Key generator

Generated by Doxygen 1.14.0

Chapter 1

Class Index

1.1 Class List

Here are the classes, structs, unions and interfaces with brief descriptions:

Chapter 2

Class Documentation

2.1 socs.keygen.AESCipher Class Reference

Public Member Functions

- AESCipher (Cipher cipher)
- byte[ ] encrypt (Key key, byte[ ] message, IvParameterSpec iv) throws InvalidKeyException, IllegalBlockSize↩ Exception, BadPaddingException, InvalidAlgorithmParameterException
- byte[ ] decrypt (Key key, byte[ ] message, IvParameterSpec iv) throws InvalidKeyException, IllegalBlockSize↩ Exception, BadPaddingException, InvalidAlgorithmParameterException
- IvParameterSpec generateIV () throws NoSuchAlgorithmException

2.1.1 Detailed Description

Class that provides functionality for encrypting and decrypting messages using AES algorithm, generating IV.

2.1.2 Constructor & Destructor Documentation

2.1.2.1 AESCipher()

```
socs.keygen.AESCipher.AESCipher (
            Cipher cipher)
```

Constructor with dependency injection.

Parameters

	cipher	Instance of Cipher

Returns

Instance of AESCipher

2.1.3 Member Function Documentation

2.1.3.1 decrypt()

```
byte[] socs.keygen.AESCipher.decrypt (
            Key key,
            byte[] message,
            IvParameterSpec iv) throws InvalidKeyException, IllegalBlockSizeException, Bad↩
PaddingException, InvalidAlgorithmParameterException
```

Function that decrypts given message using provided key and IV (in case of mode other than ECB).

Parameters

	key	Key for used for decryption
	message	Message to decrypt
	iv	Initialization vector (can be null if encryption mode is ECB)

Returns

Decrypted message in bytes

Exceptions

	InvalidKeyException	Key is ivalid
	IllegalBlockSizeException	Length of data does not match the block size of the cipher
	BadPaddingException	Data is not padded properly
	InvalidAlgorithmParameterException	Invalid or inappropriate IV

2.1.3.2 encrypt()

```
byte[] socs.keygen.AESCipher.encrypt (
            Key key,
            byte[] message,
            IvParameterSpec iv) throws InvalidKeyException, IllegalBlockSizeException, Bad↩
PaddingException, InvalidAlgorithmParameterException
```

Function that encrypts given message using provided key and IV (in case of mode other than ECB).

Parameters

	key	Key for used for encryption
	message	Message to encrypt
	iv	Initialization vector (can be null if encryption mode is ECB)

Returns

Encrypted message in bytes

Exceptions

InvalidKeyException	Key is ivalid
IllegalBlockSizeException	Length of data does not match the block size of the cipher
BadPaddingException	Data is not padded properly
InvalidAlgorithmParameterException	Invalid or inappropriate IV

2.1.3.3 generateIV()

```
IvParameterSpec socs.keygen.AESCipher.generateIV () throws NoSuchAlgorithmException
```

Function that generates initialization vector using block size from local Cipher instance.

Returns

Initialization vector in bytes

Exceptions

NoSuchAlgorithmException	Particular cryptographic algorithm is requested but is not available

2.2 socs.keygen.FileSaver Class Reference

Public Member Functions

- void save (String directory, String fileName, byte[ ] content) throws IOException

2.2.1 Detailed Description

Class that provides functionality for saving content to given directory.

2.2.2 Member Function Documentation

2.2.2.1 save()

```
void socs.keygen.FileSaver.save (
            String directory,
            String fileName,
            byte[] content) throws IOException
```

Function that saves array of bytes under given name and to given directory. If file with the same name exists, it is overwritten.

Parameters

	directory	Directory to save file in
	fileName	Name of file
	content	Content of file in bytes

Exceptions

	IOException	Directory does not exist

2.3 socs.keygen.HashGenerator Class Reference

Public Member Functions

- HashGenerator (MessageDigest digest)
- byte[] getHash (String message)
- SecretKey getHashAsKey (String message, String algorithm)

2.3.1 Detailed Description

Class that provides functionality for hashing messages and constructing keys from them.

2.3.2 Constructor & Destructor Documentation

2.3.2.1 HashGenerator()

```
socs.keygen.HashGenerator.HashGenerator (
            MessageDigest digest)
```

Constructor with dependency injection.

Parameters

	digest	Instance of MessageDigest

Returns

Instance of HashGenerator

2.3.3 Member Function Documentation

2.3.3.1 getHash()

```
byte[] socs.keygen.HashGenerator.getHash (
            String message)
```

Function that creates hash from given message.

Parameters

	message	Message to hash

Returns

Hashed message in bytes

2.3.3.2 getHashAsKey()

```
SecretKey socs.keygen.HashGenerator.getHashAsKey (
            String message,
            String algorithm)
```

Function that constructs key from message specific for provided algorithm.

Parameters

	message	Message to hash
	algorithm	Algorithm for constructing key from hash

Returns

Key constructed from hashed message

2.4 socs.keygen.KeyGenerator Class Reference

Public Member Functions

- KeyGenerator (KeyPairGenerator generator, int keySize)
- KeyPair generateKeyPair ()
- String getKeyHEX (byte[ ] key)
- String getKeyBase64 (byte[ ] key)

2.4.1 Detailed Description

Class that provides functionality for generating pair of private and public keys, converting keys to HEX or Base64 format.

2.4.2 Constructor & Destructor Documentation

2.4.2.1 KeyGenerator()

```
socs.keygen.KeyGenerator.KeyGenerator (
            KeyPairGenerator generator,
            int keySize)
```

Constructor with dependency injection.

Parameters

	generator	Instance of KeyPairGenerator
	keySize	Size of keys

Returns

Instance of KeyGenerator

2.4.3 Member Function Documentation

2.4.3.1 generateKeyPair()

```
KeyPair socs.keygen.KeyGenerator.generateKeyPair ()
```

Function that generates pair of private and public keys.

Returns

Pair of private and public keys

2.4.3.2 getKeyBase64()

```
String socs.keygen.KeyGenerator.getKeyBase64 (
            byte[] key)
```

Function that formats key to Base64.

Parameters

	key	Key to format in bytes

Returns

Key in Base64 format

2.4.3.3 getKeyHEX()

```
String socs.keygen.KeyGenerator.getKeyHEX (
            byte[] key)
```

Function that formats key to HEX.

Parameters

	key	Key to format in bytes

Returns

Key in HEX format

2.5 socs.keygen.Main Class Reference

Static Public Member Functions

- static void main (String[ ] args)

2.5.1 Detailed Description

Main class.

2.5.2 Member Function Documentation

2.5.2.1 main()

```
void socs.keygen.Main.main (
            String[] args)  [static]
```

Entrypoint of application. Function responsible for dependency injection, creating UI.

Parameters

	args	Command line arguments (not used)