# Methodology, Ethics and Practice of Data Privacy Course Exercise #3

May 30 2020

1. (10 pts) You (Eve) have intercepted two ciphertexts:

   $c_1 = 1111100101111001110011000001011110000110$

   $c_2 = 1111101001100111110111010000100110001000$

   You know that both are OTP ciphertexts, encrypted with the same key. You know that either $c_1$ is an encryption of "alpha" and $c_2$ is an encryption of "bravo" **or** $c_1$ is an encryption of "delta" and $c_2$ is an encryption of "gamma" (all converted to binary from ascii in the standard way). Which of these two possibilities is correct, and why? What was the key $k$?

2. (20 pts) Show that the following libraries are **not** interchangeable. Describe an explicit distinguishing calling program, and compute its output probabilities when linked to both libraries:

| $\mathcal{L}_{\text{left}}$ |
|---|
| $\text{EAVESDROP}(m_L, m_R \in \{0,1\}^\lambda)$: |
| $k \leftarrow \{0,1\}^\lambda$ |
| $c := k \oplus m_L$ |
| return $(k, c)$ |

| $\mathcal{L}_{\text{right}}$ |
|---|
| $\text{EAVESDROP}(m_L, m_R \in \{0,1\}^\lambda)$: |
| $k \leftarrow \{0,1\}^\lambda$ |
| $c := k \oplus m_R$ |
| return $(k, c)$ |

3. (10 pts) Which of the following are negligible functions in $\lambda$? Justify your answers.

$$\frac{1}{2^{\lambda/2}}, \frac{1}{2^{log(\lambda^2)}}, \frac{1}{\lambda^{log\lambda}}, \frac{1}{\lambda^2}, \frac{1}{2^{(log\lambda)^2}}, \frac{1}{(log\lambda)^2}, \frac{1}{\lambda^{1/\lambda}}, \frac{1}{\sqrt{\lambda}}, \frac{1}{2^{\sqrt{\lambda}}}$$

4. (20 pts) Let $G : \{0,1\}^\lambda \to \{0,1\}^{\lambda+l}$ be an injective (i.e., 1-to-1) PRG. Consider the following distinguisher:

**$\mathcal{A}$**

$x := \textsc{query}()$
for all $s' \in \{0,1\}^\lambda$:
  if $G(s') = x$ then return 1
return 0

**$\mathcal{L}^G_{\text{prg-real}}$**

$\underline{\textsc{query}():}$
  $s \leftarrow \{0,1\}^\lambda$
  return $G(s)$

**$\mathcal{L}^G_{\text{prg-rand}}$**

$\underline{\textsc{query}():}$
  $r \leftarrow \{0,1\}^{\lambda+\ell}$
  return $r$

(a) What is the advantage of $\mathscr{A}$ in distinguishing $\mathscr{L}^G_{prg-real}$ and $\mathscr{L}^G_{prg-rand}$? Is it negligible?

(b) Does this contradict the fact that G is a PRG? Why or why not?

5. (20 pts) Assume that Bob uses RSA and selects two "large" prime numbers p = 101 and q = 73.

   (a) How many possible public keys from which Bob can choose?

   (b) Assume also that Bob uses a public encryption key e = 91. Alice sends Bob a message M = 2008. What will be the ciphertext received by Bob?

   (c) Show the detailed procedure that Bob decrypts the received ciphertext.

6. (20 pts) Let $N = pq$ be a product of two distinct primes. Show that if $\phi(N)$ and $N$ are known, then it is possible to compute $p$ and $q$ in polynomial time. (Hint: Derive a quadratic equation (over the integers) in the unknown p.)