ECE 3170

Cryptographic Hardware for Embedded Systems

Midterm I

October 1, 2024

This test is open book for the Schneier textbook and the optional textbooks. This test is also open note. Calculators are permitted but no programs may be used. Open notes include electronic notes with any handwritten or typed information you may have added. For electronic notes, all wireless connectivity must be turned off, and cell phones are not allowed; in other words, no connection to any information source outside of the classroom is allowed during the exam. Open notes also include all course assignments (homeworks or labs) as well as solutions (including both your solution as well as official solutions posted on the course website). All aspects of the Georgia Tech Honor Code apply. Please follow the instructions precisely. If you need to continue a problem, please use the back of the ***previous*** *page.* The meaning of each question should be clear, but please state any assumptions and ask for clarification if necessary.

You can do it!

Name (Please print)______________________________

This test will be conducted according to the Georgia Tech Honor Code. I pledge to neither give nor receive unauthorized assistance on this exam and to abide by all provisions of the Honor Code.

Signed___________________________________

Question	Score	Max
1		**15**
2		**20**
3		**10**
4		**15**
5		**10**
6		**10**
Total		**80**

1. **(15 pts.) RSA.**

Consider RSA with public encryption key pair *{e, n}* and private decryption key pair *{d, n}*.

(a) (5 pts.) For the RSA algorithm, why is it not possible for *'e'* in the encryption key pair to be equal to 2?

(b) (10 pts.) Alice is sending Bob a message in RSA. Let the encryption key pair be thus: *´e´* = 3 and *´n´* = *pq* = 55. What is the value of *´d´* in the decryption key pair which Bob must use to decrypt the message?.

2. **(20 pts.) The Needham-Schroeder Protocol.**

Consider the Needham-Schroeder protocol as presented in the course textbook where A is an identifier for Alice, B is an identifier for Bob, $E_A()$ is encryption with a symmetric key held by Alice, $E_B()$ is encryption with a symmetric key held by Bob, K is a symmetric key, and both R_A and R_B are nonces:

1) Alice to Trent: A,B,R_A
2) Trent to Alice: $E_A(R_A,B,K,E_B(K,A))$
3) Alice to Bob: $E_B(K,A)$
4) Bob to Alice: $E_K(R_B)$
5) Alice to Bob: $E_K(R_B\text{-}1)$

Now suppose that for "efficiency" the identifiers A and B are omitted from encryption in steps 2 and 3 of the protocol with the result as follows:

1) Alice to Trent: A,B,R_A
2) Trent to Alice: $E_A(R_A,K,E_B(K))$
3) Alice to Bob: $A,E_B(K)$
4) Bob to Alice: $E_K(R_B)$
5) Alice to Bob: $E_K(R_B\text{-}1)$

Without breaking any keys (i.e., none of the symmetric keys are discovered by Mallory), is it possible for Mallory to carry out a Man-in-the-Middle (MitM) attack on the "efficient" modified protocol above? If so, give at least one clear reason why it is possible and show some of the steps (but you will be graded based on the reason given not the specific steps). If not, give at least one clear reason why not and show some attempted steps which fail to successfully carry out a MitM attack (again, you will be graded based on the reason given not the specific steps; in other words, if you give a valid and clear reason but you have a few mistakes in your specific steps shown, you can still earn full credit, but if your reason given is faulty you will not earn full credit even if your steps as given are correct). Some assumptions are likely to be needed for your answer; if so, please clearly state any assumption you require. Please note that different assumptions may lead to different answers; all reasonable assumptions will be granted for full credit.

.

3. **(10 pts.) An Attack on Documentation Signed by a Hash Function.**

Consider the following scenario describing an attack on documentation signed by a deterministic hash function that is keyless.

You are given a one-way hash function (keyless) denoted by *h*() which produces an *m*-bit output where $m = 6$.

The goal of this attack is to produce three legal documents x_1, x_2 and x_3 which hash to the same value, i.e., $h(x_1) = h(x_2) = h(x_3)$. The three documents utilize three different names inside the documentation (e.g., for inheritance of money), but you are not sure which name you will need until the very last minute, so you want to be prepared.

(a) (5 pts.) Suppose you start out with three legal documents which are the same except that they have different names, e.g., Alex, John and Zach. Considering only the hash values of x_1, x_2 and x_3, what are the different possible outcomes of the hash value comparisons (list them all)? For example, one possible outcome is {$h(x_1) = h(x_2)$ but $h(x_2) \neq h(x_3)$}. How many different possible outcomes are there? For full credit you are required to list each possible outcome with brackets (for example, {$h(x_1) = h(x_2)$ but $h(x_2) \neq h(x_3)$} is a possible outcome and is delimited by brackets).

(b) (5 pts.) Of all the possible outcomes listed in your answer to part (a), which is the least likely? You also need to give an intuitive reason for your answer, but a mathematical answer is not required. For example you could say that that least likely outcome is that none of the hash values are the same, i.e., {$h(x_1) \neq h(x_2)$, $h(x_2) \neq h(x_3)$, $h(x_1) \neq h(x_3)$}, and you need to give at least one valid intuitive reason. For full credit in case of a correct answer, and for partial credit in case of an incorrect answer, please explain your answer in detail but with 10 sentences or less; any lack of clarity in your answer will result in lost points.

4. **(15 pts.) Padding Oracle Attack.**

Consider the following message *m_2* consisting of six bytes (one per letter):

```
ATTACK
```

For simplicity, assume that an eight-byte padded ciphertext *c_2* encoding of the above message results in the following:

```
0xFE3838FEC21B0202
```

(a) (5 pts.) How many times does the padding oracle attack have to submit to the oracle to discover the padding length for the above case? For full credit in case of a correct answer, and for partial credit in case of an incorrect answer, explain reasons for your answer; a correct numeric answer with no written explanation (in legible English) will receive zero points.

(b) (10 pts.) Now consider the second step in the padding oracle attack: discovery of the last byte B_0 of data in the message. In this case, the last plaintext byte in the message is `K`. As a result, B_0 = `K`. (Note that the full message m_2 is `ATTACK`.) In the padding oracle attack, values for Δ are constructed and used to discover B_0. Please note that Δ has eight bytes.

In the **worst** case, how many times must a new value of Δ be used in a submission to the oracle to discover the last byte B_0 of data in the message? For full credit in case of a correct answer, and for partial credit in case of an incorrect answer, explain your answer; a correct numeric answer with no written explanation will receive zero points.

5. **(10 pts.) Password Cracking.**

Consider the case of building a social media network for Georgia Tech (GT) undergraduate students where passwords need to be protected and safe including in the case of a successful attack on the password server. Users are required to create a 6-digit pin as their password. Suppose a secure hash algorithm called "SHA" is used is store a 128-bit hash of each password on the server. The SHA hash algorithm takes one second to run on a typical computer, does not use a key, and is public (i.e., known to any adversary).

Using a vulnerability in the server's security, Mallory is able to obtain the list of 20,000 password hashes (please assume for this question that GT has 20,000 undergraduate students all of whom have chosen passwords already). Over the next year (12 months), can Mallory obtain the original list of passwords used to create the 20,000 hash values obtained?

If you believe Mallory **can obtain** all 20,000 original passwords in one year or less, please answer "yes" and explain intuitively how. If you believe Mallory **cannot** obtain all passwords in exactly one year or less, please answer "no" and give at least one intuitive reason why Mallory has no chance or a statistically insignificant chance, on average, of being able to obtain all of the passwords.

Please note that a correct "yes" or "no" answer with **no** correct intuitive reason(s) given will earn zero points. If multiple reasons are given some of which are correct and some of which are incorrect, partial credit will be earned. If at least one correct intuitive reason is given for the correct answer with no incorrect intuitive reason(s), full credit will be earned.

6. **(10 pts.) A Brute Force Attack on DES Encryption.**

Consider a brute force attack on DES encryption. Suppose you have a file with a computer program which you know to be encrypted using DES. The goal is to decrypt the file. Assume that the program can be decrypted in one clock cycle on a Gigahertz processor and that a correct decryption is clearly evident (e.g., the decrypted file reveals a computer program which follows C++ syntax rules nearly perfectly) with no time needed to infer that the file has been decrypted correctly. Further assume that you have 1,000 computers (i.e., 1,000 Gigahertz processors).

(a) (5 pts.) Ignoring the existence of weak keys but using the fact that DES has simple relations, how many keys need to be tested in a brute force attack to decrypt the file? Please give your answer as a power of two, e.g., 2^7 means 2 raised to the power of 7.

(b) (5 pts.) Suppose the answer to part (a) above is 2^64 = 2^{64} (this is not the right answer!). How many days have to be spent on a brute force attack to have a 50% chance of correctly decrypting the file? Please do not forget that you have 1,000 computers available to carry out the brute force attack.

THIS IS THE LAST PAGE OF THE EXAM!