

## 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

---

<b>Project</b>	Shor's Algorithm from First Principles
<b>Document</b>	Document 1.26
<b>Author</b>	mujirin
<b>Verifier</b>	Not verified
<b>Downloaded</b>	July 04, 2026 18:10 KST
<b>Status</b>	Working
<b>Document link</b>	<a href="https://www.theorytrace.com/projects/shors-algorithm-from-first-principles/documents/-chapter-22-cryptographic-consequences/">https://www.theorytrace.com/projects/shors-algorithm-from-first-principles/documents/-chapter-22-cryptographic-consequences/</a>