The ElGamal Signature Scheme

The ElGamal Signature Scheme is a protocol for digitally signing a message. There are two participants named Alice and Bob. Alice sets up the protocol, creates the message, signs it, and sends the signature to Bob. Bob uses the signature to verify the signature.

1. Alice picks three numbers, and constructs a fourth:
   - A large prime \( p \).
   - An integer \( \alpha \in \{2, \ldots, p - 2\} \) that is a primitive root mod \( p \).
   - A secret random integer \( a \in \{2, \ldots, p - 2\} \)
   - The integer \( \beta \) defined by \( \beta \equiv p^a \mod p \).

2. Alice publishes the triple \((p, \alpha, \beta)\) and keeps the integer \( a \) secret.

3. To sign a message \( m \), Alice:
   - Chooses a secret random integer \( k \in \{2, \ldots, p - 2\} \) such that \((k, p - 1) = 1\).
   - Computes \( r \equiv \alpha^k \mod p \).
   - Computes \( s \equiv k^{-1}(m - ar) \mod p - 1 \).
   - Sends Bob the signature \((m, r, s)\).

4. To verify a signature, Bob:
   - Downloads the public information \((p, \alpha, \beta)\) and the signature \((m, r, s)\).
   - Computes two numbers, namely
     - \( v_1 \equiv \beta^r r^s \mod p \), and
     - \( v_2 \equiv \alpha^m \mod p \).
   - If \( v_1 \equiv v_2 \mod p \), signature is VERIFIED.
   - If \( v_1 \not\equiv v_2 \mod p \), signature is NOT VERIFIED.

Practice Exercise 1. Execute both signing and verification algorithms for signing the message \( m = 314 \mod p = 457 \). Show all the steps (this includes finding a primitive root mod \( p \)).

Practice Exercise 2. Execute both signing and verification algorithms for signing the message \( m = 1776 \mod p = 3361 \). Show all the steps (this includes finding a primitive root mod \( p \)).