CSE 347/547 DES 306/525: Usable Security and Privacy
Quiz I (TOTAL-20 POINTS), Sept. 1. 1025
RUBRIC

1. Why do we need Diffie-Hellman key exchange. What is it vulnerable to? [4 points]
We need Diffie–Hellman to establish a shared secret key over an insecure channel without pre-sharing the key. It is vulnerable to Man-in-the-Middle attacks, where an attacker intercepts and creates separate keys with each party.

2. Is Synunetric Key Crypto systems usable? Justify your answers [3 points]
No, because key management/distribution of key is difficult. Securely sharing and storing a single secret key among many users is impractical.

3. Why is Usable Security important? [4 points]
Users make mistakes; systems must detect, tolerate, and adapt to them. Since most breaches are user-related and product success depends on ease of use, safety, and satisfaction, usable security is essential.

4. What are the various components/tuple in any Crypto system. Explain [4 points]
A cryptosystem is a 5-tuple *(E, D, M, K, C)* :

M = message/plaintext

C = ciphertext

K = keys

E = M x K → C is the set of encipher (encryption) functions

D = C x K→M is the set of deciphering (decryption) functions.

5. What makes usable security hard? [3 points]
Usable security is hard mainly because of users. Designing systems around real user needs is difficult, and usability alone is not enough. Systems must remain secure even when attackers try to fool users, or when users are careless, stressed, busy, or unmotivated.

6. How is Substitution different from Transposition[2 points]

Substitution → replace characters with others (e.g., A→X).
Transposition → rearrange characters without changing them (e.g., ABC → CAB).