Problem 1: shift cipher

SEOYKJOEJ $\Longrightarrow$ our ciphertext

18 4 14 24 10 9 14 4 9

$$e_k(x) = x + k \mod N$$

encryption function

One approach:

brute force attack

we only have 26 possible keys – test all of them

eventually get to $k=22$ $\longrightarrow$ decrypt with $d_k(y) = y - k \mod N$

then plaintext reads $\boxed{\text{WISCONSIN}}$

See Matlab/Python script

Problem 2

Proving a function is injective:

in a general case, a function F is injective (one-to-one) if:

$\forall x, u \in A,\ F(x) = F(u)$ (or equivalently: $x = u$)

"for all"

For a shift cipher: $e(k,x) = x + k \bmod 26$ (fixed choice for x)

Our claim: $e(k,x)$ is injective with respect to k

Proof: Fix any x in $\mathbb{Z}_{26}$ s.t. $e(k_1,x) = e(k_2,x)$ i.e. $x=5$

$$\cancel{5} + k_1 = \cancel{5} + k_2 \implies k_1 = k_2$$

Proving a function is NOT injective: (general case)

show two elements $x, u \in A$ s.t. $F(x) = F(u)$, $x \neq u$

For the quiz question, you were asked what would happen if the shift cipher were not injective. Three laws were given:

1. $x \otimes 1 = x$
2. $x \oplus 0 = x$
3. $x \ominus x = 0$ – we claim $e(k,x)$ is not injective w.r.t. k, implying $k_1 \neq k_2$.

Let's say: $e(k_1,x) = e(k_2,x)$, but $k_1 \neq k_2$, i.e. $k_1 = 5$, $k_2 = 3$

$x + 5 \stackrel{?}{=} x + 3 \longleftarrow$ notice for $k_1 \neq k_2$ we cannot fix x.

this violates 3

Problem 3

$e_k(x) = 3x + 1$

P A C K E R S

15 0 2 10 4 17 18

$\Downarrow$

$\boxed{\text{U B H F N A D}}$

20 1 7 5 13 0 3

$d_k(y) = a' \cdot y + b'$

to satisfy $d_k(e_k(x)) = x$: $a' \cdot a = 1$

$b' = -a' \cdot b$

$3(a') \bmod 26 = 1 \longrightarrow$ find multiplicative inverse

we know $27 \bmod 26 = 1 \longrightarrow a' = 9$

$b' = -9 \cdot 1 = -9$

$$\boxed{d_k(y) = 9y - 9}$$

Problem 4:

$$B \quad C \longrightarrow A \quad D$$

$$1 \quad 2 \qquad\quad 0 \quad 3$$

$e_k(x) = ax + b$

$0 = a + b$

$3 = 2a + b$

Solve for $e_k(x)$ as system

$a = 3$

$0 = 3 + b \longrightarrow b = -3$

(or in $\mathbb{Z}_{26}$: 23)

$\boxed{e_k(x) = 3x + 23}$

Problem 5:

$f(x) = 3x + 1$

$g(x) = 5x + 2$

f(g(x)) is just another affine cipher. not really a benefit...

$$f(g(x)) = 3(5x+2)+1$$

$$= 15x + 6 + 1 = \boxed{15x+7}$$

$$Z_N^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

note: integers in Z_N^* are <u>relatively prime to N</u>

for $N = 26$, multiples of 2 and 13 are excluded

multiplication w/ integers in Z_N^* always yields an integer in Z_N^*