CS 463/563 — Cryptography for Cybersecurity
Homework 11: Hashes for Block Ciphers

DUE DATE HERE

STUDENT NAME HERE
UIN HERE
SECTION HERE
Instructor: J. Takeshita. Institution: Old Dominion University.

This assignment has **4** questions.

Submission instructions: If you don't already have the necessary tools, then install 1) a LaTeX distribution (probably the `texlive-full` package on most Linux distributions) and 2) an IDE or other text editor suitable for LaTeX. For the latter, I suggest the use of the Kile IDE, which is available in most Linux distributions' default packages. You can also just use a web IDE such as **Overleaf**.

Download the source file(s) for this assignment. Edit the file(s) to include your solutions using the text editor or LaTeX IDE of your choice. Type your answers and personal information (e.g., name, section, etc.) into the source file at the appropriate places, and double-check that the variable `solutions` is set to be false. (I should have done this for you, but it's good to be sure.) Make sure to properly format your math! See `https://latex-tutorial.com/tutorials/` if you're not already familiar with LaTeX.

Compile the source to a PDF, either through your IDE or by using the command `pdflatex`. Make sure your compilation has no errors, and address all reasonably actionable warnings (you can ignore small things like badbox warnings, as long as they don't affect the output badly). You can toggle the variable `boilerplate` to hide these instructions, if you like.

Check your PDF to make sure it is cleanly typeset!

Turn in 1) the PDF and 2) any and all `.tex` source files, `.bib` bibliography files, source code, or other artifacts. Submissions that are handwritten or typeset with other methods will not be accepted! If you wrote any software in the course of this work, please include it using the `listing` package's utilities.

Cite any external sources, and include any code you write. The use of unauthorized outside assistance, including any AI/LLM, is strictly prohibited.

A note: While it is possible and allowed to solve these questions by writing your own computer programs, you should be able to also do them by hand, as similar questions may appear on exams.

Questions:

1. Consider the block cipher from Question 1 of Homework 5. Let $\bar{h}$ be the bitwise

complement of h, i.e., the bits of $\bar{h}$ will be the opposite value of the corresponding bit in h. Choose the function g to be $g(h) = \bar{h}$.

For an initial hash $H_0 =$ `0xF4` and a message $M =$ `0xDAB9`, compute the Martyas-Meyer-Oseas hash function (detailed in Figure 11.7 of your textbook) on these inputs, and give your result in hexadecimal.

(7 points)

Answer: $H_1 = e_{\bar{F4}}(DA) \oplus DA$
$H_1 = (0000 \oplus 1010 \| \| 1101 \oplus 1101) \oplus 11011010$
$H_1 = 01111010 = 7A$
$H_2 = e_{\bar{7A}}(B9) \oplus B9$
$H_2 = (1000 \oplus 1001 \| \| 0101 \oplus 1011) \oplus 10111001$
$H_2 = 10100111 = A7$
$\boxed{H = 7AA7}$

2. Do the same as in Question 1, but use the Davis-Meyer hash function (detailed in Figure 11.6 of your textbook). (6 points)

Answer: $H_1 = e_{DA}(F4) \oplus F4$
$H_1 = (1101 \oplus 0100 \| \| 1010 \oplus 1111) \oplus 11110100$
$H_1 = 01100001 = 61$
$H_2 = e_{B9}(61) \oplus 61$
$H_2 = (1011 \oplus 0001 \| \| 1001 \oplus 0110) \oplus 01100001$
$H_2 = 11001110 = CE$
$\boxed{H = 61CE}$

3. Do the same as in Question 1, but use the Miyaguchi-Preneel hash function (detailed in Figure 11.6 of your textbook). (7 points)

Answer: $H_1 = F4 \oplus DA \oplus e_{\bar{F4}}(DA)$
$H_1 = (11110100 \oplus 11011010) \oplus (0000 \oplus 1010 \| \| 1011 \oplus 1101)$
$H_1 = 88$
$H_2 = 88 \oplus B9 \oplus e_{\bar{F}}(B9)$
$H_2 = (10001000 \oplus 10111001) \oplus (0000 \oplus 1001 \| \| 1011 \oplus 1001)$
$H_2 = 92$
$\boxed{H = 3192}$

4. Give a new question on the topic of this week's material and its solution, suitable for inclusion in future versions of this homework assignment. Your question should be different from the other questions here – don't just change some values around! Programming problems are acceptable too, but should be nontrivial. You can use textbooks, scholarly papers, or other reputable sources of information for inspiration, but you should not directly copy someone else's work. Your question should show me that you understand the content well enough to ask and answer an interesting question about it. Include any source code used to generate/solve the problem. (10 points)

   Some free online textbooks include *The Joy of Cryptography* by Mike Rosulek (Oregon State University), or *A Graduate Course in Applied Cryptography* by Dan Boneh (Stanford University) and Victor Shoup (Offchain Labs, formerly at New York University). Your course text, *Understanding Cryptography* by Christof Paar (Universität Bochum) and Jan Pelzl (Universität Bochum), is also an excellent starting point.

   Possible topics include hashes and hashing related to block ciphers.

   Answer: Would a hash function that took the sum of all of the ASCII character values and returned that as the hash be a secure hash function?
   Answer: No, because there could be multiple inputs that return the same output. For example, the word "Tree" would return the same hash value as "erTe", "eerT", and "reeT". This means that this hash would be vulnerable to a second preimage attack.