Cryptography: Homework 5

(Deadline: 10am, 2021/11/12)

1. (30 points) Let F be a PRP, and define a fixed-length encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ as follows: On input $m \in \{0,1\}^{n/2}$ and key $k \in \{0,1\}^n$, algorithm Enc chooses a uniform string $r \in \{0,1\}^{n/2}$ of length $n/2$ and computes $c = F_k(r \| m)$. Show how to decrypt, and prove that this scheme is CPA-secure for messages of length $n/2$.

   (Hint: Consider a new scheme Π' where F_k is replaced with a truly random permutation f.)

2. (20 points) Let F be a PRP. Consider the following modifications to CTR:

   (a) The sender simply increments the ctr by 1 each time a message is encrypted (rather than choosing ctr at random each time).

   (b) The sender chooses a uniform value $ctr \in \{0,1\}^n$, and the ith ciphertext block c_i is computed as $c_i = F_k(ctr \oplus \langle i \rangle \oplus m_i)$, where $\langle i \rangle$ is the n-bit binary representation of i.

   Show that the two schemes are not CPA-secure.