Rubric for Quiz IV (CSE 347/547 | DES 306/525) - Blueprint

1. Mention the issues with the current data anonymization techniques. [4 points]

- (1 point) Mentioning the risk of re-identification using quasi-identifiers.
- (1 point) Mentioning the risk of re-identification by cross-referencing with other public datasets.
- (1 point) Stating that a common technique (e.g., k-anonymity) is insufficient to prevent inference.
- (1 point) Explaining *why* the common technique is insufficient (e.g., through a homogeneity or other inference attack).

2. How can you be anonymous but still ensure the property of non-repudiation? [4 points]

- (1 point) Identifying the core solution (e.g., digital signatures, asymmetric/public-key cryptography).
- (1 point) Explaining the non-repudiation part (proving origin with a private key).
- (1 point) Explaining the anonymity part (the public key/digital identity is not linked to a real-world identity).
- (1 point) Clarifying that anonymity is at the *channel* level and non-repudiation is at the *message* level.

3. How does Biometric authentication improve usability? [3 points]

- (1 point) Identifying the core usability problem of traditional passwords (difficult to remember/manage).
- (1 point) Defining biometric authentication as a factor of "what entity **is**."
- (1 point) Explaining the usability benefit (no need to remember a secret or carry an object).

4. How would you prevent keylogging and Shoulder Surfing? [3 points]

- (1 point) Mentioning a valid defense for Key Logging (e.g., anti-spyware, on-screen keyboard, password manager).
- (1 point) Mentioning a valid defense for Shoulder Surfing (e.g., physical shielding, privacy screen, situational awareness).
- (1 point) Mentioning an authentication method not vulnerable to simple playback/observation (e.g., One-Time Passwords, Biometrics).

5. Are PIIs mandatory for performing authentication? Justify [3 points]

- (1 point) Answer: **No**.
- (1 point) Justification (Definition): Authentication is the process of binding an identity to a subject by proving one of the three factors (know, have, or are).
- (1 point) Justification (Explanation): Explaining that an anonymous or pseudonymous identity can be authenticated without requiring PII.

6. What are Password Salts? Why are they needed? [3 points]

- (1 point) What a salt is (a unique, randomly chosen value stored in plaintext alongside the hash).
- (1 point) Why (Primary): To defeat dictionary attacks and rainbow table attacks.
- (1 point) Why (Mechanism): Explaining that it forces an attacker to compute hashes for each user individually and ensures identical passwords have different stored hashes.