1.

Ans:2,3

Since the two registers are entangled, measuring the output register will have the effect of partially collapsing the input register into an equal superposition of each state between 0 and q-1 that yielded c (the value of the collapsed output register.)

Shor's algorithm is a quantum computer algorithm that can solve prime factors of an integer in polynomial time. It allows us to factorize into prime numbers in O(logN ^3) time and O(logN) space.

2.

Ans:1,2,4

RSA's security, on the other hand, is based on the difficulty of prime factorization of very large numbers. It is known that a quantum computer can achieve an exponential speedup over classical computers using Shor's algorithm

3.

AES-CBC mode combined with decent HMAC can be as secure as AES-GCM. However, combining the cipher and MAC securely has been in practice found to be much easier said than done. Also, padding that is required by AES-CBC mode complicates things.

In particular, within the history of the SSL and TLS protocols, there is a long history of security vulnerabilities resulting from misuse of CBC mode or within combination of CBC and MAC, such as BEAST and Lucky13.

After the Lucky13 attack (a timing oracle caused by MAC-then-encrypt), it was thought that TLS should change ordering of the operations. Changing order of the operations would have affected the backwards compatibility with previous implementations so it was after all thought that it is more practical to switch to authenticated encryption only.

In addition to security aspects, there are some other practical benefits of AES-GCM over AES-CBC and HMAC:

(1)On most platforms with hardware acceleration or AES-NI instructions, AES-GCM is many times faster than AES-CBC with HMAC. This is because AES-GCM is designed to be more parallelizable.

(2)Generation of random bits is relatively slow. This is also where AES-GCM excels. Random bits are more seldomly needed than with AES-CBC (in TLS 1.1+.)

(3)AES-GCM in average does not extend the size of the message as much as equivalent combination of AES-CBC, HMAC and padding.