Project 2
Classic Techniques

Objectives

1. Practice with an interesting classic, symmetric key cipher
2. Explore the uses of the division algorithm

Tasks

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?

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

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.

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.

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

6. Using the division algorithm show that 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

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

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

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

Project Submission

Transform your LaTex (or very neatly written) work into a PDF file. Call it, project2.pdf Submit it using GitHub. The instructions can be found by following links from the class website.

GitHub Classroom Accept Link: https://classroom.github.com/a/tfS4MgGL

Project 2

1. Germanicus must use a cipher Text only Attack. See p.6 McAndrew

2. Bob and Alice wish to communicate using an algorithm requiring a secret key. To do so they must agree on a key. How do they agree on a key without making that key known to Eve who may be eavesdropping?

3. Bob and alice are vulnerable to the 'Eve in the middle attack' there are several scenarios but perhaps the most threatening is this:
   (1) Bob sends an encrypted message to Alice using her public key.
   (2) Eve intercepts the message. Using Alice's public key, she encrypts her own message and, pretending to be Bob, sends it to Alice

4. Decrypt
AVFVEDDD ADVAXGF FXVXV6X
using polybius square on p17
and ENCRYPT as Key 2

$$R = \left\lfloor \frac{len(c)}{len\,K_2} \right\rfloor = \left\lfloor \frac{21}{7} \right\rfloor = 3$$

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

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

Row F A V X A F A D F X X
Col D G V D V G V D F X X

I A M N O B O D Y

5. Division Algorithm Theorem

Given integers a, b with $b > 0$
$\exists$ unique integers q, r
Satisfying

$$a = qb + r \quad 0 \leq r < b$$

optimal q:
q is the quot
We say
q is the quotient
b is the divisor
r is the remainder

6. The Cubes of any integer has the form $9k, 9k+1, 9k+8$

D.I. Alg

Given integers a, b $b>0$

$\exists$ unique integers q, r

S.T.

$$a = qb + r \qquad 0 \le r < b$$

Let $a = 3b+0$ or

$3b+1$ or

$3b+2$

Consider

$a = 3q$

$$(3q)^3 = 27q^3 = 9(3q^3)$$

Let $k = 3q^3$. Since the integers are closed under mult., if q is an integer So is $3q^3$

$9(3q^3) = 9k$, desired form

Case 2

$a = 3q+1$

$(3q+1)^3 = 9(3q^3 + 3q^2 + q) + 1$

Let $k = 3q^3 + 3q^2 + q$

by the closure properties of integers k is an integer.

$(3q+1)^3 = 9k+1$, a desired form

Case 3

$a = 3q+2$

$(3q+2)^3 = 9(3q^3 + 6q^2 + 4q) + 8$

Let $k = 3q^3 + 6q^2 + 4q$

by the closure properties of integers, k is an integer

$(3q+2)^3 = 9k+8$, a desired form

7. The square of any integer is of the form $3k$ or $3k+1$

By the Div alg.
Given integers a, b $b>0$
$\exists$ unique integers q, r

S.T.
$a = qb + r \quad 0 \leq r < b$

Case 1

$a = 3q$

$a^2 = 9q^2 = 3(3q^2)$

Let $k = 3q^2$, an integer by the closure properties of integers

$a^2 = 3k$, the desired form

Case 2

$a = 3q+1$

$a^2 = 9q^2 + 6q + 1$

$= 3(3q^2+2q) + 1$

Let $k = 3q^2 + 2q$

$a^2 = 3k+1$, the desired form

Case 3

$a = 3q+2$

$a^2 = 9q^2 + 12q + 4$

$= 3(3q^2+4q+1) + 1$

Let $k = 3q^2 + 4q + 1$

$a^2 = 3k+1$, the desired form.

Since there are no other possibilities, the square of any integer is of the form $3k$ or $3k+1$

8 Show that $3a^2-1$ is never a perfect square

Let $K = a^2-1$, an integer by the closure properties of integers.

$$3a^2-1 = 3(a^2-1)+2$$
$$= 3K+2$$

By 7 all perfect squares are of the form $3K, 3K+1$

Since $3a^2-1$ can be rewritten as $3K+2$ it is never a perfect square

9. Compute gcd(482, 1180)
Show every step as a linear equation.

$1180 = 2 \cdot 482 + 216$

$482 = 2 \cdot 216 + 50$

$216 = 4 \cdot 50 + 16$

$50 = 3 \cdot 16 + 2$

$16 = 2 \cdot 8 + 0$

$\gcd(482, 1180) = 2$

10 $4825 + 1180 \quad \gcd(482, 1180) = 2$

$2 = 50 - 3 \cdot 16$

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

$= 50 - 3 \cdot 216 + 12 \cdot 50$

$= 13 \cdot 50 - 3 \cdot 216$

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

$= 13 \cdot 482 - 26 \cdot 216 - 3 \cdot 216$

$= 13 \cdot 482 - 29 \cdot 216$

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

$= 13 \cdot 482 + 58 \cdot 482 - 29 \cdot 1180$

$= 71 \cdot 482 - 29 \cdot 1180$

$S = 71 \quad T = -29$

$482 \cdot 71 - 29 \cdot 1180 = 34222 - 34220 = 2$