TD Bonus

Exercise 1. *CTR Security*

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF. To encrypt a message $M \in \{0,1\}^{d \cdot n}$, CTR proceeds as follows:

- Write $M = M_0 \| M_1 \| \ldots \| M_{d-1}$ with each $M_i \in \{0,1\}^n$.
- Sample IV uniformly in $\{0,1\}^n$.
- Return $IV \| C_0 \| C_1 \| \ldots \| C_{d-1}$ with $C_i = M_i \oplus F(k, IV + i \bmod 2^n)$ for all i.

The goal of this exercise is to prove the security of the CTR encryption mode against chosen plaintext attacks, when the PRF F is secure.

1. Recall the definition of security of an encryption scheme against chosen plaintext attacks.

2. Assume an attacker makes Q encryption queries. Let $IV_1, \ldots, IV_Q$ be the corresponding IV's. Let `Twice` denote the event "there exist $i, j \leq Q$ and $k_i, k_j < d$ such that $IV_i + k_i = IV_j + k_j \bmod 2^n$ and $i \neq j$." Show that the probability of `Twice` is bounded from above by $Q^2 d / 2^{n-1}$.

3. Assume the PRF F is replaced by a uniformly chosen function $f : \{0,1\}^n \to \{0,1\}^n$. Give an upper bound on the distinguishing advantage of an adversary $\mathcal{A}$ against this idealized version of CTR, as a function of d, n and the number of encryption queries Q.

4. Show that if there exists a probabilistic polynomial-time adversary $\mathcal{A}$ against CTR based on PRF F, then there exists a probabilistic polynomial-time adversary $\mathcal{B}$ against the PRF F. Give a lower bound on the advantage degradation of the reduction.

Exercise 2. *weak PRF*

In the PRF security game, the adversary may adaptively make function evaluation queries: for $i = 1, 2, \ldots$, it sends x_i of its choice, and gets $F_k(x_i)$ (resp. $f(x_i)$) from the challenger, where F_k is the PRF (resp. f is the uniformly chosen function). A weak-PRF consists of the same algorithms as a PRF, but the queries are modified as follows: the adversary does not get to see $F_k(x_i)$ (resp. $f(x_i)$) for **an input** x_i **of its choice**, but instead every time the adversary requests a new pair, **the challenger samples a fresh uniform** x_i and sends $(x_i, F_k(x_i))$ (resp. $(x_i, f(x_i))$) to the adversary.

1. Give a formal definition of a weak-PRF, based on a security game.

2. Show that a PRF is a weak-PRF, by providing a security reduction.

3. Assuming that a weak-PRF exists, build a weak-PRF that is not a PRF.

4. What is the difference between a PRG and a weak-PRF?

Let $G = (g)$ be a cyclic group of known prime order p. We recall that the DDH hardness assumption states that the distributions (g^a, g^b, g^{ab}) and (g^a, g^b, g^c) are computationally indistinguishable when a, b and c are independently and uniformly distributed in $\mathbb{Z}/p\mathbb{Z}$. Let $k \in \mathbb{Z}/p\mathbb{Z}$ a uniformly chosen key. We consider the function $F_k : h \in G \mapsto h^k \in G$.

5. Let $Q \geq 1$. Consider the (randomized) map ϕ that takes $(g_1, g_2, g_3) \in G^3$ as input, samples $(x_i, y_i) \in (\mathbb{Z}/p\mathbb{Z})^2$ uniformly and independently for $i \leq Q$ and returns $(g_1^{x_i} g^{y_i}, g_3^{x_i} g_2^{y_i})_{i \leq Q}$.

- Show that if $(g_1, g_2, g_3) = (g^a, g^b, g^{ab})$, then the output is distributed as $(g^{r_i}, g^{br_i})_{i \le Q}$ for r_i's in $\mathbb{Z}/p\mathbb{Z}$ uniform and independent.
- Show that if $(g_1, g_2, g_3) = (g^a, g^b, g^c)$ for $c \neq ab$, then the output is distributed as $(g^{r_i}, g^{s_i})_{i \le Q}$ for (r_i, s_i)'s in $(\mathbb{Z}/p\mathbb{Z})^2$ uniform and independent.

6. Show that F_k is a weak-PRF under the DDH hardness assumption.
Hint: set "$k = b$" and use the previous question to build the weak PRF challenger.

7. Is F_k a secure PRF? Justify your answer.

Exercise 3. *CBC-MAC*

Let $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a PRF, $d > 0$ and $L = nd$. Prove that the following modifications of CBC-MAC (recalled in Figure 1) do not yield a secure fixed-length MAC. Define $t_i := F(K, t_{i-1} \oplus m_i)$ for $i \in [1, d]$ and $t_0 := IV = 0$.

1. Modify CBC-MAC so that a random $IV \hookleftarrow U(\{0,1\}^n)$ (rather than $IV = \mathbf{0}$) is used each time a tag is computed, and the output is (IV, t_d) instead of t_d alone.

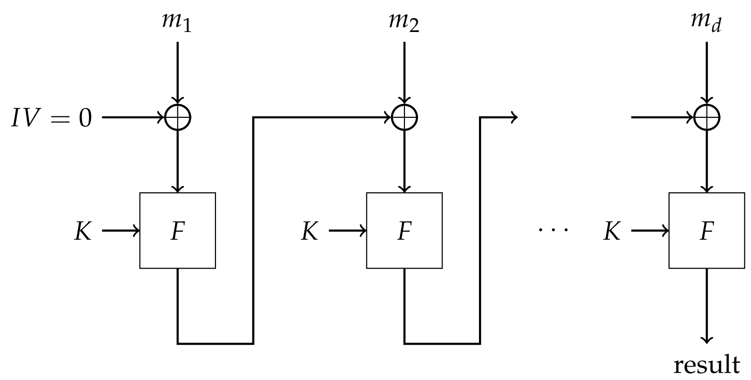

Figure 1: CBC-MAC

2. Modify CBC-MAC so that all the outputs of F are output, rather than just the last one.

We now consider the following ECBC-MAC scheme: let $F : K \times X \to X$ be a PRF, we define $F_{ECBC} : K^2 \times X^{\le L} \to X$ as in Figure 2, where K_1 and K_2 are two independent keys.
If the message length is not a multiple of the block length n, we add a pad to the last block: $m = m_1 | \ldots | m_{d-1} | (m_d \| \mathrm{pad}(m))$.

3. Show that there exists a padding for which this scheme is not secure.

For the security of the scheme, the padding must be invertible, and in particular for any message $m_0 \neq m_1$ we need to have $m_0 || \mathrm{pad}(m_0) \neq m_1 || \mathrm{pad}(m_1)$. In practice, the ISO norm is to pad with $10 \cdots 0$, and if the message length is a multiple of the block length, to add a new "dummy" block $10 \cdots 0$ of length n.

4. Prove that this scheme is not secure if the padding does not add a new "dummy" block if the message length is a multiple of the block length.

Remark: The NIST standard is called CMAC, it is a variant of CBC-MAC with three keys (k, k_1, k_2). If the message length is not a multiple of the block length, then we append the ISO padding to it and then we also XOR this last block with the key k_1. If the message length is a multiple of the block length, then we XOR this last block with the key k_2. After that, we perform a last encryption with $F(k, .)$ to obtain the tag.

Exercise 4. *Merkle-Damgård transform*

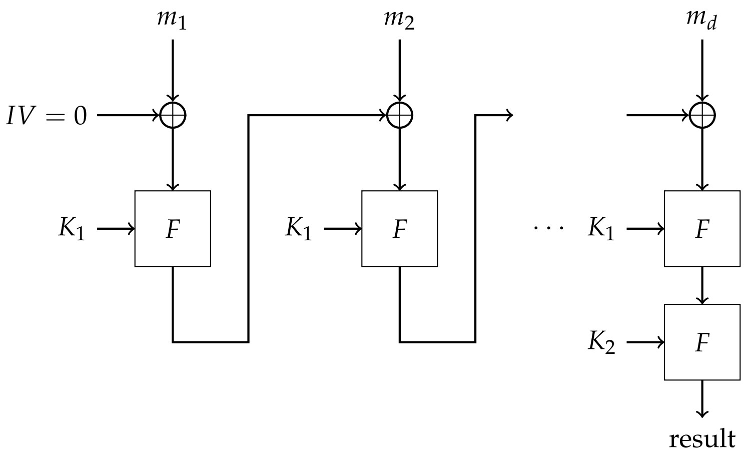

Figure 2: ECBC-MAC

1. In the Merkle-Damgård transform, the message is split into consecutive blocks, and we add as a last block the binary representation of the length of this message. Suppose that we do not add this block: does this transform still lead to a collision-resistant hash function?

2. Before HMAC was invented, it was quite common to define a MAC by $\mathrm{Mac}_k(m) = H^s(k \parallel m)$ where H is a collision-resistant hash function. Show that this is not a secure MAC when H is constructed via the Merkle-Damgård transform.