Centro Universitário Alves Faria – UniAlfa

I Jornada Internacional de Produção Técnica e Científica

# Criptografia em Java: Algoritmos DES, AES, RC4 e OTP

Professor: George Mendes Marra

20 de Maio de 2025

# Sobre mim

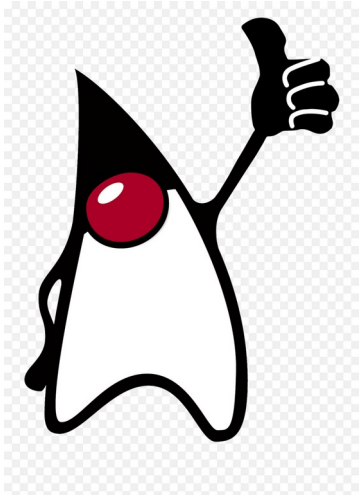
- Graduação em Ciência da Computação;
- Especialista em redes de computadores;
- Especialista em big data e machine learning;
- Mestre em História;
- Dissertação: O jogo da mímese e o uso da criptografia.

# O que é Programação Orientada a Objetos?

- Objetos;
- Classes;
- Encapsulamento;
- Herança;
- Polimorfismo;
- Abstração;

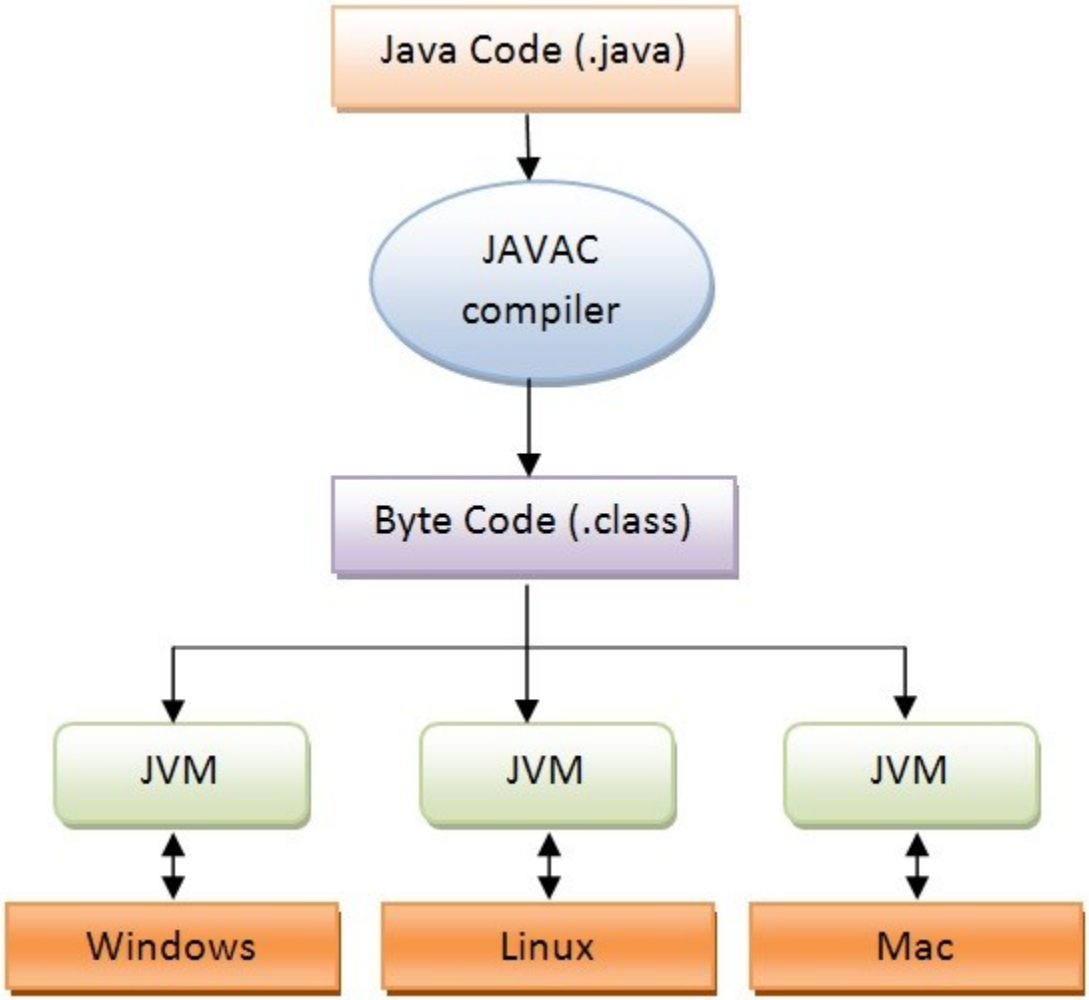
# O que é Java?


- Orientação a Objetos;
- Independência de Plataforma - JVM
- Simplicidade; Sem ponteiros e herança múltipla;
- Segurança;
- Multi-threading;
- Compilada e Interpretada;
- Grande Comunidade e Ecossistema;



# Java Virtual Machine-JVM

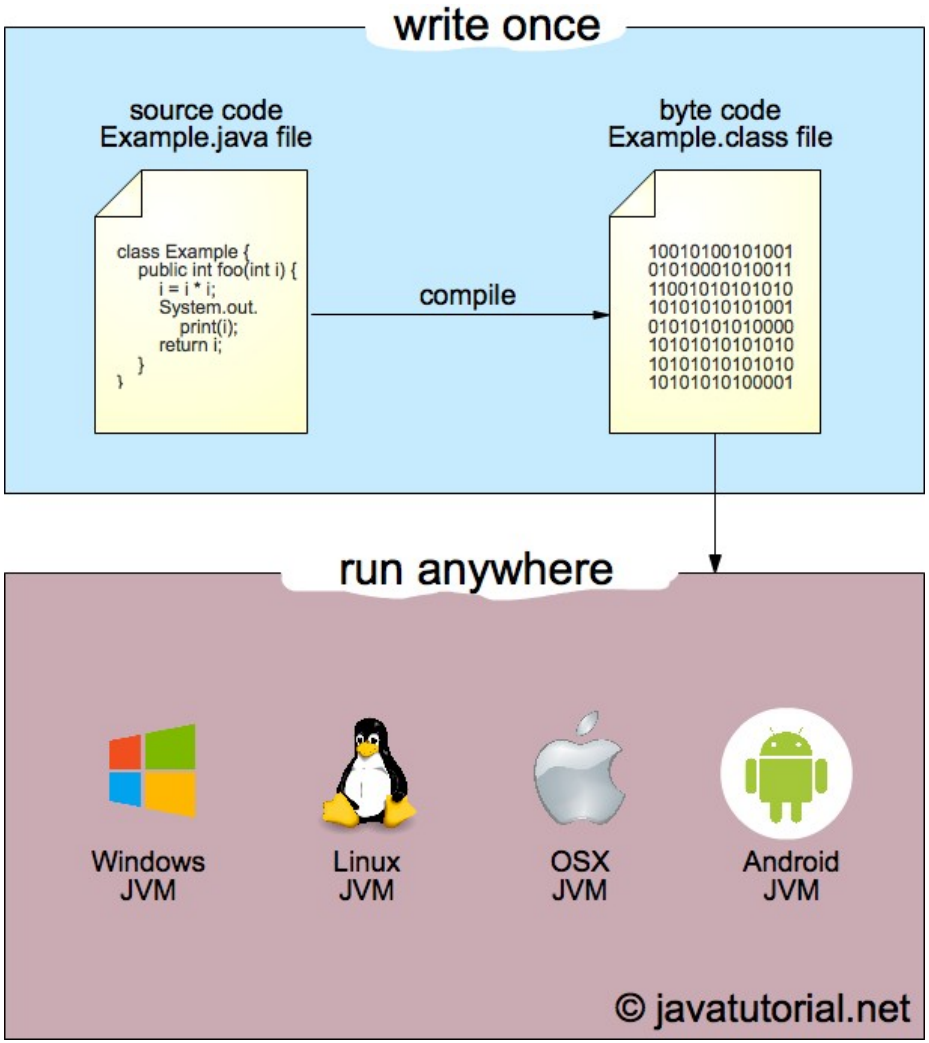
Figura 1 – Java Virtual Machine - JVM




Fonte: https://arquivo.devmedia.com.br/artigos/Allan_Romanato/JavaVirtualMachine/JavaVirtualMachine2.jpg

# Java Virtual Machine-JVM

Figura 2 – Java Virtual Machine - JVM



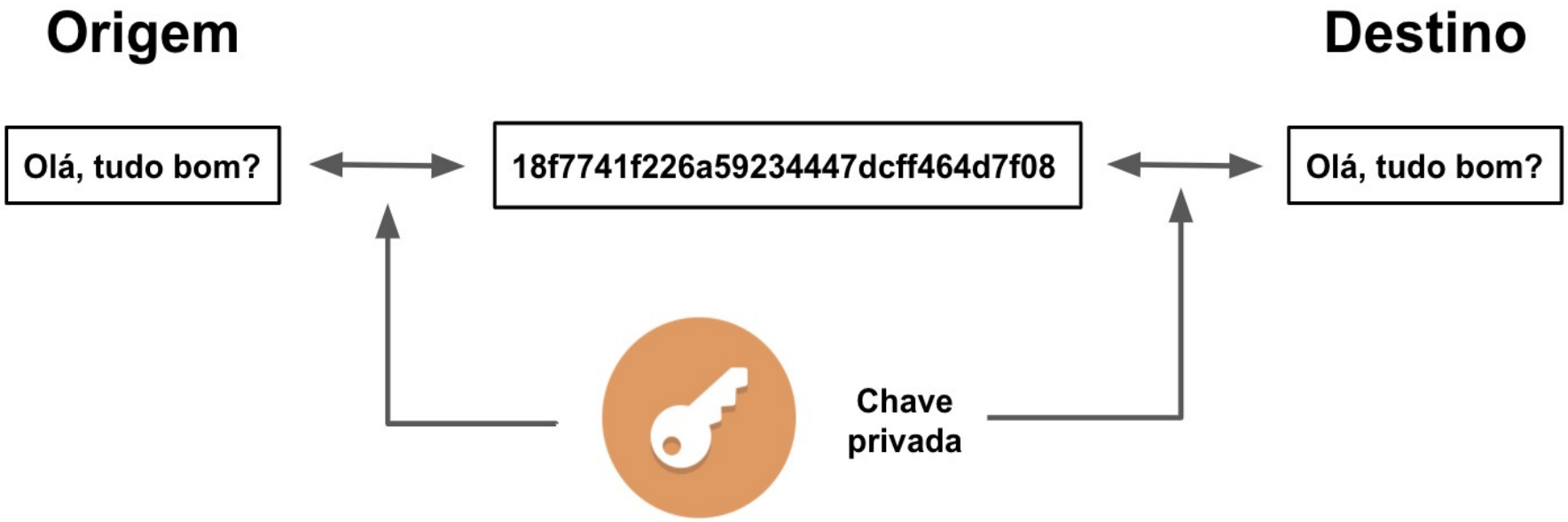

Fonte: https://javatutorial.net/wp-content/uploads/2017/10/write-once-run-anywhere-jvm.png

# O que é Criptografia?

- Criptografia é o processo de codificação de informações para protegê-las.
- Garante confidencialidade, integridade e autenticidade.
- Tipos principais: Simétrica e Assimétrica.

# Criptografia Simétrica

Figura 3 – Demonstração da criptografia simétrica



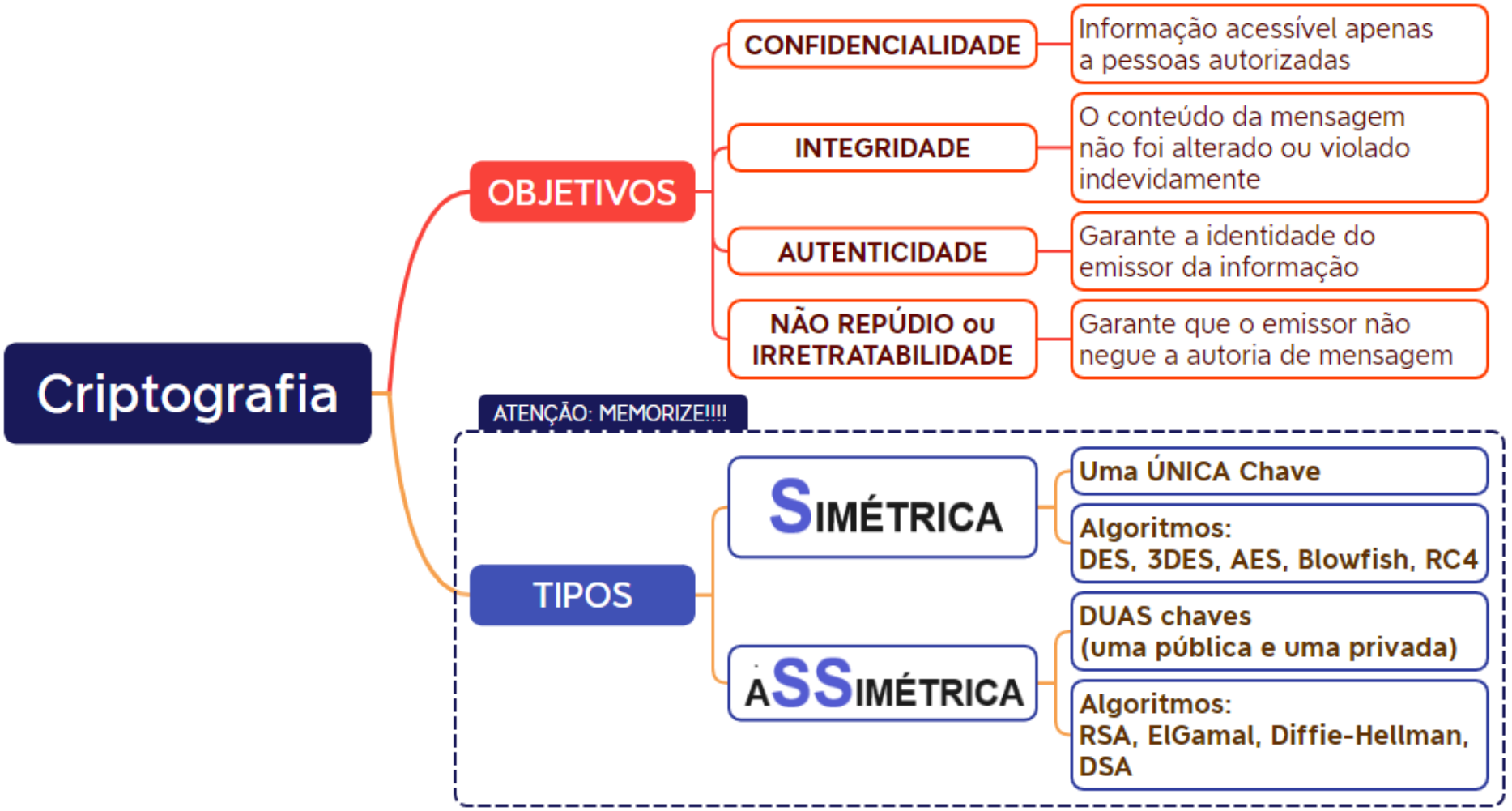

Fonte: http://www.universidadejava.com.br/images/2020-05-23-criptografia-assimetrica-01.png

# Criptografia Assimétrica

Figura 4 – Demonstração da criptografia assimétrica


Fonte:
https://www.researchgate.net/publication/332948161/figure/fig5/AS:756324753211396@1557333281925/Figura-7-Esquema-da-criptografia-assimetrica.ppm

# Figura 5 – Mapa mental sobre criptografia




Fonte: https://lh3.googleusercontent.com/9lEMZQQvR7LOV6_t9SRvon4CO_sTTpm-smDdPMuz3tM3fXemJ_1e1EnbVmO_MBoDYIOUfpZ-qN-KZzSzKKqh83Tt7p8MDbkXTS7kqnwsxwkcwUuzkjQR2pN-cNKrOcgaEhk1w18FQyGviyXM5Zj6Nlk

# Criptografia em Java

- Java Security API;
- Java Cryptography Architecture (JCA);
- Java Cryptography Extension (JCE);
- Cifradores (`javax.crypto.Cipher`);
- Geradores de Chaves (`java.security.KeyGenerator`);
- Assinaturas Digitais (`java.security.Signature`);

# DES (Data Encryption Standard)

- Algoritmo de criptografia simétrica com chave de 56 bits.
- Popular nos anos 70-90.
- Vulnerável a ataques de força bruta.
- Substituído por algoritmos mais seguros.

# AES (Advanced Encryption Standard)

- Padrão atual de criptografia simétrica.
- Chaves de 128, 192 ou 256 bits.
- Muito utilizado em sistemas modernos.
- Resistente a ataques conhecidos.

# RC4 (Rivest Cipher 4)

- Algoritmo de fluxo muito rápido, mas inseguro atualmente.
- Simples de implementar.
- Já foi usado em SSL/TLS.
- Atualmente considerado inseguro.

# OTP (One-Time Pad)

- Algoritmo simétrico com segurança teórica perfeita.
- Chave deve ser do mesmo tamanho da mensagem.
- Impraticável para uso em grande escala.
- Utilizado em situações extremamente sensíveis.

# Comparação entre Algoritmos

- Tabela de comparação entre os principais algoritmos discutidos.
- DES: Fraco, obsoleto.
- AES: Forte, amplamente utilizado.
- RC4: Rápido, mas inseguro.
- OTP: Seguro, mas pouco prático.

# Exemplo em Java: AES

https://github.com/GeorgeMendesMarra/GeorgeMendesMarra/blob/main/poo_java/criptografia/ExemploAES.java

# Exemplo em Java: DES

https://github.com/GeorgeMendesMarra/GeorgeMendesMarra/blob/main/poo_java/criptografia/ExemploDES.java

# Exemplo em Java: OTP

https://github.com/GeorgeMendesMarra/GeorgeMendesMarra/blob/main/poo_java/criptografia/ExemploOTP.java

# Exemplo em Java: RC4

https://github.com/GeorgeMendesMarra/GeorgeMendesMarra/blob/main/poo_java/criptografia/ExemploRC4.java

# Conclusão

- A criptografia é essencial para a segurança digital.
- Java oferece suporte robusto a algoritmos criptográficos.
- AES é o padrão atual mais seguro e eficiente.
- A escolha do algoritmo depende do contexto de uso.