

Ruby - Feature #4042

String#crypt should not accepted "\x00" as a salt.

11/11/2010 11:41 AM - phasis68 (Heesob Park)

Status:	Rejected	
Priority:	Normal	
Assignee:		
Target version:	2.0.0	
Description		
=begin I noticed if the salt contains non ascii value, the result is platform dependant. Especially, the salt start with "\x00", the result is empty string on Linux. On Linux, <pre>ruby 1.9.3dev (2010-11-04 trunk 29682) [i686-linux] irb(main):001:0> "foo".crypt("\x00\x00") => "" irb(main):002:0> "foo".crypt("\x00\x01") => "" irb(main):003:0> "foo".crypt("\x01\x00") => "\x01\x01Rqd3mnMHSeY" irb(main):004:0> "foo".crypt("\x01\x01") => "\x01\x01EV3MX6qznTs" irb(main):005:0> "foo".crypt("ab") => "abQ9KY.KfrYrc"</pre> On Windows, <pre>ruby 1.9.3dev (2010-11-09 trunk 29737) [i386-mswin32_90] irb(main):001:0> "foo".crypt("\x00\x00") => "..XXlp7/c78Qo" irb(main):002:0> "foo".crypt("\x00\x01") => ".\x01XXlp7/c78Qo" irb(main):003:0> "foo".crypt("\x01\x00") => "\x01.XXlp7/c78Qo" irb(main):004:0> "foo".crypt("\x01\x01") => "\x01\x01XXlp7/c78Qo" irb(main):005:0> "foo".crypt('ab') => "abQ9KY.KfrYrc"</pre> I think that String#crypt shoud raise ArgumentError if "\x00" used as a salt. =end		
Related issues:		
Related to Ruby - Bug #466: test_str_crypt(TestM17NComb) failed		Closed 08/21/2008

History

#1 - 11/11/2010 11:57 AM - naruse (Yui NARUSE)

- Status changed from Open to Rejected

=begin
String#crypt is the wrapper of crypt(3).
POSIX says crypt(3)'s algorithm is implementation-defined.
<http://www.opengroup.org/onlinepubs/9699919799/functions/crypt.html>
So your expectation, some of String#crypt's behavior is platform-independent, is wrong.

Moreover new applications should use digests.
=end