Due Date: 07 Sep 2023 CS6160: Cryptology

Assignment 1

1. Give a formal description of the Vigenere cipher, i.e. describe the sets M, C, K as well as the algorithms Gen, Enc, Dec.

2. We say that an encryption scheme is ε-perfecty secret if for every adversary A it holds that

$$Pr[PrivK^{eav}_{A,\Pi} = 1] \leq \frac{1}{2} + \varepsilon.$$

   Show that for every $\varepsilon > 0$, there is a ε-perfectly secret scheme such that $|K| < |M|$.

   Hint: Use an XOR or modular addition scheme and set $K = M \setminus \{x\}$ for some fixed element x.

3. Consider the message space $M = \{0,1\}^{n \times n}$, i.e. M consists of $n \times n$ matrices with entries in $\{0,1\}$. Let K be the set of matrices in $\{0,1\}^{n \times n}$ such that K is invertible modulo 2. Consider the function $F : M \times K \to M$ defined as $F(m,k) = mk$ where the RHS is matrix multiplication modulo 2. Show that F is not a pseudorandom permutation.

4. Do Ex 2.18 from Boneh-Shoup (Voting Protocols)

5. Consider the following mode of operation for block ciphers. Let the message blocks be $M_1, M_2, \ldots, M_L$. Let $Enc(\_, k)$ be the encryption function for each block. We first pick a random $IV \in \{0,1\}^n$ and then compute $C_i = Enc(IV \oplus M_i \oplus (i-1), k)$. That is, in contrast to the randomized counter mode, the message goes into the XOR function before encryption. Show that this is not secure by distinguishing some pair of messages.