

# CSE 690: Problem Set #1

## Problem 1: Polyalphabetic substitution ciphers

Recall that the key to a mono-alphabetic substitution cipher is a permutation,  $\pi$ , on the 26 letters of the alphabet, and the encryption of a message  $(m_0, m_1, \dots, m_{n-1})$  is  $(\pi(m_0), \pi(m_1), \dots, \pi(m_{n-1}))$ . In a polyalphabetic substitution cipher, the key consists of  $\ell$  different permutations  $\pi_0, \dots, \pi_{\ell-1}$ , and a message is encrypted as

$$(\pi_0(m_0), \pi_1(m_1), \dots, \pi_{\ell-1}(m_{\ell-1}), \pi_0(m_\ell), \dots, \pi_{i \bmod \ell}(m_i), \dots, \pi_{n-1 \bmod \ell}(m_{n-1}))$$

Suppose an attacker captures a very long ciphertext,  $c$ , encrypted using a polyalphabetic cipher. The attacker knows that the plaintext is English text and that the key consists of at most 20 permutations, i.e.  $\ell \leq 20$ .

- How can the attacker figure out what  $\ell$  is? (Hint: Guess and check using letter frequencies for English)
- Once the attacker knows  $\ell$ , how can she figure out the original plaintext?

Note: The ciphertext  $c$  is “very long”, meaning that in your solution, you may assume that  $c$  is as long as you need.

## Problem 2: Another definition of security for PRGs

Suppose  $G : \{0, 1\}^\ell \rightarrow \{0, 1\}^L$  is a  $(t, \epsilon)$  PRG. Find  $t'$  and  $\epsilon'$  such that, for any algorithm  $A$  running in time  $t'$ ,  $\left| \Pr \left[ A(\text{first}_{L-1}(G(x))) = \text{last}_1(G(x)); x \xleftarrow{\$} U \right] - 1/2 \right| \leq \epsilon'$ . Prove that your  $t'$  and  $\epsilon'$  work.

## Problem 3: Constructions involving PRGs

Suppose  $G : \{0, 1\}^\ell \rightarrow \{0, 1\}^L$  is a secure PRG (for some values of  $(t, \epsilon)$ ). For each of the following constructions, say whether it is always a secure PRG or not. Include a proof or counterexample for your answer.

- $G'(x) = G(x) \| G(x)$
- $G'(x) = G(x) \| f(G(x))$ , where  $f$  is any polynomial-time function.
- $G'(x) = G(x) \| G(x+1)$
- $G'(x) = G(f(x))$ , where  $f$  is any polynomial-time function.

## Problem 4: XOR

Suppose  $D_1$  and  $D_2$  are distributions on  $\{0, 1\}^n$  and  $D_1$  and  $D_2$  are  $\epsilon_1$  and  $\epsilon_2$ -statistically indistinguishable from  $U$ , respectively. Let  $D_1 \oplus D_2$  be the distribution on  $\{0, 1\}^n$  given by  $x \oplus y$ , where  $x \xleftarrow{\$} D_1$  and  $y \xleftarrow{\$} D_2$  (independently). Prove that  $D_1 \oplus D_2$  is at most  $2\epsilon_1\epsilon_2$  statistically distinguishable from  $U$ .