when you take advantage of the dialectical method out of a dialectical record that which you put into it,

once the key has been decrypted the attacker can use the key for all https traffic from the server until a new key is produced.