3 Cryptography (mgk25)

Your colleagues need a pseudo-random permutation $P_K : \mathbb{Z}_{10^6} \leftrightarrow \mathbb{Z}_{10^6}$, over the integers in the range 0 to 999 999, where K is a 128-bit key. The standard library of their development environment offers them only a 128-bit pseudo-random permutation, in form of the blockcipher AES-128.

(*a*) Recalling that $2^{20} = 1.048576 \times 10^6$, they first decide that implementing a 20-bit pseudo-random permutation $T_K : \{0,1\}^{20} \leftrightarrow \{0,1\}^{20}$ might get them closer to a solution. How could they implement T_K using the available AES_K function? [4 marks]

(*b*) One of your colleagues then proposes to use the function

$$P'_K(m) := \langle T_K(\langle m \rangle_{20}) \rangle^{-1} \bmod 10^6$$

as a "good enough" approximation of what is required.

Notation: $\langle\cdot\rangle_n : \mathbb{Z}_{2^n} \to \{0,1\}^n$ encodes non-negative integers as n-bit bitstrings and $\langle\cdot\rangle^{-1} : \{0,1\}^* \to \mathbb{N}$ does the opposite, i.e. $\langle\langle i \rangle_n\rangle^{-1} = i$ for all $0 \le i < 2^n$.

Propose a distinguisher D that can distinguish P'_K from a random permutation $R : \mathbb{Z}_{10^6} \leftrightarrow \mathbb{Z}_{10^6}$ using not more than 5000 oracle queries, and show that it achieves $\left|\mathbb{P}(D^{P'_K(\cdot)} = 1) - \mathbb{P}(D^{R(\cdot)} = 1)\right| > \frac{1}{2}$ averaged over all K. [6 marks]

(*c*) Another colleague then proposes the following algorithm:

```
function P_K(m):
  c := T_K(<m>_20)
  m := <c>^-1
  while m ≥ 10^6:
    c := T_K(c)
    m := <c>^-1
  return m
```

Show that this is in fact a permutation by

(*i*) explaining why this algorithm always terminates; [1 mark]

(*ii*) providing an implementation of the inverse $P_K^{-1}(m)$. [3 marks]

(*d*) What side-channel risk could the algorithm for $P_K(m)$ from part (*c*) pose, and what can an observer learn from it? [2 marks]

(*e*) Propose an alternative algorithm that reduces the risk that an observer can learn anything from this type of side channel to a negligible probability. [4 marks]