

1. Comprehensive Exam Notes

A. Quantum Threats to Classical Cryptography

- **Shor's Algorithm:**

- Efficiently factors large integers (RSA) and computes discrete logarithms (DH, ECDSA).
- Breaks most current public-key cryptography.

- **Grover's Algorithm:**

- Speeds up brute-force search: reduces complexity from $O(N)$ to $O(\sqrt{N})$.
- Weakens symmetric encryption and hash functions.

- **Impact:**

- RSA, DH, ECC become insecure.
 - AES and SHA require doubled key/length sizes for same security.
-

B. Post-Quantum Cryptography (PQC)

- Cryptographic systems believed to resist attacks by both classical and quantum computers.
- **Can be implemented on classical computers.**

Major PQC Categories:

- **Lattice-based** (e.g., Kyber, Dilithium): Based on Learning With Errors (LWE)
 - **Code-based** (e.g., Classic McEliece): Based on decoding random linear codes
 - **Hash-based** (e.g., SPHINCS+): Stateless/stateful hash trees
 - **Multivariate polynomial** (e.g., Rainbow)
 - **Isogeny-based** (e.g., SIDH - now broken)
-

C. NIST PQC Standardization Project

Timeline:

- **2016:** Project started

- **2017:** 1st round - 82 submissions
- **2019:** 2nd round - 26 proposals
- **2020:** Round 3 - 7 finalists + 8 alternates
- **2022:** Round 3 winners announced
- **2024:** Final standards (FIPS) released

Finalized Standards (FIPS):

- **FIPS 203:** ML-KEM (Kyber)
- **FIPS 204:** ML-DSA (Dilithium)
- **FIPS 205:** SLH-DSA (SPHINCS+)
- **FIPS 206:** FN-DSA (FALCON)

Key Points:

- Kyber (encryption), Dilithium/FALCON (signatures), SPHINCS+ (hash-based backup)
- Rainbow was broken before finalization

D. Migration and Future Outlook

• Quantum Readiness:

- Shelf life of data vs time to migrate
- Experts expect RSA-2048 to be broken within 25-30 years

• Big Theoretical Questions:

- Are NP-complete problems in BQP?
- Is $P = NP$?
- Are cryptographic hard problems still safe?

2. Hands-On Tasks

A. OpenSSL Simulations

- Simulate key pair generation:

```
openssl genpkey -algorithm RSA -out rsa_key.pem -pkeyopt rsa_keygen_bits:2048
```

- Replace with post-quantum tools (e.g., using liboqs + OpenSSL)

B. Research Tasks

- Compare Kyber vs RSA in terms of key size, encryption speed
 - Explore NIST PQC GitHub repo for current draft APIs
-

3. Practice Q&A

Q1: What makes Shor's algorithm dangerous to RSA?

A: It factors large integers efficiently, breaking RSA's core assumption.

Q2: Why is AES still considered safe in a quantum context?

A: Grover's algorithm only halves brute-force complexity; doubling AES key size mitigates this.

Q3: What is the significance of the Kyber algorithm?



A: It is a lattice-based KEM selected by NIST for standardization due to its efficiency and security.



Q4: What does "quantum-safe" mean?

A: Resistant to both classical and quantum attacks.

4. Active Recall Practice

MCQs

1. Which algorithm can break RSA?
2. a) Grover's
3. b) Shor's 
4. c) Regev
5. d) Kyber
6. Which of the following is post-quantum secure?
7. a) RSA
8. b) ECDSA
9. c) Kyber 
10. d) SHA-1

11. Which algorithm is used in FIPS 204?
12. a) Kyber
13. b) SPHINCS+
14. c) Dilithium 
15. d) FALCON
16. What is the best mitigation for Grover's algorithm?
17. a) Abandon symmetric crypto
18. b) Double key sizes 
19. c) Use ECC
20. d) Nothing
-

Fill in the Blanks

1. Shor's algorithm breaks cryptosystems like ____ and ____.
2. **RSA, ECDSA**
3. The NIST PQC standard for encryption is based on the ____ algorithm.
4. **Kyber**
5. A post-quantum signature scheme based on hash trees is called ____.
6. **SPHINCS+**
7. The term "quantum-safe" means resistant to ____ and ____ attacks.
8. **Classical, Quantum**
-

Short Answer Questions

1. **Why is post-quantum cryptography important today even before quantum computers exist?**
2. Data encrypted now could be stored and decrypted in the future when quantum computers become available. Early migration prevents future exposure.
3. **How does the Kyber KEM work at a high level?**

4. It uses lattice-based mathematics to perform key encapsulation securely with small key sizes and high efficiency.

5. **Explain why Grover's algorithm is not as threatening as Shor's.**

6. Grover only provides quadratic speedup for brute-force attacks, which symmetric crypto can handle by doubling key sizes.

End of Week 10 Summary