

---

Subject: bazaar: DeEncrypter

Posted by [kohait00](#) on Thu, 05 Aug 2010 19:09:25 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

in bazaar is a DeEncrypter based on AESStream. i hope i am using it right (Mindtraveller could review it). it works so far, but only for files < 200 MB or so (allocator breaks with Out of Memory sometime, if file too big, it's the upp allocator i am using, default case).

so the matter is, it can import keys. and could be extended with a functionality to derive the key from a user password...

but best would be to have a port for RSA asymetrical encryption. then one could encrypt the key and leave it encrypted with the public key, stay with the data somewhere, and 'unlock' (decrypt) it with the password, which would result somehow in the private key.

as far as i remember the major encryption programs do it the same , maybe more fancy

---