40009 ExerciseTypes.PPT2

Haskell Cryptography

Submitters

anb122	Adithya Narayanan

```
Final Tests: Summary for anb122 of j1
PPT 24
-------------------------------------

  Public Tests:
    student-tests/crypto-test/crypto/part 1/gcd:                 8 / 8
    student-tests/crypto-test/crypto/part 1/phi:                 9 / 9
    student-tests/crypto-test/crypto/part 1/modPow:              11 / 11
    student-tests/crypto-test/crypto/part 1/computeCoeffs:       6 / 6
    student-tests/crypto-test/crypto/part 1/inverse:             7 / 7
    student-tests/crypto-test/crypto/part 1/smallestCoPrimeOf:   6 / 6
    student-tests/crypto-test/crypto/part 1/genKeys:             6 / 6
    student-tests/crypto-test/crypto/part 1/rsaEncrypt:          4 / 4
    student-tests/crypto-test/crypto/part 1/rsaDecrypt:          4 / 4
    student-tests/crypto-test/crypto/part 2/toInt:               3 / 3
    student-tests/crypto-test/crypto/part 2/toChar:              3 / 3
    student-tests/crypto-test/crypto/part 2/add:                 3 / 3
    student-tests/crypto-test/crypto/part 2/subtract:            3 / 3
    student-tests/crypto-test/crypto/part 2/ecbEncrypt:          0 / 4
    student-tests/crypto-test/crypto/part 2/ecbDecrypt:          0 / 4
    student-tests/crypto-test/crypto/part 2/cbcEncrypt:          0 / 4
    student-tests/crypto-test/crypto/part 2/cbcDecrypt:          0 / 4
    original-tests/crypto-test/crypto/part 1/gcd:                8 / 8
    original-tests/crypto-test/crypto/part 1/phi:                9 / 9
    original-tests/crypto-test/crypto/part 1/modPow:             11 / 11
    original-tests/crypto-test/crypto/part 1/computeCoeffs:      6 / 6
    original-tests/crypto-test/crypto/part 1/inverse:            7 / 7
    original-tests/crypto-test/crypto/part 1/smallestCoPrimeOf:  6 / 6
    original-tests/crypto-test/crypto/part 1/genKeys:            6 / 6
    original-tests/crypto-test/crypto/part 1/rsaEncrypt:         4 / 4
    original-tests/crypto-test/crypto/part 1/rsaDecrypt:         4 / 4
    original-tests/crypto-test/crypto/part 2/toInt:              3 / 3
    original-tests/crypto-test/crypto/part 2/toChar:             3 / 3
    original-tests/crypto-test/crypto/part 2/add:                3 / 3
    original-tests/crypto-test/crypto/part 2/subtract:           3 / 3
    original-tests/crypto-test/crypto/part 2/ecbEncrypt:         0 / 4
    original-tests/crypto-test/crypto/part 2/ecbDecrypt:         0 / 4
    original-tests/crypto-test/crypto/part 2/cbcEncrypt:         0 / 4
    original-tests/crypto-test/crypto/part 2/cbcDecrypt:         0 / 4 ✓

Git Repo: git@gitlab.doc.ic.ac.uk:lab2324_autumn/haskellcrypto_anb122.git
Commit ID: 54006
```

Tests: 4/4

Correctness: 2/3

Quality : 3/3

9/10

```haskell
module Crypto ( gcd, smallestCoPrimeOf, phi, computeCoeffs, inverse
              , modPow, genKeys, rsaEncrypt, rsaDecrypt, toInt, toChar
              , add, subtract, ecbEncrypt, ecbDecrypt
              , cbcEncrypt, cbcDecrypt ) where

import Data.Char

import Prelude hiding (gcd, subtract)

{-
The advantage of symmetric encryption schemes like AES is that they are efficient
and we can encrypt data of arbitrary size. The problem is how to share the key.
The flaw of the RSA is that it is slow and we can only encrypt data of size lower
than the RSA modulus n, usually around 1024 bits (64 bits for this exercise!).

We usually encrypt messages with a private encryption scheme like AES-256 with
a symmetric key k. The key k of fixed size 256 bits for example is then exchanged
via the aymmetric RSA.
-}

-------------------------------------------------------------------------------
-- PART 1 : asymmetric encryption

-- | Returns the greatest common divisor of its two arguments
gcd :: Int -> Int -> Int
gcd m n
    | n == 0 = m
    | otherwise = gcd n (mod m n)

-- | Euler Totient function
phi :: Int -> Int
phi m = length [x | x <- [1..m], gcd m x == 1]

{-|
Calculates (u, v, d) the gcd (d) and Bezout coefficients (u and v)
such that au + bv = ds
-}
computeCoeffs :: Int -> Int -> (Int, Int)
computeCoeffs a 0 = (1, 0)
computeCoeffs a b = (v', u' - q * v')
    where
        (q, r)    = quotRem a b
        (u', v')  = computeCoeffs b r

-- | Inverse of a modulo m
inverse :: Int -> Int -> Int
inverse a m
    | gcd a m == 1 = u `mod` m
    where
        (u, _)      = computeCoeffs a m
```

should error if they're co-prime.

```haskell
-- | Calculates (a^k mod m)
modPow :: Int -> Int -> Int -> Int
modPow a k 1 = 0
modPow a 0 m = 1
modPow a k m
    | even k   = (modPow ((a * a) `mod` m) (k `div` 2) m) `mod` m
    | odd k    = (a * modPow a (k - 1) m) `mod` m

-- | Returns the smallest integer that is coprime with phi
smallestCoPrimeOf :: Int -> Int
smallestCoPrimeOf 1 = 2
smallestCoPrimeOf a = head [b | b <- [2,3..], gcd a b == 1]

{-|
Generates keys pairs (public, private) = ((e, n), (d, n))
given two "large" distinct primes, p and q
-}
genKeys :: Int -> Int -> ((Int, Int), (Int, Int))
genKeys p q = ((e, n), (d, n))
  where
    n       = p * q
    totient = (p - 1) * (q - 1)
    e       = smallestCoPrimeOf totient
    d       = inverse e totient

-- | This function performs RSA encryption
rsaEncrypt :: Int          -- ^ value to encrypt
           -> (Int, Int)   -- ^ public key
           -> Int
rsaEncrypt x (e, n) = modPow x e n

-- | This function performs RSA decryption
rsaDecrypt :: Int          -- ^ value to decrypt
           -> (Int, Int)   -- ^ public key
           -> Int
rsaDecrypt c (d, n) = modPow c d n

-------------------------------------------------------------------------------
-- PART 2 : symmetric encryption

-- | Returns position of a letter in the alphabet
toInt :: Char -> Int
toInt b = ord b - ord 'a'

-- | Returns the n^th letter
toChar :: Int -> Char
toChar n = chr ((ord 'a') + n)

-- | "adds" two letters
add :: Char -> Char -> Char
add a b
    | (l) > toInt 'z' = toChar (l - toInt 'z' - 1)
    | otherwise       = toChar l
    where
      l               = (toInt a) + (toInt b)
--Please let me know if the formatting for the spacing for the l above is
appropriate or not
```

This works but can do l mod 26 instead.

```haskell
-- | "subtracts" two letters
subtract :: Char -> Char -> Char
subtract a b
    | (l) < toInt 'a' = toChar (l + toInt 'z' + 1)
    | otherwise       = toChar (l)
    where
      l               = (toInt a) - (toInt b)

-- the next functions present
-- 2 modes of operation for block ciphers : ECB and CBC
-- based on a symmetric encryption function e/d such as "add"

-- | ecb (electronic codebook) encryption with block size of a letter
ecbEncrypt :: Char -> [Char] -> [Char]
ecbEncrypt = undefined

-- | ecb (electronic codebook) decryption with a block size of a letter
ecbDecrypt :: Char -> [Char] -> [Char]
ecbDecrypt = undefined

-- | cbc (cipherblock chaining) encryption with block size of a letter
cbcEncrypt :: Char   -- ^ public key
           -> Char   -- ^ initialisation vector `iv`
```

```
            -> [Char] -- ^ message `m`
            -> [Char]
cbcEncrypt = undefined

-- | cbc (cipherblock chaining) decryption with block size of a letter
cbcDecrypt :: Char   -- ^ private key
            -> Char   -- ^ initialisation vector `iv`
            -> [Char] -- ^ message `m`
            -> [Char]
cbcDecrypt = undefined
```

```
-------- Test Output --------
copying crypto.cabal from skeleton
Resolving dependencies...
Build profile: -w ghc-9.2.8 -O1
In order, the following will be built (use -v for more details):
 - crypto-0.1.0.0 (lib) (first run)
 - crypto-0.1.0.0 (test:crypto-test) (first run)
 - crypto-0.1.0.0 (test:crypto-properties) (first run)
Configuring library for crypto-0.1.0.0..
Preprocessing library for crypto-0.1.0.0..
Building library for crypto-0.1.0.0..
[1 of 1] Compiling Crypto           ( src/Crypto.hs, /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/build/Crypto.o, /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/build/Crypto.dyn_o )
Configuring test suite 'crypto-test' for crypto-0.1.0.0..
Configuring test suite 'crypto-properties' for crypto-0.1.0.0..
Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
Preprocessing test suite 'crypto-properties' for crypto-0.1.0.0..
Building test suite 'crypto-test' for crypto-0.1.0.0..
Building test suite 'crypto-properties' for crypto-0.1.0.0..
[1 of 1] Compiling Main             ( test/Props.hs, /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-properties/build/crypto-properties/crypto-properties-tmp/Main.o )
[1 of 1] Compiling Main             ( test/Tests.hs, /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-test/build/crypto-test/crypto-test-tmp/Main.o )
Linking /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-properties/build/crypto-properties/crypto-properties ...
Linking /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-test/build/crypto-test/crypto-test ...
Resolving dependencies...
Build profile: -w ghc-9.2.8 -O1
In order, the following will be built (use -v for more details):
 - crypto-0.1.0.0 (lib) (configuration changed)
 - crypto-0.1.0.0 (test:crypto-test) (configuration changed)
Configuring library for crypto-0.1.0.0..
Preprocessing library for crypto-0.1.0.0..
Building library for crypto-0.1.0.0..
Configuring test suite 'crypto-test' for crypto-0.1.0.0..
Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
Building test suite 'crypto-test' for crypto-0.1.0.0..
Running 1 test suites...
Test suite crypto-test: RUNNING...
crypto
  part 1
    gcd
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
      #7:  OK
      #8:  OK
    phi
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
      #7:  OK
      #8:  OK
      #9:  OK
    modPow
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
      #7:  OK
      #8:  OK
      #9:  OK
      #10: OK
      #11: OK
    computeCoeffs
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
    inverse
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
      #7:  OK
    smallestCoPrimeOf
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
    genKeys
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
    rsaEncrypt
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
    rsaDecrypt
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
  part 2
    toInt
      #1:  OK
      #2:  OK
      #3:  OK
    toChar
      #1:  OK
      #2:  OK
      #3:  OK
    add
      #1:  OK
      #2:  OK
      #3:  OK
    subtract
      #1:  OK
      #2:  OK
      #3:  OK
    ecbEncrypt
      #1:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
      #2:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
      #3:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
      #4:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
    ecbDecrypt
      #1:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
      #2:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
      #3:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
      #4:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
    cbcEncrypt
      #1:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
      #2:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
      #3:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
      #4:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
    cbcDecrypt
      #1:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
      #2:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
      #3:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
      #4:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto

16 out of 89 tests failed (0.01s)

Test suite crypto-test: FAIL
Test suite logged to:
/tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-test/test/crypto-0.1.0.0-crypto-test.log
0 of 1 test suites (0 of 1 test cases) passed.
copying test from skeleton
Resolving dependencies...
Build profile: -w ghc-9.2.8 -O1
In order, the following will be built (use -v for more details):
 - crypto-0.1.0.0 (lib) (configuration changed)
 - crypto-0.1.0.0 (test:crypto-test) (configuration changed)
 - crypto-0.1.0.0 (test:crypto-properties) (dependency rebuilt)
Configuring library for crypto-0.1.0.0..
Preprocessing library for crypto-0.1.0.0..
Building library for crypto-0.1.0.0..
Configuring test suite 'crypto-test' for crypto-0.1.0.0..
Preprocessing test suite 'crypto-properties' for crypto-0.1.0.0..
Building test suite 'crypto-properties' for crypto-0.1.0.0..
[1 of 1] Compiling Main             ( test/Props.hs, /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-properties/build/crypto-properties/crypto-properties-tmp/Main.o )
Linking /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-properties/build/crypto-properties/crypto-properties ...
Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
Building test suite 'crypto-test' for crypto-0.1.0.0..
[1 of 1] Compiling Main             ( test/Tests.hs, /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-test/build/crypto-test/crypto-test-tmp/Main.o )
Linking /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-test/build/crypto-test/crypto-test ...
Resolving dependencies...
Build profile: -w ghc-9.2.8 -O1
In order, the following will be built (use -v for more details):
 - crypto-0.1.0.0 (lib) (configuration changed)
 - crypto-0.1.0.0 (test:crypto-test) (configuration changed)
```

```
Configuring library for crypto-0.1.0.0..
Preprocessing library for crypto-0.1.0.0..
Building library for crypto-0.1.0.0..
Configuring test suite 'crypto-test' for crypto-0.1.0.0..
Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
Building test suite 'crypto-test' for crypto-0.1.0.0..
Running 1 test suites...
Test suite crypto-test: RUNNING...
crypto
  part 1
    gcd
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
      #7:  OK
      #8:  OK
    phi
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
      #7:  OK
      #8:  OK
      #9:  OK
    modPow
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
      #7:  OK
      #8:  OK
      #9:  OK
      #10: OK
      #11: OK
    computeCoeffs
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
    inverse
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
      #7:  OK
    smallestCoPrimeOf
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
    genKeys
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
    rsaEncrypt
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
    rsaDecrypt
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
  part 2
    toInt
      #1:  OK
      #2:  OK
      #3:  OK
    toChar
      #1:  OK
      #2:  OK
      #3:  OK
    add
      #1:  OK
      #2:  OK
      #3:  OK
    subtract
      #1:  OK
      #2:  OK
      #3:  OK
    ecbEncrypt
      #1:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
      #2:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
      #3:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
      #4:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
    ecbDecrypt
      #1:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
      #2:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
      #3:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
      #4:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
    cbcEncrypt
      #1:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
      #2:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
      #3:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
      #4:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
    cbcDecrypt
      #1:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
      #2:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
      #3:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
      #4:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto

16 out of 89 tests failed (0.01s)
```

```

Test suite crypto-test: FAIL
Test suite logged to:
/tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-test/test/crypto-0.1.0.0-crypto-test.log
0 of 1 test suites (0 of 1 test cases) passed.

-------- Test Errors --------
Checking https://repo1.maven.org/maven2/org/scala-lang/scala3-library_3/
Checked https://repo1.maven.org/maven2/org/scala-lang/scala3-library_3/
Downloading https://repo1.maven.org/maven2/org/scala-lang/scala3-library_3/
Downloaded https://repo1.maven.org/maven2/org/scala-lang/scala3-library_3/
Checking https://repo1.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
Checked https://repo1.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
Downloading https://repo1.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
Downloaded https://repo1.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
Warning: The package list for 'hackage.haskell.org' is 45 days old.
Run 'cabal update' to get the latest list of available packages.
Warning: The package list for 'hackage.haskell.org' is 45 days old.
Run 'cabal update' to get the latest list of available packages.
cabal: Tests failed for test:crypto-test from crypto-0.1.0.0.

Warning: The package list for 'hackage.haskell.org' is 45 days old.
Run 'cabal update' to get the latest list of available packages.
Warning: The package list for 'hackage.haskell.org' is 45 days old.
Run 'cabal update' to get the latest list of available packages.
cabal: Tests failed for test:crypto-test from crypto-0.1.0.0.

```

```
Test Preview: Summary for anb122 of j1
PPT 24
--------------------------------------

  Public Tests:
    student-tests/crypto-test/crypto/part 1/gcd:                 8 / 8
    student-tests/crypto-test/crypto/part 1/phi:                 9 / 9
    student-tests/crypto-test/crypto/part 1/modPow:              11 / 11
    student-tests/crypto-test/crypto/part 1/computeCoeffs:       6 / 6
    student-tests/crypto-test/crypto/part 1/inverse:             7 / 7
    student-tests/crypto-test/crypto/part 1/smallestCoPrimeOf:   6 / 6
    student-tests/crypto-test/crypto/part 1/genKeys:             6 / 6
    student-tests/crypto-test/crypto/part 1/rsaEncrypt:          4 / 4
    student-tests/crypto-test/crypto/part 1/rsaDecrypt:          4 / 4
    student-tests/crypto-test/crypto/part 2/toInt:               3 / 3
    student-tests/crypto-test/crypto/part 2/toChar:              3 / 3
    student-tests/crypto-test/crypto/part 2/add:                 3 / 3
    student-tests/crypto-test/crypto/part 2/subtract:            3 / 3
    student-tests/crypto-test/crypto/part 2/ecbEncrypt:          0 / 4
    student-tests/crypto-test/crypto/part 2/ecbDecrypt:          0 / 4
    student-tests/crypto-test/crypto/part 2/cbcEncrypt:          0 / 4
    student-tests/crypto-test/crypto/part 2/cbcDecrypt:          0 / 4
    original-tests/crypto-test/crypto/part 1/gcd:                8 / 8
    original-tests/crypto-test/crypto/part 1/phi:                9 / 9
    original-tests/crypto-test/crypto/part 1/modPow:             11 / 11
    original-tests/crypto-test/crypto/part 1/computeCoeffs:      6 / 6
    original-tests/crypto-test/crypto/part 1/inverse:            7 / 7
    original-tests/crypto-test/crypto/part 1/smallestCoPrimeOf:  6 / 6
    original-tests/crypto-test/crypto/part 1/genKeys:            6 / 6
    original-tests/crypto-test/crypto/part 1/rsaEncrypt:         4 / 4
    original-tests/crypto-test/crypto/part 1/rsaDecrypt:         4 / 4
    original-tests/crypto-test/crypto/part 2/toInt:              3 / 3
    original-tests/crypto-test/crypto/part 2/toChar:             3 / 3
    original-tests/crypto-test/crypto/part 2/add:                3 / 3
    original-tests/crypto-test/crypto/part 2/subtract:           3 / 3
    original-tests/crypto-test/crypto/part 2/ecbEncrypt:         0 / 4
    original-tests/crypto-test/crypto/part 2/ecbDecrypt:         0 / 4
    original-tests/crypto-test/crypto/part 2/cbcEncrypt:         0 / 4
    original-tests/crypto-test/crypto/part 2/cbcDecrypt:         0 / 4

Git Repo: git@gitlab.doc.ic.ac.uk:lab2324_autumn/haskellcrypto_anb122.git
Commit ID: 54006
```

```haskell
module Crypto ( gcd, smallestCoPrimeOf, phi, computeCoeffs, inverse
              , modPow, genKeys, rsaEncrypt, rsaDecrypt, toInt, toChar
              , add, subtract, ecbEncrypt, ecbDecrypt
              , cbcEncrypt, cbcDecrypt ) where

import Data.Char

import Prelude hiding (gcd, subtract)

{-
The advantage of symmetric encryption schemes like AES is that they are efficient
and we can encrypt data of arbitrary size. The problem is how to share the key.
The flaw of the RSA is that it is slow and we can only encrypt data of size lower
than the RSA modulus n, usually around 1024 bits (64 bits for this exercise!).

We usually encrypt messages with a private encryption scheme like AES-256 with
a symmetric key k. The key k of fixed size 256 bits for example is then exchanged
via the aymmetric RSA.
-}

-------------------------------------------------------------------------------
-- PART 1 : asymmetric encryption

-- | Returns the greatest common divisor of its two arguments
gcd :: Int -> Int -> Int
gcd m n
    | n == 0 = m
    | otherwise = gcd n (mod m n)

-- | Euler Totient function
phi :: Int -> Int
phi m = length [x | x <- [1..m], gcd m x == 1]

{-|
Calculates (u, v, d) the gcd (d) and Bezout coefficients (u and v)
such that au + bv = ds
-}
computeCoeffs :: Int -> Int -> (Int, Int)
computeCoeffs a 0 = (1, 0)
computeCoeffs a b = (v', u' - q * v')
    where
        (q, r)    = quotRem a b
        (u', v')  = computeCoeffs b r

-- | Inverse of a modulo m
inverse :: Int -> Int -> Int
inverse a m
    | gcd a m == 1 = u `mod` m
    where
        (u, _)     = computeCoeffs a m

-- | Calculates (a^k mod m)
modPow :: Int -> Int -> Int -> Int
modPow a k 1 = 0
modPow a 0 m = 1
modPow a k m
  | even k   = (modPow ((a * a) `mod` m) (k `div` 2) m) `mod` m
  | odd k    = (a * modPow a (k - 1) m) `mod` m

-- | Returns the smallest integer that is coprime with phi
smallestCoPrimeOf :: Int -> Int
smallestCoPrimeOf 1 = 2
smallestCoPrimeOf a = head [b | b <- [2,3..], gcd a b == 1]

{-|
Generates keys pairs (public, private) = ((e, n), (d, n))
```

```haskell
given two "large" distinct primes, p and q
-}
genKeys :: Int -> Int -> ((Int, Int), (Int, Int))
genKeys p q = ((e, n), (d, n))
  where
    n       = p * q
    totient = (p - 1) * (q - 1)
    e       = smallestCoPrimeOf totient
    d       = inverse e totient

-- | This function performs RSA encryption
rsaEncrypt :: Int        -- ^ value to encrypt
           -> (Int, Int) -- ^ public key
           -> Int
rsaEncrypt x (e, n) = modPow x e n

-- | This function performs RSA decryption
rsaDecrypt :: Int        -- ^ value to decrypt
           -> (Int, Int) -- ^ public key
           -> Int
rsaDecrypt c (d, n) = modPow c d n

-------------------------------------------------------------------------------
-- PART 2 : symmetric encryption

-- | Returns position of a letter in the alphabet
toInt :: Char -> Int
toInt b = ord b - ord 'a'

-- | Returns the n^th letter
toChar :: Int -> Char
toChar n = chr ((ord 'a') + n)

-- | "adds" two letters
add :: Char -> Char -> Char
add a b
    | (l) > toInt 'z' = toChar (l - toInt 'z' - 1)
    | otherwise       = toChar l
    where
      l               = (toInt a) + (toInt b)
--Please let me know if the spacing for the l above is appropriate or not

-- | "subtracts" two letters
subtract :: Char -> Char -> Char
subtract a b
    | (l) < toInt 'a' = toChar (l + toInt 'z' + 1)
    | otherwise       = toChar (l)
    where
      l               = (toInt a) - (toInt b)

-- the next functions present
-- 2 modes of operation for block ciphers : ECB and CBC
-- based on a symmetric encryption function e/d such as "add"

-- | ecb (electronic codebook) encryption with block size of a letter
ecbEncrypt :: Char -> [Char] -> [Char]
ecbEncrypt = undefined

-- | ecb (electronic codebook) decryption with a block size of a letter
ecbDecrypt :: Char -> [Char] -> [Char]
ecbDecrypt = undefined

-- | cbc (cipherblock chaining) encryption with block size of a letter
cbcEncrypt :: Char   -- ^ public key
           -> Char   -- ^ initialisation vector `iv`
           -> [Char] -- ^ message ‘m‘
           -> [Char]
cbcEncrypt = undefined

-- | cbc (cipherblock chaining) decryption with block size of a letter
cbcDecrypt :: Char   -- ^ private key
           -> Char   -- ^ initialisation vector ‘iv‘
           -> [Char] -- ^ message ‘m‘
           -> [Char]
cbcDecrypt = undefined
```

```
-------- Test Output --------
copying crypto.cabal from skeleton
Resolving dependencies...
Build profile: -w ghc-9.2.8 -O1
In order, the following will be built (use -v for more details):
 - crypto-0.1.0.0 (lib) (first run)
 - crypto-0.1.0.0 (test:crypto-test) (first run)
 - crypto-0.1.0.0 (test:crypto-properties) (first run)
Configuring library for crypto-0.1.0.0..
Preprocessing library for crypto-0.1.0.0..
Building library for crypto-0.1.0.0..
[1 of 1] Compiling Crypto           ( src/Crypto.hs, /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/build/Crypto.o, /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/build/Crypto.dyn_o )
Configuring test suite 'crypto-test' for crypto-0.1.0.0..
Configuring test suite 'crypto-properties' for crypto-0.1.0.0..
Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
Preprocessing test suite 'crypto-properties' for crypto-0.1.0.0..
Building test suite 'crypto-test' for crypto-0.1.0.0..
Building test suite 'crypto-properties' for crypto-0.1.0.0..
[1 of 1] Compiling Main             ( test/Props.hs, /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-properties/build/crypto-properties/crypto-properties-tmp/Main.o )
[1 of 1] Compiling Main             ( test/Tests.hs, /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-test/build/crypto-test/crypto-test-tmp/Main.o )
Linking /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-properties/build/crypto-properties/crypto-properties ...
Linking /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-test/build/crypto-test/crypto-test ...
Resolving dependencies...
Build profile: -w ghc-9.2.8 -O1
In order, the following will be built (use -v for more details):
 - crypto-0.1.0.0 (lib) (configuration changed)
 - crypto-0.1.0.0 (test:crypto-test) (configuration changed)
Configuring library for crypto-0.1.0.0..
Preprocessing library for crypto-0.1.0.0..
Building library for crypto-0.1.0.0..
Configuring test suite 'crypto-test' for crypto-0.1.0.0..
Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
Building test suite 'crypto-test' for crypto-0.1.0.0..
Running 1 test suites...
Test suite crypto-test: RUNNING...
crypto
  part 1
    gcd
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
      #7:  OK
      #8:  OK
    phi
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
      #7:  OK
      #8:  OK
      #9:  OK
    modPow
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
      #7:  OK
      #8:  OK
      #9:  OK
      #10: OK
      #11: OK
    computeCoeffs
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
    inverse
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
      #7:  OK
    smallestCoPrimeOf
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
    genKeys
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
    rsaEncrypt
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
    rsaDecrypt
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
  part 2
    toInt
      #1:  OK
      #2:  OK
      #3:  OK
    toChar
      #1:  OK
      #2:  OK
      #3:  OK
    add
      #1:  OK
      #2:  OK
      #3:  OK
    subtract
      #1:  OK
      #2:  OK
      #3:  OK
    ecbEncrypt
      #1:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
      #2:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
      #3:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
      #4:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
    ecbDecrypt
      #1:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
      #2:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
      #3:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
      #4:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
    cbcEncrypt
      #1:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
      #2:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
      #3:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
      #4:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
    cbcDecrypt
      #1:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
      #2:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
      #3:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
      #4:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto

16 out of 89 tests failed (0.01s)

Test suite crypto-test: FAIL
Test suite logged to:
/tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-test/test/crypto-0.1.0.0-crypto-test.log
0 of 1 test suites (0 of 1 test cases) passed.
copying test from skeleton
Resolving dependencies...
Build profile: -w ghc-9.2.8 -O1
In order, the following will be built (use -v for more details):
 - crypto-0.1.0.0 (lib) (configuration changed)
 - crypto-0.1.0.0 (test:crypto-test) (configuration changed)
 - crypto-0.1.0.0 (test:crypto-properties) (dependency rebuilt)
Configuring library for crypto-0.1.0.0..
Preprocessing library for crypto-0.1.0.0..
Building library for crypto-0.1.0.0..
Configuring test suite 'crypto-test' for crypto-0.1.0.0..
Preprocessing test suite 'crypto-properties' for crypto-0.1.0.0..
Building test suite 'crypto-properties' for crypto-0.1.0.0..
[1 of 1] Compiling Main             ( test/Props.hs, ⤦
/tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-properties/build/crypto-properties/crypto-properties-tmp/Main.o )
Linking /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-properties/build/crypto-properties/crypto-properties ...
Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
Building test suite 'crypto-test' for crypto-0.1.0.0..
[1 of 1] Compiling Main             ( test/Tests.hs, ⤦
/tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-test/build/crypto-test/crypto-test-tmp/Main.o )
Linking /tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-test/build/crypto-test/crypto-test ...
Resolving dependencies...
Build profile: -w ghc-9.2.8 -O1
In order, the following will be built (use -v for more details):
 - crypto-0.1.0.0 (lib) (configuration changed)
 - crypto-0.1.0.0 (test:crypto-test) (configuration changed)
```

```
Configuring library for crypto-0.1.0.0..
Preprocessing library for crypto-0.1.0.0..
Building library for crypto-0.1.0.0..
Configuring test suite ’crypto-test’ for crypto-0.1.0.0..
Preprocessing test suite ’crypto-test’ for crypto-0.1.0.0..
Building test suite ’crypto-test’ for crypto-0.1.0.0..
Running 1 test suites...
Test suite crypto-test: RUNNING...
crypto
  part 1
    gcd
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
      #7:  OK
      #8:  OK
    phi
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
      #7:  OK
      #8:  OK
      #9:  OK
    modPow
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
      #7:  OK
      #8:  OK
      #9:  OK
      #10: OK
      #11: OK
    computeCoeffs
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
    inverse
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
      #7:  OK
    smallestCoPrimeOf
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
    genKeys
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
      #5:  OK
      #6:  OK
    rsaEncrypt
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
    rsaDecrypt
      #1:  OK
      #2:  OK
      #3:  OK
      #4:  OK
  part 2
    toInt
      #1:  OK
      #2:  OK
      #3:  OK
    toChar
      #1:  OK
      #2:  OK
      #3:  OK
    add
      #1:  OK
      #2:  OK
      #3:  OK
    subtract
      #1:  OK
      #2:  OK
      #3:  OK
    ecbEncrypt
      #1:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
      #2:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
      #3:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
      #4:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
    ecbDecrypt
      #1:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
      #2:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
      #3:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
      #4:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
    cbcEncrypt
      #1:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
      #2:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
      #3:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
      #4:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
    cbcDecrypt
      #1:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
      #2:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
      #3:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
      #4:  FAIL
        Exception: Prelude.undefined
        CallStack (from HasCallStack):
          error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
          undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto

16 out of 89 tests failed (0.01s)
```

```

Test suite crypto-test: FAIL
Test suite logged to:
/tmp/d20231013-36-df5i7x/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-test/test/crypto-0.1.0.0-crypto-test.log
0 of 1 test suites (0 of 1 test cases) passed.

-------- Test Errors --------
Checking https://repo1.maven.org/maven2/org/scala-lang/scala3-library_3/
Checked https://repo1.maven.org/maven2/org/scala-lang/scala3-library_3/
Downloading https://repo1.maven.org/maven2/org/scala-lang/scala3-library_3/
Downloaded https://repo1.maven.org/maven2/org/scala-lang/scala3-library_3/
Checking https://repo1.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
Checked https://repo1.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
Downloading https://repo1.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
Downloaded https://repo1.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
Warning: The package list for 'hackage.haskell.org' is 45 days old.
Run 'cabal update' to get the latest list of available packages.
Warning: The package list for 'hackage.haskell.org' is 45 days old.
Run 'cabal update' to get the latest list of available packages.
cabal: Tests failed for test:crypto-test from crypto-0.1.0.0.

Warning: The package list for 'hackage.haskell.org' is 45 days old.
Run 'cabal update' to get the latest list of available packages.
Warning: The package list for 'hackage.haskell.org' is 45 days old.
Run 'cabal update' to get the latest list of available packages.
cabal: Tests failed for test:crypto-test from crypto-0.1.0.0.

```