MATH 4440
MISSION 3

AARON ALLEN, ANDREW BARBER, DANIEL KUMINKA,
MELANIE NUN, BHARADWAJ THIRUMAL

Task 1. Determine the final three digits of 2^{563}, using at most 15 multiplications, each of which is involves numbers of at most 3 digits.

Note, in $\mathbb{Z}/1000\mathbb{Z}$:

$$2^2 = 4, 2^{16} = 536, 2^{32} = 296, 2^{512} = 96.$$

Then,

$$2^{563} = 2^{512} \cdot 2^{32} \cdot 2^{16} \cdot 2^2 \cdot 2 = 96 \cdot 296 \cdot 536 \cdot 4 \cdot 2 = 808 \mod 1000.$$

So the last 3 digits of 2^{563} are 808

Task 2. Determine, as Alice, how to find A efficiently if you know k, a and p. Exhaustive search is NOT efficient. Use the Euclidean algorithm somehow, which IS efficient. Hint: the order of k modulo p is $p-1$ (this is a fact we'll study in class). Exactly which powers of k are $1 \mod p$?

For prime p where p does not divide k^a or a, find A such that

$$k^{aA} \equiv k \mod p,$$
$$k \cdot k^{aA-1} \equiv k \mod p,$$
$$k^{aA-1} \equiv 1 \mod p.$$

Then $aA - 1 \equiv 0 \mod p-1$ from Fermat's little theorem, so $aA \equiv 1 \mod p-1$. Hence, A is the inverse of a in $\mathbb{Z}/(p-1)\mathbb{Z}$, and $\gcd(a, p-1) = 1$. We can then solve for A by using the Euclidean algorithm on

$$Aa - q(p-1) = 1.$$

Task 3. Imagine now you are playing the role of Eve. Eve is the border guard suppose she can alter the messages that come through her border. Without knowing Alices key, how can she alter messages so that Bob deciphers whatever she wants, instead of Alices message? This is called a man-in-the-middle attack. Explain how it works on this system.

Since Eve controls the flow of information, we can retrieve the key, k. First, she intercepts k^a. Instead of passing k^a on to Bob, she instead modifies $(k^a)^e = k^{ae}$ where e is some element of $\mathbb{Z}/p\mathbb{Z}$ and sends it back to Alice. Alice thinks she's received k^{ab}, and so she replies with $(k^{ae})^A$. Since $A = a^{-1}$ Eve now has k^e. So now Eve passes k^e on to Bob. Bob thinks this is the k^a from Alice, so he sends back what he thinks is k^{ab}, but is actually k^{eb}. Eve takes $(k^{eb})^E$, then sends back k^b to Bob. Now Alice, Bob, and Eve all have the key, and Alice and Bob are none the wiser.

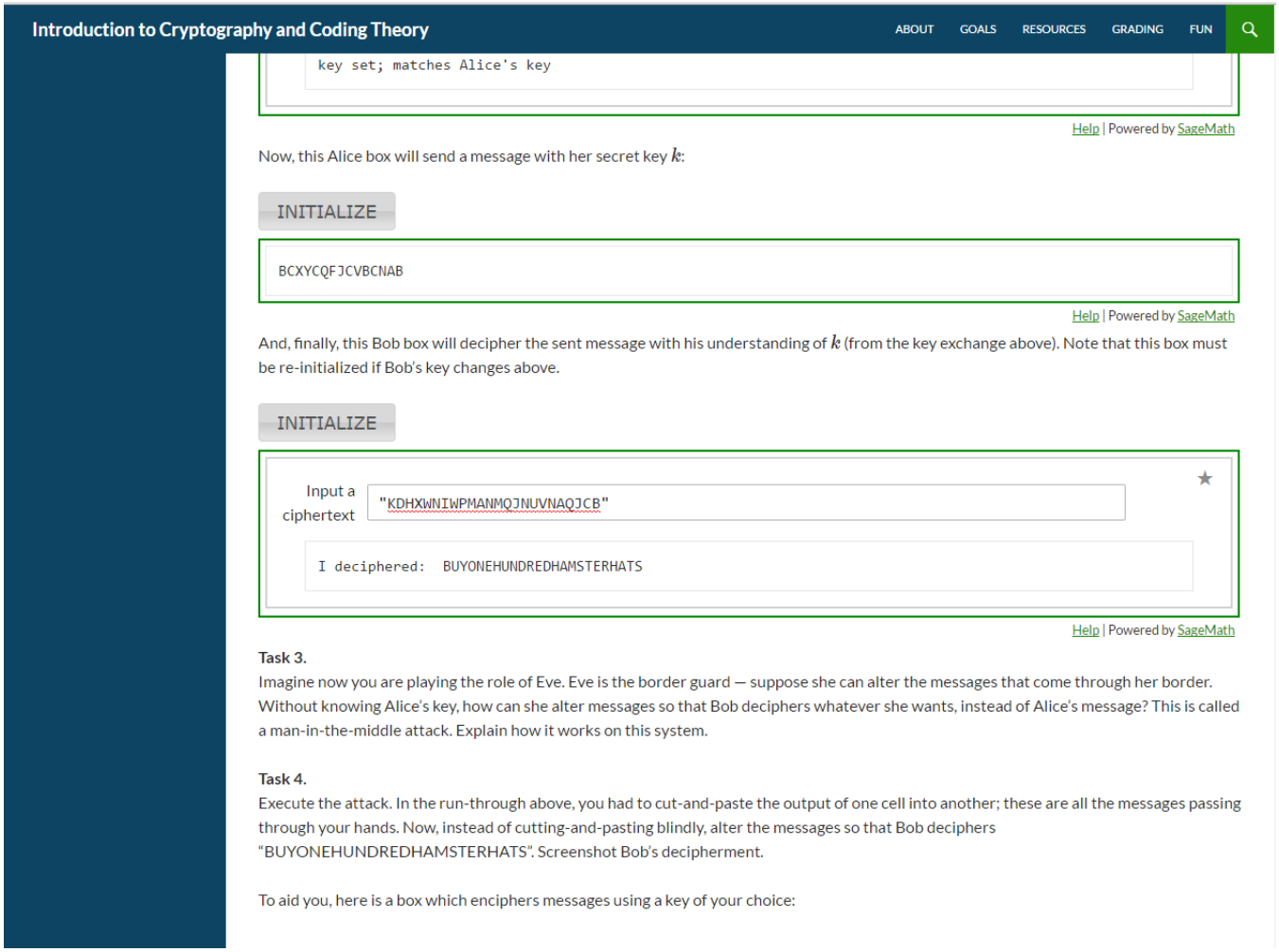

FIGURE 1. Screenshot of decipherment.

Task 4. Execute the attack. In the run-through above, you had to cut-and-paste the output of one cell into another; these are all the messages passing through your hands. Now, instead of cutting-and-pasting blindly, alter the messages so that Bob deciphers BUYONEHUNDRED-HAMSTERHATS. Screenshot Bobs decipherment.

Using $e = 7$ and $E = e^{-1} \mod (p-1) = 571428575$, we receive $k^a = 670900295$ from Alice. We send back to Alice $k^{ae} = 17570814$, then receive $k^{aeA} = k^e = 469712066$. Using E, we find $k^{eE} = k = 999999122$. We then send k^e over to Bob, who sends us back $k^{eb} = 948999362$. Again, we find $k^{ebE} = k^b = 194396212$. We send that back to him. We then intercept the original ciphertext and replace it with our ciphertext, which is "KDHXWNIWPMANMQJNUVNAQJCB". Bob gets the message, and buys way too many hats for hamsters.