Cryptography

Problem set 2

Definition [Primitive root] Let p be a prime. A generator g of he cyclic group $\mathbb{Z}_p^*$ is called a *primitive root* of $\mathbb{Z}_p^*$ or a *primitive root modulo* p.

Definition [Legendre symbol] Let p be a prime >2, and let $x \in \mathbb{Z}$ be prime to p.

$$\left(\frac{x}{p}\right) := \begin{cases} 1 & \texttt{if } x \texttt{ is a quadratic residue modulo } p \texttt{ and } x \neq 0 \bmod p \\ \text{-1} & \texttt{if } x \texttt{ is a non quadratic residue modulo p} \\ 0 & \texttt{if } x = 0 \bmod p \end{cases}$$

1. Let p be a large prime, such that $q := (p-1)/2$ is also prime. Let $\mathcal{G}$ be a subgroup of order q in $\mathbb{Z}_p^*$. Let g and h be randomly chosen generators in $\mathcal{G}$. We assume that it is infeasible to compute discrete logarithms in $\mathcal{G}$. Show that

   $$f : \{0, \ldots, q-1\}^2 \to \mathcal{G}, f(x,y) := g^x h^y$$

   can be used to obtain a collision-resistant compression function.
2. Prove the following lemma. Let p be a prime. Then $x \in \mathbb{Z}_p^*$ is a primitive root if and only if $x^{(p-1)/q} \neq 1 \bmod p$ for every prime q which divides $p-1$.

   How can one use this property to generate keys of *e.g.,* ElGamal cryptosystem?
3. Prove Euler's criterion: Let p be a prime > 2, and let $x \in \mathbb{Z}$. Then

   $$\left(\frac{x}{p}\right) \equiv x^{(p-1)/2} \bmod p.$$

4. Use Euler's criterion for proving correctness and expected running time of the algorithm for for computing square roots modulo prime.
5. Prove that the hardness of the Computational Diffie-Helman (CDH) problem relative to $\mathcal{G}$ implies the hardness of the discrete logarithm problem relative to $\mathcal{G}$.
6. Prove that the hardness of the Decisional Diffie-Helman (DDH) problem relative to $\mathcal{G}$ implies the hardness of the Computational Diffie-Hellman problem (CDH) relative to $\mathcal{G}$.
7. Prove that the DDH problem is not hard in $\mathbb{Z}_p^*$. Hint: use the fact that quadratic residuosity can be decided efficiently modulo a prime.
8. Alice receives the ElGamal ciphertext $c = (30, 7)$, her public key is $(p = 43, g = 3)$. Determine the corresponding plaintext.
9. How can two ElGamal ciphertexts be used to generate a third ElGamal ciphertext of an unknown plaintext? How can this attack be prevented?
10. Let $n = 122351821$ be a Rabin modulus and let $c = 67625338$ be a ciphertext that is obtained by Rabin encryption using this modulus. Determine all possible plaintexts.
11. Consider a "textbook Rabin" encryption scheme in which a message $m \in \mathcal{QR}_N$ is encrypted relative to a public key N (where N is a Blum integer) by computing the ciphertext $c = [m^2 \bmod N]$. Show a chosen-ciphertext attack on this scheme that recovers the entire private key.