CS 161 Spring 2025 — Introduction to Computer Security — Discussion 6

Question 1 ***Why do RSA signatures need a hash?***

To generate RSA signatures, Alice first creates a standard RSA key pair: (n, e) is the RSA public key and d is the RSA private key, where n is the RSA modulus. For standard RSA signatures, we typically set e to a small prime value such as 3; for this problem, let $e = 3$.

Suppose we used a **simplified** scheme for RSA signatures that skips using a hash function and instead uses message M directly, so the signature S on a message M is $S = M^d \bmod n$. In other words, if Alice wants to send a signed message to Bob, she will send (M, S) to Bob where $S = M^d \bmod n$ is computed using her private signing key d.

Q1.1 With this **simplified** RSA scheme, how can Bob verify whether S is a valid signature on message M? In other words, what equation should he check, to confirm whether M was validly signed by Alice?

Q1.2 Mallory learns that Alice and Bob are using the **simplified** signature scheme described above and decides to trick Bob into beliving that one of Mallory's messages is from Alice. Explain how Mallory can find an (M, S) pair such that S will be a valid signature on M.

You should assume that Mallory knows Alice's public key n, but not Alice's private key d. The message M does not have to be chosen in advance and can be gibberish.

Q1.3 Is the attack in Q1.2 possible against the **standard** RSA signature scheme (the one that includes the cryptographic hash function)? Why or why not?

Question 2 ***Ra's Al Gamal***

Recall the ElGamal scheme from lecture:

- KeyGen$() = (b, B = g^b \bmod p)$
- Enc$(B, M) = (C_1 = g^r \bmod p, C_2 = B^r \times M \bmod p)$

Q2.1 Is the ciphertext (C_1, C_2) decryptable by someone who knows the private key b? If you answer yes, provide a decryption formula. You may use C_1, C_2, b, and any public values.

○ Yes ○ No

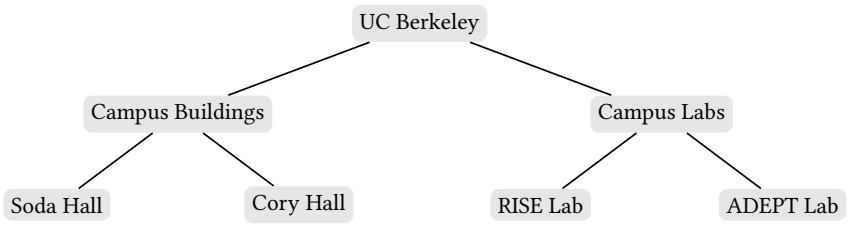
Q2.2 Consider an adversary that can efficiently break the discrete log problem. Can the adversary decrypt the ciphertext (C_1, C_2) without knowledge of the private key? If you answer yes, briefly state how the adversary can decrypt the ciphertext.

○ Yes ○ No

Q2.3 Consider an adversary that can efficiently break the Diffie-Hellman problem. Can the adversary decrypt the ciphertext (C_1, C_2) without knowledge of the private key? If you answer yes, briefly state how the adversary can decrypt the ciphertext.

○ Yes ○ No

Certificate authorities of UC Berkeley are organized in a hierarchy as follows:



Alice is a student in RISELab at UC Berkeley and wants to obtain a certificate for her public key. Assume that only RISELab is allowed to issue certificates to Alice.

Question 3 ***RISELab Shenanigans*** Q3.1

Which of the following values are included in the certificate issued to Alice? Select all that apply.

- ☐ Alice's public key
- ☐ Alice's private key
- ☐ A signature on Alice's *public* key, signed by RISELab's private key
- ☐ A signature on Alice's *private* key, signed by RISELab's private key
- ☐ None of the above

Q3.2 Assume that the only public key you trust is UC Berkeley's public key. Which certificates do you need to verify in order to be sure that you have Alice's public key? Select all that apply.

- ☐ Certificate for Alice
- ☐ Certificate for Soda Hall
- ☐ Certificate for RISELab
- ☐ Certificate for Campus Labs
- ☐ None of the above

Q3.3 RISELab issues a certificate to Alice that expires in 1 hour. Which of the following statements are true about using such a short expiration date? Select all that apply.

- ☐ It mitigates attacks where Alice's private key is stolen
- ☐ It mitigates attacks where RISELab's private key is stolen
- ☐ It mitigates attacks where Campus Labs' private key is stolen
- ☐ It forces Alice to renew the certificate more often
- ☐ None of the above