

Chapter 22: Cryptographic Consequences

This section is already in the book plan, but it has not been written fully yet. The book owner can press Generate section to write this part with the language model connected to TheoryTrace.

Section plan:

Connects Shor's algorithm to RSA, Diffie-Hellman, elliptic-curve cryptography, and the motivation for post-quantum cryptography. The chapter explains what Shor breaks, what it does not break, and how security assumptions change in a quantum world.

References

References will be added when this section is generated.

Document information

Chapter 22: Cryptographic Consequences

Project	Shor's Algorithm from First Principles
Document	Document 1.26
Author	mujirin
Verifier	Not verified
Downloaded	July 03, 2026 16:02 KST
Status	Working
Document link	https://theorytrace.com/projects/shors-algorithm-from-first-principles/documents/chapter-22-cryptographic-consequences/