Final Exam

You must work by yourself and abide by the College of Engineering Honor Code. You may consult your notes; you are also permitted to use published sources (such as books or Internet references), though this should not be necessary except as noted in the questions. If you do use published sources, you are required to cite them, as in an academic paper.

This exam is due **Sunday, December 18 at 5pm**. Email your answers to `eecs398@umich.edu` with the subject line "Exam Submission". Please attach your solutions in a `.txt` or `.pdf` file named "*your uniqname*`_final`". You should receive a confirmation email within 15 minutes.

Answer TK of the TK numbered questions below. Show your work.

1. **Key Management**. The company that runs a public certificate authority (SSLTrust.us) needs to protect its root private key. If this secret falls into the wrong hands, the company will be sunk. However, if the secret is lost or forgotten, the company will also go under, so it needs a secure back up strategy.

   The CEO proposes that they encrypt the private key with a random password that is secretly chosen (e.g., "`7cQWh0yLAK1a`"), and each of the three board members get four characters of the password. In this example, the first board member is given "`7cQW________`", the second gets "`____h0yL____`", and the third gets "`________AK1a`". Each board member will be given a copy of the encrypted file, but in order to decrypt it, all three board members must combine their password shares to recreate the original password. Despite the CEO not trusting any of the board members individually, she can feel somewhat safe knowing none of them can decrypt the encrypted file on their own.

   (a) This scheme allows a board member to brute force a smaller space than an outside party. Assume the use of random twelve-character mixed-case alphanumeric passwords, and that an attack can test 10 million passwords per second. What is the expected time to success for a brute force attack by an outsider? By a single board member? By two colluding board members?

   (b) Devise a scheme that allows the CEO to give out three keys, which are useful only when all are combined and confer no brute-forcing advantage otherwise.

   (c) Suppose the CEO worries that any one of the board members might forget their individual key, or that they might be kidnapped and held for random. Devise a scheme similar to (b) that allows the secret to be recovered when *any two* board members' keys are combined, while still not giving any brute-forcing advantage to a lone board member.

2. **Authentication**. Many organizations (including U-M) have deployed two-factor authentication through the use of key fob–sized devices that display pseudorandom codes at a fixed time interval. These codes are generated based on a built-in clock and a device-specific secret S that is also stored on a central authentication server tied to the user's account. Here is one way such a device might work: Let n be the number of minutes that have elapsed since the UNIX epoch; output the first 20 bits of $\text{HMAC}_S(n)$. Successful authentication requires the user's username and password and the current pseudorandom code from the user's device.

   (a) Name three common attacks against authentication that are mitigated by these devices.

   (b) Name one common attack against authentication that is not mitigated.

   Some devices use a counter instead of a clock and generate a single-use code each time the user presses a button on the device. One way this might work is as above, letting n be a register that is initially zero; upon each button press, display the current code for one minute and increment n on the device; on each successful authentication increment n on the server.

   (c) Describe one security advantage of single-use codes compared to time-based codes.

   (d) Describe one usability advantage of single-use codes compared to time-based codes.

   A major usability problem with single-use codes in practice is that the counter on the device gets out of sync with the counter on the server, often as a result of inadvertant button pressees in the user's pocket.

   (e) Explain how we might extend the server to mitigate this without reducing security.

   As more and more organizations adopt these devices, end-users are burdened with carrying multiple devices, one for each entity to which they authenticate. Suppose instead that a central authority distributed and managed time-based devices (like the ones described above) for all users and companies, and allowed servers to verify a user's code through a public API.

   (f) Describe at least three serious vulnerabilities that this would introduce.

   Google and Facebook have adopted authentication systems that send a single-use code to the user via an SMS text message. Compare this approach to dedicated authentication devices.

   (g) Describe at least one security advantage of the SMS approach.

   (h) Describe at least three attacks that only apply to the SMS approach.

3. **Privacy and Anonymity**. In 2006, AOL published logs from its search engine that showed the queries performed by 650,000 randomly selected users during March–May of that year. To protect privacy, the company replaced each user ID with a unique integer.

   Here is one of the 37 million records:

AnonID	Query	QueryTime	ItemRank	ClickURL
6113006	pebbles flintstone	2006-04-01 23:49:37	89	http://www.eecs.umich.edu

   This record indicates that anonymous user #6113006 searched for "pebbles flintstone" at 11:49 pm on Saturday, April 1, 2006. The user subsequently clicked the 89th search result, which was something on the EECS website (the URLs are truncated after the hostname).

   People who downloaded the data quickly found that they could identify individuals by combining their search history with information from other sources. For instance, user #4417749 searched for "landscapers in Lilburn, Ga," several people with the last name Arnold, and "homes sold in shadow lake subdivision gwinnett county georgia." A reporter for the New York Times identified this user as Thelma Arnold from Lilburn, Georgia by matching these queries to area phonebook listings.

   AOL soon apologized and pulled the dataset, but it is still available for download from a variety of other sources, and sites such as AOLStalker.com and search-logs.com visitors to search an online copy interactively.

   (a) Who is user #4952848? Give a full name, location, and occupation. Make as convincing a case as you can that your identification is correct, drawing on information from other public sources. (Please do not attempt to contact this person.)

   (b) User #785409 is a minor celebrity who apparently is aware that his search data was disclosed and publicly identified. What specific inferences can people make about this person's life based on his search history that he would presumably have wanted to remain private? Point to specific queries to support each inference.

   (c) Suppose AOL had sanitized the data in each of the following ways prior to releasing it. Give a plausible scenario in which the release would still impact specific individuals by revealing information about them to third parties who otherwise would not have known it. State whatever assumptions you need about the information available to the third parties beforehand.

      i. If AOL had released the data without the AnonID field...
      ii. If AOL had released the data without the Query field...
      iii. If AOL had released *only* the AnonID and QueryTime fields...

   (d) **Extra credit.** Repeat part (a) for an AnonID that has not already been identified or flagged as identifiable in public. (Search carefully to make sure this is the case.) Do not attempt to contact the individual or publicly divulge your hypothesis about their identity.

4. **Applied Cryptography**. Professor Vuln would like to provide a simple mechanism to allow members of his massive research group to exchange confidential data in a peer-to-peer fashion. He decides to distribute a shared secret key k that will allow the group members to mutually authenticate each other. The protocol is given below.

	Alice		Bob
1	"Hello", random nonce n_1	$\longrightarrow$	
2		$\longleftarrow$	random nonce n_2, $\text{HMAC}_k(n_1)$
3	*verifies:* $\text{HMAC}_k(n_1)$		
4	$\text{HMAC}_k(n_2)$	$\longrightarrow$	
5			*verifies:* $\text{HMAC}_k(n_2)$

   (a) Mallory, an unauthorized outsider, is able to engage in authentication attempts with the group members (but she cannot intercept or modify the messages they send to each other). How can she gain access to the confidential data?

   (b) Modify the protocol so that it achieves mutual authentication securely while still using a single shared secret, and argue that your answer is correct.

   Professor Vuln has decided to use public-key cryptography with his class to reporting the grades from a recent test. He instructs each student to create a 2048-bit RSA key pair and post the public key (e,N) to the class discussion forum. The professor will encrypt each student's score s by computing $c := s^e \bmod N$ and post c to the forum alongside the student's name. The test was out of 100 points and the professor doesn't award partial points.

   (c) Assume that the professor safely receives the public key for each student. How can an attacker still easily learn the score of every student?

   (d) What additional steps should Professor Vuln take to prevent this?

5. **Distributed Denial of Service**. A popular attack tool among novice hackers recently has been the Low Orbit Ion Cannon (LOIC), which features a user-friendly GUI as well as an option to voluntarily add yourself to a botnet controlled via an IRC channel. TK(background).

   (a) Under the surface, LOIC is actually a fairly simple program. Find a copy of the LOIC source code, and explain how its primary (default) attack mechanism works.

   (b) Explain how you would defend against a distributed LOIC assualt as:

      i. the assault target;

      ii. an ISP upstream from the target.

   (c) Explain how to improve the LOIC to:

i. attack sucessfully despite your defense from (b)(i);

ii. attack sucessfully despite your defense from (b)(ii).

(d) What security principle that we have discussed this semester does this question embody [Ans: "Cat and Mouse game", or however you introduced this idea]

(e) (Bonus?) Describe how you would take over a LOIC instance who had voluntarily joined the botnet controlled by l33thax0r.net. State any assumptions your attack is making and ensure that they are reasonable.