

```

1  -- Caesar cipher example from chapter 5 of Programming in Haskell,
2  -- Graham Hutton, Cambridge University Press, 2016.
3
4  import Data.Char
5
6  -- Encoding and decoding
7
8  let2int :: Char -> Int
9  let2int c = ord c - ord 'a'
10
11 int2let :: Int -> Char
12 int2let n = chr (ord 'a' + n)
13
14 shift :: Int -> Char -> Char
15 shift n c | isLower c = int2let ((let2int c + n) `mod` 26)
16           | otherwise = c
17
18 encode :: Int -> String -> String
19 encode n xs = [shift n x | x <- xs]
20
21 -- Frequency analysis
22
23 table :: [Float]
24 table = [8.1, 1.5, 2.8, 4.2, 12.7, 2.2, 2.0, 6.1, 7.0,
25         0.2, 0.8, 4.0, 2.4, 6.7, 7.5, 1.9, 0.1, 6.0,
26         6.3, 9.0, 2.8, 1.0, 2.4, 0.2, 2.0, 0.1]
27
28 lowers :: String -> Int
29 lowers xs = length [x | x <- xs, x >= 'a' && x <= 'z']
30
31 count :: Char -> String -> Int
32 count x xs = length [x' | x' <- xs, x == x']
33
34 percent :: Int -> Int -> Float
35 percent n m = (fromIntegral n / fromIntegral m) * 100
36
37 freqs :: String -> [Float]
38 freqs xs = [percent (count x xs) n | x <- ['a'..'z']]
39           where n = lowers xs
40
41 chisqr :: [Float] -> [Float] -> Float
42 chisqr os es = sum [((o-e)^2)/e | (o,e) <- zip os es]
43
44 rotate :: Int -> [a] -> [a]
45 rotate n xs = drop n xs ++ take n xs
46
47 positions :: Eq a => a -> [a] -> [Int]
48 positions x xs = [i | (x',i) <- zip xs [0..n], x == x']
49               where n = length xs - 1
50
51 crack :: String -> String
52 crack xs = encode (-factor) xs
53           where
54             factor = head (positions (minimum chitab) chitab)
55             chitab = [chisqr (rotate n table') table | n <- [0..25]]
56             table' = freqs xs

```