Score: ________ Name: ______________________________

Project 3 - Cryptography

Math 1030Q – Fall 2014

Professor Hohn

Show all of your work! Write neatly. No credit will be given to unsupported answers. Projects are due *at the beginning of class.* Any project not collected by the instructor at the beginning of class is considered late (and will receive 0 points on the project). No late projects will be accepted!

Part 1: Vignere Ciphering

A Vignere cipher is a method of encrypting text by using a series of Caesar ciphers. The ciphers are set up based upon a key word. This cipher was formulated in the mid 15th century and used throughout the next 3 centuries (even used by the Confederate States of America in the Civil War). Here is the idea.
Suppose we use the key MATH and wanted to encrypt the message SURF'S UP DUDE. We set up our series of Caesar ciphers as follows:

Table 1: Vignere cipher with key MATH.

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
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
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
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
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

Plaintext: SURF SUPD UDE
Key: MATH MATH MAT
Ciphertext: EUKM EUIK GDX

The first encoded letter corresponds to the cipher created by the first letter of the keyword. So, encoding S is done by finding what S would correspond to on the Caesar cipher shifted such that A goes to M (M is the first letter in the keyword $MATH$). The second encoded letter corresponds to the cipher created by the second letter of the keyword. So, encoding U is done by finding what U would correspond to on the Caesar cipher shifted such that A goes to A (A is the second letter in the keyword $MATH$). The third encoded letter corresponds to the cipher created by the third letter of the keyword. So, encoding R is done by finding what R would correspond to on the Caesar cipher shifted such that A goes to T (T is the third letter in the keyword $MATH$). We continue encoding in this way until we are done.

1. Encrypt the message I AM GROOT using the key GUARDIAN. Show your work, including a table of the cipher used.

2. Knowing the key DISCRETEMATHROCKS, decode the message

   PILJ ZPEMFEKHTM CPXHKLU VMZLF ONA FT GFWUG XKMI IIAPEL.

   Show your work, including a table of the cipher used.

3. Look for a new cipher that was not talked about in class or on this sheet. In your own words, explain the cipher and how it works (cite your source of information). List at least one advantage and one disadvantage of using this cipher.

Part 2: Minion Messengers

Cruela Di Vil has a good idea of where the Group of Good is hiding out; she plans to stop them from retrieving the painting from the art gallery. To thwart her newest diabolical scheme, the group divides into two smaller subgroups that will each have their own hideout. In order to stay in contact with one another, the Group of Good decides to use RSA encryption to stay in touch. They publish to the world the encoding number e and the number n. Recall that each group will keep their secret decoding number d to themselves.

Group of Good: Subgroup 1 consists of Elroy, Wyldstyle (aka Lucy), and Megamind. Group of Good: Subgroup 2 consists of Merida, Batman, Lisa Simpson, and Kenny. All 9 of Gru's finest minions volunteer to transport messages between the groups. Subgroup 1 says openly that they will use $e = 5$ and $n = 11899$. Subgroup 2 says openly that they will use $e = 3$ and $n = 81997$.

4. Kenny of Subgroup 2 eagerly volunteers to write the first encoded message to Subgroup 1 consisting of the latitude and longitude of their new secret hideout. Sitting at the swivel chair and antique desk in their secret hideout, Kenny begins writing the code with his favorite mechanical pencil. Oh, no! The sharp pencil slips off the page and into his finger. His punctured finger is bleeding profusely and is unstoppable! Saddened by their colleague's sudden pencil death, Subgroup 2 has Batman encode the message

$$7699$$

which stands for $76°\text{N}, 99°\text{W}$, the location of their new hideout. What is Batman's encoded message? Show how to set up the problem. Then, using a computer (e.g. the website Wolfram Alpha) compute the encoded message. Cite the program that you used to compute the modular arithmetic. (Recall that Subgroup 2 is sending a message to Subgroup 1. Hence, Subgroup 2 must use the encoding numbers that Subgroup 1 has pronounced to the world to encode the message.)

5. Gru's finest minions deliver the message to Subgroup 1. Show how Subgroup 1 would decrypt the message using the secret number $d = 2333$. Show how to set up the problem. Then, using a computer, decode the message. Cite the program that you used to compute the modular arithmetic.

6. Subgroup 1 notices that Cruela's henchmen have be lurking outside their hideout. Subgroup 1 decides to relocate, so they send to Subgroup 2 their coordinates for the new hideout

   $$4212$$

   which stands for $42°\text{N}, 12°\text{E}$. What is the encoded message? Show how to set up the problem. Then, using a computer, compute the encoded message. Cite the program that you used to compute the modular arithmetic.

7. Gru's finest minions deliver the message to Subgroup 2. Show how Subgroup 2 would decrypt the message using the secret number $d = 54227$. Show how to set up the problem. Then, using a computer, compute the encoded message. Cite the program that you used to compute the modular arithmetic.