Database Security and Blockchain

IMPORTANT NOTES:
Study lecture materials at least 1 hour and prepare Q1-2 prior to the tutorial session. Prepared questions will be discussed in the tutorial session.

1. Explain the nature of the inference threat to a relational database management system (RDBMS).
2. List and briefly describe two approaches to inference prevention for statistical database.
3. What are the disadvantages to database encryption?
4. A database of customer transactions purchased from a supermarket has a column 'Product type' that indicates the type of item purchased. This database column is encrypted with a searchable encryption system using deterministic encryption. Suppose an attacker having access to the encrypted database knows that the most common item type purchased from a supermarket is usually bread. Explain how the attacker can use this information to determine which rows of the encrypted database correspond to a purchase of bread.
5. If the hash function in the Bitcoin blockchain is not one-way secure, explain how the attacker can double spend a coin.

Optional Questions

1. In Bitcoin, miners need to produce a proof-of-work consisting of finding a hash input x such that $H(x \parallel h)_N = 0^N$ ($\parallel$ is the concatenation symbol), where h is a given hash of the previous blocks, $H(z)_N$ denotes the N leftmost bits of the hash value $H(z)$ and 0^N denotes the string of N 0 bits. Assume that one hash evaluation of H takes 1 microsecond (10^{-6} seconds) on a miner computer. For a proof-of-work challenge with $N = 32$, how long does it take for the miner to solve this challenge on average?