CS161 Fall 2025	Introduction to Computer Security	Discussion 6

Q1 *Why do RSA signatures need a hash?* (3 points)

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 (1 point) 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?

> **Solution:** $S^3 = M \bmod n$.

Q1.2 (1 point) Mallory learns that Alice and Bob are using the **simplified** signature scheme described above and decides to trick Bob into believing 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.

> **Solution:** Mallory should choose some random value to be S and then compute $S^3 \bmod n$ to find the corresponding M value. This (M, S) pair will satisfy the equation in part (a).
>
> **Alternative solution:** Choose $M = 1$ and $S = 1$. This will satisfy the equation.

Q1.3 (1 point) 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?

> **Solution:** This attack is not possible. A hash function is one way, so the attack in part (b) won't work: we can pick a random S and cube it, but then we'd need to find some message M such that $H(M)$ is equal to this value, and that's not possible since H is one-way.
>
> Comment: This is why the real RSA signature scheme includes a hash function: exactly to prevent the attack you've seen in this question.

Q2 *Ra's al Gamal* **(3 points)**

Recall the ElGamal scheme from lecture:

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

Q2.1 (1 point) 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

Solution: The decryption formula is $M = C_1^{-b} \times C_2$.

Q2.2 (1 point) 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

Solution: An adversary that can break the discrete log problem can recover r from $C_1 = g^r$ or b from $B = g^b$, so they can compute g^{br} and recover the original message.

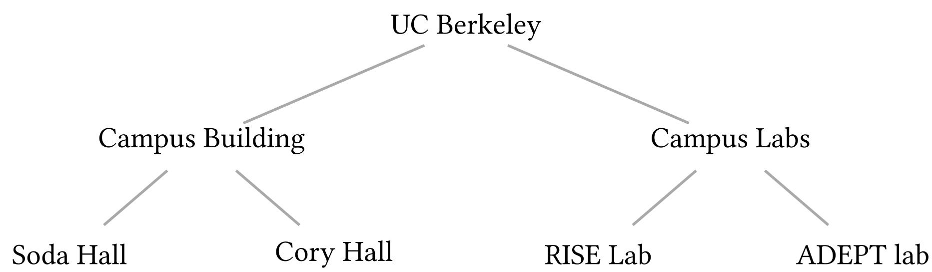
Q2.3 (1 point) Consider an adversary that can efficiently break the Diffie-Hellman problem. Can the adversary decrypt the ciphertext (C_1, C_2) without knowledge of the private key? If you answer yes, briefly state how the adversary can decrypt the ciphertext.

● Yes ○ No

Solution: An adversary that can break the Diffie-Hellman problem can recover g^{br} from $C_1 = g^r$ and $B = g^b$, so they can recover the original message.

Q3 *RISELab Shenanigans* **(3 points)**

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.

Q3.1 (1 point) Which of the following values are included in the certificate issued to Alice? Select all that apply.

- [x] Alice's public key
- [ ] Alice's private key
- [x] 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

Solution: This follows from the definition of certificates: they include a user's public key, and a signature on the enclosed public key, signed by the issuer (which we state in the prologue is RISELab).

Q3.2 (1 point) 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.

- [x] Certificate for Alice
- [ ] Certificate for Soda Hall
- [x] Certificate for RISELab
- [x] Certificate for Campus Labs
- [ ] None of the above

Solution: To validate Alice's public key, we can follow our way up to our root of trust (which is UC Berkeley's public key). As such, we need certificates for Alice, RISELab, and Campus Labs.

Q3.3 (1 point) 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

Solution: Short expiration times only mitigate the situation where Alice's private key is stolen. If RISELab's private key is compromised, the attacker can issue certificates with any expiration date, and it is up to the parent CA to revoke RISELab's certificate, not RISELab itself. The same argument applies to Campus Labs' private key.