Gary Hobson
MAT 260
Southern New Hampshire University
May 4, 2025

2)

A shift cipher encrypts by applying a Caesar shift:

$$E(x) = (x + k) \mod 26,$$

and decryption reverses this

$$D(y) = (y - k) \mod 26.$$

Since the key k is unknown, we brute-force all 25 non-trivial shifts and identify valid English words.

For the ciphertext ZOMCIH:

- Shift by 11 $\rightarrow$ OLIVES
- Shift by 13 $\rightarrow$ NIGHTY

For the ciphertext ZKNGZR:

- Shift by 6 $\rightarrow$ TIGERS
- Shift by 19 $\rightarrow$ ALMOND

4)

$$D(y) = a^{-1}(y - b) \mod 26$$

where $a = 9$, $b = 1$, and a^{-1} is the modular inverse of 9 modulo 26. Since $\gcd(9, 26) = 1$, an inverse exists. Testing small values, we find:

$$9 \cdot 3 = 27 \equiv 1 \mod 26 \quad \Rightarrow \quad a^{-1} = 3$$

Now apply the decryption formula to each letter:

- J $\to$ 9: $D(9) = 3(9 - 1) = 3 \cdot 8 = 24 \mod 26 = 24 \to$ Y
- L $\to$ 11: $D(11) = 3(11 - 1) = 3 \cdot 10 = 30 \mod 26 = 4 \to$ E
- H $\to$ 7: $D(7) = 3(7 - 1) = 3 \cdot 6 = 18 \mod 26 = 18 \to$ S

Plaintext: YES

31)

part 1

If Eve can try 2^{64} keys per day, then the time to exhaust the full keyspace is:

$$\frac{2^{128}}{2^{64}} = 2^{64} \text{ days}$$

$$= 18,446,744,073,709,551,616 \text{ days}$$

part 2

If Alice waits 10 years and then uses a computer 100 times faster, her new rate becomes:

$$2^{64} \times 100 = 2^{64} \times 10^2 \text{ keys per day.}$$

However, even waiting 3650 days this rate will finish sooner that using a slower computer.

$$\frac{2^{128}}{2^{64} \cdot 10^2} = \frac{2^{64}}{10^2} + 3650 \text{ days}$$

$$= 184,467,440,737,099,166 \text{ days}$$

This duration is not as long. It would be faster to buy in 10 years that it would be to start now with a slower computer.