CS 463/563 — Cryptography for Cybersecurity
Homework 7: Public-Key Cryptography

DUE DATE HERE

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

This assignment has **5** 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.

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. Suppose parties Alice and Bob are performing a Diffie-Hellman key exchange. For the following combinations of the prime p, a shared value $\alpha \in [2, p-2] \cap \mathbb{Z}$ (the

integers from 2 to $p-2$, inclusive), and choices of the private values a by Alice and b by Bob, compute the values $A = \alpha^a \pmod p$, $B = \alpha^b \pmod p$, and compute the shared keys Alice and Bob would generate: Alice's key $B^a \pmod p$ and Bob's key $A^b \pmod p$. (Hint: these values should end up being the same!) (10 points)

(a) $p = 11$, $\alpha = 6$, $a = 4$, $b = 5$.

(b) $p = 37$, $\alpha = 11$, $a = 13$, $b = 9$.

(c) $p = 59$, $\alpha = 15$, $a = 17$, $b = 20$.

Answer:

(a) $A = 6^4 \pmod{11} = \boxed{9}$
$B = 6^5 \pmod{11} = \boxed{10}$
$K_{AB} = 6^{4*5} \pmod{11} = \boxed{1}$

(b) $A = 11^{13} \pmod{37} = \boxed{11}$
$B = 11^9 \pmod{37} = \boxed{36}$
$K_{AB} = 11^9 \pmod{37} = \boxed{36}$

(c) $A = 15^{17} \pmod{59} = \boxed{35}$
$B = 15^{20} \pmod{59} = \boxed{7}$
$K_{AB} = 7^{20} \pmod{59} = \boxed{46}$

2. Show that in Diffie-Hellman key exchange, the keys $B^a \pmod p$ and $A^b \pmod p$ are equivalent. (5 points)

Answer: $B = \alpha^b \pmod p$
$B^a = \alpha^{ab} \pmod p$
$A = \alpha^a \pmod p$
$A^b = \alpha^{ba} \pmod p = B^a = \alpha^{ab} \pmod p$

3. Suppose you constructed an algorithm that can efficiently solve the discrete logarithm problem. What are the implications of this for Internet communication using Diffie-Hellman key exchange to derive initial keys? (5 points)

Answer: If an algorithm was developed to solve the Discrete Logarithm Problem, the Diffie-Hellman Key exchange would become insecure. Currently, it is computationally infeasable to solve $a = log\alpha A \pmod{p}$

4. Suppose Alice is sending a message to Bob, using ElGamal encryption. Suppose you are given the parameters of a prime p, a primitive element $\alpha \in \mathbb{Z}_p^*$, $K_{pr} = d \in [2, p-2] \cap \mathbb{Z}$ chosen by Bob, and the parameter $i \in [2, p-2] \cap \mathbb{Z}$ and message $x \in \mathbb{Z}_p^*$ chosen by Alice. For the following sets of values, first do Alice's computations: compute $K_{pub} = \beta = \alpha^d \pmod{p}$, $K_E = \alpha^i \pmod{p}$, $K_M = \beta^i \pmod{p}$, and the ciphertext $y = x \cdot K_M \pmod{p}$. Then, do Bob's computations: compute $K_M = (K_E)^d \pmod{p}$ (this should be equal to the K_M that Alice computed), $(K_M)^{-1} \pmod{p}$, and recover $x = y \cdot (K_M)^{-1} \pmod{p}$ (this should be equal to the x that Alice chose).
   (a) $p = 11$, $\alpha = 7$, $K_{pr} = 6$, $i = 4$, $x = 7$.
   (b) $p = 31$, $\alpha = 3$, $K_{pr} = 9$, $i = 5$, $x = 7$.
   (c) $p = 59$, $\alpha = 2$, $K_{pr} = 3$, $i = 7$, $x = 9$.

Answer:

(a) $K_{pub} = 7^6 \pmod{11} = \boxed{4}$
$K_E = 7^4 \pmod{11} = \boxed{3}$
$K_M = 4^4 \pmod{11} = \boxed{3}$
$y = 7 * 3 \pmod{11} = \boxed{10}$
$K_M = 3^6 \pmod{11} = \boxed{3}$
$x = 10 * 4 \pmod{11} = \boxed{7}$

(b) $K_{pub} = 3^9 \pmod{31} = \boxed{29}$
$K_E = 3^5 \pmod{3`} = \boxed{26}$
$K_M = 29^5 \pmod{31} = \boxed{30}$
$y = 7 * 30 \pmod{31} = \boxed{24}$
$K_M = 26^9 \pmod{31} = \boxed{30}$
$x = 24 * 30^{-1} \pmod{31} = \boxed{7}$

(c) $K_{pub} = 2^3 \pmod{59} = \boxed{8}$
$K_E = 2^7 \pmod{59} = \boxed{10}$
$K_M = 8^7 \pmod{59} = \boxed{50}$
$y = 9 * 50 \pmod{59} = \boxed{32}$

$K_M = 10^3 \pmod{59} = \boxed{56}$
$x = 32 * 39 \pmod{59} = \boxed{9}$

5. 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 discrete logarithms, Diffie-Hellman key exchange, or ElGamal encryption.

Answer: In regards to the discrete logarithm problem, using a brute fore attack, how large does n have to be to be considered resistant?
$\boxed{n = 2^{80}}$
If one was using a square root attack to solve the discrete logarithm problem, how large does n have to be to be consdidered resistant?
$\boxed{n = 2^{160}}$