

MATH 470: Communications and Cryptography**Homework 1***Due date: 30 August 2023**Name: Huy Lai***Problem 1.** Decode the following Caesar cipher:

EREKK MIHSI WRSXP MIGLI EXSVW XIEPS VXSPI VEXIX LSWIA LSHS

Solution:A shift of the encoded message by 4 \leftarrow or by 22 \rightarrow would decode the message

ANAGG IEDOE SNOTL IECHE ATORS TEALO RTOLE RATET HOSEW HODO

This message can be further parsed into the following:

An Aggie does not lie cheat or steal or tolerate those who do

Problem 2. Encrypt the plaintext message using the substitution encryption table

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

Table 1: Simple substitution encryption table

Plain Text:

The gold is hidden in the garden

Solution:

“IBXFE PAQLB QAAXW QWIBX FSVAX W”

Problem 3. Let $a, b, c \in \mathbb{Z}$. Use the definition of divisibility to directly prove that if $a|b$ and $b|a$, then $a = \pm b$.

Solution:

Prove that if $a|b$ and $b|a$, then $a = \pm b$

Proof. By definition $\exists x, y \in \mathbb{Z}$ such that $a = bx$ and $b = ay$

$$a = bx \Rightarrow a = ayx$$

Dividing both sides by a results in:

$$1 = yx$$

Since both x and y are integers and their product is 1, $x = y = \pm 1$

Using this result in the equation for a gives:

$$a = \pm b$$

□

Problem 4. Use the Euclidean algorithm to compute the greatest common divisor of 291 and 252.

Solution:

$$\gcd(291, 252)$$

$$292 = 1 * 252 + 40$$

$$252 = 6 * 40 + 12$$

$$40 = 3 * 12 + 4$$

$$12 = 3 * 4 + 0$$

$$\gcd(291, 252) = 3$$

Problem 5. Let a and b be positive integers.

Subproblem 1. Suppose that there are integers u and v satisfying $au + bv = 1$. Prove that $\gcd(a, b) = 1$.

Solution:

Prove that $\gcd(a, b) = 1$.

Proof. Suppose that there are integers u and v satisfying $au + bv = 1$. Prove that $\gcd(a, b) = 1$

Let $g = \gcd(a, b)$. Then $\exists x, y \in \mathbb{Z}$ such that $a = gx \wedge b = gy$

Substituting this into the given equation $au + bv = 1$ results in:

$$1 = au + bv = gxu + gyv = g(xu + yv)$$

$$u, v, x, y \in \mathbb{Z} \rightarrow (xu + yv) \in \mathbb{Z}$$

As a result of the previous statement:

$$g|1$$

This requires that $g = 1$. □

Subproblem 2. Suppose that there are integers u and v satisfying $au + bv = 6$. Is it necessarily true that $\gcd(a, b) = 6$? If not, give a specific counterexample, and describe in general all of the possible values of $\gcd(a, b)$?

Solution:

$au + bv = 6$ does not imply that $\gcd(a, b) = 6$.

Counterexample: $a = 3, b = 2$

$$a \cdot (6) + b \cdot (-6) = 6$$

but $\gcd(a, b) = 1$

In general, if $au + bv = c$ has a solution, then $\gcd(a, b) | c$.

Let $g = \gcd(a, b)$. Divide c by g with remainder r such that

$$c = gq + r \text{ with } 0 \leq r < g$$

We know that we can find a solution to $g = ax + by$, so we get

$$au + bv = c = gq + r = (ax + by)q + r$$

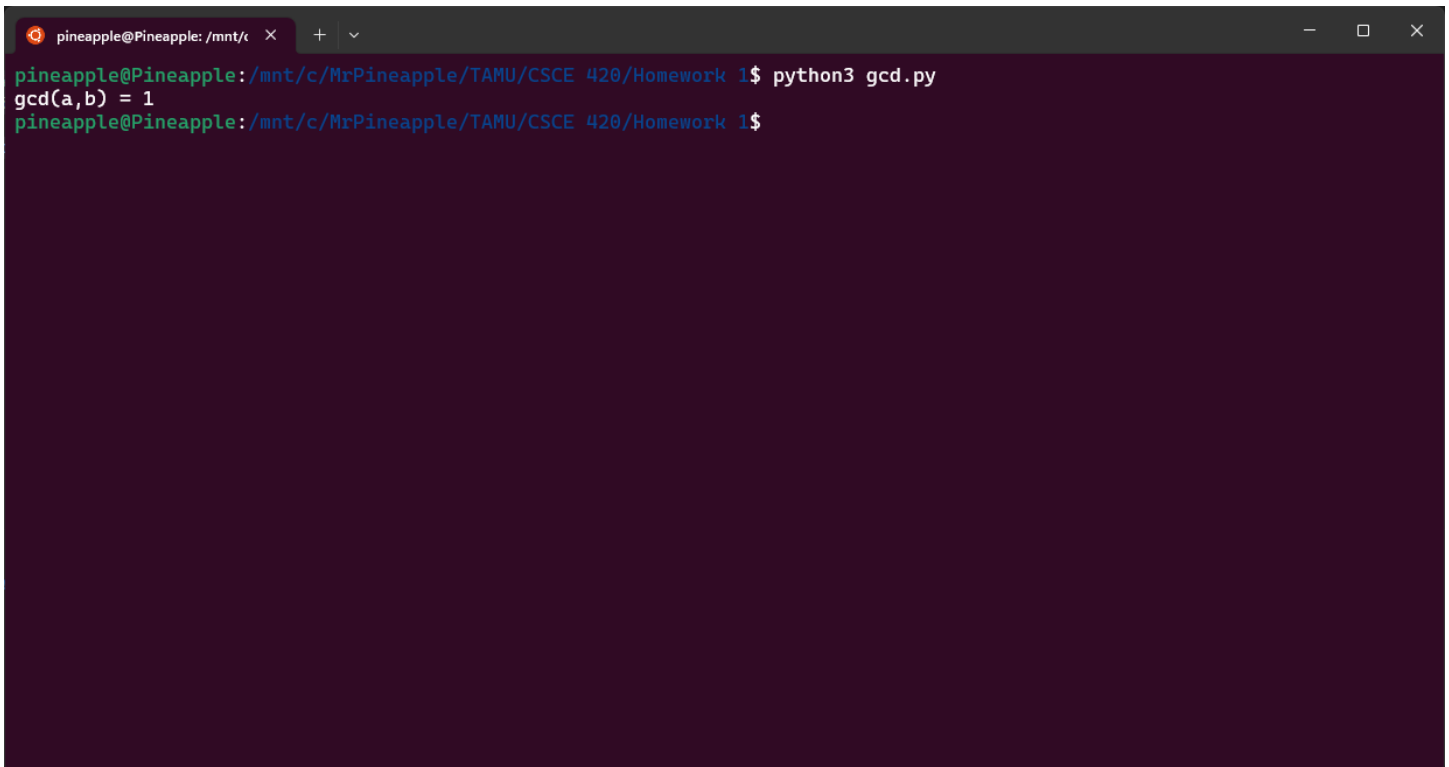
Rearranging this statement results in:

$$a(u - xq) + b(v - yq) = r$$

The left hand side is divisible by g since $\gcd(a, b) = g$. Therefore, $g|r$. But the only r that can satisfy both $0 \leq r < g$ and $g|r$ is $r = 0$. This results in $c = gq$. This implies that $\gcd(a, b) | c$

Solution:

$$b = 23456789012345678901234567890123456789012345678901234567890123456789$$



```
pineapple@Pineapple: /mnt/c  x + | v
pineapple@Pineapple:/mnt/c/MrPineapple/TAMU/CSCE 428/Homework 1$ python3 gcd.py
gcd(a,b) = 1
pineapple@Pineapple:/mnt/c/MrPineapple/TAMU/CSCE 428/Homework 1$
```

Figure 1: Output of the Code