CSE 130 – INTRO TO CRYPTOGRAPHY
Spring 2025 Homework 2

Private-Key Encryption:

1. Define $G(s) \overset{\text{def}}{=} s||s$ (where "$||$" denotes concatenation). Describe and analyze an attack showing that G is not a psudorandom generator.
2. Define the keyed function F as $F_k(x) \overset{\text{def}}{=} k\&x$, where "&" denotes bitwise AND. Describe and analyze an attack showing that F is not a psudorandom function.
3. Let Π denote Construction 3.30 instantiated with the keyed function from Example 3.26. Describe and analyze an attack showing that Π is not CPA-secure.
4. Prove that the unsynchronized stream-cipher mode of operation (described in pg. 88) is CPA-secure if the underlying stream cipher is secure (Hint: proof follows along the lines of the proof of Theorem 3.31).
5. Let F be a pseudorandom function, and consider the following construction of a stream cipher accepting an n-bit initialization vector (IV):
   - $\mathsf{Init}(s, IV)$ outputs $\mathsf{st} = (s, IV)$.
   - $\mathsf{Next}(s, IV)$ outputs $y := F_s(IV)$ and $\mathsf{st}' = (s, IV + 1)$.

   Show that this stream cipher is not secure.

Message Authentication Codes and CCA-Secure Encryption:

6. Define a version of CBC-MAC for message of length at most $l \cdot 2^n$ as follows: given a message m, pad it with 0s so that it has length exactly $l \cdot 2^n$; apply basic CBC-MAC to the result. Is this secure? Explain.
7. Show that the CBC, OFB, and CTR modes of operation do not give CCA-secure encryption schemes.
8. Write pseudocode for obtaining the entire plaintext via a padding-oracle attack on CBC-mode encryption using PKCS #7 (explained in the lecture slides or PKCS #5 in textbook) padding, as sketched in the text.
9. Describe a padding-oracle attack on CTR-mode encryption, assuming PKCS #7 padding is used to pad messages to a multiple of the block length before encrypting.

Your submission must contain the following:

- Title that states "CSE 130 Homework 2 Solutions (Spring 2025)".
- Your full name (as it appears on CatCourses).
- The question number associated with each answer.
- Page numbers on each page. If submitting a handwritten scanned document (see below), your page numbers must be in the following format (1 of n, 2 of n, etc.), where n indicates the total number of pages.

The submission format is PDF. You may use the following to write your solutions:

- LaTeX: You may use the Overleaf online editor.

- Markdown: You may use VS Code for this (supports it natively). Please use the Print extension to save your rendered Markdown file as PDF.

- MS Word: You may use the built-in Equation Editor. Please make sure to save your Word file as PDF before submitting.

- Pen and Paper: Please make sure to scan your work as PDF before submitting (image formats like JPEG **will not be accepted**). Please make sure that your scanned document is **clearly legible** before submitting.