How Secure is the Virtual Disk Encryption?

If you use the default settings selected by our engineers, it is practically impossible with current or foreseen computing technology to open the virtual disk without knowing the password. The virtual disk uses the same encryption standard as used by banks and the US Government to protect classified data. The Mac version of the virtual disk uses the built in encryption service in Mac OSX. For Windows and Linux users we have added this capability. Some estimates are that it would take all the computing power currently available thousands of years to crack the encryption.

For Windows and Linux users our default is to apply three successive levels of encryption. The first level uses 256 bit AES(Rijndael) the government and banking standard. The next two levels use algorithms that were finalists in the AES competition.

The National Security Agency (NSA) reviewed all the AES finalists, including Rijndael, and stated that all of them were secure enough for US Government non-classified data. In June 2003, the US Government announced that AES may be used for classified information: "The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths." — [more]

A number of scientists felt that the runnerups actually had stronger methods, but the Rijndael algorithm had the most votes. To be on the safe side we employ all three.

You have the option create your own virtual disk and select the algorithm and strength you prefer.

Because of the strong encryption we can not (and neither should you) export this technology outside the United States.