

# 40009 ExerciseTypes.PPT2

## Haskell Cryptography

### Submitters

---

**anb122**

Adithya Narayanan

# Emarking

**Final Tests**

TestSummary.txt: 1/1 Adithya Narayanan - anb122:j1:24

```
1: Final Tests: Summary for anb122 of j1
2: PPT 24
3: -----
4:
5:   Public Tests:
6:     student-tests/crypto-test/crypto/part 1/gcd:      8 / 8
7:     student-tests/crypto-test/crypto/part 1/phi:      9 / 9
8:     student-tests/crypto-test/crypto/part 1/modPow:   11 / 11
9:     student-tests/crypto-test/crypto/part 1/computeCoeffs: 6 / 6
10:    student-tests/crypto-test/crypto/part 1/inverse:  7 / 7
11:    student-tests/crypto-test/crypto/part 1/smallestCoPrimeOf: 6 / 6
12:    student-tests/crypto-test/crypto/part 1/genKeys:   6 / 6
13:    student-tests/crypto-test/crypto/part 1/rsaEncrypt: 4 / 4
14:    student-tests/crypto-test/crypto/part 1/rsaDecrypt: 4 / 4
15:    student-tests/crypto-test/crypto/part 2/toInt:     3 / 3
16:    student-tests/crypto-test/crypto/part 2/toChar:    3 / 3
17:    student-tests/crypto-test/crypto/part 2/add:       3 / 3
18:    student-tests/crypto-test/crypto/part 2/subtract:  3 / 3
19:    student-tests/crypto-test/crypto/part 2/ecbEncrypt: 0 / 4
20:    student-tests/crypto-test/crypto/part 2/ecbDecrypt: 0 / 4
21:    student-tests/crypto-test/crypto/part 2/cbcEncrypt: 0 / 4
22:    student-tests/crypto-test/crypto/part 2/cbcDecrypt: 0 / 4
23:    original-tests/crypto-test/crypto/part 1/gcd:      8 / 8
24:    original-tests/crypto-test/crypto/part 1/phi:      9 / 9
25:    original-tests/crypto-test/crypto/part 1/modPow:   11 / 11
26:    original-tests/crypto-test/crypto/part 1/computeCoeffs: 6 / 6
27:    original-tests/crypto-test/crypto/part 1/inverse:  7 / 7
28:    original-tests/crypto-test/crypto/part 1/smallestCoPrimeOf: 6 / 6
29:    original-tests/crypto-test/crypto/part 1/genKeys:   6 / 6
30:    original-tests/crypto-test/crypto/part 1/rsaEncrypt: 4 / 4
31:    original-tests/crypto-test/crypto/part 1/rsaDecrypt: 4 / 4
32:    original-tests/crypto-test/crypto/part 2/toInt:     3 / 3
33:    original-tests/crypto-test/crypto/part 2/toChar:    3 / 3
34:    original-tests/crypto-test/crypto/part 2/add:       3 / 3
35:    original-tests/crypto-test/crypto/part 2/subtract:  3 / 3
36:    original-tests/crypto-test/crypto/part 2/ecbEncrypt: 0 / 4
37:    original-tests/crypto-test/crypto/part 2/ecbDecrypt: 0 / 4
38:    original-tests/crypto-test/crypto/part 2/cbcEncrypt: 0 / 4
39:    original-tests/crypto-test/crypto/part 2/cbcDecrypt: 0 / 4
40:
41: Git Repo: git@gitlab.doc.ic.ac.uk:lab2324_autumn/haskellcrypto_anb122.git
42: Commit ID: 54006
```

Tests: 4/4  
Correctness: 2/3  
Quality: 3/3

9/10

```

1: module Crypto ( gcd, smallestCoPrimeOf, phi, computeCoeffs, inverse
2:                 , modPow, genKeys, rsaEncrypt, rsaDecrypt, toInt, toChar
3:                 , add, subtract, ecbEncrypt, ecbDecrypt
4:                 , cbcEncrypt, cbcDecrypt ) where
5:
6: import Data.Char
7:
8: import Prelude hiding (gcd, subtract)
9:
10: {-
11: The advantage of symmetric encryption schemes like AES is that they are efficient
12: and we can encrypt data of arbitrary size. The problem is how to share the key.
13: The flaw of the RSA is that it is slow and we can only encrypt data of size lower
14: than the RSA modulus n, usually around 1024 bits (64 bits for this exercise!).
15:
16: We usually encrypt messages with a private encryption scheme like AES-256 with
17: a symmetric key k. The key k of fixed size 256 bits for example is then exchanged
18: via the asymmetric RSA.
19: -}
20:
21: -----
22: -- PART 1 : asymmetric encryption
23:
24: -- | Returns the greatest common divisor of its two arguments
25: gcd :: Int -> Int -> Int
26: gcd m n
27:   | n == 0 = m
28:   | otherwise = gcd n (mod m n)
29:
30: -- | Euler Totient function
31: phi :: Int -> Int
32: phi m = length [x | x <- [1..m], gcd m x == 1]
33:
34: {-
35: Calculates (u, v, d) the gcd (d) and Bezout coefficients (u and v)
36: such that au + bv = ds
37: -}
38: computeCoeffs :: Int -> Int -> (Int, Int)
39: computeCoeffs a 0 = (1, 0)
40: computeCoeffs a b = (v', u' - q * v')
41:   where
42:     (q, r) = quotRem a b
43:     (u', v') = computeCoeffs b r
44:
45: -- | Inverse of a modulo m
46: inverse :: Int -> Int -> Int
47: inverse a m
48:   | gcd a m == 1 = u 'mod' m
49:   where
50:     (u, _) = computeCoeffs a m
51:
52: -- | Calculates (a^k mod m)
53: modPow :: Int -> Int -> Int -> Int
54: modPow a k 1 = 0
55: modPow a 0 m = 1
56: modPow a k m
57:   | even k = (modPow ((a * a) 'mod' m) (k 'div' 2) m) 'mod' m
58:   | odd k  = (a * modPow a (k - 1) m) 'mod' m
59:
60: -- | Returns the smallest integer that is coprime with phi
61: smallestCoPrimeOf :: Int -> Int
62: smallestCoPrimeOf 1 = 2
63: smallestCoPrimeOf a = head [b | b <- [2,3..], gcd a b == 1]
64:
65: {-
66: Generates keys pairs (public, private) = ((e, n), (d, n))

```

should error if they're co-prime.

```

67: given two "large" distinct primes, p and q
68: -}
69: genKeys :: Int -> Int -> ((Int, Int), (Int, Int))
70: genKeys p q = ((e, n), (d, n))
71:   where
72:     n = p * q
73:     totient = (p - 1) * (q - 1)
74:     e = smallestCoPrimeOf totient
75:     d = inverse e totient
76:
77: -- | This function performs RSA encryption
78: rsaEncrypt :: Int -- ^ value to encrypt
79:            -> (Int, Int) -- ^ public key
80:            -> Int
81: rsaEncrypt x (e, n) = modPow x e n
82:
83: -- | This function performs RSA decryption
84: rsaDecrypt :: Int -- ^ value to decrypt
85:            -> (Int, Int) -- ^ public key
86:            -> Int
87: rsaDecrypt c (d, n) = modPow c d n
88:
89: -----
90: -- PART 2 : symmetric encryption
91:
92: -- | Returns position of a letter in the alphabet
93: toInt :: Char -> Int
94: toInt b = ord b - ord 'a'
95:
96: -- | Returns the nth letter
97: toChar :: Int -> Char
98: toChar n = chr ((ord 'a') + n)
99:
100: -- | "adds" two letters
101: add :: Char -> Char -> Char
102: add a b
103:   | (1) > toInt 'z' = toChar (1 - toInt 'z' + 1)
104:   | otherwise = toChar 1
105:   where
106:     1 = (toInt a) + (toInt b)
107: --Please let me know if the formatting for the spacing for the 1 above is ✓
appropriate or not
108:
109: -- | "subtracts" two letters
110: subtract :: Char -> Char -> Char
111: subtract a b
112:   | (1) < toInt 'a' = toChar (1 + toInt 'z' + 1)
113:   | otherwise = toChar (1)
114:   where
115:     1 = (toInt a) - (toInt b)
116:
117: -- the next functions present
118: -- 2 modes of operation for block ciphers : ECB and CBC
119: -- based on a symmetric encryption function e/d such as "add"
120:
121: -- | ecb (electronic codebook) encryption with block size of a letter
122: ecbEncrypt :: Char -> [Char] -> [Char]
123: ecbEncrypt = undefined
124:
125: -- | ecb (electronic codebook) decryption with a block size of a letter
126: ecbDecrypt :: Char -> [Char] -> [Char]
127: ecbDecrypt = undefined
128:
129: -- | cbc (cipherblock chaining) encryption with block size of a letter
130: cbcEncrypt :: Char -- ^ public key
131:            -> Char -- ^ initialisation vector 'iv'

```

This is a bit more but can do 1 mod 26 instead.

**Final Tests**

Crypto.hs: 3/3

Adithya Narayanan - anb122:j1:24

```
132:      -> [Char] -- ^ message 'm'
133:      -> [Char]
134: cbcEncrypt = undefined
135:
136: -- | cbc (cipherblock chaining) decryption with block size of a letter
137: cbcDecrypt :: Char -- ^ private key
138:      -> Char -- ^ initialisation vector 'iv'
139:      -> [Char] -- ^ message 'm'
140:      -> [Char]
141: cbcDecrypt = undefined
```

## Final Tests

testResults.txt: 1/8

Adithya Narayanan - anb122:j1:24

```
1: ----- Test Output -----
2: copying crypto.cabal from skeleton
3: Resolving dependencies...
4: Build profile: -w ghc-9.2.8 -O1
5: In order, the following will be built (use -v for more details):
6: - crypto-0.1.0.0 (lib) (first run)
7: - crypto-0.1.0.0 (test:crypto-test) (first run)
8: - crypto-0.1.0.0 (test:crypto-properties) (first run)
9: Configuring library for crypto-0.1.0.0..
10: Preprocessing library for crypto-0.1.0.0..
11: Building library for crypto-0.1.0.0..
12: [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 )
13: Configuring test suite 'crypto-test' for crypto-0.1.0.0..
14: Configuring test suite 'crypto-properties' for crypto-0.1.0.0..
15: Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
16: Preprocessing test suite 'crypto-properties' for crypto-0.1.0.0..
17: Building test suite 'crypto-test' for crypto-0.1.0.0..
18: Building test suite 'crypto-properties' for crypto-0.1.0.0..
19: [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 )
20: [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 )
21: 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 ...
22: 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 ...
23: Resolving dependencies...
24: Build profile: -w ghc-9.2.8 -O1
25: In order, the following will be built (use -v for more details):
26: - crypto-0.1.0.0 (lib) (configuration changed)
27: - crypto-0.1.0.0 (test:crypto-test) (configuration changed)
28: Configuring library for crypto-0.1.0.0..
29: Preprocessing library for crypto-0.1.0.0..
30: Building library for crypto-0.1.0.0..
31: Configuring test suite 'crypto-test' for crypto-0.1.0.0..
32: Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
33: Building test suite 'crypto-test' for crypto-0.1.0.0..
34: Running 1 test suites...
35: Test suite crypto-test: RUNNING...
36: crypto
37:   part 1
38:     gcd
39:       #1: OK
40:       #2: OK
41:       #3: OK
42:       #4: OK
43:       #5: OK
44:       #6: OK
45:       #7: OK
46:       #8: OK
47:     phi
48:       #1: OK
49:       #2: OK
50:       #3: OK
51:       #4: OK
52:       #5: OK
53:       #6: OK
54:       #7: OK
55:       #8: OK
56:       #9: OK
57:   modPow
58:     #1: OK
```

## Final Tests

testResults.txt: 2/8

Adithya Narayanan - anb122:j1:24

```
59:      #2: OK
60:      #3: OK
61:      #4: OK
62:      #5: OK
63:      #6: OK
64:      #7: OK
65:      #8: OK
66:      #9: OK
67:     #10: OK
68:     #11: OK
69: computeCoeffs
70:      #1: OK
71:      #2: OK
72:      #3: OK
73:      #4: OK
74:      #5: OK
75:      #6: OK
76: inverse
77:      #1: OK
78:      #2: OK
79:      #3: OK
80:      #4: OK
81:      #5: OK
82:      #6: OK
83:      #7: OK
84: smallestCoPrimeOf
85:      #1: OK
86:      #2: OK
87:      #3: OK
88:      #4: OK
89:      #5: OK
90:      #6: OK
91: genKeys
92:      #1: OK
93:      #2: OK
94:      #3: OK
95:      #4: OK
96:      #5: OK
97:      #6: OK
98: rsaEncrypt
99:      #1: OK
100:     #2: OK
101:     #3: OK
102:     #4: OK
103: rsaDecrypt
104:     #1: OK
105:     #2: OK
106:     #3: OK
107:     #4: OK
108: part 2
109: toInt
110:     #1: OK
111:     #2: OK
112:     #3: OK
113: toChar
114:     #1: OK
115:     #2: OK
116:     #3: OK
117: add
118:     #1: OK
119:     #2: OK
```

**Final Tests****testResults.txt: 3/8****Adithya Narayanan - anb122:j1:24**

```
120:      #3: OK
121: subtract
122:      #1: OK
123:      #2: OK
124:      #3: OK
125: ecbEncrypt
126:      #1: FAIL
127:      Exception: Prelude.undefined
128:      CallStack (from HasCallStack):
129:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
130:        undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
131:      #2: FAIL
132:      Exception: Prelude.undefined
133:      CallStack (from HasCallStack):
134:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
135:        undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
136:      #3: FAIL
137:      Exception: Prelude.undefined
138:      CallStack (from HasCallStack):
139:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
140:        undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
141:      #4: FAIL
142:      Exception: Prelude.undefined
143:      CallStack (from HasCallStack):
144:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
145:        undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
146: ecbDecrypt
147:      #1: FAIL
148:      Exception: Prelude.undefined
149:      CallStack (from HasCallStack):
150:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
151:        undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
152:      #2: FAIL
153:      Exception: Prelude.undefined
154:      CallStack (from HasCallStack):
155:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
156:        undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
157:      #3: FAIL
158:      Exception: Prelude.undefined
159:      CallStack (from HasCallStack):
160:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
161:        undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
162:      #4: FAIL
163:      Exception: Prelude.undefined
164:      CallStack (from HasCallStack):
165:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
166:        undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
167: cbcEncrypt
168:      #1: FAIL
169:      Exception: Prelude.undefined
170:      CallStack (from HasCallStack):
171:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
172:        undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
173:      #2: FAIL
174:      Exception: Prelude.undefined
175:      CallStack (from HasCallStack):
176:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
177:        undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
178:      #3: FAIL
179:      Exception: Prelude.undefined
180:      CallStack (from HasCallStack):
```

**Final Tests****testResults.txt: 4/8****Adithya Narayanan - anb122:j1:24**

```
181: error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
182: undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
183: #4: FAIL
184: Exception: Prelude.undefined
185: CallStack (from HasCallStack):
186:   error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
187:   undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
188: chbDecrypt
189: #1: FAIL
190: Exception: Prelude.undefined
191: CallStack (from HasCallStack):
192:   error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
193:   undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
194: #2: FAIL
195: Exception: Prelude.undefined
196: CallStack (from HasCallStack):
197:   error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
198:   undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
199: #3: FAIL
200: Exception: Prelude.undefined
201: CallStack (from HasCallStack):
202:   error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
203:   undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
204: #4: FAIL
205: Exception: Prelude.undefined
206: CallStack (from HasCallStack):
207:   error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
208:   undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
209:
210: 16 out of 89 tests failed (0.01s)
211:
212: Test suite crypto-test: FAIL
213: Test suite logged to:
214: /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
215: 0 of 1 test suites (0 of 1 test cases) passed.
216: copying test from skeleton
217: Resolving dependencies...
218: Build profile: -w ghc-9.2.8 -O1
219: In order, the following will be built (use -v for more details):
220: - crypto-0.1.0.0 (lib) (configuration changed)
221: - crypto-0.1.0.0 (test:crypto-test) (configuration changed)
222: - crypto-0.1.0.0 (test:crypto-properties) (dependency rebuilt)
223: Configuring library for crypto-0.1.0.0..
224: Preprocessing library for crypto-0.1.0.0..
225: Building library for crypto-0.1.0.0..
226: Configuring test suite 'crypto-test' for crypto-0.1.0.0..
227: Preprocessing test suite 'crypto-properties' for crypto-0.1.0.0..
228: Building test suite 'crypto-properties' for crypto-0.1.0.0..
229: [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)
230: 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 ...
231: Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
232: Building test suite 'crypto-test' for crypto-0.1.0.0..
233: [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)
234: 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 ...
235: Resolving dependencies...
236: Build profile: -w ghc-9.2.8 -O1
237: In order, the following will be built (use -v for more details):
238: - crypto-0.1.0.0 (lib) (configuration changed)
239: - crypto-0.1.0.0 (test:crypto-test) (configuration changed)
```



## Final Tests

testResults.txt: 5/8

Adithya Narayanan - anb122:j1:24

```
240: Configuring library for crypto-0.1.0.0..
241: Preprocessing library for crypto-0.1.0.0..
242: Building library for crypto-0.1.0.0..
243: Configuring test suite 'crypto-test' for crypto-0.1.0.0..
244: Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
245: Building test suite 'crypto-test' for crypto-0.1.0.0..
246: Running 1 test suites...
247: Test suite crypto-test: RUNNING...
248: crypto
249:   part 1
250:     gcd
251:       #1: OK
252:       #2: OK
253:       #3: OK
254:       #4: OK
255:       #5: OK
256:       #6: OK
257:       #7: OK
258:       #8: OK
259:     phi
260:       #1: OK
261:       #2: OK
262:       #3: OK
263:       #4: OK
264:       #5: OK
265:       #6: OK
266:       #7: OK
267:       #8: OK
268:       #9: OK
269:     modPow
270:       #1: OK
271:       #2: OK
272:       #3: OK
273:       #4: OK
274:       #5: OK
275:       #6: OK
276:       #7: OK
277:       #8: OK
278:       #9: OK
279:       #10: OK
280:       #11: OK
281:     computeCoeffs
282:       #1: OK
283:       #2: OK
284:       #3: OK
285:       #4: OK
286:       #5: OK
287:       #6: OK
288:     inverse
289:       #1: OK
290:       #2: OK
291:       #3: OK
292:       #4: OK
293:       #5: OK
294:       #6: OK
295:       #7: OK
296:     smallestCoPrimeOf
297:       #1: OK
298:       #2: OK
299:       #3: OK
300:       #4: OK
```

**Final Tests**

testResults.txt: 6/8

Adithya Narayanan - anb122:j1:24

```
301:      #5: OK
302:      #6: OK
303:      genKeys
304:      #1: OK
305:      #2: OK
306:      #3: OK
307:      #4: OK
308:      #5: OK
309:      #6: OK
310:      rsaEncrypt
311:      #1: OK
312:      #2: OK
313:      #3: OK
314:      #4: OK
315:      rsaDecrypt
316:      #1: OK
317:      #2: OK
318:      #3: OK
319:      #4: OK
320:      part 2
321:      toInt
322:      #1: OK
323:      #2: OK
324:      #3: OK
325:      toChar
326:      #1: OK
327:      #2: OK
328:      #3: OK
329:      add
330:      #1: OK
331:      #2: OK
332:      #3: OK
333:      subtract
334:      #1: OK
335:      #2: OK
336:      #3: OK
337:      ecbEncrypt
338:      #1: FAIL
339:          Exception: Prelude.undefined
340:          CallStack (from HasCallStack):
341:            error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
342:            undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
343:      #2: FAIL
344:          Exception: Prelude.undefined
345:          CallStack (from HasCallStack):
346:            error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
347:            undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
348:      #3: FAIL
349:          Exception: Prelude.undefined
350:          CallStack (from HasCallStack):
351:            error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
352:            undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
353:      #4: FAIL
354:          Exception: Prelude.undefined
355:          CallStack (from HasCallStack):
356:            error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
357:            undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
358:      ecbDecrypt
359:      #1: FAIL
360:          Exception: Prelude.undefined
361:          CallStack (from HasCallStack):
```

**Final Tests****testResults.txt: 7/8****Adithya Narayanan - anb122:j1:24**

```
362: error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
363: undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
364: #2: FAIL
365: Exception: Prelude.undefined
366: CallStack (from HasCallStack):
367:   error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
368:   undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
369: #3: FAIL
370: Exception: Prelude.undefined
371: CallStack (from HasCallStack):
372:   error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
373:   undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
374: #4: FAIL
375: Exception: Prelude.undefined
376: CallStack (from HasCallStack):
377:   error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
378:   undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
379: cbcEncrypt
380: #1: FAIL
381: Exception: Prelude.undefined
382: CallStack (from HasCallStack):
383:   error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
384:   undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
385: #2: FAIL
386: Exception: Prelude.undefined
387: CallStack (from HasCallStack):
388:   error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
389:   undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
390: #3: FAIL
391: Exception: Prelude.undefined
392: CallStack (from HasCallStack):
393:   error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
394:   undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
395: #4: FAIL
396: Exception: Prelude.undefined
397: CallStack (from HasCallStack):
398:   error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
399:   undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
400: cbcDecrypt
401: #1: FAIL
402: Exception: Prelude.undefined
403: CallStack (from HasCallStack):
404:   error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
405:   undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
406: #2: FAIL
407: Exception: Prelude.undefined
408: CallStack (from HasCallStack):
409:   error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
410:   undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
411: #3: FAIL
412: Exception: Prelude.undefined
413: CallStack (from HasCallStack):
414:   error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
415:   undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
416: #4: FAIL
417: Exception: Prelude.undefined
418: CallStack (from HasCallStack):
419:   error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
420:   undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
421:
422: 16 out of 89 tests failed (0.01s)
```

**Final Tests****testResults.txt: 8/8****Adithya Narayanan - anb122:j1:24**

```
423:
424: Test suite crypto-test: FAIL
425: Test suite logged to:
426: /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
427: 0 of 1 test suites (0 of 1 test cases) passed.
428:
429: ----- Test Errors -----
430: Checking https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/
431: Checked https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/
432: Downloading https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/
433: Downloaded https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/
434: Checking https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
435: Checked https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
436: Downloading https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
437: Downloaded https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
438: Warning: The package list for 'hackage.haskell.org' is 45 days old.
439: Run 'cabal update' to get the latest list of available packages.
440: Warning: The package list for 'hackage.haskell.org' is 45 days old.
441: Run 'cabal update' to get the latest list of available packages.
442: cabal: Tests failed for test:crypto-test from crypto-0.1.0.0.
443:
444: Warning: The package list for 'hackage.haskell.org' is 45 days old.
445: Run 'cabal update' to get the latest list of available packages.
446: Warning: The package list for 'hackage.haskell.org' is 45 days old.
447: Run 'cabal update' to get the latest list of available packages.
448: cabal: Tests failed for test:crypto-test from crypto-0.1.0.0.
449:
```

**Test Preview****TestSummary.txt: 1/1 Adithya Narayanan - anb122:j1:24**

```
1: Test Preview: Summary for anb122 of j1
2: PPT 24
3: -----
4:
5:   Public Tests:
6:     student-tests/crypto-test/crypto/part 1/gcd:          8 / 8
7:     student-tests/crypto-test/crypto/part 1/phi:          9 / 9
8:     student-tests/crypto-test/crypto/part 1/modPow:       11 / 11
9:     student-tests/crypto-test/crypto/part 1/computeCoeffs: 6 / 6
10:    student-tests/crypto-test/crypto/part 1/inverse:       7 / 7
11:    student-tests/crypto-test/crypto/part 1/smallestCoPrimeOf: 6 / 6
12:    student-tests/crypto-test/crypto/part 1/genKeys:       6 / 6
13:    student-tests/crypto-test/crypto/part 1/rsaEncrypt:    4 / 4
14:    student-tests/crypto-test/crypto/part 1/rsaDecrypt:    4 / 4
15:    student-tests/crypto-test/crypto/part 2/toInt:         3 / 3
16:    student-tests/crypto-test/crypto/part 2/toChar:        3 / 3
17:    student-tests/crypto-test/crypto/part 2/add:           3 / 3
18:    student-tests/crypto-test/crypto/part 2/subtract:      3 / 3
19:    student-tests/crypto-test/crypto/part 2/ecbEncrypt:    0 / 4
20:    student-tests/crypto-test/crypto/part 2/ecbDecrypt:    0 / 4
21:    student-tests/crypto-test/crypto/part 2/cbcEncrypt:    0 / 4
22:    student-tests/crypto-test/crypto/part 2/cbcDecrypt:    0 / 4
23:    original-tests/crypto-test/crypto/part 1/gcd:          8 / 8
24:    original-tests/crypto-test/crypto/part 1/phi:          9 / 9
25:    original-tests/crypto-test/crypto/part 1/modPow:       11 / 11
26:    original-tests/crypto-test/crypto/part 1/computeCoeffs: 6 / 6
27:    original-tests/crypto-test/crypto/part 1/inverse:       7 / 7
28:    original-tests/crypto-test/crypto/part 1/smallestCoPrimeOf: 6 / 6
29:    original-tests/crypto-test/crypto/part 1/genKeys:       6 / 6
30:    original-tests/crypto-test/crypto/part 1/rsaEncrypt:    4 / 4
31:    original-tests/crypto-test/crypto/part 1/rsaDecrypt:    4 / 4
32:    original-tests/crypto-test/crypto/part 2/toInt:         3 / 3
33:    original-tests/crypto-test/crypto/part 2/toChar:        3 / 3
34:    original-tests/crypto-test/crypto/part 2/add:           3 / 3
35:    original-tests/crypto-test/crypto/part 2/subtract:      3 / 3
36:    original-tests/crypto-test/crypto/part 2/ecbEncrypt:    0 / 4
37:    original-tests/crypto-test/crypto/part 2/ecbDecrypt:    0 / 4
38:    original-tests/crypto-test/crypto/part 2/cbcEncrypt:    0 / 4
39:    original-tests/crypto-test/crypto/part 2/cbcDecrypt:    0 / 4
40:
41: Git Repo: git@gitlab.doc.ic.ac.uk:lab2324_autumn/haskellcrypto_anb122.git
42: Commit ID: 54006
```

```

1: module Crypto ( gcd, smallestCoPrimeOf, phi, computeCoeffs, inverse
2:                 , modPow, genKeys, rsaEncrypt, rsaDecrypt, toInt, toChar
3:                 , add, subtract, ecbEncrypt, ecbDecrypt
4:                 , cbcEncrypt, cbcDecrypt ) where
5:
6: import Data.Char
7:
8: import Prelude hiding (gcd, subtract)
9:
10: {-
11: The advantage of symmetric encryption schemes like AES is that they are efficient
12: and we can encrypt data of arbitrary size. The problem is how to share the key.
13: The flaw of the RSA is that it is slow and we can only encrypt data of size lower
14: than the RSA modulus n, usually around 1024 bits (64 bits for this exercise!).
15:
16: We usually encrypt messages with a private encryption scheme like AES-256 with
17: a symmetric key k. The key k of fixed size 256 bits for example is then exchanged
18: via the asymmetric RSA.
19: -}
20:
21: -----
22: -- PART 1 : asymmetric encryption
23:
24: -- | Returns the greatest common divisor of its two arguments
25: gcd :: Int -> Int -> Int
26: gcd m n
27:   | n == 0 = m
28:   | otherwise = gcd n (mod m n)
29:
30: -- | Euler Totient function
31: phi :: Int -> Int
32: phi m = length [x | x <- [1..m], gcd m x == 1]
33:
34: {-|
35: Calculates (u, v, d) the gcd (d) and Bezout coefficients (u and v)
36: such that au + bv = ds
37: -}
38: computeCoeffs :: Int -> Int -> (Int, Int)
39: computeCoeffs a 0 = (1, 0)
40: computeCoeffs a b = (v', u' - q * v')
41:   where
42:     (q, r) = quotRem a b
43:     (u', v') = computeCoeffs b r
44:
45: -- | Inverse of a modulo m
46: inverse :: Int -> Int -> Int
47: inverse a m
48:   | gcd a m == 1 = u 'mod' m
49:   where
50:     (u, _) = computeCoeffs a m
51:
52: -- | Calculates (a^k mod m)
53: modPow :: Int -> Int -> Int -> Int
54: modPow a k 1 = 0
55: modPow a 0 m = 1
56: modPow a k m
57:   | even k = (modPow ((a * a) 'mod' m) (k `div` 2) m) 'mod' m
58:   | odd k  = (a * modPow a (k - 1) m) 'mod' m
59:
60: -- | Returns the smallest integer that is coprime with phi
61: smallestCoPrimeOf :: Int -> Int
62: smallestCoPrimeOf 1 = 2
63: smallestCoPrimeOf a = head [b | b <- [2,3..], gcd a b == 1]
64:
65: {-|
66: Generates keys pairs (public, private) = ((e, n), (d, n))

```

```

67: given two "large" distinct primes, p and q
68: -}
69: genKeys :: Int -> Int -> ((Int, Int), (Int, Int))
70: genKeys p q = ((e, n), (d, n))
71:   where
72:     n = p * q
73:     totient = (p - 1) * (q - 1)
74:     e = smallestCoPrimeOf totient
75:     d = inverse e totient
76:
77: -- | This function performs RSA encryption
78: rsaEncrypt :: Int -- ^ value to encrypt
79:            -> (Int, Int) -- ^ public key
80:            -> Int
81: rsaEncrypt x (e, n) = modPow x e n
82:
83: -- | This function performs RSA decryption
84: rsaDecrypt :: Int -- ^ value to decrypt
85:            -> (Int, Int) -- ^ public key
86:            -> Int
87: rsaDecrypt c (d, n) = modPow c d n
88:
89: -----
90: -- PART 2 : symmetric encryption
91:
92: -- | Returns position of a letter in the alphabet
93: toInt :: Char -> Int
94: toInt b = ord b - ord 'a'
95:
96: -- | Returns the n^th letter
97: toChar :: Int -> Char
98: toChar n = chr ((ord 'a') + n)
99:
100: -- | "adds" two letters
101: add :: Char -> Char -> Char
102: add a b
103:   | (l) > toInt 'z' = toChar (l - toInt 'z' - 1)
104:   | otherwise       = toChar l
105:   where
106:     l = (toInt a) + (toInt b)
107: --Please let me know if the formatting for the spacing for the l above is ✓
appropriate or not
108:
109: -- | "subtracts" two letters
110: subtract :: Char -> Char -> Char
111: subtract a b
112:   | (l) < toInt 'a' = toChar (l + toInt 'z' + 1)
113:   | otherwise       = toChar (l)
114:   where
115:     l = (toInt a) - (toInt b)
116:
117: -- the next functions present
118: -- 2 modes of operation for block ciphers : ECB and CBC
119: -- based on a symmetric encryption function e/d such as "add"
120:
121: -- | ecb (electronic codebook) encryption with block size of a letter
122: ecbEncrypt :: Char -> [Char] -> [Char]
123: ecbEncrypt = undefined
124:
125: -- | ecb (electronic codebook) decryption with a block size of a letter
126: ecbDecrypt :: Char -> [Char] -> [Char]
127: ecbDecrypt = undefined
128:
129: -- | cbc (cipherblock chaining) encryption with block size of a letter
130: cbcEncrypt :: Char -- ^ public key
131:            -> Char -- ^ initialisation vector 'iv'

```

```
132:      -> [Char] -- ^ message 'm'
133:      -> [Char]
134: cbcEncrypt = undefined
135:
136: -- | cbc (cipherblock chaining) decryption with block size of a letter
137: cbcDecrypt :: Char -- ^ private key
138:      -> Char -- ^ initialisation vector 'iv'
139:      -> [Char] -- ^ message 'm'
140:      -> [Char]
141: cbcDecrypt = undefined
```

**Test Preview****testResults.txt: 1/8****Adithya Narayanan - anb122:j1:24**

```
1: ----- Test Output -----
2: copying crypto.cabal from skeleton
3: Resolving dependencies...
4: Build profile: -w ghc-9.2.8 -O1
5: In order, the following will be built (use -v for more details):
6: - crypto-0.1.0.0 (lib) (first run)
7: - crypto-0.1.0.0 (test:crypto-test) (first run)
8: - crypto-0.1.0.0 (test:crypto-properties) (first run)
9: Configuring library for crypto-0.1.0.0..
10: Preprocessing library for crypto-0.1.0.0..
11: Building library for crypto-0.1.0.0..
12: [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 )
13: Configuring test suite 'crypto-test' for crypto-0.1.0.0..
14: Configuring test suite 'crypto-properties' for crypto-0.1.0.0..
15: Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
16: Preprocessing test suite 'crypto-properties' for crypto-0.1.0.0..
17: Building test suite 'crypto-test' for crypto-0.1.0.0..
18: Building test suite 'crypto-properties' for crypto-0.1.0.0..
19: [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 )
20: [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 )
21: 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 ...
22: 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 ...
23: Resolving dependencies...
24: Build profile: -w ghc-9.2.8 -O1
25: In order, the following will be built (use -v for more details):
26: - crypto-0.1.0.0 (lib) (configuration changed)
27: - crypto-0.1.0.0 (test:crypto-test) (configuration changed)
28: Configuring library for crypto-0.1.0.0..
29: Preprocessing library for crypto-0.1.0.0..
30: Building library for crypto-0.1.0.0..
31: Configuring test suite 'crypto-test' for crypto-0.1.0.0..
32: Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
33: Building test suite 'crypto-test' for crypto-0.1.0.0..
34: Running 1 test suites...
35: Test suite crypto-test: RUNNING...
36: crypto
37:   part 1
38:     gcd
39:       #1: OK
40:       #2: OK
41:       #3: OK
42:       #4: OK
43:       #5: OK
44:       #6: OK
45:       #7: OK
46:       #8: OK
47:     phi
48:       #1: OK
49:       #2: OK
50:       #3: OK
51:       #4: OK
52:       #5: OK
53:       #6: OK
54:       #7: OK
55:       #8: OK
56:       #9: OK
57:   modPow
58:     #1: OK
```



**Test Preview**

testResults.txt: 2/8

Adithya Narayanan - anb122:j1:24

```
59:      #2: OK
60:      #3: OK
61:      #4: OK
62:      #5: OK
63:      #6: OK
64:      #7: OK
65:      #8: OK
66:      #9: OK
67:     #10: OK
68:     #11: OK
69: computeCoeffs
70:      #1: OK
71:      #2: OK
72:      #3: OK
73:      #4: OK
74:      #5: OK
75:      #6: OK
76: inverse
77:      #1: OK
78:      #2: OK
79:      #3: OK
80:      #4: OK
81:      #5: OK
82:      #6: OK
83:      #7: OK
84: smallestCoPrimeOf
85:      #1: OK
86:      #2: OK
87:      #3: OK
88:      #4: OK
89:      #5: OK
90:      #6: OK
91: genKeys
92:      #1: OK
93:      #2: OK
94:      #3: OK
95:      #4: OK
96:      #5: OK
97:      #6: OK
98: rsaEncrypt
99:      #1: OK
100:     #2: OK
101:     #3: OK
102:     #4: OK
103: rsaDecrypt
104:     #1: OK
105:     #2: OK
106:     #3: OK
107:     #4: OK
108: part 2
109: toInt
110:     #1: OK
111:     #2: OK
112:     #3: OK
113: toChar
114:     #1: OK
115:     #2: OK
116:     #3: OK
117: add
118:     #1: OK
119:     #2: OK
```

**Test Preview****testResults.txt: 3/8****Adithya Narayanan - anb122:j1:24**

```
120:      #3: OK
121: subtract
122:      #1: OK
123:      #2: OK
124:      #3: OK
125: ecbEncrypt
126:      #1: FAIL
127:      Exception: Prelude.undefined
128:      CallStack (from HasCallStack):
129:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
130:        undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
131:      #2: FAIL
132:      Exception: Prelude.undefined
133:      CallStack (from HasCallStack):
134:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
135:        undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
136:      #3: FAIL
137:      Exception: Prelude.undefined
138:      CallStack (from HasCallStack):
139:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
140:        undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
141:      #4: FAIL
142:      Exception: Prelude.undefined
143:      CallStack (from HasCallStack):
144:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
145:        undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
146: ecbDecrypt
147:      #1: FAIL
148:      Exception: Prelude.undefined
149:      CallStack (from HasCallStack):
150:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
151:        undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
152:      #2: FAIL
153:      Exception: Prelude.undefined
154:      CallStack (from HasCallStack):
155:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
156:        undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
157:      #3: FAIL
158:      Exception: Prelude.undefined
159:      CallStack (from HasCallStack):
160:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
161:        undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
162:      #4: FAIL
163:      Exception: Prelude.undefined
164:      CallStack (from HasCallStack):
165:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
166:        undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
167: cbcEncrypt
168:      #1: FAIL
169:      Exception: Prelude.undefined
170:      CallStack (from HasCallStack):
171:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
172:        undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
173:      #2: FAIL
174:      Exception: Prelude.undefined
175:      CallStack (from HasCallStack):
176:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
177:        undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
178:      #3: FAIL
179:      Exception: Prelude.undefined
180:      CallStack (from HasCallStack):
```

```
181:         error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
182:         undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
183:     #4: FAIL
184:         Exception: Prelude.undefined
185:         CallStack (from HasCallStack):
186:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
187:           undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
188: chbDecrypt
189:     #1: FAIL
190:         Exception: Prelude.undefined
191:         CallStack (from HasCallStack):
192:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
193:           undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
194:     #2: FAIL
195:         Exception: Prelude.undefined
196:         CallStack (from HasCallStack):
197:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
198:           undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
199:     #3: FAIL
200:         Exception: Prelude.undefined
201:         CallStack (from HasCallStack):
202:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
203:           undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
204:     #4: FAIL
205:         Exception: Prelude.undefined
206:         CallStack (from HasCallStack):
207:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
208:           undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
209:
210: 16 out of 89 tests failed (0.01s)
211:
212: Test suite crypto-test: FAIL
213: Test suite logged to:
214: /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
215: 0 of 1 test suites (0 of 1 test cases) passed.
216: copying test from skeleton
217: Resolving dependencies...
218: Build profile: -w ghc-9.2.8 -O1
219: In order, the following will be built (use -v for more details):
220: - crypto-0.1.0.0 (lib) (configuration changed)
221: - crypto-0.1.0.0 (test:crypto-test) (configuration changed)
222: - crypto-0.1.0.0 (test:crypto-properties) (dependency rebuilt)
223: Configuring library for crypto-0.1.0.0..
224: Preprocessing library for crypto-0.1.0.0..
225: Building library for crypto-0.1.0.0..
226: Configuring test suite 'crypto-test' for crypto-0.1.0.0..
227: Preprocessing test suite 'crypto-properties' for crypto-0.1.0.0..
228: Building test suite 'crypto-properties' for crypto-0.1.0.0..
229: [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 )
230: 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 ...
231: Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
232: Building test suite 'crypto-test' for crypto-0.1.0.0..
233: [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 )
234: 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 ...
235: Resolving dependencies...
236: Build profile: -w ghc-9.2.8 -O1
237: In order, the following will be built (use -v for more details):
238: - crypto-0.1.0.0 (lib) (configuration changed)
239: - crypto-0.1.0.0 (test:crypto-test) (configuration changed)
```

## Test Preview

testResults.txt: 5/8

Adithya Narayanan - anb122:j1:24

```
240: Configuring library for crypto-0.1.0.0..
241: Preprocessing library for crypto-0.1.0.0..
242: Building library for crypto-0.1.0.0..
243: Configuring test suite 'crypto-test' for crypto-0.1.0.0..
244: Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
245: Building test suite 'crypto-test' for crypto-0.1.0.0..
246: Running 1 test suites...
247: Test suite crypto-test: RUNNING...
248: crypto
249:   part 1
250:     gcd
251:       #1: OK
252:       #2: OK
253:       #3: OK
254:       #4: OK
255:       #5: OK
256:       #6: OK
257:       #7: OK
258:       #8: OK
259:     phi
260:       #1: OK
261:       #2: OK
262:       #3: OK
263:       #4: OK
264:       #5: OK
265:       #6: OK
266:       #7: OK
267:       #8: OK
268:       #9: OK
269:     modPow
270:       #1: OK
271:       #2: OK
272:       #3: OK
273:       #4: OK
274:       #5: OK
275:       #6: OK
276:       #7: OK
277:       #8: OK
278:       #9: OK
279:       #10: OK
280:       #11: OK
281:     computeCoeffs
282:       #1: OK
283:       #2: OK
284:       #3: OK
285:       #4: OK
286:       #5: OK
287:       #6: OK
288:     inverse
289:       #1: OK
290:       #2: OK
291:       #3: OK
292:       #4: OK
293:       #5: OK
294:       #6: OK
295:       #7: OK
296:     smallestCoPrimeOf
297:       #1: OK
298:       #2: OK
299:       #3: OK
300:       #4: OK
```

**Test Preview**

testResults.txt: 6/8

Adithya Narayanan - anb122:j1:24

```
301:      #5: OK
302:      #6: OK
303:      genKeys
304:      #1: OK
305:      #2: OK
306:      #3: OK
307:      #4: OK
308:      #5: OK
309:      #6: OK
310:      rsaEncrypt
311:      #1: OK
312:      #2: OK
313:      #3: OK
314:      #4: OK
315:      rsaDecrypt
316:      #1: OK
317:      #2: OK
318:      #3: OK
319:      #4: OK
320:      part 2
321:      toInt
322:      #1: OK
323:      #2: OK
324:      #3: OK
325:      toChar
326:      #1: OK
327:      #2: OK
328:      #3: OK
329:      add
330:      #1: OK
331:      #2: OK
332:      #3: OK
333:      subtract
334:      #1: OK
335:      #2: OK
336:      #3: OK
337:      ecbEncrypt
338:      #1: FAIL
339:          Exception: Prelude.undefined
340:          CallStack (from HasCallStack):
341:            error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
342:            undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
343:      #2: FAIL
344:          Exception: Prelude.undefined
345:          CallStack (from HasCallStack):
346:            error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
347:            undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
348:      #3: FAIL
349:          Exception: Prelude.undefined
350:          CallStack (from HasCallStack):
351:            error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
352:            undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
353:      #4: FAIL
354:          Exception: Prelude.undefined
355:          CallStack (from HasCallStack):
356:            error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
357:            undefined, called at src/Crypto.hs:123:14 in crypto-0.1.0.0-inplace:Crypto
358:      ecbDecrypt
359:      #1: FAIL
360:          Exception: Prelude.undefined
361:          CallStack (from HasCallStack):
```

**Test Preview****testResults.txt: 7/8****Adithya Narayanan - anb122:j1:24**

```
362:     error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
363:     undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
364: #2: FAIL
365:     Exception: Prelude.undefined
366:     CallStack (from HasCallStack):
367:       error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
368:       undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
369: #3: FAIL
370:     Exception: Prelude.undefined
371:     CallStack (from HasCallStack):
372:       error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
373:       undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
374: #4: FAIL
375:     Exception: Prelude.undefined
376:     CallStack (from HasCallStack):
377:       error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
378:       undefined, called at src/Crypto.hs:127:14 in crypto-0.1.0.0-inplace:Crypto
379: cbcEncrypt
380: #1: FAIL
381:     Exception: Prelude.undefined
382:     CallStack (from HasCallStack):
383:       error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
384:       undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
385: #2: FAIL
386:     Exception: Prelude.undefined
387:     CallStack (from HasCallStack):
388:       error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
389:       undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
390: #3: FAIL
391:     Exception: Prelude.undefined
392:     CallStack (from HasCallStack):
393:       error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
394:       undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
395: #4: FAIL
396:     Exception: Prelude.undefined
397:     CallStack (from HasCallStack):
398:       error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
399:       undefined, called at src/Crypto.hs:134:14 in crypto-0.1.0.0-inplace:Crypto
400: cbcDecrypt
401: #1: FAIL
402:     Exception: Prelude.undefined
403:     CallStack (from HasCallStack):
404:       error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
405:       undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
406: #2: FAIL
407:     Exception: Prelude.undefined
408:     CallStack (from HasCallStack):
409:       error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
410:       undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
411: #3: FAIL
412:     Exception: Prelude.undefined
413:     CallStack (from HasCallStack):
414:       error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
415:       undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
416: #4: FAIL
417:     Exception: Prelude.undefined
418:     CallStack (from HasCallStack):
419:       error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
420:       undefined, called at src/Crypto.hs:141:14 in crypto-0.1.0.0-inplace:Crypto
421:
422: 16 out of 89 tests failed (0.01s)
```

```
423:
424: Test suite crypto-test: FAIL
425: Test suite logged to:
426: /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
427: 0 of 1 test suites (0 of 1 test cases) passed.
428:
429: ----- Test Errors -----
430: Checking https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/
431: Checked https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/
432: Downloading https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/
433: Downloaded https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/
434: Checking https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
435: Checked https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
436: Downloading https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
437: Downloaded https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
438: Warning: The package list for 'hackage.haskell.org' is 45 days old.
439: Run 'cabal update' to get the latest list of available packages.
440: Warning: The package list for 'hackage.haskell.org' is 45 days old.
441: Run 'cabal update' to get the latest list of available packages.
442: cabal: Tests failed for test:crypto-test from crypto-0.1.0.0.
443:
444: Warning: The package list for 'hackage.haskell.org' is 45 days old.
445: Run 'cabal update' to get the latest list of available packages.
446: Warning: The package list for 'hackage.haskell.org' is 45 days old.
447: Run 'cabal update' to get the latest list of available packages.
448: cabal: Tests failed for test:crypto-test from crypto-0.1.0.0.
449:
```