Lattices & CRYSTALS-Kyber - GoHack24

Verifier: **R. Hedayat**

Prover: _____

1. Wofür steht Kyber in CRYSTALS-Kyber?
    A. Ein Algorithmus für symmetrische Verschlüsselung.
    B. Ein Schlüssel-Kapselungs-Mechanismus (KEM).
    C. Ein digitales Signaturschema.
    D. Eine Alternative zu AES.

2. Auf welchem mathematischen Problem basiert die Sicherheit von Kyber?
    A. Faktorisierung grosser Zahlen.
    B. Diskreter Logarithmus.
    C. Learning With Errors (LWE) über Modulgittern.
    D. Hash-Kollisionen.

3. Welchen Sicherheitsstandard zielt Kyber ab?
    A. Post-Quantum-Kryptographie.
    B. Klassische Kryptographie.
    C. Blockchain-Kryptographie.
    D. Symmetrische Kryptographie.

4. Welche Rolle spielt Rauschen (Noise) in Kyber?
    A. Es verschlüsselt die Nachricht direkt.
    B. Es sorgt für Robustheit gegen Fehler.
    C. Es macht das Lösen des LWE-Problems schwerer.
    D. Es reduziert die Grösse des Schlüssels.

5. Was macht Kyber im Vergleich zu klassischen kryptographischen Algorithmen sicher?
    A. Es verwendet Blockchiffren.
    B. Es basiert auf Problemen, die auch mit Quantencomputern schwer zu lösen sind.
    C. Es verwendet sehr grosse symmetrische Schlüssel.
    D. Es nutzt keine modularen Operationen.

6. Welche der folgenden Eigenschaften beschreibt CRYSTALS-Kyber NICHT?
    A. Geeignet für den Schlüsselaustausch.
    B. Bietet Quantenresilienz.
    C. Kompakte Schlüsselgrössen im Vergleich zu anderen Post-Quantum-Algorithmen.
    D. Basierend auf elliptischen Kurven.

7. In welchem Projekt wurde Kyber als Standardisierungskandidat ausgewählt?
    A. ISO Blockchain-Projekt.
    B. TLS 1.3-Projekt.
    C. NIST Post-Quantum-Kryptographie-Projekt.
    D. FHE-Standardisierungsprojekt.

8. Welche der folgenden Algorithmen ist kein Teil von CRYSTALS?
    A. Kyber
    B. Dilithium
    C. ElGamal
    D. Module-LWE

9. Bei der vorgestellten Enkodierungsfunktion des simplen LWE-basierten Systems würde eine Nachricht $msg \in \mathbb{Z}_7$ auf die folgende Menge gemappt:
    A. $\{0, 1\}$.
    B. $\{0, 3\}$.
    C. $\{0, 1, 2, 3, 4, 5, 6\}$.
    D. Ein Wert zwischen 0 und 1.

10. Die Multi-Bit Verschlüsselung beim simplen LWE-basierten Kryptosystem kann durch die folgende Massnahme erreicht werden:
    A. Einführen von Polynomringe als Datenstruktur.
    B. Reduzierung der Dimension im Lattice.
    C. Erhöhung der Anzahl der Fehlerwerte (Noise).
    D. Verwendung eines konstanten Schlüssels für alle Nachrichten.