
Homework 3

Due: Wednesday, October 20 at 9PM.

You may discuss the problems in general terms in a group of size at most three. You are expected to write up your solutions yourself. Please credit your collaborators on your submission. You may use your course notes and slides to solve these problems.

This complements the PlayCrypt version of this problem set. You need turn in only the latter, on Gradescope. This version is being given out so that you can see what the problems look like in mathematical notation. **Do not rename your homework file from hw3.py.**

We suggest that you start with this version. Work out a solution using pencil and paper. Move to implementation in PlayCrypt only after that.

As usual our convention is that the running time of an adversary does not include the time taken by game procedures to compute responses to adversary queries.

Problem 1 [10 points] Let $k, n \geq 8$ be integers and let $F: \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a family of functions. Let T_F be the time to compute F . Let \mathcal{K} be the key-generation algorithm that returns a random k -bit string as the key K . Let \mathcal{E} be the following encryption algorithm:

Alg $\mathcal{E}_K(M)$

$M[1] \dots M[m] \leftarrow M$

$R_0 \xleftarrow{\$} \{0, 1\}^n$; $R_1 \xleftarrow{\$} \{0, 1\}^n$; $C[0] \leftarrow R_0 \| R_1$; $d[0] \leftarrow \text{lsb}(C[0])$; $M[0] \leftarrow 0^n$

for $i = 1, \dots, m$ do

$W[i] \leftarrow R_{d[i-1]} \oplus M[i-1]$; $P[i] \leftarrow F(K, W[i])$

$C[i] \leftarrow P[i] \oplus M[i]$; $d[i] \leftarrow \text{lsb}(C[i])$

$C \leftarrow C[0]C[1] \dots C[m]$

return C

The message space is the set of all strings whose length is a positive multiple of n , meaning these are the allowed messages. The first line above indicates that M is broken into n -bit blocks, with $M[i]$ denoting the i -th block and m the number of blocks. (For example if $n = 4$ and $M = 01101011$ then $M[1] = 0110$ and $M[2] = 1011$ and $m = 2$.) The ciphertext C is $(2 + m)n$ bits long, with $C[0]$ being $2n$ bits and $C[i]$ being n bits for $i = 1, \dots, m$. By $\text{lsb}(X)$ we denote the least significant (rightmost) bit of X . (For example, $\text{lsb}(011) = 1$.)

- [3 points]** Specify decryption algorithm \mathcal{D} such that $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a symmetric encryption scheme satisfying the correct decryption condition of Slide 3. If the input ciphertext has length $(2 + m)n$ then the running time of \mathcal{D} should be $\mathcal{O}(m \cdot (T_F + n))$.

2. [7 points] Show that this scheme is not IND-CPA secure by presenting a $\mathcal{O}(T_F + n)$ -time adversary A making one query to its **LR** oracle and achieving $\mathbf{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A) \geq 0.9$.
-

Problem 2 [10 points] Let $E: \{0, 1\}^k \times \{0, 1\}^l \rightarrow \{0, 1\}^l$ be a block cipher and let T_E denote the time to compute E or E^{-1} . Let D be the set of all strings whose length is a positive multiple of l .

1. [4 points] Define the hash function $H_1: \{0, 1\}^k \times D \rightarrow \{0, 1\}^l$ via the CBC construction, as follows:

Alg $H_1(K, M)$
 $M[1]M[2] \dots M[n] \leftarrow M$
 $C[0] \leftarrow 0^l$
For $i = 1, \dots, n$ do $C[i] \leftarrow E(K, C[i-1] \oplus M[i])$
Return $C[n]$

Show that H_1 is not collision-resistant by presenting an $\mathcal{O}(T_E + l)$ time adversary A_1 with $\mathbf{Adv}_{H_1}^{\text{cr}}(A_1) = 1$.

2. [6 points] Define the hash function $H_2: \{0, 1\}^k \times D \rightarrow \{0, 1\}^l$ as follows:

Alg $H_2(K, M)$
 $M[1]M[2] \dots M[n] \leftarrow M$
 $C[0] \leftarrow 0^l$
For $i = 1, \dots, n$ do $W[i] \leftarrow E(K, C[i-1] \oplus M[i])$; $C[i] \leftarrow E(K, W[i] \oplus M[i])$
Return $C[n]$

Show that H_2 is not collision-resistant by presenting an $\mathcal{O}(T_E + l)$ time adversary A_2 with $\mathbf{Adv}_{H_2}^{\text{cr}}(A_2) = 1$.
