endava

Raiffeisen Bank International

Unlocking the unknowns,

Cryptography essentials for Java devs

Laurențiu Spilcă
Ionuț Balosin

endava

youtube.com/@laurspilca

@laurspilca

Laurențiu Spilcă

Raiffeisen Bank International

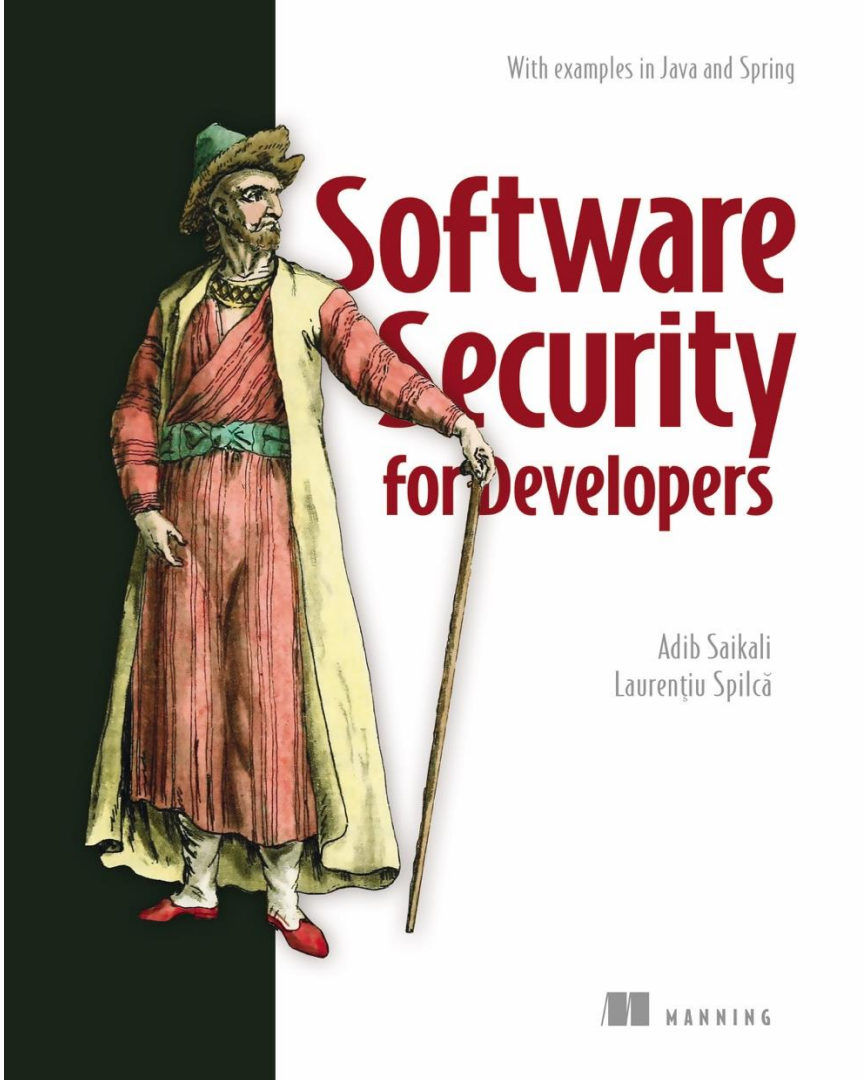
- Principal IT Architect
- Technical Trainer
- Security Champion
- Oracle ACE Associate
- Blogger
- Speaker

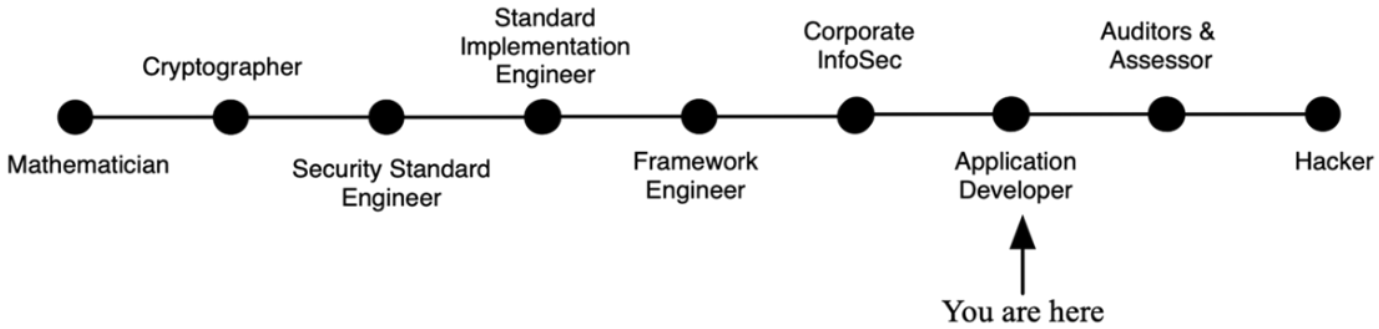
@ionutbalosin

www.IonutBalosin.com

Ionut Balosin

ionut.balosin@gmail.com


With examples in Java and Spring
Software Security for Developers
Adib Saikali
Laurențiu Spilcă
MANNING


Mathematician
Cryptographer
Security Standard Engineer
Standard Implementation Engineer
Framework Engineer
Corporate InfoSec
Application Developer
Auditors & Assessor
Hacker
You are here

Integrity

Authentication

Confidentiality

Non-repudiation

Use Case 1

Acme Inc. needs to implement a ZIP file transfer capability between two services. Developers must ensure that **faulty transfers are detected and excluded** to prevent the application from processing incorrect files.

Integrity

Authentication

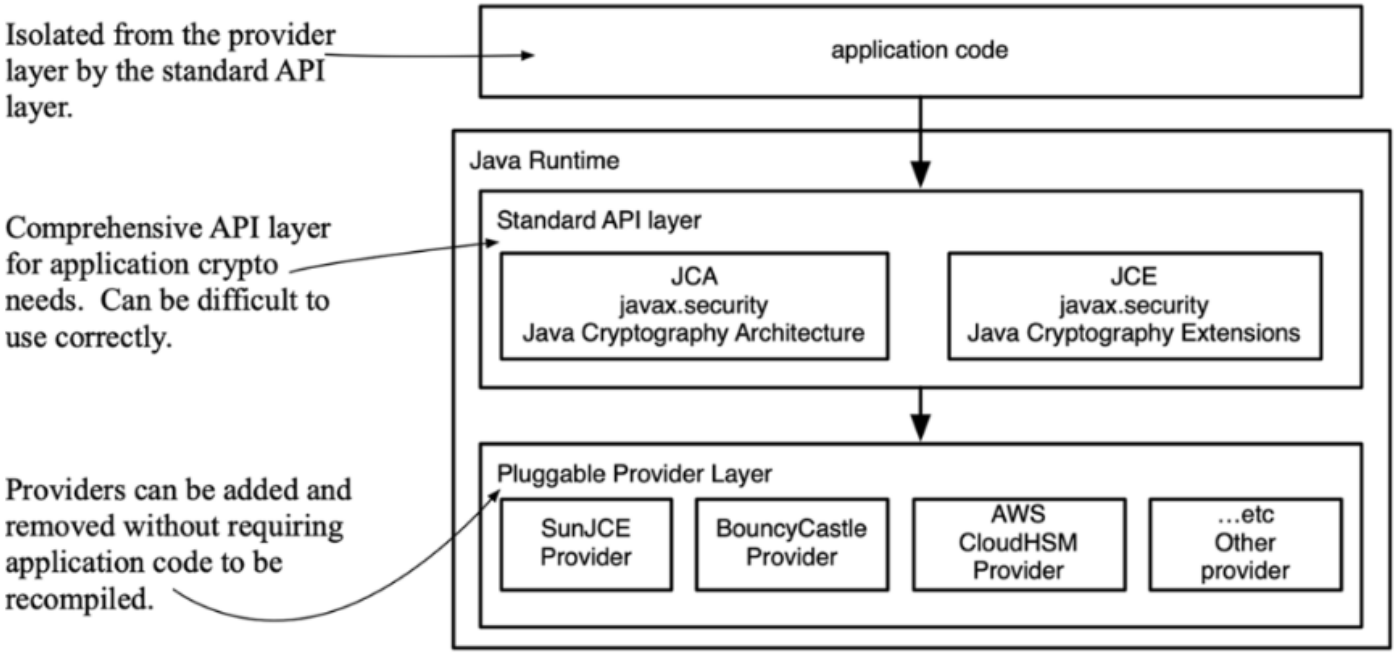
Confidentiality

Non-repudiation

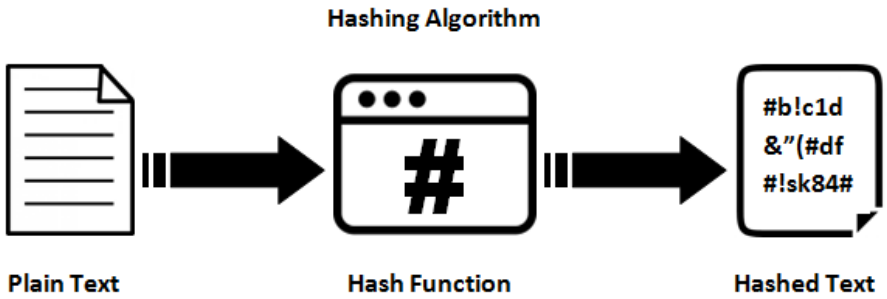
Third Parties

Google Tink
Libsodium (Kalium)
Apache Shiro

Security providers



Hash function digests



Source: [MessageHashing.java]

Use Case 2

Acme Inc. needs to **store employee passwords in hashed form in databases to ensure they cannot be viewed in plain text**. This approach will enhance security by protecting passwords from unauthorized access and ensuring that even if the database is compromised, the actual passwords remain secure.

Source: [PasswordHashing.java]

Use Case 3

Acme Inc. needs to implement a ZIP file transfer capability between two services. Developers must ensure that **faulty transfers are detected and excluded, maintaining data integrity** throughout the process. Although the data is not confidential, preserving its accuracy and completeness is essential.

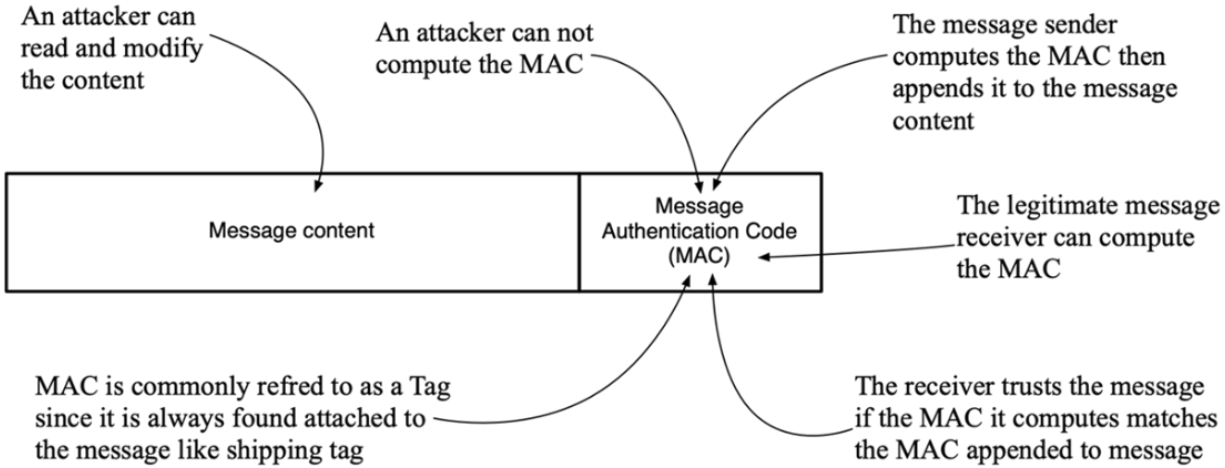
Integrity

Authentication

Confidentiality

Non-repudiation

Message Authentication Code (MAC)



Source: [HmacMessageAuthenticator.java]

Goal	SHA-2	SHA-3	HMAC
Integrity	✅	✅	✅
Authentication	❌	❌	✅
Confidentiality	❌	❌	❌
Non-repudiation	❌	❌	❌

Use Case 4

Acme Inc. needs to implement a ZIP file transfer capability between two services. Developers must ensure that the **data remains confidential and cannot be accessed by unauthorized parties during transit or at rest**. Additionally, **faulty transfers should be detected and excluded to maintain data integrity**.

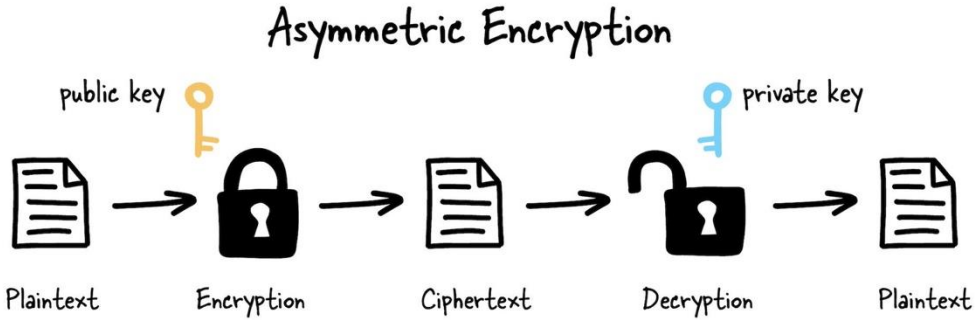
Integrity

Authentication

Confidentiality

Non-repudiation

Asymmetric Key Encryption



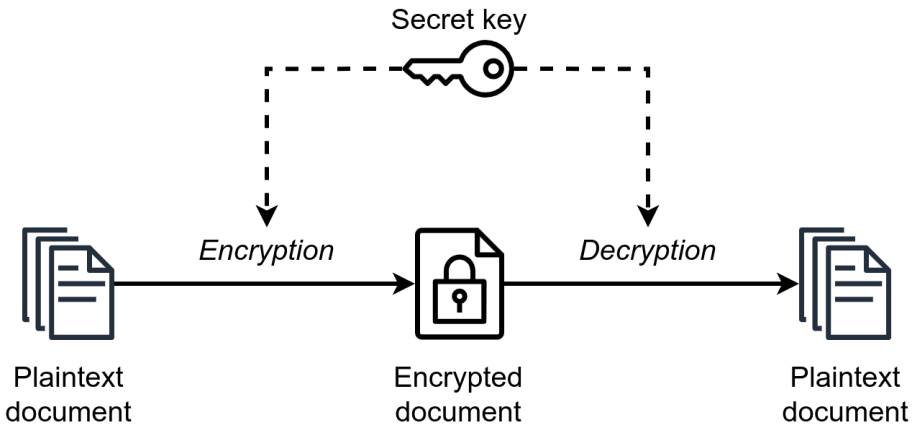
RSA (Rivest-Shamir-Adleman): Widely used for secure data transmission, RSA is notable for its use in digital signatures and secure key exchange.

ECC (Elliptic Curve Cryptography): Offers higher security with smaller key sizes compared to RSA, making it efficient for mobile devices and smart cards.

DSA (Digital Signature Algorithm): Primarily used for digital signatures, ensuring the authenticity and integrity of a message.

Diffie-Hellman: A method for secure key exchange, allowing two parties to establish a shared secret over an insecure channel.

Symmetric Key Encryption



Use symmetric key encryption for:


Encrypting files


Encrypting databases


Encrypting disk partitions

Use asymmetric key encryption for:


Key exchange


Digital signatures


Digital certificates

Source: [MessageEncryptDecrypt.java]

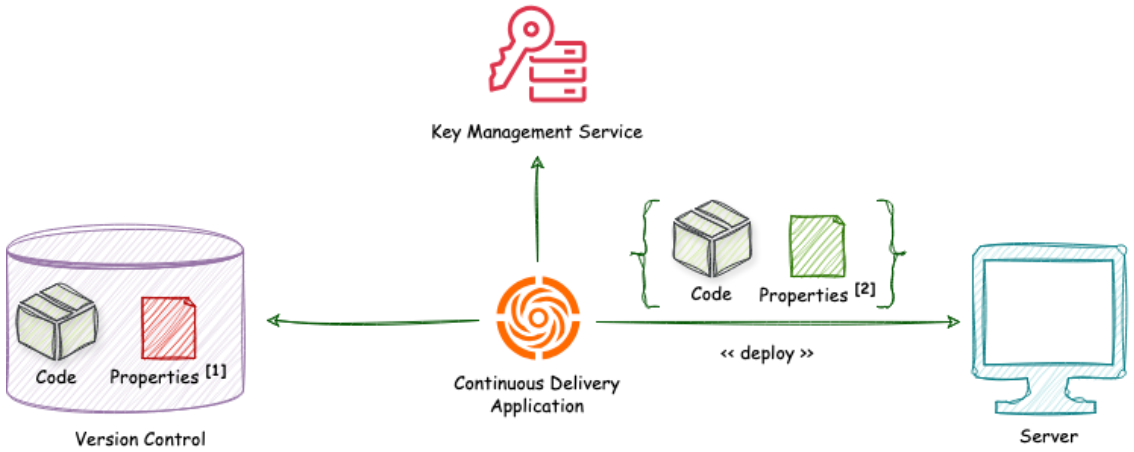
Sources:

[FileEncryption.java]

[FileDecryption.java]

Use Case 5

Acme Inc. needs to ensure the secure management of sensitive information to mitigate critical security risks. Developers must **avoid storing secrets unencrypted or in plain text within the source code.** Instead, they should utilize secrets management services and environment variables to protect sensitive data effectively.



Source: [https://ionutbalosin.com/2025/03/core-application-security-for-java-developers]

Source: [application.properties]

Symmetric Key Encryption

AES/CBC/PKCS5Padding

AES/CFB/NoPadding

AES/OFB/NoPadding

AES/GCM/NoPadding

AES/CTR/NoPadding

Goal	SHA-2	SHA-3	HMAC	AES/CBC
Integrity	✅	✅	✅	❌
Authentication	❌	❌	✅	❌
Confidentiality	❌	❌	❌	✅
Non-repudiation	❌	❌	❌	❌

Use Case 6

Acme Inc. needs to implement a ZIP file transfer capability between two services. Developers must ensure that **each transfer is verifiable, preventing senders from denying their actions.** Additionally, **faulty transfers should be excluded to maintain data integrity and reliability.**

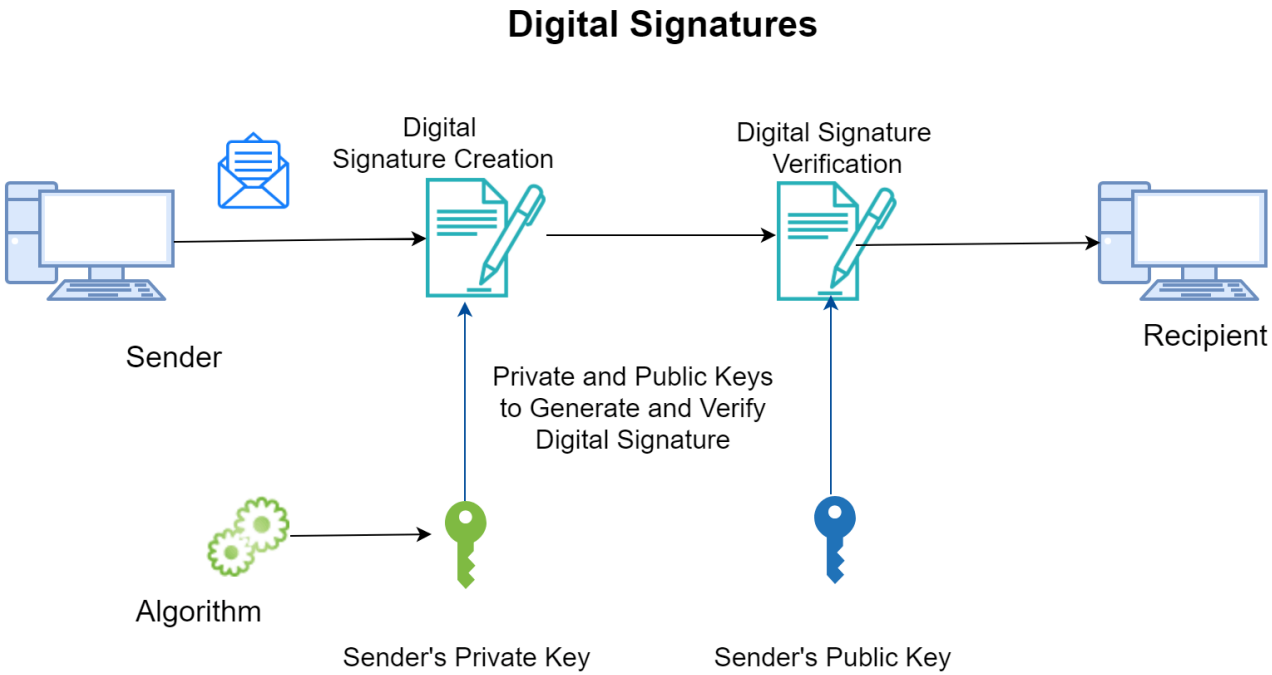
Integrity

Authentication

Confidentiality

Non-repudiation

Generating and Verifying Signatures



Source: [DigitalSignatureVerifier.java]

Thank You

Supercharge Your Knowledge 🚀 with My Training Catalogue

Software Architecture Essentials

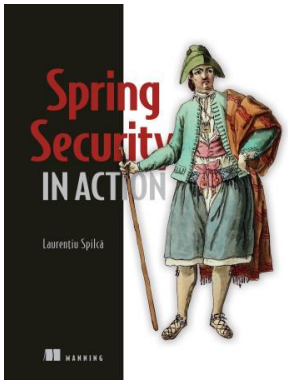
Java Performance Tuning

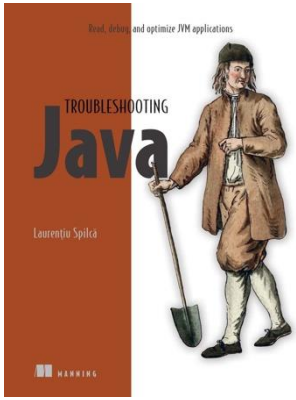
Designing High-Performance, Scalable, and Resilient Applications

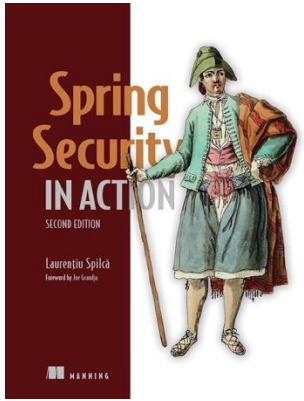
Application Security for Java Developers

Training figures: 90+ sessions | 1000+ trainees | 1400+ hours | 12+ clients | 5+ countries
Conference figures: 40+ sessions | 15+ countries

www.IonutBalosin.com/training 📚







youtube.com/@laurspilca

@laurspilca

Laurențiu Spilcă