Zac Foteff

HW #2

1.) The class of attack one must use is a brute force attack. One must go through all 26 possible shifts in the Caesar Cipher until a readable message is uncovered.

2.) Bob and Alice would like to communicate securely in the face of an adversary, Eve. Despite all of Bob and Alice's efforts, Eve is still able to view their messages. In encrypting their messages however, Bob and Alice encounter an issue. Neither can outright send the key to decrypt future messages over normal channels, that would defeat the purpose of encryption because the pair broadcast that information to Eve. Therefore, the issue becomes about developing a secure way to encrypt their message, while also securely delivering the decryption key to the intended party.

3.) Bob and Alice immidiately become Vunerable to a man in the middle attack. Eve could intercept Bob's public key, send a message to Alice posing as Bob, and use this chanel to interfere with the pair's Communications

4.) $C =$ AVFFDDD ADVAXGF FXVXVGX

$K =$ Encrypt

$$\text{Rows} = \left\lfloor \frac{len(c)}{len(k)} \right\rfloor = \left\lfloor \frac{21}{7} \right\rfloor = 3$$

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

$\Rightarrow$

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

I A M N O B O D Y

row	F	A	V	X	A	F	A	D	F	X	X
col	D	G	V	D	V	G	V	D	F	X	X

$\Rightarrow$ **IAMNOBODY**

5.) The division algorithm: Given integers a, b, $b > 0$, there exists unique integers q, r such that: $a = qb + r$, $0 \leq r \leq b$

6.) Claim: The cube of any integer is of the form $9k$, $9k+1$, or $9k+8$ using the division algorithm.

Let $a = 9k + r$, $r \in \mathbb{Z}$, $0 \le r < 9$, every int. of the form $3q$, $3q+1$, $3q+2$

Suppose

$a_0 = 3q$

$a_1 = 3q+1$

$a_2 = 3q+2$

Case a_0

$$a_0 = 3q$$
$$a_0^3 = 27q^3$$
$$= 9(3q^3) \quad \text{Let } k = 3q^3$$
$$= 9k$$

Case a_1

$$a_1 = 3q+1$$
$$a_1^3 = 27q^3 + 27q^2 + 9 + 1$$
$$= 9(3q^3 + 3q^2 + 1) + 1$$
Let $k = 3q^3 + 3q^2 + 1$
$$= 9k + 1$$

Case a_2

$$a_2 = 3q+2$$
$$a_2^3 = 27q^3 + 45q^2 + 36q + 8$$
$$= 9(3q^3 + 5q^2 + 4q) + 8$$
Let $k = 3q^3 + 5q^2 + 4q$
$$= 9k + 8$$

Therefore, the cube of any integer is of the form $3q$, $3q+1$, $3q+2$

7.) Claim: The square of any integer is of the form $3k$ or $3k+1$ using the division algorithm

Every int of the form $3q$, $3q+1$, $3q+2$

Suppose

$$\boxed{\begin{aligned} a_0 &= 3q \\ a_1 &= 3q+1 \\ a_2 &= 3q+2 \end{aligned}}$$

Case $a_0 = 3q$

$$a_0^2 = 3q^2$$
$$= 9q^2 \quad \text{Let } k = 3q^2$$
$$= 3(3q^2) = 3k$$

Case $a_1 = 3q+1$

$$a_1^2 = 9q^2 + 6q + 1$$
$$= 3(3q^2 + 2q) + 1$$
Let $k = 3q^2 + 2q$
$$= 3k + 1$$

Case $a_2 = 3q+2$

$$a_2^2 = 9q^2 + 12q + 4$$
$$= 3(3q^2 + 4q + 1) + 1$$
Let $k = 3q^2 + 4q + 1$
$$= 3k + 1$$

8.) Claim $3a^2 - 1$ is never a perfect square

Let $k = a^2$

$X = 3K - 1$, we know this is impossible b/c of problem 7, were I have proved that the square of any number is of the form $3k$, or $3k+1$. Therefore, $3a^2 - 1$ is never a perfect square

9.) $\gcd(482, 1180)$

$1180 = 2(482) + 216$

$482 = 2(216) + 50$

$216 = 4(50) + 16$

$50 = 3(16) + 2$

$16 = 2(8) + 0 \quad \therefore \gcd(482, 1180) = 2$

10.) $482S + 1180T = \gcd(482, 1180)$, extended Euclid

$\gcd(x, y) = xS + yT$

$X = Y \cdot q_k + r_k \quad \Rightarrow \quad r_k = X - Y \cdot q_k$

$Y = r_k \cdot q_{k+1} \cdot r_{k+1} \quad\quad r_{k+1} = Y - r_k \cdot q_{k+1}$

$0 = 16 - 2 \cdot 8$

$2 = 50 - 3 \cdot 16 \Rightarrow$ GCD

$16 = 216 - 4 \cdot 50$

$50 = 482 - 2 \cdot 216$

$216 = 1180 - 2 \cdot 482$

$2 = 50 - 3 \cdot 16$

$2 = 50 - 3(216 - 4 \cdot 50)$

$2 = 13(50) - 3(216)$

$2 = 13(482 - 2 \cdot 216) - 3(216)$

$2 = 13(482) - 29(216)$

$2 = 13(482) - 29(1180 - 2(482))$

$\underbrace{2}_{\text{GCD}} = 71 \underbrace{(482)}_{X} - 29 \underbrace{(1180)}_{Y}$

$S = 71, \quad T = 29$