55 | 55

Kenneth Jahnke

Assignment 3 – 02 Feb 2025 (Due date extension approved)

CSCI 389 (Online) - Spring 2025

3.1.a.

No, there are no restrictions on the value of `b`. `b` shifts the result of `ap` by any value from 0 to 25 (inclusive). Since the value of `b` does not affect whether the algorithm is one-to-one, there are no restrictions.

3.1.b.

Values of `a` where `gcd(a, 26) = 1`:

1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25

Therefore, the values of `a` that are not allowed:

2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24, 26

10|10

3.1.c.

The values of `a` that are not allowed are those values that are not coprime to 26, that is, those values where $\gcd(a, 26) \neq 1$, namely, multiples of 2 and 13. Those values of `a` that are allowed are those that are coprime to 26, that is, those values where $\gcd(a, 26) = 1$. Justification by example:

$p = 2$

$b = 3$

If $a = 2$, then:

$C = (ap + b) \bmod 26 = (2 \cdot 2 + 3) \bmod 26 = 7 \bmod 26 = 7$

If $a = 15$, then:

$C = (ap + b) \bmod 26 = (15 \cdot 2 + 3) \bmod 26 = 33 \bmod 26 = 7$

While both $a = 2$ and $a = 15$ equate to $C = 7$, only the $a = 15$ equation is valid because $\gcd(15, 26) = 1$, thus 15 has an inverse modulo 26, hence decryption is possible.

3.2.

Equation: C = (ap + b) mod 26

5|5 Number of possible values for a: 12

Number of possible values for b: 26

12 • 26 = 312

Number of one-to-one affine Caesar ciphers (assuming 26 letter alphabet): 312

3.3.

Using Figure 3.5 from the textbook, we know that “E” is the most common letter and “T” is the second most common letter. Thus, encryption likely transforms “E” to “B”, and “T” to “U”. In terms of numerical values, 4 transforms to 1, and 19 transforms to 20.

$C = (ap + b) \bmod 26$

$1 = (a \cdot 4 + b) \bmod 26$

$20 = (a \cdot 19 + b) \bmod 26$

$4a + b \equiv 1 \bmod 26$

$19a + b \equiv 20 \bmod 26$

$(19a + b) - (4a + b) \equiv (20 - 1) \bmod 26$

$19a + b - 4a - b \equiv 19 \bmod 26$

$15a \equiv 19 \bmod 26$

`a` is equal to `x` where $15x + 26y = 1$

$26 = 1 \cdot 15 + 11$

$15 = 1 \cdot 11 + 4$

$11 = 2 \cdot 4 + 3$

$4 = 1 \cdot 3 + 1$

$3 = 3 \cdot 1 + 0$

$4 - 1(3) = 1$

$4 - 1(11 - 2(4)) = 1$

$4 - 11 + 8 = 1$

$12 - 11 = 1$

$3(4) - 1(11) = 1$

$3(15 - 1(11)) - 1(11) = 1$

$3(15) - 3(11) - 1(11) = 1$

$3(15) - 4(11) = 1$

$3(15) - 4(26 - 1(15)) = 1$

$3(15) - 4(26) + 4(15) = 1$

$7(15) - 4(26) = 1$

modular inverse 15 mod 26 --> 7

$15^{(-1)} \equiv 7 \mod 26$

$15a \equiv 19 \mod 26$

$a \equiv (19 \cdot 7) \mod 26$

$a \equiv 133 \mod 26$

$a \equiv 3 \mod 26$

$a = 3$

$19a + b \equiv 20 \bmod 26$

$19(3) + b \equiv 20 \bmod 26$

10\10 $57 + b \equiv 20 \bmod 26$

$b \equiv (20 - 57) \bmod 26$

$b \equiv -37 \bmod 26$

$b \equiv -11 \bmod 26$

$b \equiv 15 \bmod 26$

$b = 15$

$C = (ap + b) \bmod 26$

$(C - b) \equiv ap \bmod 26$

$a^{(-1)} (C - b) \equiv ap \cdot a^{(-1)} \bmod 26$

$a^{(-1)} (C - b) \equiv p \bmod 26$

$p = a^{(-1)} (C - b) \bmod 26$ <-- Use this formula to decrypt

$p = 7(C - 15) \bmod 26$ <-- The formula using known values

3.10.a.

10|10

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

3.10.b.

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

Given each letter is represented in the matrix only once, it is reasonable (dare I say logical) to assume that a letter of the within the matrix is passed over.

3.11.a.

MU → UZ

ST → TB

SE → DL

EY → GZ

OU → PN

OV → NW

ER → LG

CA → TG

DO → TU

GA → ER

NW → OV

ES → LD

TC → BD

10/10

OM → UH

IN → FP

GA → ER

TO → HW

NC → QS

E(X) → RZ

Full:

UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ

3.19.

e/l → p

x/e → b

p/g → v

l/l → w

a/e → e

n/g → t

a/l → l

t/e → x

10|10 i/g → o

o/l → z

n/e → r

Full:

pbvwetlxozr