Subject: Re: Encrypting password in .ini file with aes
Posted by Mindtraveller on Sat, 12 Sep 2015 20:19:57 GMT
View Forum Message <> Reply to Message

Hi Giorgio,

According to Kerckhoffs's principle, you can't leave any kind of key in the source code, because it is almost the same "security" as unencrypted password.
It all usually means you'll have to split into parts the information needed to construct the key. At least one part of it can't be reverse engineered from source code or app data files. The truth is everything you construct programmatically will be reconstructible and reverse engineerable. The honest solution here is to make user remember the key (or part of it) himself. More dirty solution is to make this key generated by a number of algorithms wich will just separate lazy hackers.
And the last note is about the key itself. Please don't make user's password an encryption key. It lowers security level. Please use at least this formula:
key = hash(salt + password)

Thanks
Pavel