Lab 3

Isabel Lally, Collin Bauer

Part 1 - Simple Cipher Attack

1. `1-20-20-1-3-11 1-20 4-1-23-14 23-9-20-8 4-18-15-14-5-19`
    - **Type:** Letter-Numbers
    - **Message:** ATTACK AT DAWN WITH DRONES
2. `y. Tshoem eE yteo obfe Pervoivdiednecnec eo,f oar ctohnes pailrla-csye eiinnvgo levyien go ft hGeo df,o usnedeenr sh eorfe tohne tUhnei tUeSd $S1t abtielsl ,a nhda st hbee eInl ltuamkienna tbi`
    - **Type:** Railfence, or Rotate, depending on parameters
        - We tried different strategies for this one. We noticed that we could take one alternate the letters and end up with two halves of the whole message, but some words were still scrambled.
        - After some fiddling, and looking it up, we found both Railfence and Rotate work, with two columns, rotated left/shift of 2.
    - **Message:** The Eye of Providence, or the all-seeing eye of God, on the US bill, has been taken by some to be evidence of a conspiracy involving the founders of the United States and the Illuminati.
3. `.--. .-.. . .-... . / .-.. . -/ -.... . / --.-..-. . -. / -.--. ---.--/ -.... .--/ .. / .--.. .-.. .-.. / -.-. .-.-. .-. -.--/ ---..--/ -.... . / --.. ... . ----. / .--.-. -.-. ---.-. -.. ..-. --. / ----/ .... . .-. / .--.. ... .-.-.-/ .... . .-. / ..-. .-.. -.... ..-. ..-.-.. / ... . .-. ...-.--. ---..--/ -..-`
    - **Type:** Morse Code

- **Message:** PLEASE LET THE QUEEN KNOW THAT I WILL CARRY OUT THE MISSION ACCORDING TO HER WISH, HER FAITHFUL SERVANT, X

4. `QW4gdW5pZGVudGlmaWVkIGZseWluZyBvYmplY3Qgb3IgVUZPLCBpcyBkZWZpb mVkIGFzIGEgcGV yY2VpdmVkIG9iamVjdCBpbiB0aGUgc2t5LCBub3QgaWRlbnRpZ mlhYmxlIGJ5IHN0YW5kYXJkIGNyaXRlcmlhLiBNb3N0IFVGT3MgYXJlIGxhdGV yIGlkZW50aWZpZWQgYXMgY29udmVudGlvbmFsIG9iamVjdHMgb3IgcGhlbm9tZW5 hLiBUaGUgdGVybSBpcyB3aWRlbHkgdXNlZCBmb3IgY2xhaW1lZCBvYnNlcnZhdGl vbnMgb2YgZXh0cmF0ZXJyZXN0cmlhbCBjcmFmdC4=`

   - **Type:** Base64

   - **Message:** An unidentified flying object or UFO, is defined as a perceived object in the sky, not identifiable by standard criteria. Most UFOs are later identified as conventional objects or phenomena. The term is widely used for claimed observations of extraterrestrial craft.

5. `Tn'tnhteotrdn a kr iur  evoero yact lseen n, ncciaraaeefmo urZcpre 0s e7 sh sh.ahpweernoee mhhy ttleftg`

   - **Type:** Ubchi 14325. Took a lot of guessing.

     - We knew that it used this cipher because it had a Z in it, and found this cipher would put a Z in a speudo-random spot in the ciphered text.

     - The only other capital letter was T, at the beginning, so the first value would have to be 1.

     - One of the most common words in the english alphabet is "the" so we attempted to force the first word in the cipher to be "The". After that, we just got lucky, and 14325 happened to work.

     - There are several words that could match, including bleep, alley, Sheep and Trees (assuming case-sensitive, duplicating backwards). Profx also works.

   - **Message:** The oceans cover more than 70 percent of the earth's surface, yet their depths remain largely unknown.

Part 2: AES, RSA practice

1. RSA: n = 899 e = 47 d = 143

   Bob(public, private, N) = Bob(47, 143, 899)

   Message to send = "1 7 3 5 1"

```
Ek(m) = text^47 mod 899
      = 1^47 mod 899 = 1
      = 7^47 mod 899 = 886
      = 3^47 mod 899 = 859
      = 5^47 mod 899 = 428
      = 1^47 mod 899 = 1
```

   - Message Alice Sends to Bob = "1 886 859 428 1"

```
Dk(c) = cipher^143 mod 899
      = 1^143 mod 899 = 1
      = 886^143 mod 899 = 7
      = 859^143 mod 899 = 3
      = 428^143 mod 899 = 5
      = 1^143 mod 899 = 1
```

   - Bob's Decrypted Message = "1 7 3 5 1"

---

2. AES: Probability of guessing the AES-128 key in single try = $1/(2^{128})$

   How many times in a row must you win the lotto to have better chances of guessing AES-128?

   To win lotto: 7 different numbers ranging from 1-36

- Since the numbers must be different, These are the number of choices for each number:

  ‾‾ ‾‾ ‾‾ ‾‾ ‾‾ ‾‾ ‾‾

  36 * 35 * 34 * 33 * 32 * 31 * 30 = 42,072,307,200

- Only 1 ticket wins, so odds are 1/42,072,307,200
  This is approximately $1/(2^{35})$ to win once

- Since winning each time is a separate event, to find the odds, multiply:
  $1/(2^{35}) * 1/(2^{35}) * 1/(2^{35}) * 1/(2^{35}) = 1/(2^{140})$

- $1/(2^{128}) < 1/(2^{140})$

- Therefore, you would have better odds guessing the AES-128 key than winning the lottery 4 times in a row.