CPT_S 327 - Homework 2

In this homework, please send one pdf file with the following information: (1) Your name, (2) your WSU ID, (3) the write up for the following two questions. More details are specified in each question.

Problem 1

Please write down the Hash value by using the provided r as input and provided the SHA3-256 (which can be found in Canvas), r is set as

abcdefgh

You can copy and paste from the screen.

Problem 2

In practice, a common use of SHA3 is to assume that it is a PRG. Let's consider $\{0,1\}^{128}$ as the input domain and $\{0,1\}^{256}$ as the output domain of to SHA3-256, as the following

$$\text{SHA3} \equiv \text{G}\colon \{0,1\}^{128} \to \{0,1\}^{256}.$$

I.e., we denote SHA3$(\cdot)$ as G$(\cdot)$.

Now we want to use this to generate more pseudorandom bits as $\text{G}' : \{0,1\}^{128} \to \{0,1\}^{512}$. Particularly, G$'$ on input $r \in \{0,1\}^{128}$ works as follows:

- First compute $r_1 \| r_2 = \text{G}(r)$, where $r_1 \in \{0,1\}^{128}$, $r_2 \in \{0,1\}^{128}$ and $\|$ denotes concatenation.
- Then compute $r^* = \text{G}(r_1) \| \text{G}(r_2) \in \{0,1\}^{512}$.
- Output r^*.

Our goal is to show that the output of G'$(\cdot)$ is also pseudorandom, i.e., G'(U_{128}) is computationally indistinguishable from U_{512}, where U_m denotes the uniform distribution of m bits. Below we divide this into the following subtasks.

Subtasks: Consider the following hybrids distributions:

- H_0: this is the output distribution of G' given a random input in U_{128}, i.e., $\mathrm{G}'(r) = \mathrm{G}(r_1)\|\mathrm{G}(r_2)$, where $r_1\|r_2 = \mathrm{G}(r)$ and $r \leftarrow U_{128}$.
- H_1: this is a modified version of H_0. The output of H_1 is $\mathrm{G}(r_1)\|\mathrm{G}(r_2)$ where both $r_1 \leftarrow U_{128}$ and $r_2 \leftarrow U_{128}$, i.e., they are both truly uniform strings. This is the only difference between H_1 and H_0.
- H_2: this is a modified version of H_1. The output of this variant is $r_1^*\|\mathrm{G}(r_2)$ where $r_1^* \leftarrow U_{256}$ is truly random, and $r_2 \leftarrow U_{128}$.
- H_3: this is a truly uniform string, i.e., U_{512}.

Show that each adjacent hybrids are computationally indistinguishable, under the assumption that G is a secure PRG. That is, you need to prove $H_0 \approx_c H_1 \approx_c H_2 \approx_c H_3$. Then argue why this suffices to show our overall goal.

Problem 3

If the secret key has length 128 bits, is the encryption scheme secure in practice? Please explain your answer after doing the following task.

Let $\Sigma = \{\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}\}$ be an encryption scheme that uses the above G' as a building block. Set $\lambda = 128$, and the algorithms work as follow.

- $\mathsf{KeyGen}(1^{128})$: First choose r randomly from $\{0,1\}^8$. Then set $\mathsf{sk} = r\|(0110)^{30}$. Note: $(0110)^j$ means repeating the concatenation of (0110) by j times. The total length of sk is 128. The message space is $\{0,1\}^{512}$.
- $\mathsf{Enc}(\mathsf{sk}, m)$: Given $\mathsf{sk} \in \{0,1\}^{128}$ and $m \in \{0,1\}^{512}$ as inputs, compute $r^* = G'(\mathsf{sk})$. Output $c = m \oplus r^*$ as the ciphertext.
- $\mathsf{Dec}(\mathsf{sk}, c)$: Given $\mathsf{sk} \in \{0,1\}^{128}$ and $c \in \{0,1\}^{512}$ as inputs, compute $r^* = G'(\mathsf{sk})$. Output $m = c \oplus r^*$ as the message.

Now please compute your WSUID modulo 8 and take the corresponding ciphertext file, i.e., "cipherX.txt", where X is the result of modulo 8. We know that the plaintexts are all English sentences of 512 bits (including space and punctuations. The last word might be truncated.) The ciphertexts are encrypted under the above procedure.

Task: (1) Given only the ciphertext (without the key), figure out the plaintext. (2) Answer the very first question of this problem.