A Challenge

A group of ducks has gone missing. The suspect is Beb (short for Bebediah), the less well-known brother of the world-famous Bob. The secretive Springfield-based Golden Duck Hunters are looking for a few good (i.e. brilliant and trustworthy) citizens to help find these ducks and restore order. Before joining such an important team, though, you must prove your mettle in a test situation during the week of May 16. No, there is no guarantee of an offer of employment at the end of the test; but yes, there might be swag (duck-themed, of course). And for the competition-minded, yes, the first team to complete the challenge will receive trophies.

As discussed earlier this week, you will need to complete an individual test from 3 to 3:50 pm on Monday. Some results from that test will be used in the team portion that follows for the remainder of the week. Naturally, there are some ground rules for the team-portion:

1. Be sure to be well-equipped for this challenging work. Your team will need a laptop with an internet connection (including in class on Wednesday). You will also need a pen or pencil and paper. You can quickly and easily get everywhere you need to go on foot. Bicycles, cars, camels, etc will not help.

2. Your whole team must be present at each step. One way to prove you were all there is to take a picture. Signatures next to each item on the sheet will also be viewed as acceptable verification that everyone was present for each step. Safety in numbers, folks! (On the off-chance that someone from your team defects or gets eaten by a lion, just report that as soon as possible. It will not be held against you. There is a willing volunteer standing by as a potential replacement, so that you are not short on brain power.)

3. Some items (which will be clearly marked) NEED to be completed between 3 and 3:50 pm on Wednesday. Aside from the hour in class on Wednesday, it will take approximately three hours (possibly much less) to complete the exercise. You may wait until Wednesday to start, but if your whole team agrees, you may start as early as 3:50 pm on Monday. In any case, the final results of your search are due by 3 pm on Friday via email to math458missingducks@gmail.com. Each team may submit ONE answer sheet total.

4. Your team may consult the internet, library books, your textbook, and your notes. You must cite any sources you use.

5. Under no circumstances may you talk to other teams about any items on this hunt.

6. Do NOT reveal any private information to the known spy, once you deduce who that is.

7. Do not reveal your sources to anyone except math458missingducks@gmail.com. You must cite all sources you used for your work in the document sent to math458missingducks@gmail.com. Of course, you also may not plagiarize. Golden Duck Hunters enforces the same exact guidelines and policies as the Student Conduct Code and your Math 458 class.

8. The trophies will go to the team whose submission is received at the earliest time via email. In the event that two complete answer sheets arrive at the same time, the answer will be decided by the questions marked "tie-breaker" (which are not otherwise a required part of the assignment). If your team is in a tie for first place, you will receive email notification that you should submit answers to the tie-breaker questions.

9. Failure to read or understand these ground rules will not be viewed as a valid reason to break them.

Questions that must be answered between 3 and 3:50 pm on Wednesday appear in **bold**. All others can be answered any time before 3 pm on Friday, although note that some questions require building access (as indicated clearly in the relevant problems). By the way, depending on your speed and schedule, you might encounter some of the missing ducks. Beware: Not surprisingly, Beb's associates might have disguised them (e.g. as clowns, trolls, cats, etc). If you encounter ducks in any form at a location, you can rescue (i.e. take) up to one duck per team member. Unless a question explicitly says it relies on a prior answer, it can be done independently of the other problems. (i.e. Many problems can be done in a different order than how they are listed here.) If you would like, you may use Sage code that was shared with the class; just say that you copy and pasted (or whatever you did). (You do not need to come up with code from scratch.)

1. To warm up your search-muscles, why not look for something pretty mundane: math. Some number theory related to your class (as well as some other math) is hidden (in plain sight!) in the design of a building on campus.

   (a) Use RSA (with $N = 1279566703335949188203$, $d = 558198387797099050675$) to decrypt the following message:
   [1234985303350878336389, 204508426892201937442]
   (Hint: For this and the next part, use the Sage code for the longer message example linked from Canvas, i.e. the example in which we broke the message into blocks and did not reverse the numbers.)

   (b) Optional: You will likely find the following url (encrypted in RSA with the same keys) very helpful completing the next several parts of this problem. (For an extra challenge, ignore this hint; but the rest of the items in this problem will quite possibly be too difficult without this extra information.)
   [189158269411362860133, 812383418481321652961, 1129181252448662472098, 927231835264695548067, 1085458558221591603608, 280107346119835725314, 1057569981208542929688, 855099876737034734449, 154129334433759102646, 986810685935160421163, 597921608809154141314]

   (c) Go to the first floor, and look at the tiles. What do they have to do with prime numbers? Which prime numbers appear in that pattern?

   (d) Go to the third floor, and look at the ceiling. What does this have to do with Euclidean algorithm? [Hint1: You will probably also need to do a google search, using information from the previous item. For example, see p.3 of this link on Hellman's (yes, *that* Hellman) webpage:
   `https://www-ee.stanford.edu/~hellman/pkc.pdf`.
   Hint2: "Golden"]

   (e) Now, go to the second floor, and look at the linoleum. What is there? Does this have anything to do with the *name* of the topic of our course for weeks 9 and 10?

   (f) Tie-breaker (not required): Does the pattern in the linoleum on the second floor have anything to do with the *topic* of our course for weeks 9 and 10?

   (g) Tie-breaker (not required): What math is hidden in the tiles of the bathrooms?

   Hint: If you're stuck, use google. Remember to cite your source(s)!

2. The prime numbers on the first floor of the building above were small. Going to the opposite extreme, what is the largest known prime number? (After all, we need large prime numbers for cryptography.) Read this article to find out: `http://www.slate.com/articles/health_and_science/science/2016/01/the_world_s_largest_prime_number_has_22_338_618_digits_here_s_why_you_should.html`.

3. These days, how large is it believed that a prime should be in order to be suitable for secure transmission of information via RSA or ElGamal? Remember to cite your source(s).

4. How long did it take researchers to factor a 232-digit number? Read this article to find out: `http://www.slate.com/articles/health_and_science/science/2013/06/online_credit_card_security_the_rsa_algorithm_prime_numbers_and_pierre_fermat.html`

5. It could take a while to check whether such large numbers are prime! What is an industrial grade prime? Look it up, and cite your source(s). Hint: Wikipedia has a nice, concise answer.

6. There's a book about mathematics and a family living in the same town as the secret Golden Duck Hunters (mentioned in the scavenger hunt instructions)...and there's supposedly a statue of the founder of that family's town on our campus. Maybe that book will give you a clue as to how Beb generates primes. Encrypted using the same RSA information as in the first question (i.e. with $N = 127956670333594918820 3$, $d = 558198387797099050675$), the call number of the book is

   [866417132569186659911, 669776021447247632247]

   (a) Find the book in the math library. Identify at least two types of primes from that book.

   (b) The author of that book wrote several other books, including one more directly relevant to this class. What is it?

   (c) In the library, find that book more directly relevant to this class. Go to p. 321. It talks about ducks (how appropriate!), but what is it *really* about? Just name the type of encryption it discusses. Come back to it later, if you want to learn more. (Several people mentioned they do want to learn about this topic, in the mid-quarter feedback collected in class.) [Tie-breaker (not required): Write more about this topic.]

   (d) What is the last word on the page in the previous item?

7. The word in the last item above was used to encrypt the following message using a *Vigenere cipher*. (Look it up, and use the attached table.)

   BQMB

   What does the message say?

8. **The answer to the previous item should remind you that you never solved that cipher from back on the second day of class. Come to the classroom, and solve it now. You may use google to try to figure out how the cipher works. (Hint: Try keyword "scytale.")**

9. Beb has hired a spy to spy on agents he thinks are after him. The spy's office is in Deady(!). (The NSA is the largest employer of mathematicians in the US. So maybe it's not that weird that Beb's spy is in a math department in Oregon...)

   Beb is not nearly as smart as Bob, but Beb is thorough. Beb encrypted the spy's office number using RSA with three different encryption constants.

$$e_1 = 35$$
$$e_2 = 15$$
$$e_3 = 21$$

and one modulus:

$$N = 115 = 5 * 23.$$

Decrypt the office number m, given that

$$\begin{aligned} m^{e_1} &\equiv 17 \mod N \\ m^{e_2} &\equiv 102 \mod N \\ m^{e_3} &\equiv 113 \mod N \end{aligned}$$

What is the spy's office number? (Hint: Do not use an encoding scheme here. Also, you will need to apply the extended Euclidean algorithm twice, for example by hand or using the xgcd function in Sage. For example, first u, v, d such that $u * 35 + v * 15 = d$ and then find u', v' such that $u' * d + v' * 21 = 1$...)

10. **Go to the spy's office. The spy doesn't just collect evidence. The spy also removes it. Tell the spy to give you tools for removing evidence, in case you make any miscalculations and need to remove signs of them. To get the spy to give them to you, you will need to exchange Diffie-Hellman keys with $g = 123456789$, $p = 161231938271320089919162941 67$. Your private key is the answer to Q4 lying between 1 and 100 on your test from Monday. Of course, don't give the spy your private key! Which number do you give spy? Which number S did the spy give you? What is your shared secret key with the spy (i.e. S raised to your secret key $\mod p$)?**

11. The spy gave Beb the same number S the spy gave you. In return, the not-so-bright Beb revealed his *private* key b to the spy. The numbers on the bottom of the implements the spy gives you are:

    white: Beb's private key b for ElGamal

    pink: $p = 161231938271320089919162941 67$

    yellow: $g = 123456789$

    The spy also scribbled a message to Beb on the piece of paper spy gave you. It was encrypted using that ElGamal input. Decrypt it. What does it say? (Note: Beb and the spy use an encoding scheme and reverse the numbers like in the ElGamal/DH Sage example linked from Canvas.) For convenience, the encrypted message is copied here:

    $$(1995, 14323509060614675511452999355)$$

    (i.e. $c_1 = 1995$, $c_2 = 14323509060614675511452999355$).

    (The long numbers p and g are the same as in the problem above, so you can copy them and paste them and don't risk making a mistake copying by hand.)

12. Beb slowly catches on the fact that somehow, his information has not been secure. He communicates with the spy, whom he has just begun to suspect might not be 100% loyal to him: "Did you reveal any of my information to anyone? Send (encrypted) 1 if the answer is 'yes.' Send (encrypted) 0 if the answer is 'no.' Use probablistic encryption with public key N from Question 8 of the in-class test from Monday (i.e. $N = 76591$), and use $a = 519$." The spy sends the following message:

    517

    Was the spy honest with Beb?

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y