CS 463/563— Cryptography for Cybersecurity
Homework 12: Key Exchange

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 as an encryption function.

Suppose Alice and Bob are establishing a secure session with the use of a Key Distribution Center (KDC). The KDC shares $k_A = \texttt{0xA6}$ with Alice and $k_B = \texttt{0xD8}$ with Bob.

(a) Upon a request to establish a session, the KDC randomly selects $k_{ses} = \texttt{0x7B}$. The KDC sends $y_A = Enc_{k_A}(k_{ses})$ to Alice and $y_B = Enc_{k_B}(k_{ses})$ to Bob. What are these values?

(b) Alice and Bob will then compute $Dec_{k_A}(y_A)$ and $Dec_{k_B}(y_B)$, respectively. What are these values?

(c) Suppose Alice chooses a message $m = \texttt{0x45}$. She will compute $y = Enc_{k_{ses}}(m)$, and send it to Bob. What is the value of y?

(d) Bob will decrypt y using k_{ses}. What is the result of this operation? Validate that it matches Alice's message and operations.

(10 points)

Answer:

(a) $e_{k_A}(K_{ses}) = A \oplus B \| \| 6 \oplus 7$
$e_{k_A}(K_{ses}) = 1010 \oplus 1011 \| \| 0110 \oplus 0111 = 00010001 = \boxed{= 11}$

$e_{k_B}(K_{ses}) = D \oplus B \| \| 8 \oplus 7$
$e_{k_B}(K_{ses}) = 1101 \oplus 1011 \| \| 1000 \oplus 0111 = 0110111 = \boxed{6F}$

(b) $d = Y_R \oplus K_R \| \| Y_L \oplus K_L$
$d_{K_A}(Y_A) = 6 \oplus 1 \| \| A \oplus 1$
$d_{K_A}(Y_A) = 0110 \oplus 0001 \| \| 1010 \oplus 0001 = 01111011 = \boxed{7B}$

$d_{K_B}(Y_B) = 8 \oplus F \| \| D \oplus 6$
$d_{K_B}(Y_B) = 1000 \oplus 1111 \| \| 1101 \oplus 0110 = 01111011 = \boxed{7B}$

(c) $e_{7B}(45) = 7 \oplus 5 \| \| B \oplus 4$
$e_{7B}(45) = 0111\ oplus 0101 \| \| 1011 \oplus 0100 = 00101111 = \boxed{2F}$

(d) $d_{7B}(2F) = B \oplus F \| \| 7 \oplus 2$
$d_{7B}(2F) = 1011 \oplus 1111 \| \| 0111 \oplus 0010 = \boxed{45 = m}$

2. Consider an adversary Carol who mounts a man-in-the-middle attack against Alice and Bob, who are attempting to perform a Diffie-Hellman key exchange.

Public parameters are $p = 17$, $\alpha = 4$. Alice and Bob choose $sk_A = 7$ and $sk_B = 8$, respectively. (10 points)

(a) What are Alice's public key pk_A and Bob's public key pk_B? What formula(e) did you use to derive these?

(b) Carol intercepts pk_A and pk_B, chooses $c = 6$, and computes $pk'_A = pk'_B = \alpha^c \pmod p$. What is this value?

(c) Carol sends pk'_A to Bob as if it were from Alice, and sends pk'_B to Alice as if it were from Bob. What are the shared session keys computed by each of Alice, Bob, and Carol? What formula(e) did you use to find this value? (Hint: Alice and Bob will each compute one key, and Carol should be able to compute both of these.)

Answer:

(a) $pk_x = \alpha^x$
$pk_A = 4^7 \pmod{17} = \boxed{13}$
$pk_B = 4^8 \pmod{17} = \boxed{1}$

(b) $pk'_A = pk'_B = 4^6 \pmod{17} = \boxed{16}$

(c) α^{ca}, α^{cb}
$\alpha^{ca} = 4^{6*7} = 16$
$\alpha^{cb} = 4^{6*8} = 1$

3. Research the concept of *key escrow*, and describe it in your own words. What are two (or more) potential risks from the mandated use of key escrow? (Hint: the Wikipedia page on key escrow is a good start, but it is insufficient.) (5 points)

Answer: Key escrow is having a trusted entity keep a decryption key until an authenticated person requires the key for decryption. This adds additional encryption, and it also keeps the amount of people who will need to see the key to a minimum.

One potential risk from mandated use of key escrow is that it defeats one of the key points of key escrow in that it keeps the amount of people who sees a key to a minimum. The key will become less secure every time someone new gets access to the key. So if an entity mandates that a key needs to be provided to them, that key becomes less secure and would need to be changed. The changing of keys could also be an inconvenient process.

Another potential risk from mandated use of key escrow is that once one key is compromised, any other data encrypted with that key becomes compromised if the principle of key freshness is not followed. It also makes key escrow a more severe central point of failure. For example, if every law enforcement agency could mandate access to a key, there would be thousands of entities that have a chance to compromise a key.

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 key exchange, man-in-the-middle attacks, and key escrow or theft.

Answer: How do certificates prevent man in the middle attacks?

By adding a layer of authentication to the communication. Certificates prove that a message comes from a certain person. By adding a certificate by using a certified authority, any message must first pass the verifiaction test from a user to know that the message matches the real identity of the sender of the message. So unless an attacker hijacks the certified authority long before communications take place, the attacker would not be able to format a message in a way that would pass the verification checks.