CSCI471/971
Modern Cryptography

Workshop

Question-1

Question 1. In the El Gamal encryption scheme over a cyclic group G of order q, assume that there exists a bijective function f that can efficiently map a group element into a number in Z_q, and we modify the ciphertext of El Gamal as $CT = (g^r, f(h^r) \oplus m)$. Please show that the scheme is not IND-CPA secure in general. Here, we write $f(h^r)$ as its binary representation and xor it with m.

Question-1 (The modified scheme)

- Key generation:
  - Choose a cyclic group G of order q and a generator *g* of G. Then choose a uniform $x \in Z_q$ and compute $h = g^x$. Let f be a map from G to Z_q (i.e., numbers in [0,q-1]). Also let k be the length of the binary representation of q and assume that outputs of f are represented by binary strings.
  - The public key is (G, q, g, h, f) and the private key is (G, q, g, x, f).
- Encryption:
  - on input a public key pk = (G, q, g, h, f) and a message $m \in \{0,1\}^k$, choose a uniform $r \in Z_q$ and output the ciphertext $(g^r, f(h^r) \oplus m)$
- Decryption:
  - on input a private key sk = (G, q, g, x, f) and a ciphertext (c_1 , c_2), output the message $m= c_2 \oplus f((c_1^x))$.

Question-2

Question 2. Please show that a FHE scheme cannot be IND-CCA2 secure.

END