ProCrypto Cryptographic Library for Squeak.

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 metaverse is available here: http://squeak.org.

The core Cryptography library is:
http://www.squeaksource.com/Cryptography.html.

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 the squeak-dev list. There is also a Slack server: https://squeak-slack-sign-in.herokuapp.com/

Have fun!

ProCryptoChallenges

1) **CryptoChallengeNumberOne**: AESPlugin.

2) **CryptoChallengeNumberTwo**: SHA512 evolve off Register.

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

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	Size (kb)	Dependencies	Algorithms
1	CryptographyCore-rww.5	18		HMAC, CBC, CFB, CTR, OFB
2	CryptographyASN1-rww.4	58		ASN1Module, ASN1InputStream, ASN1OutputStream
3	CryptographyHashing-rww.12	204	CryptographyCore-rww.5	ND2, MD4, MD5, SHA1, SHA256, SHA512
4	CryptographyRandom-rww.9	21	CryptographyHashing-rww.12	RandomPool, PrimesFinder, Miller-Rabin, Fortuna, SecureRandom
5	CryptographyCiphers-rww.13	81	CryptographyRandom-rww.9 CryptographyASN1-rww.4	ARC2, ARC4, DES, TripleDES, Blowfish, Rijndael
6	CryptographySignatures-rww.13	37	CryptographyCiphers-rww.13	DSAKeyPairGenerator, ElGamalKeyPairGenerator, RSAKeyPairGenerator
7	CryptographyKeyExchange-rww.11	5	CryptographySignatures-rww.13	Diffie-Hellman
8	CryptographyArchive-rww.13	17	CryptographyKeyExchange-rww.11	PBKDF2WithHmacSHA1, PBKDF2WithHmacSHA256, PKCS12
9	CryptographyX509-rww.11	34	CryptographyArchive-rww.13	X509Certificate, X509CertificateDerReader, DSAPrivateKeyFileReader, RSAPublicKeyFileGenerator, RSAPrivateKeyFileGenerator
		475		

Loadable Unloadable