Mandatory Problem 3: Digital Signature Algorithm and Discrete Logarithms

The deadline is Monday, November 1, midnight. You have to hand in a short description of the algorithms you implemented, the implementation code as a collection of subroutines (functions), and computational results.

1. Let the parameters of ElGamal Signature Algorithm be

$$\begin{aligned} p &= 274742860459763, \\ g &= 5, \end{aligned}$$

   where p is prime and g is a primitive root modulo p. Let $x \mod p-1$ be a system private key and $y \equiv 5^x \mod p$ be the system public key, where $y = 262274678376340$.

   Forge an ElGamal signature without knowledge of the private key, by constructing a triple m, a, b, where m is an integer and a, b is its signature.

2. Let the parameters of DSA(Digital Signature Algorithm) be

$$\begin{aligned} p &= 39866254172498138\,09, \\ q &= 19928344283621, \\ g &= 28900265122656260\,20, \end{aligned}$$

   where p, q are primes, $q|p-1$ and g is a residue modulo p of order q. Let $x \mod q$ be a system private key and

$$y \equiv g^x \mod p \tag{1}$$

   be the system public key, where

$$y = 1621561995432343084.$$

   (a) Let

$$m_1 = 1115209791959069177061830, m_2 = 2151657259407048953791701$$

be two messages(hash values) encoded by integers and their DSA signatures

$$111520979195906917706183 0, 12880312906177, 14706957637905$$
$$215165725940704895379170 1, 12880312906177, 16242187205965.$$

Find the DSA private key x.

(b) Compute the DSA private key x by solving the discrete logarithm problem (1) with ρ-method by Pollard.

3. The integer 2 is a primitive root modulo $p = 2599739$. Compute $x \mod p-1$ such that

$$2^x \equiv 1629414 \mod p$$

with the Index Calculus Algorithm, take smoothness bound $B = 30$.