rustlang-play-rsa

Jens Getreu

Version 1.0, 31.7.2015

`rustlang-play-rsa` is an implementation of RSA cryptography in Rust [1: Rust version 1.1].

The algorithms are implemented as described on wikipedia. Please find concrete links and pseudocode samples in the source code. Most of the tests and some helper functions are taken from https://github.com/jsanders/rust-rsa .

WARNING	*Disclaimer* This code is written for pedagogical use only. It does not provide security in real world settings.

Usage

Download, unpack and change into directory `play-rsa` where the file `Cargo.toml` resides.

Build and execute the encryption/decryption binary

```
cargo run --release
```

With my notebook the key generation of the a 1024 bit key takes about a minute. Because all calculations are preformed with the `BigUint` type the key length is mainly limited by the execution time. 1024 bit seems to be the limit for the chosen algorithms and hardware.

Sample output for a key length of 256 bit

```
$ cargo run --release
   Compiling rustplay-rsa v0.3.0 (file:///.../rustlang-play-rsa)
     Running `target/release/play-rsa`

FINDING BIG PRIME NUMBERS

'6333312509593372218021623837860812567377323498385494952977391603923315279051 7 is prime'
is a true statement!


RSA PUBLIC KEY ENCRYPTION

Plaintext:            'Coming tomorrow!'

Generating key pair...
* Private key is: d=0x0143d1750c576bc798e6451886bd2df18e5b3acf3c0126d0df4d2b3d039e322b,
n=0x01e5ba2f928321ab655967a4ca1bc4eafc4fcc2f880b52b62672dee01b2e0825,
* Public key is:  e=0x03,
n=0x01e5ba2f928321ab655967a4ca1bc4eafc4fcc2f880b52b62672dee01b2e0825, key_size=256

Ciphertext:
'0x0160c64347ec4dd78ae8e2a490dd5677bd6be3d970850c34cd285e5de794cd36'

Decrypted ciphertext: 'Coming tomorrow!'
```

Build and run module tests

```
cargo test --release -- --nocapture
```

Output

```
$ cargo test --release -- --nocapture
   Compiling rustlang-play-rsa v0.3.0 (file:///.../rustlang-play-rsa)
     Running target/release/libplayrsa-560318058ffc81cd

running 12 tests
test primes::test_primes::test_extended_gcd ... ok
test primes::test_primes::test_invmod ... ok
test primes::test_primes::test_rewrite ... ok
test primes::test_primes::test_mod_exp ... ok
test primes::test_primes::test_small_primes ... ok
test test_rsa::test_conversions ... ok
test primes::test_primes::test_big_prime ... ok
test primes::test_primes::test_is_prime ... ok
test primes::test_primes::test_rsa_prime ... ok
test test_rsa::test_encrypt_decrypt_five ... ok
test test_rsa::test_encrypt_decrypt_biguint ... ok
test test_rsa::test_encrypt_decrypt_default ... ok

test result: ok. 12 passed; 0 failed; 0 ignored; 0 measured

     Running target/release/playrsa-1abc5a2643e406ef

running 0 tests

test result: ok. 0 passed; 0 failed; 0 ignored; 0 measured
```