UW Math Circle

1 Decrypting in Cryptography

Below is a series of encrypted messages that are made using different encryption algorithms. Your job is to decode the messages! Each message is of the form

THIS IS CALLED XXXXXXXXX

where instead of XXXXXXXXX, the message will contain the name of the algorithm.

1. Decrypt the following secret message.

```
20 8 9 19 0 9 19 0 3 1 12 12 5 4 0 12 5 20 20 5 18 0 14 21 13 2 5 18 0 3 15 4 5
```

2. Decrypt the following secret message.

```
wklv lv fdoohg fdhvdu
```

3. Decrypt the following secret message.

```
tilrrpt hsloaoi icewnso sadtsin
```

4. Decrypt the following secret message.

```
gsrh rh xzoovw zgyzhs
```

5. Decrypt the following secret message.

```
tilrfe hssaldalec icein
```

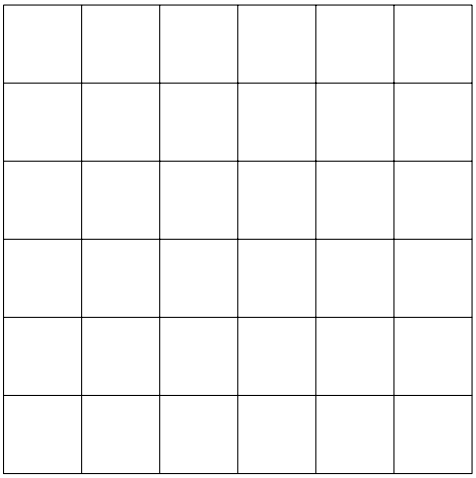
6. Pick one of the previous five encryption methods and give **one pro** and **one con** of using this encryption method to share secret messages.

Stop here. Request the next page from your instructor when your group is done.

2 Physical Key Encryption

7. Decrypt the following secret message using the decryption tool and the grid below.

`crtylhigespigtdritiscoualrlnleexnnin`



Then, explain to an instructor how you decrypted the secret message.

Stop here. Request the next page from your instructor when your group is done.

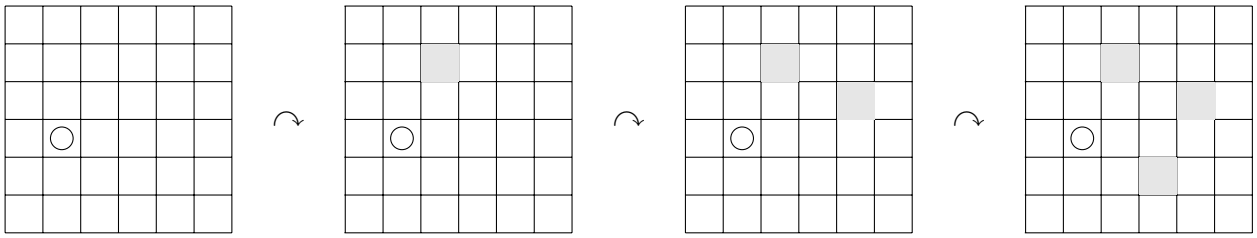
8. Let's build our own turning grille key.

   (a) Pick a square on the cut out grid to hole punch.

   (b) Shade each square the punch from (a) can rotate to by 90° turns.

   (c) Repeat steps (a) and (b) until each square in the grid is either shaded or hole punched.

   (d) Mark which side is the top and which direction your key will turn.



9. What length will an encrypted message made using your turning grille key be? Did this depend on where you placed your hole punches?

10. Encrypt a message using your key and have a group member use your key to decrypt it.

11. You find a turning grille key and an encrypted message, but it has no markings on it. How many ways will you need to try the key to ensure that you decrypt the secret message?

12. Are there any turning grille keys that produce the same encrypted message whether you turn the key clockwise or counter clockwise? Give an example or explain why not.

13. Are there any turning grille keys that produce the same encrypted message whether the key is flipped upside down or right side up? Give an example or explain why not.

14. (Challenge) Encrypt a message which yields a false message when you rotate your turning grille key the opposite direction.

3 Modern Encryption

15. What if you want to share a secret message with your group members, but the instructor can look at *all* notes between you and your group members – even the first note that describes your encryption and decryption method. Do you think it is still possible to send a secret message?

16. Let's review modular arithmetic. For each of the equations below, try to find integers b and r that make the equation true. Make the integer r as small as possible.

    (a) $16 = b \cdot 5 + r$.

    (b) $64 = b \cdot 5 + r$.

    (c) $1 = b \cdot 5 + r$.

17. Given integers n and p, if we can find integers b and r so that $n = b \cdot p + r$, we say $r = n \bmod p$. For example, $8 = 100 \bmod 23$ because we can write $100 = 4 \cdot 23 + 8$. To practice this new notation, compute the following.

    (a) Find $4^2 \bmod 5$ and call this number A.

    (b) Find $A^3 \bmod 5$ and call this number N.

    (c) Find $4^3 \bmod 5$ and call this number B.

    (d) Find $B^2 \bmod 5$ and call this number M.

18. Notice that $N \equiv M$ in the above problem. Is this a coincidence?

Stop here. Request the next page from your instructor when your group is done.

19. With your group members practice the following method.

    Step 1: You and a group member agree on a prime number p (for example $p = 5$) and a number g so that $1 \leq g < p$ (for example $g = 4$). The instructor will also know these numbers, but that's okay.

    Step 2: You secretly choose a number a so that $1 \leq a < p$. Only you and no one else will know this number. Your group member does the same.

    Step 3: Compute the number $A = g^a \bmod p$. Tell your group member this number. The instructor will also know A, but that's okay. Your group member does the same.

    Step 4: You will receive a number B from your group member once they complete step 3. Compute $N = B^a \bmod p$. Your group member does the same.

    At the end, because we are just practicing, check that both you and your group member got the same secret number N.

20. Once you have mastered the above method, try to combine it with an encryption method. Using the fact that both you and your group member know a secret number that your instructor does not know, send a secret message that your group member can decrypt, but the instructor can't, even if the instructor overhears your encryption and decryption methods.

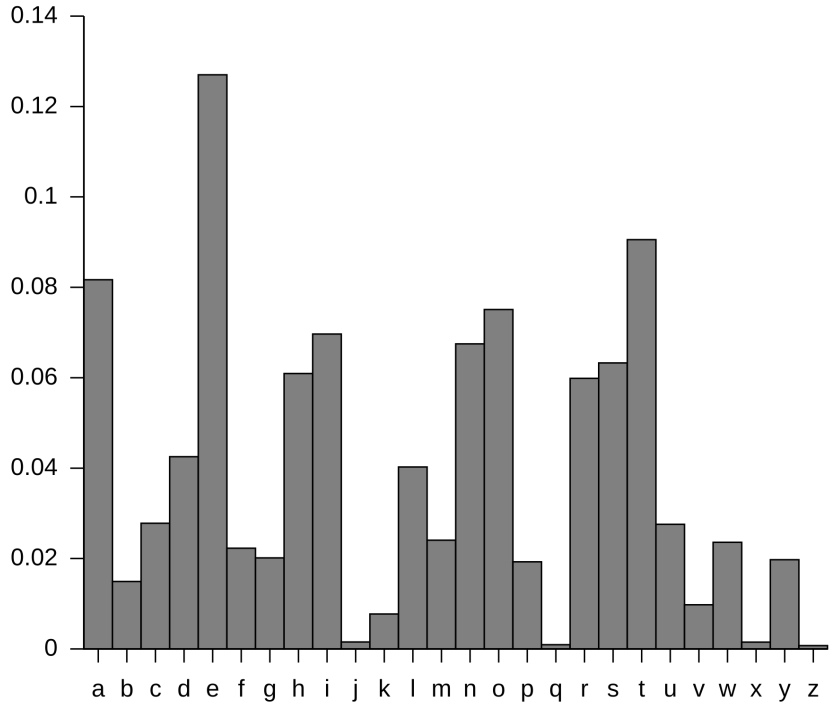
    This is called **Diffie Hellman** key exchange!

21. Why does the method in question 19 always result in both you and your group member getting the same number N?

22. Is it possible for the instructor to figure out your secret number N when using the prime number $p = 5$ in the method? What if $p = 101$?

4 Frequency Analysis

The following chart shows the typical distribution of letter use in the English language.



23. Use the chart (and knowledge of the English language) to decrypt the following secret message.

```
kpk x pkmb qbjfzhrbq k rwh ybjfbr nbyyklb spbfb bkjp gbrrbf

xy fkvqwngz yadyrxrarbq sxrp k qxccbfbvr gbrrbf
```