UW Math Circle

Week 15 – 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. Invent your own method of encrypting and decrypting messages. Once you have your method, you can test it by doing the following.

   (a) Describe how your method of decryption works on a piece of paper and pass that piece of paper to a classmate in your group.

   (b) Encrypt a message and copy down the encrypted message on two pieces of paper. Give one to the instructor in your group and one to your classmate.

   (c) If your encryption works well, your classmate will be able to decrypt the message you wrote down, but the instructor will not.

5. Let's review. 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) $1 = b \cdot 5 + r$.

6. 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.

7. Notice that $N = M$ in the above problem. Is this a coincidence?

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

Part 2

9. Find a classmate and practice the following method demonstrated at the board.

   Step 1: You and your classmate 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 classmate does the same.

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

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

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

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

11. Why does the method in question 9 always result in both you and your classmate getting the same number N?

12. 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 $p = 101$?

Bonus Questions

The secret messages below will still be of the form

THIS IS CALLED XXXXXXXXX

13. Decrypt the following secret message.

GSRH RH XZOOVW ZGYZHS

14. Decrypt the following secret message.

TILRFE HSSALDALEC ICEIN

15. You saw (or will see soon) in part 2 a way to send a secret message with a classmate that the instructor will not know, even if they overhear all messages between you. Can you invent your own encryption and decryption method that also does this?