Cryptography & Security: Course Preview

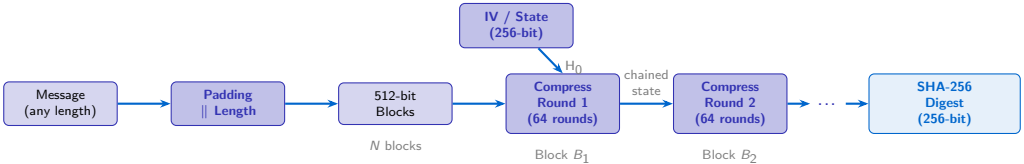
INTRO Preview – What You Will Learn

Prof. Dr. Joerg Osterrieder

University Lecture Series

February 19, 2026

Hash Function Anatomy



Input Processing

Append bit 1, pad to $\equiv 448 \pmod{512}$, append 64-bit length.

Compression Function

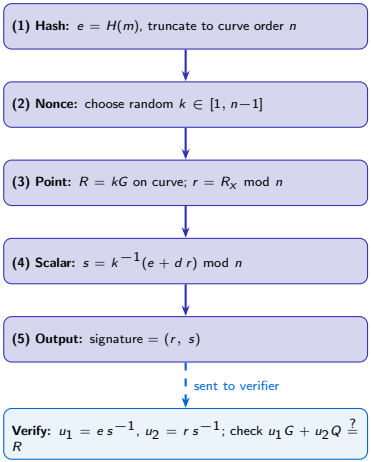
64 rounds per block; eight 32-bit state words (a–h); Ch, Maj, Σ operations.

Output

256-bit digest; collision resistance $\approx 2^{128}$; pre-image resistance $\approx 2^{256}$.

SHA-256 (FIPS 180-4) – Merkle-Damgård construction – 512-bit blocks, 64 rounds, 256-bit state

ECDSA Signature Flow



Key Variables

G	base point on curve
n	curve order
d	private key (scalar)
$Q = dG$	public key (point)
k	ephemeral nonce
r, s	signature components

Security Note

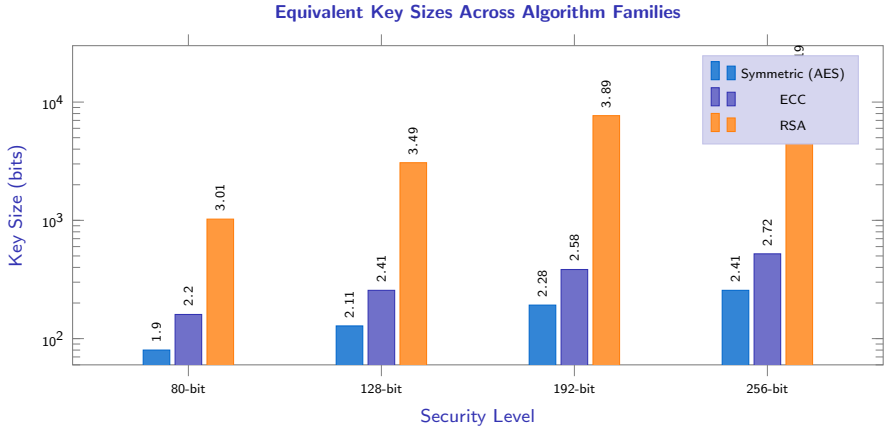
Never reuse k! Same k for two different messages exposes private key d.

Curve Parameters

secp256k1 (Bitcoin):
256-bit field, $\approx 2^{128}$ security.

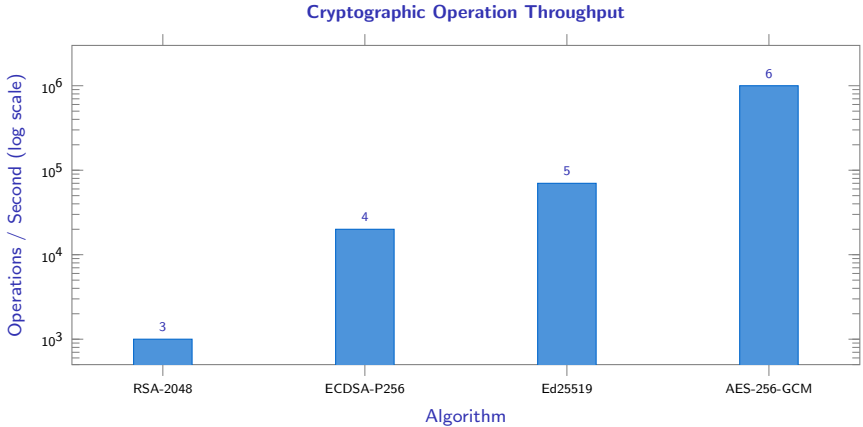
ECDSA (ANSI X9.62) – secp256k1 used in Bitcoin/Ethereum – Nonce reuse is catastrophic

Key Sizes vs. Security Levels



NIST SP 800-57 – RSA key sizes grow exponentially; ECC provides equivalent security with far smaller keys

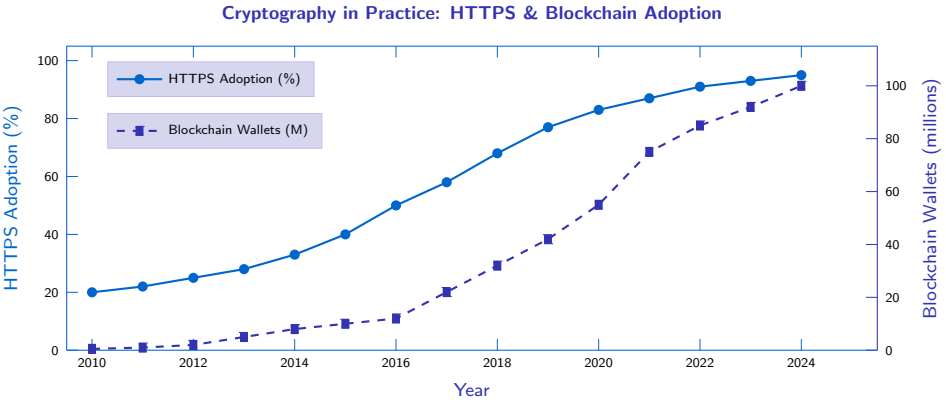
Algorithm Performance Comparison



Key takeaway: AES-256-GCM (symmetric) is $\sim$1000$\times$ faster than RSA-2048. Ed25519 outperforms ECDSA-P256 by 3.5$\times$ with equivalent security. Use hybrid encryption in practice.

Indicative benchmarks on modern x86-64 hardware – actual throughput varies by implementation and hardware acceleration

Crypto Adoption Timeline (2010–2025)



HTTPS data: Google Transparency Report – Blockchain wallet data: blockchain.com / industry estimates