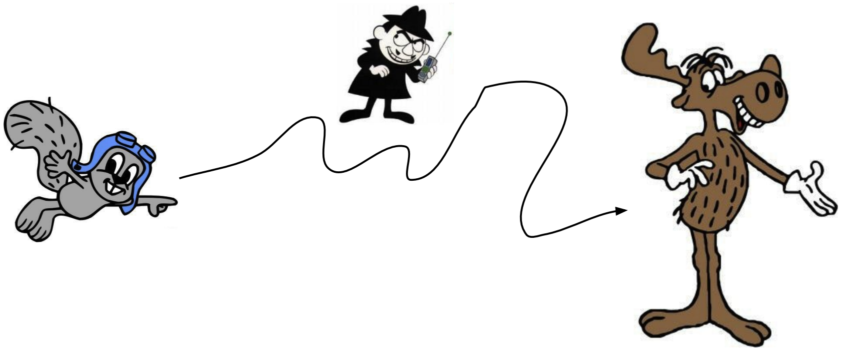
Math Circle - Encryption

Rocky has some secret information (let's call it a secret nonnegative number N) that he wants to share with his pal Bullwinkle. Rocky and Bullwinkle live thousands of miles from each other, so Rocky needs to send this secret to his friend. However, the spy Boris Badenov is constantly attempting to intercept Rocky's secret message.



In order to keep the information secret, Rocky has to somehow ENCRYPT his secret number. But Rocky also needs to make sure that Bullwinkle can DECRYPT the message and read it. Moreover, Boris is a pretty good spy, and so he'll probably get his eyes on the sent information at some point. So whatever encryption scheme Rocky uses, it needs to be something that Boris cannot decrypt without the proper knowledge.

To keep the analysis simple, let's say that Rocky's secret number N is less than 17. Rocky uses an encryption method E and sends Bullwinkle the number $E(N)$. Bullwinkle uses a decryption method D: if he receives the number M, he will decrypt it to the number $D(M)$. We want an encryption/decryption scheme so that $D(E(N)) = N$. *Why?*

What method should Rocky and Bullwinkle use to communicate?

1. Rocky picks an integer K between 1 and 16. Consider the two situations
(a) $E(N) = N + K \pmod{17}$.
(b) $E(N) = N \cdot K \pmod{17}$.

Answer the following questions for both of the two situations:

- Do you think it is possible to give an efficient (i.e. easy) decryption method D for Bullwinkle to use without him knowing the value of K?
- What is Bullwinkle's decryption plan D, assuming he knows the value of K?
- What problems need to be easy to solve in order for Bullwinkle to be able to easily decrypt $E(N)$?
- Can Bullwinkle obtain the value of K without Boris knowing what it is?
- What problems need to be difficult to solve in order for Boris to not be able to easily decrypt $E(N)$?

2. Bullwinkle picks an exponent e between 1 and 16 such that $\gcd(e, 16) = 1$. He tells Rocky (and hence Boris) this integer e. Rocky encrypts N with the encryption scheme

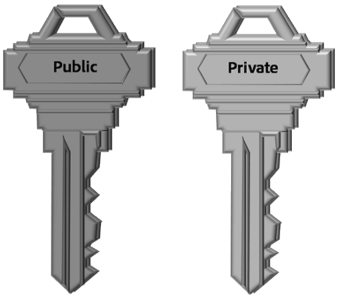
$$E(N) = N^e \pmod{17}.$$

Bullwinkle also knows some integer d such that $e \cdot d \equiv 1 \pmod{16}$, but he keeps this secret d to himself. Bullwinkle plans on decrypting with the scheme

$$D(M) = M^d \pmod{17}.$$

(a) Test this algorithm on a few different choices of exponent e to see if this will work — that is, check whether or not $D(E(N)) = N$.

(b) Will Boris be able to easily crack this encryption scheme without being explicitly told the secret d?



3. Rocky picks some personal *private key* S_R between 1 and 16. Bullwinkle does the same; call it S_B. These are two secret keys that the friends don't share with each other.

Rocky now calculates $P_R = 2^{S_R} \pmod{17}$ and tells Bullwinkle the value of P_R. This is Rocky's *public key*. Bullwinkle also tells Rocky his value of $P_B = 2^{S_B} \pmod{17}$. Boris now knows both public keys P_R and P_B.

Using his secret key, Rocky calculates his *private multiplier* $K_R = P_B^{S_R} \pmod{17}$; similarly, Bullwinkle calculates a private multiplier $K_B = P_R^{S_B} \pmod{17}$.

(a) Your team should create a private key and public key, just like Rocky does. Share your *public key* with another group, and obtain their public key, too. Create your *private multiplier* and compare it with the private multiplier of the other team. What happens?

(b) Prove that the phenomenon you observed in part (a) will always be the case.

(c) Will Boris be able to calculate either Rocky's or Bullwinkle's *private multiplier*?