University of Maryland
CMSC858K — Introduction to Cryptography
Professor Jonathan Katz

Problem Set 4

Due at the *beginning* of class on April 12
Please type your solutions, preferably using latex.

1. This question concerns the group $\mathbb{Z}_p^*$, where $p = 2q + 1$ with p, q prime. Let $g \in \mathbb{Z}_p^*$ be a generator.
   (a) Let $h \in \mathbb{Z}_p^*$. Show that h is a quadratic residue modulo p if and only if $h^q = 1 \bmod p$. (Hint: it is relatively easy to show that h is a quadratic residue implies $h^q = 1 \bmod p$. For the other direction, use the fact that $\mathbb{Z}_p^*$ is cyclic.)
   (b) The discrete logarithm problem is assumed to be hard in $\mathbb{Z}_p^*$, meaning that the function $\mathsf{exp} : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$ defined by $\mathsf{exp}(x) = g^x \bmod p$ is assumed to be one-way. Let $\mathsf{lsb}(x)$ denote the least-significant bit of x. Prove that lsb is not a hard-core predicate for exp.
   (c) Prove that the decisional Diffie-Hellman assumption does not hold in $\mathbb{Z}_p^*$.
   (d) **(Extra credit:)** The decisional Diffie-Hellman assumption is believed to hold in the subgroup $\mathbb{G} < \mathbb{Z}_p^*$ of quadratic residues modulo p. Show that this implies that the *computational* Diffie-Hellman assumption holds in $\mathbb{Z}_p^*$. (Note: this question requires a small bit of group theory not covered in class. Specifically, use the fact that $\mathbb{Z}_p^* \cong \mathbb{Z}_q \times \mathbb{Z}_2$.)

2. Consider the following *interactive protocol* Π' for encrypting a message: first, the sender and receiver run a key-exchange protocol Π to generate a shared key k. Next, the sender computes $c \leftarrow \mathsf{Enc}_k(m)$ and sends c to the other party, who can decrypt and recover m using k.
   (a) Formulate a definition of indistinguishable encryptions in the presence of an eavesdropper appropriate for this interactive setting.
   (b) Prove that if Π is secure in the presence of an eavesdropper, and $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a private-key encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper (and $\mathsf{Gen}(1^n)$ outputs a key chosen uniformly at random from $\{0,1\}^n$), then Π' satisfies your definition given in part (a).

3. In class we discussed hybrid encryption. The natural way of applying this to the El Gamal encryption scheme is as follows. The public key is $pk = \langle \mathbb{G}, q, g, y \rangle$, and to encrypt a message m the sender chooses random $k \leftarrow \{0,1\}^n$ and sends

$$\langle \mathsf{ElGamal}_{pk}(k), \mathsf{Enc}_k(m) \rangle = \langle g^r,\, h^r \cdot k,\, \mathsf{Enc}_k(m) \rangle,$$

   where $r \leftarrow \mathbb{Z}_q$ is chosen at random and we assume k can be encoded as an element of $\mathbb{G}$. Suggest an improvement that results in a shorter ciphertext containing only a *single* group element (in addition to a private-key encryption of m).