Issues

#	Project	Tracker	Status	Subject	Assignee	Updated
7846	Ruby	Feature	Closed	[ext/openssl] Disable TLS/SSL compression by default?		10/08/2015 05:28 AM
6941	Ruby	Bug	Closed	ID_H_TARGET no longer created after running make	nobu (Nobuyoshi Nakada)	10/15/2012 09:01 PM
6928	Ruby	Bug	Closed	SecureRandom.random_bytes: assume zero entropy for seed value	akr (Akira Tanaka)	04/03/2013 12:09 AM
6822	Ruby	Bug	Closed	Race Condition with Fiber and Process	ko1 (Koichi Sasada)	09/26/2012 07:04 AM
6571	Ruby	Bug	Closed	Time.mktime Y2K38 problem on 1.9.3p125 i386-mingw32		05/30/2016 01:02 PM
6567	Ruby	Bug	Closed	Let OpenSSL::PKey::EC follow the general PKey interface		05/21/2016 05:30 AM
6497	Ruby	Feature	Closed	Disabling TLS client-side renegotation	MartinBosslet (Martin Bosslet)	09/04/2012 08:06 AM
6362	Ruby	Feature	Closed	Modular exponentiation/inverse	matz (Yukihiro Matsumoto)	01/04/2021 01:42 AM
6361	Ruby	Feature	Rejected	Bitwise string operations		08/02/2012 11:20 AM
6256	Ruby	Feature	Feedback	Slightly improve ruby_qsort performance	MartinBosslet (Martin Bosslet)	01/10/2019 01:51 PM
6219	Ruby	Feature	Feedback	Return value of Hash#store	matz (Yukihiro Matsumoto)	12/10/2020 08:46 AM
6102	Ruby	Bug	Closed	Crash when calling OpenSSL::Integer#to_der with nil value	MartinBosslet (Martin Bosslet)	03/29/2012 07:53 AM
6065	Ruby	Feature	Closed	Allow Bignum marshalling/unmarshalling from C API	mrkn (Kenta Murata)	07/28/2013 11:19 AM
6047	Ruby	Feature	Closed	read_all: Grow buffer exponentially in generic case		12/02/2022 08:54 AM
5741	Ruby	Feature	Assigned	Secure Erasure of Passwords	matz (Yukihiro Matsumoto)	12/25/2017 06:15 PM
5678	Ruby	Feature	Closed	StringIO#to_str	nobu (Nobuyoshi Nakada)	11/29/2011 04:12 AM
5677	Ruby	Feature	Rejected	IO C API	akr (Akira Tanaka)	05/05/2014 04:03 PM
5633	Ruby	Bug	Closed	Suppress output during Engine cipher test	MartinBosslet (Martin Bosslet)	11/24/2011 10:09 AM
5462	Ruby	Feature	Closed	TLS support for WEBrick::HTTPProxyServer		10/24/2016 07:11 AM
5353	Ruby	Bug	Closed	TLS v1.0 and less - Attack on CBC mode	MartinBosslet (Martin Bosslet)	12/18/2012 11:02 AM
5103	Ruby	Feature	Feedback	[ext/openssl] Object equality for objects based on ASN.1 structures		09/13/2015 03:32 AM
5102	Ruby	Feature	Feedback	[ext/openssl] Purpose of OpenSSL::PKCS12.new / Allow changing the password		09/13/2015 03:33 AM
4961	Ruby	Bug	Closed	[ext/openssl] SSLSession#initialize fails with OpenSSL 0.9.7	MartinBosslet (Martin Bosslet)	09/23/2011 01:51 PM
4923	Ruby	Bug	Closed	[ext/openssl] test_ssl.rb: test_client_auth fails	MartinBosslet (Martin Bosslet)	01/26/2013 06:51 AM
4918	Ruby	Feature	Closed	Make all core tests inherit from Test::Unit::TestCase	MartinBosslet (Martin Bosslet)	06/23/2011 09:04 PM
4885	Ruby	Bug	Closed	[ext/openssl] Use BIO_reset and ERR_get_error in conjuntion	MartinBosslet (Martin Bosslet)	06/22/2011 05:41 PM
4734	Ruby	Bug	Closed	[ext/openssl] DSA#sign error	MartinBosslet (Martin Bosslet)	05/22/2011 07:57 AM
4424	Ruby	Feature	Closed	[ext/openssl] Allow public/private key creation from arbitrary data	MartinBosslet (Martin Bosslet)	06/13/2011 05:47 AM
4423	Ruby	Feature	Closed	[ext/openssl] Allow encryption for PEM-encoding Elliptic Curve private keys	MartinBosslet (Martin Bosslet)	05/12/2011 08:05 AM
4422	Ruby	Bug	Closed	[ext/openssl] Fix DSA public key PEM encoding	MartinBosslet (Martin Bosslet)	05/12/2011 07:27 AM
4421	Ruby	Bug	Closed	[ext/openssl] Fix RSA public key encoding	MartinBosslet (Martin Bosslet)	12/09/2013 10:32 PM

#	Project	Tracker	Status	Subject	Assignee	Updated
4412	Ruby	Feature	Closed	[ext/openssl] Create Digest by OID	MartinBosslet (Martin Bosslet)	06/13/2011 11:37 AM
4374	Ruby	Bug	Closed	[ext/openssl] ASN1.decode wrong for infinite length values	MartinBosslet (Martin Bosslet)	05/23/2011 10:32 AM
4344	Ruby	Bug	Closed	[ext/openssl] BN comparison to nil fails		04/30/2011 10:04 PM
4325	Ruby	Bug	Closed	[ext/openssl] Encoding of subclasses fails when it shouldn't	MartinBosslet (Martin Bosslet)	06/26/2011 10:43 PM
4324	Ruby	Bug	Closed	[ext/openssl] Parsing of incorrect ASN.1 values succeeds		04/30/2011 10:04 PM
4309	Ruby	Feature	Closed	[ext/openssl] ASN1 performance enhancement	MartinBosslet (Martin Bosslet)	05/22/2011 09:03 AM
4183	Ruby	Feature	Closed	[ext/openssl] Timestamp support	rhenium (Kazuki Yamaguchi)	10/21/2021 08:48 PM
4030	Ruby	Bug	Closed	ext/openssl OpenSSL::ASN1::decode / to_der	tenderlovemaking (Aaron Patterson)	04/30/2011 10:04 PM