CS 463/563 — Cryptography for Cybersecurity
Homework 3: Symmetric Cryptography

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).

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. Recall that a linearly congruent generator is defined by $s_{i+1} = a \cdot s_i + b \pmod{m}$. Given a seed $s_0 = 13$ and parameters $a = 11$, $b = 8$, $m = 15$, use the linearly congruent generator to find the first ten values generated after s_0, i.e., the values $s_1, \cdots, s_{10}$. (10 points)

Answer: $11 * 13 + 8 \pmod{15}$
$s1 = 1$
$11 * 1 + 8 \pmod{15}$
$s2 = 4$
$11 * 4 + 8 \pmod{15}$
$s3 = 7$
$11 * 7 + 8 \pmod{15}$
$s4 = 10$
$11 * 10 + 8 \pmod{15}$
$s5 = 5$
$11 * 5 + 8 \pmod{15}$
$s6 = 3$
$11 * 3 + 8 \pmod{15}$
$s7 = 11$
$11 * 11 + 8 \pmod{15}$
$s8 = 9$
$11 * 9 + 8 \pmod{15}$
$s9 = 2$
$11 * 2 + 8 \pmod{15}$
$s10 = 0$

2. Consider the LSFR with $m = 5$ shown in Figure 1. (Note that this figure uses $\otimes$ to represent XOR gates; the usual notation for an XOR gate or operation is $\oplus$.) Suppose the LSFR is initialized with the values $FF4 = 1$, $FF3 = 0$, $FF2 = 0$, $FF1 = 1$, $FF0 = 0$. Give the first 30 bits generated from this LSFR, and determine the length of its period. (10 points)

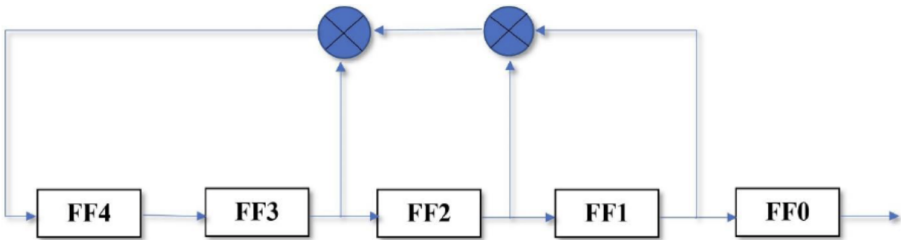

Figure 1: A LSFR with $m = 5$

Answer:
period length: $2^5 - 1 = 31$

$s_{i+m} \sum_{J=0}^{m-1} p_J * s_{i+J} \pmod 2$
$p_1 = 0\ p_2 = 0\ p_3 = 0$
$p_0 = 1\ p_4 = 1$
Since $p_{1,2,3}$ are 0, the formula used is $p_0 * s_{i+0} + p_4 * s_{i+4} \pmod 2$

$s_0 = 0$
$s_1 = 1$
$s_2 = 0$
$s_3 = 0$
$s_4 = 1$

$s_5 = 1$
$s_6 = 0$
$s_7 = 0$
$s_8 = 0$
$s_9 = 1$

$s_{10} = 0$
$s_{11} = 0$
$s_{12} = 0$
$s_{13} = 0$
$s_{14} = 1$

$s_{15} = 1$
$s_{16} = 1$
$s_{17} = 1$
$s_{18} = 1$
$s_{19} = 0$

$s_{20} = 1$
$s_{21} = 0$
$s_{22} = 1$
$s_{23} = 0$
$s_{24} = 0$

$s_{25} = 1$
$s_{26} = 1$
$s_{27} = 0$
$s_{28} = 0$
$s_{29} = 0$

3. Consider the DES f-function. For a 32-bit input to this function `0xF5A6B7C8` and a 48-bit subkey `0xAAB1C2D3E4F5`,
determine the 32-bit output and give it in hexadecimal. (20 points)

Answer: Step 1.) Expansion
1111 0101 1010 0110 1011 0111 1100 1000
011110 101011 110100 001101 010110 101111 111001 010001

Step 2.) XOR
101010 101011 000111 000010 110100 111110 010011 110101 key
011110 101011 110100 001101 010110 101111 111001 010001 bits
110100 000000 110011 001111 100010 010001 101010 100100 XOR'd

Step 3 S-Boxes
s1
10 = 2
1010 = 10
s1 = 09

s2
00 = 0
0000 = 0
s2 = 15

s3
11 = 3
1001 = 9
s3 =15

s4
01 = 1
0111 = 7
s4 = 03

s5
10 = 2
0001 = 1
s5 = 02

s6
01 = 1
1000 = 8
s6 = 06

s7
10 = 2
0101 = 5
s7 = 03

s8 10 = 2
0010 = 2
s8 = 04
result
1001 1111 1111 0011 0010 0110 0011 0100

Step 4
permutation via table 3.12
11000110 11101001 01000101 10111110

C6E945BE

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! 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.

   Some free online textbooks include *Understanding Cryptography* by Paar et al., *The Joy of Cryptography* by Rosulek, or *A Graduate Course in Applied Cryptography* by Boneh and Shoup.

   Possible topics include the one-time pad, stream ciphers, LSFRs, or DES.

Answer: Use the stream cipher encryption operation to encrypt the ASCII characters "Hello" with the key "Crypto", and give its output in binary

01001000 01100101 01101100 01101100 01101111 00001010: Message
01000011 01110010 01111001 01110000 01110100 01101111: Key
00001011 00010111 00010101 00011100 00011011 01100101: Output