CSE 347/547 DES 306/525: Usable Security and Privacy

Quiz II (TOTAL - 20 POINTS), September 11, 2025

RUBRIC

---

1. How does Hashing techniques make Authentication systems more Usable? [4 Points]

Hashing converts data into fixed-length values, enabling secure verification without storing original text, protecting against leaks and keeping login simple.

4 Marks if the idea of secure verification without storing original data is explained (wording may vary).

---

2. Is Public key crypto more usable than Symmetric? If so, why? [4 Points]

Yes, because it removes the need for secret key sharing and allows easy, safe key distribution.

Yes = 1 Mark, Correct reason (key sharing vs distribution) = 3 Marks.

---

3. What are the usability issues with current Public key Crypto systems? [4 Points]

Issues include **difficult key management**, **complex certificates/trust models**, **confusing interfaces**, and **user errors (lost keys, fake certificates)**.

1 Mark per valid issue (max 4).

---

4. What is the difference between usability studies and usability testing? [4 Points]

Usability studies are broader, focusing on understanding user needs and behavior.

Usability testing is task-based, checking how real users perform on the system.

Studies explanation = 2 Marks, Testing explanation = 2 Marks.

---

5. Is Security & Usability always a trade-off? Illustrate with an example. [4 Points]

Often yes—stricter security (e.g., complex passwords) lowers usability; but not always, as solutions like biometrics or password managers can improve both.

Yes/Often Yes (Trade-off point) = 1 Marks, Valid explanation = 3 Marks.