Quiz 6

109550135 范恩宇

1. **Shor's Algorithm can be used to do which of the following?**

   Answer : 3

   Shor's algorithm is known for its ability of factoring very large integers efficiently , by taking advantage of the properties of quantum , superposition and entanglement as part of its implementation , but it doesn’t directly create superposition nor entanglement . In additionally , it doesn’t increase algorithm time but decrease it .

2. **Why would RSA encryption be considered unsafe from quantum algorithms?**

   Answer : 1,2,4

   Shor's Algorithm exploits quantum principles , making large-integer factoring efficient , which can be done in polynomial time . This results in the insecurity of RSA from quantum algorithms .

3. **Why is AES-GCM preferred and the AES-CBC support was removed in TLS1.3 ?**

Answer :

The reasons are :

I. AES-GCM provides authenticated encryption , making it able to do encryption and authentication in single step . It uses Galois/Counter Mode to provide confidentiality and integrity protection at the same time . In contrast , AES-CBC requires an additional step for integrity protection , such as using HMAC , which also introduces complexity and potential vulnerabilities .

II. AES-GCM is parallelizable and can take advantage of modern hardware acceleration (ex : AES-NI instructions in many modern processors) , speeding up encryption and decryption process significantly . While AES-CBC requires sequential processing and has a higher computational overhead .

III. TLS 1.3 aims to simplify and streamline the protocol , so it removes older or less secure cipher suites and focusing on modern cryptographic algorithms , which results in removement of AES-CBC .

IV. AES-GCM is widely supported and has become the recommended encryption mode for many applications and protocols.