Assignment: Project 2
Name 1: Jonathan Smoley
Name 2: Samuel Sovi
GitHub Name: JT2M0L3Y

1. Suppose I am Germanicus and have intercepted an encrypted message from Caesar to the Roman Senate. I have no information message beyond the encrypted text that I have stolen from Caesar's courier. Which class of attack must I use to decrypt the message? We'll discuss these this week.

If Germanicus had more messages that were encrypted using the same encryption key and method, he could use a Cipher-Text Only attack. This is because he has access to multiple encrypted ciphertexts but has no additional information about the message. However, since only one message was intercepted, Germanicus has no choice but to use a Brute-Force attack where he tries every possible key until a key is found that works.

2. Describe the key exchange problem using the three characters who play a role in the description of ciphers (p. 8)

Bob, Alice, Mallory

Let's suppose that Bob wants to send a private message to Alice without it being read by anyone else. If Bob wants to encrypt the message, he must give Alice a key to decrypt it in some way. However, if Mallory wishes to read the message, Mallory may attempt to intercept the key. This poses an issue because 1) Mallory is now able to read the messages and 2) Mallory can substitute the key with another key to change the decryption of the messages that Alice is reading.

3. Bob and Alice beat the key exchange problem by using public key cryptography. Assuming that there is no public key infrastructure, what attack do they immediately face?

They can face some sort of man in the middle attack. This can be through public key substitution of a third party. Even if the public key is kept on a public server, requests to the server can be intercepted and altered.

4. Using ADFGVX as described in class, the permutation of A to Z and 0 to 9 shown on p. 17, and ENCRYPT as the second key, decrypt this cipher text: AVFFDDD ADVAXGF FXVXVGX. Show every step.

Decryption:
Organize the cipher text into a column for each letter in ENCRYPT alphabetically.

C	E	N	P	R	T	Y
A	F	D	V	G	X	V

V	D	A	A	F	V	G
F	D	D	X	F	X	X

Order columns into the word ENCRYPT.

E	N	C	R	Y	P	T
F	D	A	G	V	V	X
D	A	V	F	G	A	V
D	D	F	F	X	X	X

Take letter pairs, reading row-by-row, one letter for each axis in the ADFGVX matrix.

F	A	V	X	A	F	A	D	F
D	G	V	D	V	G	V	D	F

Parse ADFGVX Matrix from pg. 17 to find the plain text.

	A	D	F	G	V	X
A	F	L	1	A	O	2
D	J	D	W	3	G	U
F	C	I	Y	B	4	P
G	R	5	Q	8	V	E
V	6	K	7	Z	M	X
X	S	N	H	0	T	9

I AM NOBODY

5. The division algorithm is actually a theorem, though we didn't prove it. State the division algorithm theorem exactly as stated in class.

Division Algorithm

Given integers a, b with $b > 0$, there exists unique integers q, r satisfying $a = qb + r,\ 0 \leq r \leq b$
We say:

- q is the quotient
- b is the divisor
- r is the remainder

6. Using the division algorithm show that the cube of any integer is of the form 9k, 9K+1, or 9k+8

Let int $x = 3k$

$$x^3 = (3k)^3 = 9 * (3k^3) \equiv 0\, mod(9)$$

Now let int $x = 3k + 1$

$$x^3 = (3k + 1)^3 = 9(3k^3) + 9(3k^2) + 9k + 1 = 9(3k^3 + 3k^2 + k) + 1 \equiv 1\, mod(9)$$

Now let int $x = 3k + 2$

$$x^3 = (3k + 2)^3 = 9(3k^3) + 9(6k^2) + 9(4k) + 8 = 9(3k^3 + 6k^2 + 4k) + 8 \equiv 8\, mod(9)$$

Since all integers can be represented by either 3k, 3k + 1 or 3k + 2 (if k is in the set of integers), the cube of any integer is of the form 9k, 9k + 1 or 9k + 8.

7. Using the division algorithm, show that the square of any integer is of the form 3k or 3k+1

Let int $x = 3j$ where j is an integer

$$x^2 = (3j)^2 = 3(3j^2) \equiv 0\, mod(3)$$

Let int $x = 3j + 1$ where j is an integer

$$x^2 = (3j + 1)^2 = 3(3j^2 + 2j) + 1 \equiv 1\, mod(3)$$

Let $x = 3j + 2$

$$x^2 = (3j + 2)^2 = 3(3j^2 + 4j + 1) + 1 \equiv 1\, mod(3)$$

Since all integers can be represented by either 3j, 3j+1 or 3j + 2 (if j is in the set of integers), the square of any integer is of the form 3k or 3k + 1 and not 3k + 2

8. Using the result from problem 7, show that $3a^2 - 1$ is never a perfect square.

Let a be an integer. Then, a^2 must also be an integer, call it k, because the set of integers is closed under multiplication.

$k = a^2$

Then, $3a^2 - 1 = 3k - 1$

In the expression $3k - 1$, k can be written as a sum of 1 and some integer j (where $j = k - 1$)

So, $3(j + 1) - 1 \equiv 3j + 3 - 1 \equiv 3j + 2$.

By the result of problem 7, $3j + 2$ is not a perfect square.

Therefore, $3a^2 - 1$ is never a perfect square since $3j + 2 \equiv 3a^2 - 1$.

9. Using Euclid's algorithm and showing every step as a linear equation, compute the greatest common divisor of 482 and 1180.

Euclid's Algorithm:
$1180 = 2 * 482 + 216$
$482 = 2 * 216 + 50$
$216 = 4 * 50 + 16$
$50 = 3 * 16 + 2$
$16 = 8 * 2 + 0$

$gcd(482, 1180) = 2$

10. Let 482S + 1180T = gcd(482,1180). Solve for S and T using extended Euclid and showing every step as a linear equation.

Extended Euclid:
$2 = 50 - (3 * 16)$
$2 = (482 - 2 * 216) - (3 * 16)$
$2 = (482 - 2 * (1180 - 2 * 482)) - (3 * 16)$
$2 = (482 - 2 * 1180 + 4 * 482) - (3 * 16)$
$2 = (5 * 482 - 2 * 1180) - (3 * 16)$

$2 = (5 * 482 - 2 * 1180) - (3 * (216 - 4 * 50))$
$2 = (5 * 482 - 2 * 1180) - (3 * ((1180 - 2 * 482) - 4 * 50))$
$2 = (5 * 482 - 2 * 1180) - (3 * (1180 - 2 * 482)) + 12 * 50$
$2 = (5 * 482 - 2 * 1180 - 3 * 1180 + 6 * 482) + 12 * 50$
$2 = (11 * 482 - 5 * 1180) + 12 * 50$

$2 = (11 * 482 - 5 * 1180) + 12 * (482 - 2 * 216)$
$2 = (11 * 482 - 5 * 1180) + 12 * (482 - 2 * (1180 - 2 * 482))$
$2 = (11 * 482 - 5 * 1180) + 12 * (482 - 2 * 1180 + 4 * 482)$
$2 = (11 * 482 - 5 * 1180) + 12 * (5 * 482 - 2 * 1180)$
$2 = (11 * 482 - 5 * 1180 + 60 * 482 - 24 * 1180)$
$2 = 71 * 482 - 29 * 1180$

Answer:
$S = 71 \qquad T = (- 29)$