

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:         0 / 3
16:    student-tests/crypto-test/crypto/part 2/toChar:        0 / 3
17:    student-tests/crypto-test/crypto/part 2/add:           0 / 3
18:    student-tests/crypto-test/crypto/part 2/subtract:      0 / 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:         0 / 3
33:    original-tests/crypto-test/crypto/part 2/toChar:        0 / 3
34:    original-tests/crypto-test/crypto/part 2/add:           0 / 3
35:    original-tests/crypto-test/crypto/part 2/subtract:      0 / 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: 2c617
```

```

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 = undefined
95:
96: -- | Returns the n^th letter
97: toChar :: Int -> Char
98: toChar = undefined
99:
100: -- | "adds" two letters
101: add :: Char -> Char -> Char
102: add = undefined
103:
104: -- | "subtracts" two letters
105: subtract :: Char -> Char -> Char
106: subtract = undefined
107:
108: -- the next functions present
109: -- 2 modes of operation for block ciphers : ECB and CBC
110: -- based on a symmetric encryption function e/d such as "add"
111:
112: -- | ecb (electronic codebook) encryption with block size of a letter
113: ecbEncrypt :: Char -> [Char] -> [Char]
114: ecbEncrypt = undefined
115:
116: -- | ecb (electronic codebook) decryption with a block size of a letter
117: ecbDecrypt :: Char -> [Char] -> [Char]
118: ecbDecrypt = undefined
119:
120: -- | cbc (cipherblock chaining) encryption with block size of a letter
121: cbcEncrypt :: Char -- ^ public key
122:             -> Char -- ^ initialisation vector 'iv'
123:             -> [Char] -- ^ message 'm'
124:             -> [Char]
125: cbcEncrypt = undefined
126:
127: -- | cbc (cipherblock chaining) decryption with block size of a letter
128: cbcDecrypt :: Char -- ^ private key
129:             -> Char -- ^ initialisation vector 'iv'
130:             -> [Char] -- ^ message 'm'
131:             -> [Char]
132: cbcDecrypt = undefined

```

```
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/d20231013-37-2e0rsw/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/build/Crypto.o, /tmp/d20231013-37-2e0rsw/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-properties' for crypto-0.1.0.0..
16: Building test suite 'crypto-properties' for crypto-0.1.0.0..
17: Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
18: Building test suite 'crypto-test' for crypto-0.1.0.0..
19: [1 of 1] Compiling Main          ( test/Props.hs, /tmp/d20231013-37-2e0rsw/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/d20231013-37-2e0rsw/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/d20231013-37-2e0rsw/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/d20231013-37-2e0rsw/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: 2/10****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: FAIL
111:         Exception: Prelude.undefined
112:         CallStack (from HasCallStack):
113:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
114:           undefined, called at src/Crypto.hs:94:9 in crypto-0.1.0.0-inplace:Crypto
115:     #2: FAIL
116:         Exception: Prelude.undefined
117:         CallStack (from HasCallStack):
118:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
119:           undefined, called at src/Crypto.hs:94:9 in crypto-0.1.0.0-inplace:Crypto
```

Test Preview**testResults.txt: 3/10****Adithya Narayanan - anb122:j1:24**

```
120:      #3: FAIL
121:         Exception: Prelude.undefined
122:         CallStack (from HasCallStack):
123:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
124:         undefined, called at src/Crypto.hs:94:9 in crypto-0.1.0.0-inplace:Crypto
125: toChar
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:98:10 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:98:10 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:98:10 in crypto-0.1.0.0-inplace:Crypto
141: add
142:      #1: FAIL
143:         Exception: Prelude.undefined
144:         CallStack (from HasCallStack):
145:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
146:         undefined, called at src/Crypto.hs:102:7 in crypto-0.1.0.0-inplace:Crypto
147:      #2: 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:102:7 in crypto-0.1.0.0-inplace:Crypto
152:      #3: 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:102:7 in crypto-0.1.0.0-inplace:Crypto
157: subtract
158:      #1: FAIL
159:         Exception: Prelude.undefined
160:         CallStack (from HasCallStack):
161:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
162:         undefined, called at src/Crypto.hs:106:12 in crypto-0.1.0.0-inplace:Crypto
163:      #2: FAIL
164:         Exception: Prelude.undefined
165:         CallStack (from HasCallStack):
166:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
167:         undefined, called at src/Crypto.hs:106:12 in crypto-0.1.0.0-inplace:Crypto
168:      #3: 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:106:12 in crypto-0.1.0.0-inplace:Crypto
173: ecbEncrypt
174:      #1: FAIL
175:         Exception: Prelude.undefined
176:         CallStack (from HasCallStack):
177:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
178:         undefined, called at src/Crypto.hs:114:14 in crypto-0.1.0.0-inplace:Crypto
179:      #2: FAIL
180:         Exception: Prelude.undefined
```

```
181:      CallStack (from HasCallStack):
182:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
183:        undefined, called at src/Crypto.hs:114:14 in crypto-0.1.0.0-inplace:Crypto
184:    #3: FAIL
185:      Exception: Prelude.undefined
186:      CallStack (from HasCallStack):
187:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
188:        undefined, called at src/Crypto.hs:114:14 in crypto-0.1.0.0-inplace:Crypto
189:    #4: 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:114:14 in crypto-0.1.0.0-inplace:Crypto
194:  ecbDecrypt
195:    #1: FAIL
196:      Exception: Prelude.undefined
197:      CallStack (from HasCallStack):
198:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
199:        undefined, called at src/Crypto.hs:118:14 in crypto-0.1.0.0-inplace:Crypto
200:    #2: FAIL
201:      Exception: Prelude.undefined
202:      CallStack (from HasCallStack):
203:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
204:        undefined, called at src/Crypto.hs:118:14 in crypto-0.1.0.0-inplace:Crypto
205:    #3: FAIL
206:      Exception: Prelude.undefined
207:      CallStack (from HasCallStack):
208:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
209:        undefined, called at src/Crypto.hs:118:14 in crypto-0.1.0.0-inplace:Crypto
210:    #4: FAIL
211:      Exception: Prelude.undefined
212:      CallStack (from HasCallStack):
213:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
214:        undefined, called at src/Crypto.hs:118:14 in crypto-0.1.0.0-inplace:Crypto
215:  cbcEncrypt
216:    #1: FAIL
217:      Exception: Prelude.undefined
218:      CallStack (from HasCallStack):
219:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
220:        undefined, called at src/Crypto.hs:125:14 in crypto-0.1.0.0-inplace:Crypto
221:    #2: FAIL
222:      Exception: Prelude.undefined
223:      CallStack (from HasCallStack):
224:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
225:        undefined, called at src/Crypto.hs:125:14 in crypto-0.1.0.0-inplace:Crypto
226:    #3: FAIL
227:      Exception: Prelude.undefined
228:      CallStack (from HasCallStack):
229:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
230:        undefined, called at src/Crypto.hs:125:14 in crypto-0.1.0.0-inplace:Crypto
231:    #4: FAIL
232:      Exception: Prelude.undefined
233:      CallStack (from HasCallStack):
234:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
235:        undefined, called at src/Crypto.hs:125:14 in crypto-0.1.0.0-inplace:Crypto
236:  cbcDecrypt
237:    #1: FAIL
238:      Exception: Prelude.undefined
239:      CallStack (from HasCallStack):
240:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
241:        undefined, called at src/Crypto.hs:132:14 in crypto-0.1.0.0-inplace:Crypto
```

Test Preview**testResults.txt: 5/10****Adithya Narayanan - anb122:j1:24**

```
242:      #2: FAIL
243:      Exception: Prelude.undefined
244:      CallStack (from HasCallStack):
245:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
246:        undefined, called at src/Crypto.hs:132:14 in crypto-0.1.0.0-inplace:Crypto
247:      #3: FAIL
248:      Exception: Prelude.undefined
249:      CallStack (from HasCallStack):
250:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
251:        undefined, called at src/Crypto.hs:132:14 in crypto-0.1.0.0-inplace:Crypto
252:      #4: FAIL
253:      Exception: Prelude.undefined
254:      CallStack (from HasCallStack):
255:        error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
256:        undefined, called at src/Crypto.hs:132:14 in crypto-0.1.0.0-inplace:Crypto
257:
258: 28 out of 89 tests failed (0.01s)
259:
260: Test suite crypto-test: FAIL
261: Test suite logged to:
262: /tmp/d20231013-37-2e0rsw/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
263: 0 of 1 test suites (0 of 1 test cases) passed.
264: copying test from skeleton
265: Resolving dependencies...
266: Build profile: -w ghc-9.2.8 -O1
267: In order, the following will be built (use -v for more details):
268: - crypto-0.1.0.0 (lib) (configuration changed)
269: - crypto-0.1.0.0 (test:crypto-test) (configuration changed)
270: - crypto-0.1.0.0 (test:crypto-properties) (dependency rebuilt)
271: Configuring library for crypto-0.1.0.0..
272: Preprocessing library for crypto-0.1.0.0..
273: Building library for crypto-0.1.0.0..
274: Configuring test suite 'crypto-test' for crypto-0.1.0.0..
275: Preprocessing test suite 'crypto-properties' for crypto-0.1.0.0..
276: Building test suite 'crypto-properties' for crypto-0.1.0.0..
277: [1 of 1] Compiling Main                ( test/Props.hs, /
/tmp/d20231013-37-2e0rsw/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 )
278: Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
279: Building test suite 'crypto-test' for crypto-0.1.0.0..
280: Linking /tmp/d20231013-37-2e0rsw/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-properties/build/crypto-properties/crypto-properties ...
281: [1 of 1] Compiling Main                ( test/Tests.hs, /
/tmp/d20231013-37-2e0rsw/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 )
282: Linking /tmp/d20231013-37-2e0rsw/dist-newstyle/build/x86_64-linux/ghc-9.2.8/crypto-0.1.0.0/t/crypto-test/build/crypto-test/crypto-test ...
283: Resolving dependencies...
284: Build profile: -w ghc-9.2.8 -O1
285: In order, the following will be built (use -v for more details):
286: - crypto-0.1.0.0 (lib) (configuration changed)
287: - crypto-0.1.0.0 (test:crypto-test) (configuration changed)
288: Configuring library for crypto-0.1.0.0..
289: Preprocessing library for crypto-0.1.0.0..
290: Building library for crypto-0.1.0.0..
291: Configuring test suite 'crypto-test' for crypto-0.1.0.0..
292: Preprocessing test suite 'crypto-test' for crypto-0.1.0.0..
293: Building test suite 'crypto-test' for crypto-0.1.0.0..
294: Running 1 test suites...
295: Test suite crypto-test: RUNNING...
296: crypto
297:   part 1
298:     gcd
299:       #1: OK
300:       #2: OK
```

Test Preview**testResults.txt: 6/10****Adithya Narayanan - anb122:j1:24**

```
301:      #3: OK
302:      #4: OK
303:      #5: OK
304:      #6: OK
305:      #7: OK
306:      #8: OK
307:  phi
308:      #1: OK
309:      #2: OK
310:      #3: OK
311:      #4: OK
312:      #5: OK
313:      #6: OK
314:      #7: OK
315:      #8: OK
316:      #9: OK
317:  modPow
318:      #1: OK
319:      #2: OK
320:      #3: OK
321:      #4: OK
322:      #5: OK
323:      #6: OK
324:      #7: OK
325:      #8: OK
326:      #9: OK
327:      #10: OK
328:      #11: OK
329:  computeCoeffs
330:      #1: OK
331:      #2: OK
332:      #3: OK
333:      #4: OK
334:      #5: OK
335:      #6: OK
336:  inverse
337:      #1: OK
338:      #2: OK
339:      #3: OK
340:      #4: OK
341:      #5: OK
342:      #6: OK
343:      #7: OK
344:  smallestCoPrimeOf
345:      #1: OK
346:      #2: OK
347:      #3: OK
348:      #4: OK
349:      #5: OK
350:      #6: OK
351:  genKeys
352:      #1: OK
353:      #2: OK
354:      #3: OK
355:      #4: OK
356:      #5: OK
357:      #6: OK
358:  rsaEncrypt
359:      #1: OK
360:      #2: OK
361:      #3: OK
```


Test Preview**testResults.txt: 7/10****Adithya Narayanan - anb122:j1:24**

```
362:      #4: OK
363:      rsaDecrypt
364:      #1: OK
365:      #2: OK
366:      #3: OK
367:      #4: OK
368:  part 2
369:      toInt
370:      #1: FAIL
371:          Exception: Prelude.undefined
372:          CallStack (from HasCallStack):
373:            error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
374:            undefined, called at src/Crypto.hs:94:9 in crypto-0.1.0.0-inplace:Crypto
375:      #2: FAIL
376:          Exception: Prelude.undefined
377:          CallStack (from HasCallStack):
378:            error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
379:            undefined, called at src/Crypto.hs:94:9 in crypto-0.1.0.0-inplace:Crypto
380:      #3: 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:94:9 in crypto-0.1.0.0-inplace:Crypto
385:  toChar
386:      #1: FAIL
387:          Exception: Prelude.undefined
388:          CallStack (from HasCallStack):
389:            error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
390:            undefined, called at src/Crypto.hs:98:10 in crypto-0.1.0.0-inplace:Crypto
391:      #2: FAIL
392:          Exception: Prelude.undefined
393:          CallStack (from HasCallStack):
394:            error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
395:            undefined, called at src/Crypto.hs:98:10 in crypto-0.1.0.0-inplace:Crypto
396:      #3: FAIL
397:          Exception: Prelude.undefined
398:          CallStack (from HasCallStack):
399:            error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
400:            undefined, called at src/Crypto.hs:98:10 in crypto-0.1.0.0-inplace:Crypto
401:  add
402:      #1: FAIL
403:          Exception: Prelude.undefined
404:          CallStack (from HasCallStack):
405:            error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
406:            undefined, called at src/Crypto.hs:102:7 in crypto-0.1.0.0-inplace:Crypto
407:      #2: FAIL
408:          Exception: Prelude.undefined
409:          CallStack (from HasCallStack):
410:            error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
411:            undefined, called at src/Crypto.hs:102:7 in crypto-0.1.0.0-inplace:Crypto
412:      #3: FAIL
413:          Exception: Prelude.undefined
414:          CallStack (from HasCallStack):
415:            error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
416:            undefined, called at src/Crypto.hs:102:7 in crypto-0.1.0.0-inplace:Crypto
417:  subtract
418:      #1: FAIL
419:          Exception: Prelude.undefined
420:          CallStack (from HasCallStack):
421:            error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
422:            undefined, called at src/Crypto.hs:106:12 in crypto-0.1.0.0-inplace:Crypto
```

Test Preview**testResults.txt: 8/10****Adithya Narayanan - anb122:j1:24**

```
423:      #2: FAIL
424:          Exception: Prelude.undefined
425:          CallStack (from HasCallStack):
426:              error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
427:              undefined, called at src/Crypto.hs:106:12 in crypto-0.1.0.0-inplace:Crypto
428:      #3: FAIL
429:          Exception: Prelude.undefined
430:          CallStack (from HasCallStack):
431:              error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
432:              undefined, called at src/Crypto.hs:106:12 in crypto-0.1.0.0-inplace:Crypto
433: ecbEncrypt
434:      #1: FAIL
435:          Exception: Prelude.undefined
436:          CallStack (from HasCallStack):
437:              error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
438:              undefined, called at src/Crypto.hs:114:14 in crypto-0.1.0.0-inplace:Crypto
439:      #2: FAIL
440:          Exception: Prelude.undefined
441:          CallStack (from HasCallStack):
442:              error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
443:              undefined, called at src/Crypto.hs:114:14 in crypto-0.1.0.0-inplace:Crypto
444:      #3: FAIL
445:          Exception: Prelude.undefined
446:          CallStack (from HasCallStack):
447:              error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
448:              undefined, called at src/Crypto.hs:114:14 in crypto-0.1.0.0-inplace:Crypto
449:      #4: FAIL
450:          Exception: Prelude.undefined
451:          CallStack (from HasCallStack):
452:              error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
453:              undefined, called at src/Crypto.hs:114:14 in crypto-0.1.0.0-inplace:Crypto
454: ecbDecrypt
455:      #1: FAIL
456:          Exception: Prelude.undefined
457:          CallStack (from HasCallStack):
458:              error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
459:              undefined, called at src/Crypto.hs:118:14 in crypto-0.1.0.0-inplace:Crypto
460:      #2: FAIL
461:          Exception: Prelude.undefined
462:          CallStack (from HasCallStack):
463:              error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
464:              undefined, called at src/Crypto.hs:118:14 in crypto-0.1.0.0-inplace:Crypto
465:      #3: FAIL
466:          Exception: Prelude.undefined
467:          CallStack (from HasCallStack):
468:              error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
469:              undefined, called at src/Crypto.hs:118:14 in crypto-0.1.0.0-inplace:Crypto
470:      #4: FAIL
471:          Exception: Prelude.undefined
472:          CallStack (from HasCallStack):
473:              error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
474:              undefined, called at src/Crypto.hs:118:14 in crypto-0.1.0.0-inplace:Crypto
475: cbcEncrypt
476:      #1: FAIL
477:          Exception: Prelude.undefined
478:          CallStack (from HasCallStack):
479:              error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
480:              undefined, called at src/Crypto.hs:125:14 in crypto-0.1.0.0-inplace:Crypto
481:      #2: FAIL
482:          Exception: Prelude.undefined
483:          CallStack (from HasCallStack):
```

Test Preview**testResults.txt: 9/10****Adithya Narayanan - anb122:j1:24**

```
484:         error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
485:         undefined, called at src/Crypto.hs:125:14 in crypto-0.1.0.0-inplace:Crypto
486:     #3: FAIL
487:         Exception: Prelude.undefined
488:         CallStack (from HasCallStack):
489:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
490:           undefined, called at src/Crypto.hs:125:14 in crypto-0.1.0.0-inplace:Crypto
491:     #4: FAIL
492:         Exception: Prelude.undefined
493:         CallStack (from HasCallStack):
494:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
495:           undefined, called at src/Crypto.hs:125:14 in crypto-0.1.0.0-inplace:Crypto
496: cbcDecrypt
497:     #1: FAIL
498:         Exception: Prelude.undefined
499:         CallStack (from HasCallStack):
500:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
501:           undefined, called at src/Crypto.hs:132:14 in crypto-0.1.0.0-inplace:Crypto
502:     #2: FAIL
503:         Exception: Prelude.undefined
504:         CallStack (from HasCallStack):
505:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
506:           undefined, called at src/Crypto.hs:132:14 in crypto-0.1.0.0-inplace:Crypto
507:     #3: FAIL
508:         Exception: Prelude.undefined
509:         CallStack (from HasCallStack):
510:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
511:           undefined, called at src/Crypto.hs:132:14 in crypto-0.1.0.0-inplace:Crypto
512:     #4: FAIL
513:         Exception: Prelude.undefined
514:         CallStack (from HasCallStack):
515:           error, called at libraries/base/GHC/Err.hs:74:14 in base:GHC.Err
516:           undefined, called at src/Crypto.hs:132:14 in crypto-0.1.0.0-inplace:Crypto
517:
518: 28 out of 89 tests failed (0.02s)
519:
520: Test suite crypto-test: FAIL
521: Test suite logged to:
522: /tmp/d20231013-37-2e0rsw/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
523: 0 of 1 test suites (0 of 1 test cases) passed.
524:
525: ----- Test Errors -----
526: Checking https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/
527: Checked https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/
528: Downloading https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/
529: Downloaded https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/
530: Checking https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
531: Checked https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
532: Downloading https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
533: Downloaded https://repol.maven.org/maven2/org/scala-lang/scala3-library_3/maven-metadata.xml
534: Warning: The package list for 'hackage.haskell.org' is 43 days old.
535: Run 'cabal update' to get the latest list of available packages.
536: Warning: The package list for 'hackage.haskell.org' is 43 days old.
537: Run 'cabal update' to get the latest list of available packages.
538: cabal: Tests failed for test:crypto-test from crypto-0.1.0.0.
539:
540: Warning: The package list for 'hackage.haskell.org' is 43 days old.
541: Run 'cabal update' to get the latest list of available packages.
542: Warning: The package list for 'hackage.haskell.org' is 43 days old.
543: Run 'cabal update' to get the latest list of available packages.
544: cabal: Tests failed for test:crypto-test from crypto-0.1.0.0.
```

545: