ECB is broken
11/16/2018 01:55 AM - sevk (kk kk)

Status: Closed
Priority: Normal
Assignee: rhenium (Kazuki Yamaguchi)
Target version: ruby -v: ruby 2.0 2.2 2.3 2.4 2.5 2.6
Backport: 2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: UNKNOWN

Description
#!/usr/bin/env ruby
require 'openssl'

# AES-128 ECB mode test vectors
KEY = ['2b7e151628aed2a6abf7158809cf4f3c'].pack('H*')
PLAINTEXT = ['6bc1bee22e409f96e93d7e117393172a'].pack('H*')
CIPHERTEXT = ['3ad77bb40d7a3660a89ecaf32466ef97'].pack('H*')
cipher = OpenSSL::Cipher::Cipher.new('aes-128-ecb')
cipher.key = KEY
cipher.padding = 0 # Padding is enabled by default o_O
puts "test encrypt : "
cipher.encrypt
ctext = cipher.update(PLAINTEXT) << cipher.final
if ctext == CIPHERTEXT
  puts "OK!"
else
  puts "FAILED!"
end
puts "test decrypt : "
cipher.reset
cipher.decrypt
ptext = cipher.update(CIPHERTEXT) << cipher.final
if ptext == PLAINTEXT
  puts "OK!"
else
  puts "FAILED!"
end

History
#1 - 11/16/2018 01:56 AM - sevk (kk kk)
  test encrypt:
  FAILED!
  test decrypt:
  OK!

#2 - 11/16/2018 02:05 AM - sevk (kk kk)
  Description updated

#3 - 11/16/2018 02:14 AM - sevk (kk kk)
  - ruby -v changed from ruby 2.5.3p105 [2018-10-18 revision 65156] [x86_64-linux] to ruby 2.0 2.2 2.3 2.4 2.5 2.6

#4 - 03/20/2019 05:19 AM - hsbt (Hiroshi SHIBATA)
  - Assignee set to rhenium (Kazuki Yamaguchi)
This is because encrypt is called after key, which goes against the documentation. It is not specific to ECB. This is fixed by https://github.com/ruby/openssl/pull/263, which raises an exception for this broken code instead of silently failing.