One-Way Hash Function

C2.1. Why is the hash function $f(x) = x \mod 10000$ not a good one-way hash function?

C2.2. What does the number 2 means in the name of SHA-2? What does the number 256 means in the name of SHA-256?

C2.3. Please list the functions that can be used to calculate one-way hash function in PHP, SQL, and Python, respectively.

C2.4. An attacker gets a copy of the `shadow` file, and he tries to guess Bob's password. It was said that the salt value makes it much more difficult for the attacker to do so. Do you agree or not?

C2.5. Currently, the salt used in the `shadow` file is saved in the file in plaintext. Isn't it better not to save the salt in plaintext? Please explain.

C2.6. A developer writes the following in a post: "I am writing a login for a forum, and I would like to hash the password at the client side in JavaScript before sending it to the server. If the hash matches with the one stored on the server, the user will be allowed to log in." The developer believes that by sending the hash of the password, instead of sending the password directly, can improve the security. Do you agree or not, why?

C2.7. In Linux, the password hash is produced by applying a hash function for many rounds (e.g., 5000 rounds for SHA-512). This seems to waste time, Why does Linux do this?

C2.8. Suppose that in 1998, Alice used MD5 to generate a hash from her novel, and published the hash in the *Wall Street Journal*. She never had a chance to publish her book. Recently, a movie was made based exactly on the ideas of her novel, and a lot of scripts in the movie are from her novel verbatim, but she has received no credit or loyalty from the movie. She decided to sue the movie studio, but she heard that MD5's collision-resistance property had already been broken since 2004. She is not sure whether the hash she published can still serve as a valid timestamp. If you are a lawyer representing Alice, what would you do to convince the judge?

C2.9. Given `h = Sha256(K || M)`, where `K` is a secret and "||" means concatenation (no padding is involved in calculating `h`). Please describe how one can calculate `Sha256(K || X)` for a different message `X` without knowing `K`.

C2.10. Given `h = Sha256(M || K)`, where `K` is a secret and "||" means concatenation (no padding is involved in calculating `h`). Can you calculate `Sha256(X || K)` for a different message `X` without knowing `K`?

C2.11. In the length extension attack, do we need to know the length of the key?

C2.12. The following message K:M is fed into SHA256. (1) What will be used as the padding? (2) Given hash(K:M), we need to calculate hash(K:M:N) without knowing the value K. The string N should contain the following message "extra content". Please describe the actual content of N.

```
K   = abcd9313x
M   = 1234567890123456789012345678901234567890
K:M = abcd9313x:1234567890123456789012345678901234567890
```

C2.13. Charlie has arranged a blind date for Alice and Bob, who are both cryptographers, and they do not know each other before. Charlie also gave Alice and Bob a secret number K (nobody else knows K). Bob wants to make sure that the person he is dating is actually Alice, not somebody else. Please describe how Bob can ask Alice to securely prove that she is Alice (Alice will not reveal the secret number K to anybody).

C2.14. ★

You are safe guarding a gate; anybody passing the gate has to tell you a name and password. Since there is no sound protection, anybody nearby can hear what they say and get the password. To solve that problem, you are requesting that each password can only be used once. Initially, you give each authorized person a list of passwords, and ask them to cross one out each time when a password is used, so each password is used only once. However, you do not want to maintain such a list yourself; you only want to remember one number for each person (up to 32 bytes). You do not mind changing this number each time when a secret password is used. Please describe how you can do this.

C2.15. ★

You have a super-nature talent in stock prediction. You want to prove your talent to the entire world. You have predicted the next 10 days' stock values. Each day after the market is closed, you plan to reveal that day's prediction, so others can verify whether your prediction is correct or not. Obviously, you need to convince others that you know that day's stock value beforehand. You don't want to reveal your prediction before the market is closed, because you don't want others to benefit from your predictions. At the beginning, you can publish some numbers in a popular newspaper, but you can only afford to publish 64 characters in the newspaper.

C2.16. Can we use the hash collision attack to find a message M' for a given message M, such that hash(M') = hash(M)?

C2.17. If Bob happens to find two different messages M1 and M2 (each has 64 bytes), such that SHA256(M1) = SHA256(M2). Can you find another pair M3 and M4, such that SHA256(M3) = SHA256(M4)?