Botan Python Interface Documentation

Jack Lloyd
lloyd@randombit.net

2009/10/10

Contents

1 Ciphers

Botan's Python interface provides a generic interface to any cipher supported by the library. The class `botan.Cipher` takes three arguments, all strings: first, the name of the algorith, second the direction (which can be either "encrypt" or "decrypt"), and lastly, the key to use. For instance

```
encryptor = botan.Cipher("AES-128/EAX", "encrypt", key)
```

creates an object that will encrypt and authenticate messages using the EAX mode of operation using the AES cipher. To use this object, call the **cipher** function with two arguments - the input to encrypt, and the IV to use:

```
ciphertext = encryptor.cipher(input, salt)
```

1.1 Cryptobox

1.2 RNGs

2 RSA