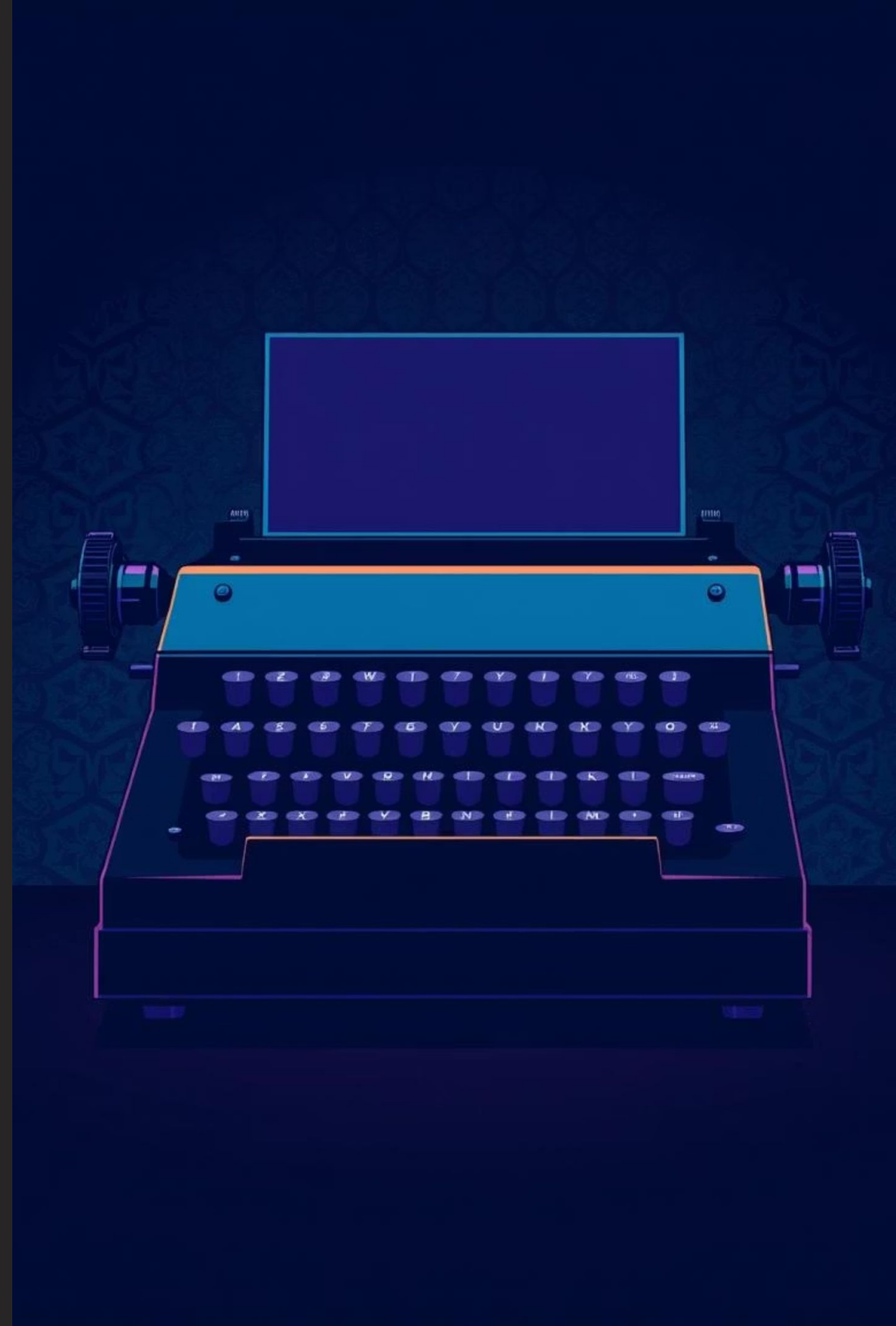


# Criptografia: História e Algoritmos Atuais

Uma jornada da guerra à era digital, explorando a evolução da segurança da informação.



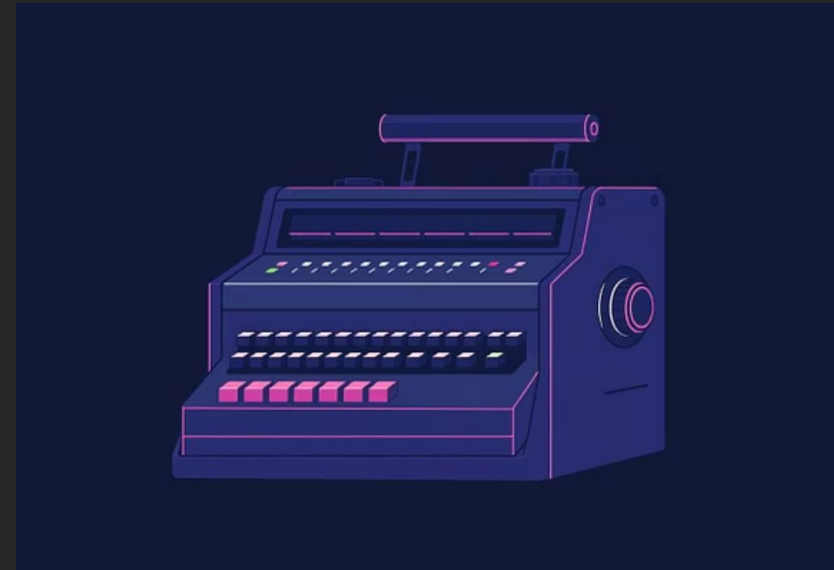
# Exemplos Históricos: A Criptografia na Guerra

## Código Purple (Japão - II Guerra Mundial)

Usado para comunicações diplomáticas e militares japonesas. Quebrado pelos EUA antes de Pearl Harbor, teve um impacto estratégico crucial no conflito.

## Códigos Navajo (EUA - II Guerra Mundial)

Baseado na complexa língua Navajo, era praticamente indecifrável pelos japoneses. Fundamental para a vitória aliada no Pacífico.





# Criptografia de Chave Simétrica: A Base da Segurança Atual

Algoritmos modernos que utilizam uma única chave para criptografar e descriptografar dados.



## **AES (Advanced Encryption Standard)**

Padrão mundial, essencial em VPNs, HTTPS e transações bancárias, garantindo a confidencialidade das informações.



## **Blowfish**

Algoritmo rápido e eficiente, frequentemente empregado na proteção de senhas e arquivos, oferecendo alta performance.



# Criptografia de Chave Assimétrica: Autenticação e Eficiência

Algoritmos que utilizam um par de chaves (pública e privada) para maior segurança e autenticidade.



## **RSA**

Amplamente utilizado em certificados digitais e autenticação, assegurando a identidade e a integridade dos dados.



## **ECC (Elliptic Curve Cryptography)**

Oferece alta segurança com chaves menores, ideal para dispositivos IoT e aplicações móveis, otimizando recursos.

A criptografia é essencial para segurança, autenticidade e privacidade no mundo digital moderno. O uso combinado de simétrica e assimétrica é o padrão atual.





# integrantes:

Felipe Pereira do Nascimento - RA: 825126069

Guilherme Dourado Nascimento - RA: 825116419

Bruno de Oliveira Santos - RA: 823223513

Pedro Miranda Rabelo - RA:825243591

Kauane Sandes Brandão - RA: 825113309

Stephany Ramos Rodrigues - RA: 82512339