CS306: Introduction to IT Security (Fall 2021)
Homework #1, October 26, 2021

Instructor: Nikos Triandopoulos

Instructions

Please carefully read the following guidelines on how to complete and submit your solutions.

1. The homework is due on Tuesday, November 9, 2020, at 11:59pm. Late submissions are accepted subject to the policy specified in the course syllabus. Starting early always helps!
2. Solutions are accepted only via Canvas, where all relevant files should be submitted as a single .zip archive. This should include your typed answers as a .pdf file and the source code of any programming possibly used in your solutions.
3. Unless otherwise specified, for any assignment involving programming you may use any programming language of your choice. If asked, you should be able to explain details in your source code (e.g., related to the design of your program and its implementation).
4. You are bound by the Stevens Honor System. For this homework assignment you may work either by yourself or in pairs (in this case, your team of two should be named sufficiently well in your hand-in). Any collaboration beyond this is not allowed. You may use any sources related to course materials, but information from external sources must be properly cited. Your submission acknowledges that you have abided by this policy.

Problem 1: Shared or forgotten keys? (20%)

Long ago, Alice and Bob shared an n-bit secret key but now they are no longer sure they still possess the same key. To verify that the key k_a currently held by Alice is the same as the key k_b currently held by Bob, they need to communicate over an insecure channel.

(1) Which two basic security properties should be considered in the design of a secure protocol for solving the above problem and why these properties become relevant in this setting?

(2) Suppose that Alice and Bob use the following protocol to check if they store the same secret.

1. Alice generates a random n-bit value r.
2. Alice computes $x = k_a \oplus r$, and sends x to Bob.
3. Bob computes $y = k_b \oplus x$ and sends y to Alice.
4. Alice compares r and y. If $r = y$, she concludes that $k_a = k_b$—that is, Alice and Bob share a secret key.

Does the above protocol satisfy the two security properties identified in question (1)?

Problem 2: Perfect or imperfect ciphers? (30%)

(1) Assume that an attacker knows that a user's password is either $p_1 = \texttt{abcd}$ or $p_2 = \texttt{bedg}$. Say the user encrypts his password using the Vigenére cipher, and the attacker sees the resulting ciphertext c. Show how the attacker can determine the user's password, or explain why this is not possible, when the period t used by cipher is 1, 2, 3, or 4 respectively.

(2) Show that the mono-alphabetic substitution cipher is trivial to break when the attacker launches a chosen-plaintext attack. How much chosen plaintext is needed to recover the entire secret key? What is the shortest chosen single-message plaintext that you can find, which is a valid English message and would successfully recover the key? Finally, under which conditions, and why, is the mono-alphabetic substitution cipher perfectly secure (against a ciphertext-only attacker)?

Problem 3: Crypt-analyze this! (60%)

I just discovered that two of my TAs, Alice and Bob, have been secretly communicating with each other in our common group chat that we use for course matters. I often see unintelligible short texts on my screen to which I didn't pay attention, but now I suspect they plan behind my back. I am pretty sure they make use of one-time pad encryption with the following parameters: The message space consists of English messages which are 33 characters long, where only letters (of either case), spaces and possibly punctuation marks are used. Please help me break their code!

(1) Below are eleven ciphertexts (in hex format) that they exchanged just minutes before our class last week, on Tuesday, October 19, 2021:

```
2d0a0612061b0944000d161f0c1746430c0f0952181b004c1311080b4e07494852
200a054626550d051a48170e041d011a001b470204061309020005164e15484f44
3818101500180b441b06004b11104c064f1e0616411d064c161b1b04071d460101
200e0c4618104e071506450604124443091b09520e125522081f061c4e1d4e5601
304f1d091f104e0a1b48161f101d440d1b4e04130f5407090010491b061a520101
2d0714124f020111180c450900595016061a02520419170d1306081c1d1a4f4601
351a160d061917443b3c354b0c0a01130a1c01170200191541070c0c1b01440101
3d0611081b55200d1f07164b161858431b0602000454020d1254084f0d12554249
340e0c040a550c1100482c4b0110450d1b4e1713185414181511071b071c4f0101
2e0a5515071a1b081048170e04154d1a4f020e0115111b4c151b492107184e5201
370e1d4618104e05060d450f0a104f044f080e1c04540205151c061a1a5349484c
```

Write down the 11 plaintext messages that were exchanged. You may write a program that will help you with your cryptanalysis. In designing your program, remember that most likely spaces will be among the most frequent characters in the plaintexts, and carefully observe what their role may be in the mapping from plaintexts to ciphertexts. Explain what your cryptanalysis strategy is and what algorithm your program implements.

(2) To ease key management, my TAs change their shared key only every midnight. But rather than randomly generating (and securely exchanging) a new key every midnight, the TAs created an algorithm to automatically generate the new key pseudorandomly using the current (i.e., previous day's) key as input. That is, they replace the current key k_i with the new key $k_{i+1} = \mathsf{SHA}_{256}(k_i)\|00100001$, where $\|$ denotes concatenation. What is the key the TAs will be using the day that this homework is due?