Q1: 3. Factor very large numbers.

Q2: 2. Its factors can be determined using Shor’s algorithm.

Q3: AES-GCM is preferred because of two main reasons, one is that is has better security, the ciphering step for AES-CBC requires padding, and thus might get padding Oracle attack; another is that is has better efficiency because it supports parallel calculating.