Cryptography

The Art oft Secret Messages

Kai kai@42.us.org

Summary: This project covers some basic codes in cryptography. They may not keep your banking accounts safe, but they can hide some secrets from all but the most dedicated hackers.

This work is licensed under a Creative Commons Attribution-Noncommercial-ShareAlike 4.0 International License.

Contents

Copyright © 2019 Code for fun

Chapter I

Guidelines

- Corrections will take place according to the peer-corrections model.
- Questions? Ask the neighbor on your right. Next, ask the neighbor on your left.
- Read the examples carefully. The exercises might require things that are not specified in the subject...
- Your reference manual is called Google / "Read the Manual!" / the Internet / ...

Copyright © 2019 Code for fun

Chapter II

Preamble

Some other fellow–one who actually bothered to shave, shower, and put on a uniform–introduces bathrobe man as Commander Shane-spelled-s-c-h-o-e-n, but Schoen is having none of it; he turns his back on them, exposing the back side of his bathrobe, which around the buttocks is worn transparent as a negligee. Reading from a notebook, he writes out the following in block letters:

19 17 17 19 14 20 23 18 19 8 12 16 19 8 3

21 8 25 18 14 18 6 3 18 8 15 18 22 18 11

Around the time that the fourth or fifth number is going up on the chalkboard, Waterhouse feels the hairs standing up on the back of his neck. By the time the third group of five numbers is written out, he has not failed to notice that none of them is larger than 26–that being the number of letters in the alphabet. His heart is pounding more wildly than it did when Nipponese bombs were tracing parabolic trajectories toward the deck of the grounded Nevada. He pulls a pencil out of his pocket. Finding no paper handy, he writes down the numbers from 1 to 26 on the surface of his little writing desk.

By the time the man in the bathrobe is done writing out the last group of numbers, Waterhouse is already well into his frequency count. He wraps it up as Bathrobe Man is saying something along the lines of "this might look like a meaningless sequence of numbers to you, but to a Nip naval officer it might look like something entirely different." Then the man laughs nervously, shakes his head sadly, squares his jaw resolutely, and runs through a litany of other emotion-laden expressions not a single one of which is appropriate here.

Waterhouse's frequency count is simply a tally of how frequently each number appears on the blackboard. It looks like this:

1
2
3 ||
4
5
6 |
7
8 ||||
9
10
11 |
12 |

Copyright © 2019 Code for fun

13
14 ||
15 |
16 |
17 ||
18 ||||||
19 ||||
20 |
21 |
22 |
23 |
24
25 |
26

The most interesting thing about this is that ten of the possible symbols (viz. 1, 2, 4, 5, 7, 9, 10, 13, 24, and 26) are not even used. Only sixteen different numbers appear in the message. Assuming each of those sixteen represents one and only one letter of the alphabet, this message has (Lawrence reckons in his head) 111136315345735680000 possible meanings. This is a funny number because it begins with four ones and ends with four zeroes; Lawrence snickers, wipes his nose, and gets on with it.

The most common number is 18. It probably represents the letter E. If he substitutes E into the message everywhere he sees an 18, then–

Well, to be honest, then he'll have to write out the whole message again, substituting Es for 18s, and it will take a long time, and it might be time wasted because he might have guessed wrong. On the other hand, if he just restrains his mind to construe 18s as Es–an operation that he thinks of as being loosely analogous to changing the presets on a pipe organ's console–then what he sees in his mind's eye when he looks at the blackboard is

19 17 17 19 14 20 23 E 19 8 12 16 19 8 3
21 8 25 E 14 E 6 3 E 8 15 E 22 E 11

which only has 10103301395066880000 possible meanings. This is a funny number too because of all those ones and zeroes–but it is an absolutely meaningless coincidence.

"The science of making secret codes is called cryptography," Commander Schoen says, "and the science of breaking them is cryptanalysis." Then he sighs, grapples visibly with some more widely divergent emotional states, and resignedly plods into the mandatory exercise of breaking these words down into their roots, which are either Latin or Greek (Lawrence isn't paying attention, doesn't care, only glimpses the stark word CRYPTO written in handsized capitals).

The opening sequence "19 17 17 19" is peculiar. 19, along with 8, is the second most common number in the list. 17 is only half as common. You can't have four vowels or four consonants in a row (unless the words are German) so either 17 is a vowel and 19 a consonant or the other way round. Since 19 appears more frequently (four times) in the message, it is more likely to be the vowel than 17 (which only appears twice). A is the most common vowel after E, so if he assumes that 19 is A, he gets

A 17 17 A 14 20 23 E A 8 12 16 A 8 3
21 8 25 E 14 E 6 3 E 8 15 E 22 E 11

This narrows it down quite a bit, to a mere 841941782922240000 possible answers. He's already reduced the solution space by a couple of orders of magnitude!

Copyright © 2019 Code for fun

Schoen has talked himself up into a disturbingly heavy sweat, now, and is almost bodily flinging himself into a historical overview of the science of CRYPTOLOGY, as the union of cryptography and cryptanalysis is called. There's some talk about an English fellow name of Wilkins, and book called Cryptonomicon that he wrote hundreds of years ago, but (perhaps because he doesn't rate the intelligence of his audience too highly) he goes very easy on the historical background, and jumps directly from Wilkins to Paul Revere's "one if by land, two if by sea" code. He even makes a mathematics in-joke about this being one of the earliest practical applications of binary notation. Lawrence dutifully brays and snorts, drawing an appalled look from the saxophonist seated in front of him.

Earlier in his talk, the Schoen mentioned that this message was (in what's obviously a fictional scenario ginned up to make this mathematical exercise more interesting to a bunch of musicians who are assumed not to give a shit about math) addressed to a Nip naval officer. Given that context, Lawrence cannot but guess that the first word of the message is ATTACK. This would mean that 17 represented T, 14 C, and 20 K. When he fills these in, he gets

A T T A C K 23 E A 8 12 16 A 8 3

21 T 25 E C E 6 3 E 8 15 E 22 E 11

and then the rest is so obvious he doesn't bother to write it out. He cannot restrain himself from jumping to his feet. He's so excited he forgets about the weak legs and topples over across a couple of his neighbors' desks, which makes a lot of noise.

"Do you have a problem, sailor?" says one of the officers in the corner, one who actually bothered to wear a uniform.

"Sir! The message is, 'Attack Pearl Harbor December Seven!' Sir!" Lawrence shouts, and then sits down. His whole body is quivering with excitement. Adrenalin has taken over his body and mind. He could strangle twenty sumo wrestlers on the spot.

Commander Schoen is completely impassive except that he blinks once, very slowly. He turns to one of his subordinates, who is standing against the wall with his hands clasped behind his back, and says, "Get this one a copy of the Cryptonomicon. And a desk–as close to the coffee machine as possible. And why don't you promote the son of a b**** as long as you're at it."

Copyright © 2019 Code for fun

Chapter III

Exercise 00 : Rot21

- Create a script `rot21.rb` which takes a string and displays it, replacing each of its letters by the letter 21 spaces ahead in alphabetical order.

  'z' becomes 'u' and 'Z' becomes 'U'. Case remains unaffected.

  The output will be followed by a newline.

  If the number of arguments is not 1, the program displays a newline.

```
?> ./rot21.rb | cat -e
$
?> ./rot21.rb "The method is named after Julius Caesar, who used it in his private
 correspondence." | cat -e
Ocz hzocjy dn ivhzy vaozm Epgdpn Xvznvm, rcj pnzy do di cdn kmdqvoz xjmmznkjiyzixz.$
```

Copyright © 2019 Code for fun

Chapter IV

Exercise 01 : Brute Force

- Create a script `bruteforce.rb` which shows multiple sets of output but eventually decodes any string encoded by any "rotN" cipher.

```
?> ruby bruteforce.rb | cat -e
$
?> ruby bruteforce.rb "Epgdpn Xvznvm" | cat -e
Fqheqo Ywaown$
Grifrp Zxbpxo$
Hsjgsq Aycqyp$
Itkhtr Bzdrzq$
Julius Caesar$
```

Copyright © 2019 Code for fun

Chapter V

Exercise 02 : Wingdings

- Create a script `wingdings.rb` which encodes each letter of the English alphabet to a secret alphabet of your own. Feel free to use other English characters, or anything from Unicode: accent marks, symbols, emojis... the alphabets are your oysters.

`Unicode escape in Ruby, \u`

Copyright © 2019 Code for fun

Chapter VI

Exercise 03 : Vignere

- Create a script `vignere.rb` which enrypts a text using the Vignere cipher.
- This cipher involves using a secret password which repeats to mask the full length fo the message. For example, if the password is "KEY" and the secret message is "thekeysarehiddenbelowthepottedplant", you should enrypt it to:
  k + t = d
  e + h = l
  y + e = c
  k + k = u
  e + e = i
  y + y = w
  k + s = c
  e + a = e
  ..and so forth.

  Keep all spaces, punctuation, numbers, and capitalization patterns of the encrypted text intact.

```
?> ruby vignere.rb | cat -e
$
?> .ruby vignere.rb "key" "thekeysarehiddenbelowthepottedplant" | cat -e
dlcuiwcepolgnhcxfcvsudlczsrdibzpyxx$
?> .ruby vignere.rb "coal" "Watch out, Santa Claus knows what we did!" | cat -e
Yotnj cue, Uonec Qllwg kyqks hjot hg rio!$
```

Copyright © 2019 Code for fun