Lab 8

CS 135

Problem 1

Callie wants to send the message M = 13 to Alice. Using Alice's public and private keys, calculate the ciphertext C, and the value for R when Alice recovers the message.

Encryption/Decryption Setup:

Alice's Setup:

- Choose 2 prime numbers (11, 3)
- Calculate the product n=pq
- Calculate m=(p-1)(q-1)
- Choose numbers e and d so that ed has a remainder of 1 when divided by m
- Publish her public key (n, e)

XYZ encrypts a message M for Alice:

- Finds Alice's public key (n, e)
- Finds the remainder C when M^e is divided by n
- Sends ciphertext C to Alice

Alice receives and decrypts ciphertext C:

- Uses her private key (n, d)
- finds remainder R when C^d is divided by n.
- R matches the message M that XYZ wanted to send to Alice.

Problem 1 Answer

Callie encrypts message M = 13:

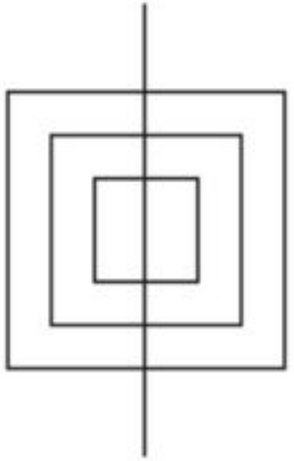
- Alice's public key is (n, e) = (33, 3) (e is 3, d is 7)
- When $M^e = 13^3 = 2197$ is divided by 33, the remainder is C = 19
- Callie sends the ciphertext C = 19 to Alice

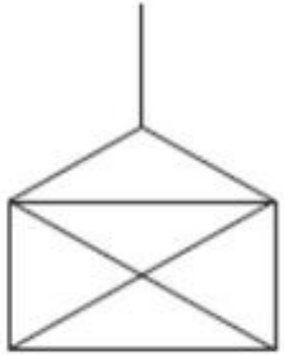
Alice receives and decrypts ciphertext **C = 19**:

- Alice uses her private key (n, d) = (33, 7)
- When $19^7 = 893, 871, 739$ is divided by 33, the remainder R = 13
- **R = 13 = M**, aka the OG message

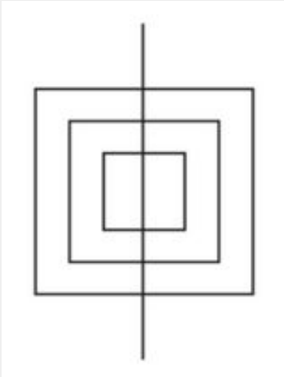
Problem 2

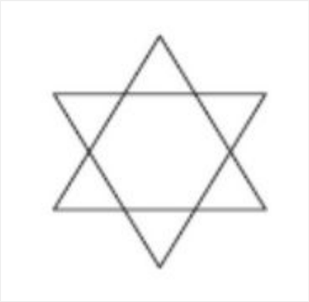
Determine whether each of the following figures can be drawn in one continuous motion without lifting the pencil or retracing any part of the drawing. Explain your reasoning (Hint: think about vertex degrees!)

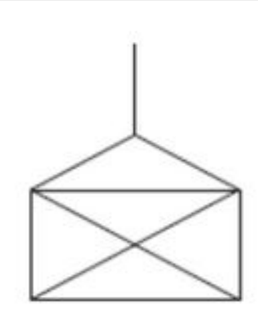




Problem 2 Answer







Condition: The drawing must have 0 or 2 vertices with odd degree.

RACKET TIME