Applications in Cryptography and Security

Distinguish quantum effects on factoring, generic search and communication security.

Core 22 min lesson Dr. Charith Jayasekara

By the end, you'll be able to

- Trace a toy order-finding factor recovery.
- State the assumptions behind a generic search advantage.
- Match post-quantum standards to KEM and signature roles.

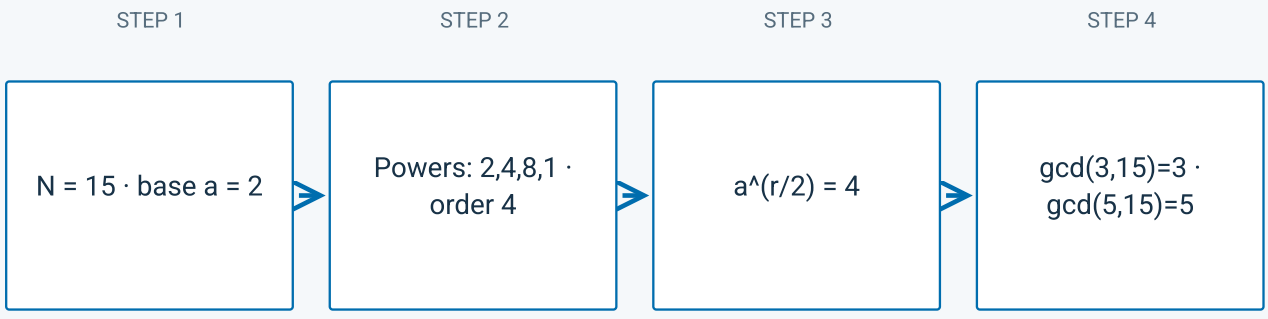
Match the algorithm to the cryptographic assumption

Quantum algorithms affect different security mechanisms in different ways. Shor-type algorithms address factoring and discrete logarithms. Grover-type search changes a generic exhaustive-search query scale. Quantum key distribution uses physical protocols with a different security model. Post-quantum cryptography is designed to run on classical systems while resisting known quantum attacks. These categories should not be merged into a claim that "quantum breaks encryption."

Prerequisites: oracles, complexity and the Shor/Grover chapters. This lesson explains algorithmic relationships; an operational cryptographic migration must follow current standards, implementation guidance and an organisation's threat model.

WORKED DIAGRAM · A33

Toy factor recovery



This small arithmetic example explains the period-to-factor mechanism; it is not a resource estimate for RSA-2048 or a completed cryptographic attack.

The security-task setup

Specify the primitive, parameter set, attacker goal and access model. Factoring an RSA modulus is not the same task as searching a symmetric key, forging a signature, finding a hash collision or distinguishing a protocol transcript. State whether an attacker has classical examples, a coherent verification oracle or physical access to quantum states. Different access assumptions produce different bounds.

Also distinguish mathematical algorithm cost from a feasible attack implementation. A logical circuit count excludes error correction, routing, resource-state preparation and control unless those are explicitly added. A conditional resource study is neither a completed break nor a prediction of the date at which one will occur.

Worked example: toy RSA arithmetic

Use the small modulus 15 only to understand the algebra. Choose base two. Its powers modulo 15 cycle through two, four, eight and one, so the order is four. Half that order is two, giving two squared equal to four. The greatest common divisors of four minus one and four plus one with 15 are three and five.

This is the classical postprocessing used after an order-finding result. The tiny example is easy by hand and does not model the physical resources needed for RSA-2048. Its purpose is to explain why a period can reveal factors. A scalable attack requires coherent modular arithmetic, sufficient precision and a reliable full computation. Shor's primary algorithm paper.

For dated resource context, use the noise and hardware lesson and the resource-estimation chapter. They compare primary architecture studies through their error, timing, connectivity and reliability assumptions. The correctness of the factoring algorithm and the engineering feasibility of a cryptographic-scale implementation are separate questions.

Write the order and the two factor-extraction calculations together.

$$2^4 \equiv 1 \pmod{15}, \quad r = 4, \quad x = 2^{r/2} = 4, \qquad \gcd(x-1, 15) = 3, \quad \gcd(x+1, 15) = 5.$$

The order is the smallest positive exponent returning one. This tiny example explains the factoring reduction; physical resources for cryptographic parameters require a separate dated analysis.

Generic search is a different advantage

In an ideal one-marked-item black-box model, a key space of size two to the power k has a Grover query scale of two to the power half k. This is a quadratic query improvement, not the polynomial-time factoring behaviour associated with Shor. The oracle must implement the relevant encryption and verification coherently, with its reversible-workspace and gate costs.

For a toy eight-bit key space, there are 256 candidates and a square-root scale of 16. This illustrates the exponent change but is not an attack estimate for a deployed cipher. Multiple matching keys, limited known plaintext, parallelisation, depth limits and fault-tolerant costs can all affect the concrete analysis. Grover's primary search paper.

Hash preimages and hash collisions are different problems with different quantum algorithms and bounds. Do not apply a square-root rule to every security property by analogy. Identify the attacker's actual success condition before choosing a resource model or interpreting a nominal security-bit count.

A quadratic search improvement changes the exponent of a key-space size.

$$N = 2^k, \qquad \sqrt{N} = 2^{k/2}, \qquad k = 8: \quad N = 256, \quad \sqrt{N} = 16.$$

k is the key length and the square-root expression is the characteristic query scale for one marked key with a coherent verification oracle. It is a scaling illustration, rather than an exact iteration count or a complete attack time.

Post-quantum standards run on classical computers

NIST's ML-KEM standard specifies a module-lattice-based key-encapsulation mechanism. It establishes shared-secret material under its security assumptions; it is not a digital signature or a quantum communication protocol. FIPS 203.

ML-DSA and SLH-DSA are digital-signature standards with different underlying constructions and trade-offs. FIPS 204, FIPS 205. Naming their roles correctly matters: replacing an RSA use requires understanding whether it supplies key establishment, authentication or another protocol function. Standard pages and their errata should be checked when implementing current systems.

Quantum key distribution is another task

In a simplified BB84 experiment, random preparation and measurement bases create a sifted subset of shared bits. Errors can indicate noise or an adversary, but an error statistic alone does not identify their cause. A full secure protocol needs authenticated classical communication, parameter estimation, error reconciliation, privacy amplification and a finite-key analysis.

The book's BB84 lab is a statistical teaching model and does not generate a secure key. Quantum transmission does not remove endpoint compromise, authentication requirements or implementation vulnerabilities. Keep the theorem's physical and adversarial assumptions attached to any security statement.

A practical reasoning workflow

Inventory the security function and its parameters. Identify the best relevant classical and quantum algorithmic attacks. Translate their abstract access models into a plausible implementation, including physical resources and uncertainty. Separate long-lived confidentiality risks from immediate attack capability. Consult current standardisation and implementation sources before choosing replacements.

For education, compare one factoring example, one generic-search example and one key-establishment/signature classification exercise. This gives students a concrete map of the field without implying that all primitives share one failure mechanism or one migration action.

Separate a resource update from a security conclusion

A lower qubit estimate changes one part of a conditional attack analysis. It does not establish that the necessary qubits, gates, connectivity, timing and control have all been demonstrated together. Conversely, uncertainty about hardware arrival does not make mathematical vulnerabilities disappear. Security planning and hardware forecasting answer different questions and should use different evidence.

A student can practise this distinction by writing two sentences about the same resource paper. The first states its target, assumptions and estimated resources. The second states what was actually demonstrated or calculated. If those sentences become identical without an experimental basis, the explanation has probably promoted a design estimate into a hardware claim.

For a protocol inventory exercise, record whether each cryptographic use protects long-lived confidentiality, authenticates messages or establishes session material. That role classification comes before selecting a replacement. It also reveals why one post-quantum algorithm cannot be substituted blindly at every location where an older public-key primitive appears.

Practical migration work: an Australian example

Start with a cryptographic inventory. Record the service, cryptographic purpose, algorithm and implementation, protected-data lifetime, owner, supplier dependency and an acceptance test. Work with a fictional system first so the exercise can be shared without exposing operational details.

Fictional service	Present use	Migration question	Acceptance evidence
Patient-record exchange	Public-key key establishment for encrypted transport	How long must recorded traffic remain confidential, and which peers support the replacement?	Interoperability, failure handling and downgrade tests
Software updater	Digital signatures on release manifests	How will old devices obtain and verify a new trust chain?	Valid, invalid, expired and rollback manifest tests
Backup archive	AES-256 data encryption with public-key wrapping	Which wrapping keys and historical records need attention?	Restore, key rotation and recovery tests

A KEM and a signature have different jobs. Keep the protocol purpose visible while choosing a standard and implementation. Plan a staged test environment, vendor coordination, performance and message-size measurements, monitoring and rollback. Cryptographic agility means being able to change supported mechanisms through a controlled process.

Guidance checked 6 November 2026. ASD's September 2026 Information Security Manual says RSA, DH, ECDH and ECDSA will no longer be approved beyond 2030, and includes a maintained post-quantum transition-plan control. These are requirements within the ISM's scope, rather than a prediction of when a quantum attack machine will arrive. Check the controls and applicability for the system being assessed. ASD cryptography guidelines, September 2026.

NIST's final standards include FIPS 203 (ML-KEM), 204 (ML-DSA) and 205 (SLH-DSA), released in August 2024. Its current process lists FN-DSA/FIPS 206 as under development, while HQC has been selected for standardisation and that work is continuing. Distinguish a final standard, a selected candidate and a deployed implementation. NIST standardisation status.

Migration checkpoint

Choose the software updater. Produce an inventory row and two tests that must pass before a signature migration can be rolled out.

> Compare a worked response
>
> Record the signature's purpose, supported formats and algorithms, verifier library, trust-anchor distribution, device lifetime, owner and vendor support. Test that the new verifier accepts a correctly signed release and rejects a changed manifest. Also test old-device compatibility, trust-chain updates, downgrade attempts, rollback policy and recovery when a supplier or trust anchor changes. A deployment decision needs evidence from the actual system and its applicable requirements.

Exercises and worked answers

Exercise 1. For modulus 15 and base four, find the order and test the factor-recovery step.

Check the worked answer

Four squared is one modulo 15, so the order is two. Half-order power is four. The greatest common divisors of three and five with 15 give three and five. A valid order result still requires checking the standard factor-recovery conditions.

Exercise 2. Can ML-KEM directly replace a digital-signature verification function?

Check the worked answer

No. A KEM establishes secret material, while a signature authenticates a signed message under its verification model. Protocol roles must be matched before selecting a replacement. The fact that both are post-quantum standards does not make their interfaces interchangeable.

Check your understanding

PAUSE & THINK

Can a key-encapsulation mechanism directly replace a digital-signature verifier?

- ☐ Yes, because both are cryptographic
- ☐ No; their protocol functions differ
- ☐ Only if it uses quantum transmission

Answer: No; their protocol functions differ. A KEM establishes shared-secret material. A signature authenticates a signed message under its verification model. Match the protocol role before selecting a replacement.

Sources

- Shor's primary algorithm paper
- Grover's primary search paper
- FIPS 203
- FIPS 204
- FIPS 205
- ASD cryptography guidelines, September 2026
- NIST PQC standards and process