COM S 4830 – Cryptography Due Sep 9, 2010

Homework 1

Instructor: Rafael Pass *TA: Huijia (Rachel) Lin*

You may collaborate with other students on the homework but you must submit your own individually written solution and you must identify your collaborators. If you make use of any other external source, you must acknowledge it. You are not allowed to submit a problem solution which you cannot explain orally to the course staff.

Problem 1. *Modular arithmetic and Probability*

Let $a \equiv b \mod n$ denote $a \bmod n = b \bmod n$.

1. Prove that $(a \bmod n) + (b \bmod n) \equiv a + b \mod n$
2. Prove that $(a \bmod n) \cdot (b \bmod n) \equiv a \cdot b \mod n$
3. Fact: If Bob is given a randomly chosen Skittle, he will eat it 85% of the time.

   Fact: 20% of all Skittles are yellow.

   Assume Bob eats each individual Skittle with an independent probability solely based on its color. If Bob is fed only yellow Skittles, give tight upper and lower bounds on the percentage that he eats.

Problem 2. *Perfect Security*

Alice claims to use a perfectly-secure encryption scheme to encrypt messages to Bob. However, Eve shows Alice that she can recover 90% of the bits of Alice's key even after just seeing one encrypted message from Alice.

1. Explain how this is possible by constructing a perfectly-secure encryption scheme which has these properties.
2. Eve claims she can always recover 10% of the message from the encryptions. Prove that this means that the encryption scheme cannot be perfectly secure.

Problem 3. *Correlated Random Bits*

Describe a procedure to uniformly pick $x_1, \dots, x_n \in \{0, 1, \dots, 2n-1\}$ conditioned on

$$\sum_{j=1}^{n} x_j \equiv v \bmod n$$

where $v \in \{0, 1, \dots, 2n-1\}$. Prove that your procedure is correct.

Problem 4. *Guess the Secret Key*

There is an encryption scheme such that given any fresh ciphertext encrypted using a secret key, one can independently guess the last bit of the secret key with probability 51%. Describe a procedure that will recover the last bit of the secret key with probability 99%. Provide an estimation on how many ciphertexts the procedure needs to see, and explain why (numerical justification is allowed).

BONUS: Justify your estimation on the number of ciphertexts needed analytically.

Problem 5. *Breaking codes*

Download the file cipher.txt from the course webpage and decrypt it. You must provide the plaintext and the methodology used to decrypt.