Puzzle of the Day

The PGP secure mailing system uses both RSA and a classical cipher called IDEA. When one installs PGP, the software generates two large (500 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 classical cipher using a user-supplied pass phrase as the key. To send a message, a 64-bit key is randomly generated, and the message enciphered using IDEA 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 PGP private key, what approaches would you take?
2. It's often said that PGP gets you the security of a key with length 1024. Do you agree?