages are vulnerable to frequency analysis. Ie any message longer than the key can be broken.
3. The cipher is vulnerable to attack if the same key is ever used twice

**Man in the Middle**

To implement a Man In the Middle (MiM) attack, one would need to set up a server to pass messages between the two intended attack victims (ALICE AND BOB).

When ALICE tries to contact BOB to set up the original connection and pass a shared key between them, you (EVE) would intercept her message to BOB, and send back the “SERVER\_HELLO” msg to indicate to her a connection had been made. Because this message contains no identifying information, ALICE would have no way of knowing her messages had been intercepted, and she was in communication with EVE rather than BOB.

At this point in time EVE will start a session with BOB, replaying the “CLIENT\_HELLO” msg ALICE sent earlier, with ALICE’S ID attached, and wait for the “SERVER\_HELLO” msg from BOB

Upon ALICE receiving the “SERVER\_HELLO” msg, she will respond with the CLIENT\_DHEX\_START message, to which EVE will reply SERVER\_DHEX. It is at this point that EVE puts her own key values in to the exchange protocol, rather than BOBS.

Ie Instead of replying with SERVER\_DHEX(g, p,g^b), she will reply with SERVER\_DHEX(g, p, g^e)

At the same time EVE sends CLIENT\_DHEX\_START to BOB, and then exchanges keys with BOB.

ALICE now replys to EVE ( thinking she is replying to BOB), with CLIENT\_DHEX(g^a). ALICE and BOB now have established a key exchange, and they can communicate using encrypted communications. ALICE has no way of knowing she has exchanged keys with EVE instead of BOB.

EVE can now reply to BOB with CLIENT\_DHEX(g^e), and thus EVE and BOB now also have a different, separate set of keys to communicate with.

At this point, both ALICE and BOB have a set a of keys to use communicating with what they think is one another. But EVE has two sets of keys, one for each of them, and can decrypt their messages, and make any altercation she likes, before encrypting the messages with the suitable key and sending it forward.

See diagram next page

