CS 463/563 — Cryptography for Cybersecurity
Homework 5: Block Cipher Modes

DUE DATE HERE

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

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.

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 a simple block cipher with 8-bit blocks. For a plaintext $P_L||P_R$ and key $K_L||K_R$ (where all of P_L, P_R, K_L, K_R are 4 bits wide), the ciphertext resulting from encryption is $C_L||C_R$, where $C_L = K_L \oplus P_R$ and $C_R = K_R \oplus P_L$. The plaintext, ciphertext, and key are all 8 bits wide. Similarly, for decryption we compute the

operations in reverse: given a ciphertext $C_L||C_R$ and a key $K_L||K_R$, compute $P_L = C_R \oplus K_R$ and $P_R = C_L \oplus K_L$ to find the plaintext $P_L||P_R$. Suppose you have a 16-bit input `0xA8B9` and an 8-bit IV `0xA9`.

For CTR mode, we use a counter bitstream that is expressed as a sequence of 4-bit chunks, where the i^{th} chunk is $i + 1 \pmod{16}$ expressed as a 4-bit number. i.e., the stream is `0001 0010 0011 0100 0101` $\cdots$, etc. Where you need an 8-bit key, use the value `0xC5`. Give outputs in hexadecimal. (25 points)

(a) Compute the encrypted output of this cipher in ECB mode.

(b) Compute the encrypted output of this cipher in CBC mode.

(c) Compute the encrypted output of this cipher in OFB mode.

(d) Compute the encrypted output of this cipher in CFB mode.

(e) Compute the encrypted output of this cipher in CTR mode with an IV of `0101`.

Answer:

(a) $C_i = e_k(X_i)$
$C_L = (C \oplus 8)||(A \oplus 5)$
$1100 \oplus 1000||1010 \oplus 0101 = 4F$
$C_R = e_{C5}(B9)$
$C_R = (C \oplus 9)||(5 \oplus B)$
$1100 \oplus 1001||0101 \oplus 1011 = 5E$ $C = C_L||C_R$
$\boxed{C = 485E}$

(b) $C_L = e_k(X_L \oplus IV)$
$C_R = e_k(X_R \oplus C_L)$
$C_L = e_{C5}(A8 \oplus A9) = D5$
$C_R = e_{C5}(B9 \oplus D5) = 03$ $C = C_L||C_R$
$\boxed{C = D503}$

(c) $S_1 = e_k(IV)$
$S_2 = e_k(S_1)$
$C_L = s_1 \oplus X_L$
$C_R = S_2 \oplus X_R$
$S_1 = e_{C5}(A9) = 5f$
$S_2 = e_{C5})(5F) = 30$
$C_L = 5F \oplus A8 = F7$
$C_R = 30 \oplus B9 = 89$
$C = C_L||C_R$
$\boxed{C = F789}$

(d) $C_L = e_k(IV) \oplus X_L$
$C_R = e_k(C_L) \oplus X_R$
$C_L = e_{C5}(A||9) \oplus A8 = F7$
$C_R = e_{C5}(F||7) \oplus B9 = 03$
$C = C_L||C_R$
$\boxed{C = F703}$

(e) $C_L = e_k(IV||CTR_L) \oplus X_L$
$C_R = e_k(IV + 1||CTR_R) \oplus X_R$
$C_L = e_{C5}(5||0) \oplus A8 = 68$
$C_R = e_{C5}(5||1) \oplus B9 = 69$
$C = C_L||C_R$
$\boxed{C = 6869}$

2. Answer the following questions on the security of different block cipher modes. (10 points)
   (a) Why is ECB insecure?
   (b) Show an example of ECB's insecurity.
   (c) Why does CTR mode not have this vulnerability?

Answer:

(a) ECB encrypts all blocks the same, and if two encrypted blocks are identical, it is automatically inferred that the corresponding plaintext are also identical.

(b) Encryption never needs to be cracked because a replay attack using ciphertext that would be used again can be launched to get information to be sent somewhere else. For example if two parties use the same key whenever they encrypt, if an attacker injects a message with a different end point address that has the expected cipher text instead of the expected address, they could get sensitive information.

(c) CTR mode makes it so that the ciphertext is different for each block of code encrypted, making the encrypted blocks not identical.

3. 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 fields, finite fields, prime fields, extension fields, or AES.

Answer: Decrypt 6869 in CTR mode w/ an IV of 0101, and a key of C5, with an encryption scheme of $Y = (K_R \oplus X_L)||(K_L \oplus X_R)$
$X_L = e_{C5}(0101||0000) \oplus 68$
$1100 \oplus 0000||0101 \oplus 0101 = 11000000$
$X_L = 01101000 \oplus 11000000 = A8$
$X_R = e_{C5}(0101||0001) \oplus 69$
$(1100 \oplus 0001)||(0101 \oplus 0101) = 11010000$
$X_R = 11010000 \oplus 01101001 = 10111001 = B9$
$\boxed{X = X_L||X_R = A8B9}$