Hardware-Oriented Security and Trust
ECE 4156 HST / ECE 6156 HST
Spring 2025

Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology

Homework 4, 75 pts. (ECE 4156) 90 pts. (ECE 6156)
Due Friday February 7 prior to 11:55pm

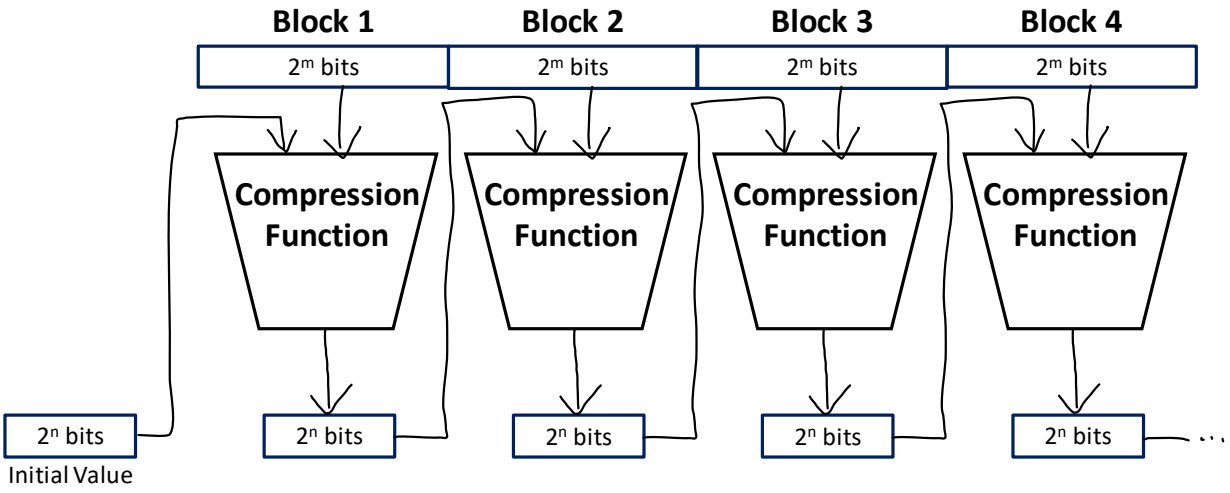
1) (15 pts.) Consider the stateful variant of CBC-mode encryption where the sender simply increments the *IV* by 1 each time a message is encrypted (rather than choosing *IV* at random each time). Show that the resulting scheme is *not* CPA-secure. (NOTE: this is problem 3.20 on page 104 of the 2nd edition of Katz and Lindell but appears to have been remove from the 3rd edition; I am not sure why.)

2) (10 pts.) What is the effect of a single-bit error in the ciphertext when using the CBC and CTR modes of operation? (NOTE: this is slightly simpler version of problem 3.21 on page 104 of the 2nd edition of Katz and Lindell which is problem 3.29 on page 103 of the 3rd edition.)

3) (10 pts.) What is the effect of a dropped ciphertext block (e.g., if the transmitted ciphertext $c_1, c_2, c_3, \ldots$ is received as $c_1, c_3, \ldots$) when using CBC and CTR modes of operation? (NOTE: this is slightly simpler version of problem 3.22 on page 104 of the 2nd edition of Katz and Lindell which is problem 3.30 on page 104 of the 3rd edition Katz and Lindell.)

4) (10 pts.) Say CBC-mode encryption is used with a block cipher having a 256-bit key and 128-bit block length to encrypt a 1024-bit message. What is the length of the resulting ciphertext? (NOTE: this is problem 3.23 on page 105 of the 2nd edition of Katz and Lindell which is problem 3.26 on page 103 of the 3rd edition of Katz and Lindell.)

5) (20 pts.) Use your own words (do not copy from any source!) to explain the Merkle-Damgård construction. Please assume four blocks and a compression function from $<2^m,2^n>$ to 2^n where n = 8 and m = 9. In your answer, make sure to answer the following questions: (i) what is the goal of the Merkle-Damgård construction and (ii) what does the Merkle-Damgård construction prove? You may use the picture on the next page in your answer.



6) (10 pts.) Consider the case where $N = 5$ and $t = 2$. This is a secret sharing scenario, e.g., five company executives where 2 out of the 5 must be present to enter their password information in order to open a safe. Now consider the case of a 10-bit key required to carry out an action (e.g., open a safe). This key will be predicted from the inputs provided by any two of the executives. Please note that as discussed in class the key would in an actual practical scenario have a large number of bits, e.g., 128; however, in this homework we are going to use a number less than one thousand (i.e., can be represented in ten bits) for ease of providing an answer.

a. (1 pt.) Choose a `key` between two and one thousand, email the TA, Arman Allahverdi, at aallahverdi3@gatech.edu and then check the course webpage for homeworks http://mooney.gatech.edu/Courses/ECE4156/hwlabexam/index.html to see if your number has already been taken or not. You need to make a first attempt to choose a number prior to 10am on Tuesday Feb. 4. If your first name, first letter of your last name, and selected number appear under hw4, you are done. Otherwise, prior to 10am on Wednesday Feb. 5, you need to make a second attempt to choose a number between one and one thousand and send another email to the TA. Again, if your first name and number appears under homework 4, you are done. Otherwise, prior to 10am on Thursday Feb. 6, you need to choose a third number. Please just use a decimal representation, i.e., choose between 2 and 999.

b. (9 pts.) For your given `key`, set the 10-bit key on the y-axis of a Cartesian plane consisting of zero to 1023 on the y-axis and zero to 1023 on the x-axis. Choose two points in Cartesian coordinates which define a line that intersects the y-axis at the `key` location. Specify these two 2-dimensional points `x1,y1` and `x2,y2`.

   NOTE: the points you choose must all have a y-axis coordinate different than the key, i.e., `y1` $\neq$ `key` and `y2` $\neq$ `key`.

7) [ECE 6156 only!] (15 pts.) Given your choice in 6.b, write pseudocode in a C-like syntax (or C++-like syntax or even a Java-like syntax) which, given two inputs from two of the executives, calculates the key. Use the code below as a starting point for your pseudocode. Please note that this problem will **not** be graded on *syntax* but rather on readability and correctness, so do please explain any assumptions with comments. For example, below the value `key` is the number you selected via email to the TA. Finally, please note that your pseudocode should work independently of the values of `key`, `x1`, `y1`, `x2` and `y2`.

```
int key;              /*  this is your key value selected in 2.a  */
int testkey(x1, y1, x2, y2) {
int x1,x2,y1,y2;
Boolean condition;   /*  condition is either equal to 1 or is equal to 0  */

/*  fill in pseudocode here  */

if (condition)
  return (1);         /*  if  x1,y1 and x2,y2  intercept the y-axis at  key  */
else
  return (0);     /*  if  x1,y1 and x2,y2  do not intercept the y-axis at  key  */
}
```

YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES, INCLUDING OTHER/PREVIOUS SECTIONS OF ECE COURSES TAUGHT BY PROFESSOR MOONEY SUCH AS THOSE WITH NAMES INCLUDING HARDWARE ORIENTED SECURITY AND TRUST AS WELL AS CRYPTOGRAPHIC HARDWARE FOR EMBEDDED SYSTEMS. ALL HOMEWORK SUBMISSIONS MUST INCLUDE YOUR NAME, COURSE NUMBER, SECTION, AND THE HOMEWORK SET NUMBER. ALL SUBMISSIONS MUST BE DONE ONLINE. ALL WRITING MUST BE EASY TO READ (FOR EXAMPLE, YOU MAY HAVE TO WRITE WITH THICK INK AND MAY NOT BE ABLE TO USE LOW RESOLUTION PHOTOS OF HANDWRITTEN DIAGRAMS). FAILURE TO PROVIDE CLEAR AND LEGIBLE ANSWERS MAY RESULT IN ZERO POINTS. ALL WORK MUST BE YOUR OWN. NO PLAGIARISM IS ALLOWED, AND YOU MUST PROPERLY REFERENCE ALL SOURCES OF YOUR INFORMATION – ALTHOUGH YOU SHOULD NOT LOOK FOR AND MAY NOT CONSULT "SOLUTIONS" AVAILABLE FROM OTHER SOURCES (TO REPEAT, YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES!).