Computer Science and Engineering, UCSD　　Fall 10
CSE 107: Introduction to Modern Cryptography　　**Instructor:** Mihir Bellare
Problem Set 1　　September 27, 2010

Problem Set 1

Due: Monday October 4, 2010, in class.

See course information section (on course web page) for instructions and rules on working on problem sets and turning them in.

Problem 1. [**20 points**] Discuss some privacy-related problem, created by modern technology, that concerns you. Explain why it concerns you, and what one might do about it. (Note the question is about privacy, not security in general!)

Problem 2. [**20 points**] The ciphertext

```
QFL HCVPS PX V ANSWLCEZK NCJVS; PQ XQVCQX QFL BPSZQL RNZ JLQ ZT PS QFL
BNCSPSJ VSW WNLX SNQ XQNT ZSQPK RNZ JLQ QN DKVXX
```

has been created using a punctuation-respecting substitution cipher on the alphabet of English letters. Your task is to decrypt this ciphertext and recover the plaintext. Show the steps you used to arrive at your solution, the final plaintext, and a table providing, for each letter, its decoding. (*Hint:* `J` decodes to `G`.)

Problem 3. [**30 points**] Let $m = 6$, and let $\mathbf{Z}_m$ denote the set $\{0, \ldots, m-1\}$. Let $X \bmod m$ denote the remainder obtained when dividing X by m.

1. [**15 points**] Consider the symmetric encryption scheme in which the encryption of message $M \in \mathbf{Z}_m$ under key $K \in \mathbf{Z}_m$ is $M + K \bmod m$. Is this encryption scheme perfectly secure? Why or why not?

2. [**15 points**] Consider the symmetric encryption scheme in which the encryption of message $M \in \mathbf{Z}_m$ under key $K \in \mathbf{Z}_m$ is $M + 2K \bmod m$. Is this encryption scheme perfectly secure? Why or why not?

In both cases, the key is a randomly chosen element of $\mathbf{Z}_m$ and the message space is also $\mathbf{Z}_m$.