ProCrypto 1.1.1

Cryptographic Library for Squeak.

This pdf document: https://shorturl.at/kAFLT

An industrial strength Cryptography library, written in Squeak Smalltalk, needs modernizing. To educate and progress, a series of challenges have been formed to teach Squeak Smalltalk, VM building, plugin writing, and Algorithm work in Squeak. This is meant as a fun educational experience, please let us know if you are not having fun.

ProCrypto Instructions

Welcome to Squeak! The newly released version 5.3 of the Squeak vm & image can be found here: http://squeak.org.

The core ProCrypto library packages is in the Cryptography project.
http://www.squeaksource.com/Cryptography.

To load ProCrypto & ProCryptoTests, doIt to this code:

```
[Installer ss
    Project: 'Cryptography';
    Install: 'ProCrypto-1-1-1';
    Install: 'ProCryptoTests-1-1-1'] timeToRun.
```

Crypto Plugins can be found:
https://www.dropbox.com/sh/yhv253rwrhq0q5p/AAB7PKP2KPiGpDnIyule2h_Ia.

Open Monticello Browser (World menu-→open...-→ Monticello Browser), add a HTTP repository to Cryptography and open the repo. Load the Cryptography package of your choice.
Join both the squeak-dev list [1] and the Cryptography list [2].
[1] http://lists.squeakfoundation.org/cgi-bin/mailman/listinfo/squeak-dev .
[2] http://lists.squeakfoundation.org/cgi-bin/mailman/listinfo/cryptography .

Send an announcement email to those lists that you are joining and you are choosing to challenge yourself with one of the seven challenges. Which one?
Any questions, please feel free to ask on the squeak-dev list. There is also a Slack server: https://squeak-slack-sign-in.herokuapp.com.

Have FUN!!

ProCryptoChallenges

1) **CryptoChallengeNumberOne**: AESPlugin.

[Levente Uzonyi] 2)
CryptoChallengeNumberTwo: SHA512 HashFunction

3) **CryptoChallengeNumberThree**: Live animated Spec System monitor with graphs and plugin load information, tinyBenchmarks in a loop, network io, profiling etc..

[Levente Uzonyi] 4)
CryptoChallengeNumberFour: SHA512Plugin.

5) **CryptoChallengeNumberFive**: Signal Encryption/Protocol.

6) **CryptoChallengeNumberSix**: Hack Bluetooth and other connections with AddressInformation, build thunk stacks and get those ParrotsTalking.

7) **CryptoChallengeNumberSeven**: TLS 1.3.

ProCrypto packages and dependencies

	Package	Tests	Size (kb)	Dependencies	Algorithms
	CryptographyCore-rww.5	CryptographyCoreTests-rww.1	18		HMAC, CBC, CFB, CTR, OFB
1	CryptographyASN1-rww.4	CryptographyASN1Tests-rww.1	58		ASN1Module, ASN1InputStream, ASN1OutputStream
2	CryptographyHashing-rww.22	CryptographyHashingTests-rww.1	41	CryptographyCore-rww.5	ND2, MD4, MD5, SHA1, SHA256, SHA512
3	CryptographyRandom-rww.12	CryptographyRandomTests-rww.1	19	CryptographyHashing-rww.22	RandomPool, PrimesFinder, Miller-Rabin, Fortuna, SecureRandom
4	CryptographyCiphers-rww.16	CryptographyCiphersTests-rww.1	67	CryptographyRandom-rww.12 CryptographyASN1-rww.4	ARC2, ARC4, DES, TripleDES, Blowfish, Rijndael
5	CryptographySignatures-rww.16	CryptographySignaturesTests-rww.1	26	CryptographyCiphers-rww.16	DSAKeyPairGenerator, ElGamalKeyPairGenerator, RSAKeyPairGenerator
6	CryptographyKeyExchange-rww.14	CryptographyKeyExchangeTests-rww.1	3	CryptographySignatures-rww.16	Diffie-Hellman
7	CryptographyArchive-rww.17	CryptographyArchiveTests-rww.1	14	CryptographyKeyExchange-rww.14	PBKDF2WithHmacSHA1, PBKDF2WithHmacSHA256, PKCS12
8	CryptographyX509-rww.14	CryptographyX509Tests-rww.1	20	CryptographyArchive-rww.17	X509Certificate, X509CertificateDerReader, DSAPrivateKeyFileReader, RSAPublicKeyFileGenerator, RSAPrivateKeyFileGenerator
9			266		
	Loadable			Unloadable