0.1 ECDSA Signature Scheme

- Public Parameters:A cyclic group G of prime order q, a generator g, a hash function $H : \{0,1\}^* \to Z_q$, a hash function $H' : G \to Z_q$
- KeyGen(λ): It takes security parameter λ as input, outputs a private key $sk : x$, which is a random number in Z_q, and a public key $pk : y = g^x \in G$.
- Sign(M, sk): It takes the message M and secret key as input, and generate the signature by the performing the following steps.
  1. Compute $m = H(M) \in Z_q$;
  2. Randomly choose a number $k \in Z_q$;
  3. Compute $R = g^{k^{-1}}, r = H'(R) \in Z_q$;
  4. Compute $s = k(m + xr) mod q$
  5. Output the signature as $\sigma = (r, s)$
- Verify(σ, M, pk): It takes M, σ, pk as input, verify the signature as follows:
  1. Check whether $r, s \in Z_q$ or not;
  2. Compute $R' = g^{ms^{-1} mod q} y^{rs^{-1} mod q}$;
  3. Check whether $H'(R') = r$ or not. Outputs $true$ if the equation holds, otherwise outputs $false$.
- Correctness:$R' = g^{ms^{-1} mod q} g^{xrs^{-1}} = g^{(m+xr)s^{-1}} = g^{k^{-1}} = R$. Hence, $H'(R') = r$