May 28, 2021 Opener

The GPG secure mailing system uses both RSA and a symmetric cipher. When one installs GPG, the software generates two large (2048 bits or so) numbers, to produce a modulus of 1024 bits. Such a number is too large to be factored easily. The private and public keys are generated from these quantities. The private key is enciphered with a symmetric cipher using a user-supplied pass phrase as the key. To send a message, a symmetric key is randomly generated, and the message enciphered using the symmetric with that key; the key is enciphered using the recipient's public key, and the message and enciphered key are sent.

1. If you needed to compromise a user's GPG private key, what approaches would you take?
2. It's often said that GPG gets you the security of a key with length 2048. Do you agree?