AULA 04 - PROTEÇÃO DE DADOS E INFORMAÇÕES 2

1. Exemplos Históricos de Criptografia Não Citados no Material

a) Código Navajo (Segunda Guerra Mundial)

KAHN, D. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. 2. ed. Nova York: Scribner, 1996. Cap. 17, p. 540-550.

NATIONAL WWII MUSEUM. **Code Talkers: The Navajo Heroes of World War II**. Nova Orleans, 2021. Disponível em: https://www.nationalww2museum.org. Acesso em: 10 mar. 2025.

Descrição:

O Código Navajo foi utilizado pelos "Code Talkers" (marines indígenas) durante a Segunda Guerra Mundial. A língua Navajo, adaptada para termos militares (ex.: "besh-lo" = "tanque"), nunca foi decifrada pelas potências do Eixo, mesmo com a captura de falantes Navajo.

b) Máquina SIGABA (EUA, 1930-1945)

BAUER, C. *Secret History: The Story of Cryptology*. Boca Raton: CRC Press, 2013. p. 215.

DEPARTMENT OF THE ARMY. **Technical Manual for SIGABA ECM Mark II**. Washington, DC: U.S. Government Printing Office, 1944. Disponível em: https://www.archives.gov. Acesso em: 10 mar. 2025.

Descrição:

A SIGABA, máquina de criptografia americana, empregava 15 rotores com 10^77 combinações, superando a complexidade da Enigma alemã. Considerada "inquebrável" durante a guerra, foi usada para comunicações estratégicas.

2. Algoritmos de Criptografia Simétrica Atuais

a) AES (Advanced Encryption Standard)

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **FIPS PUB 197: Advanced Encryption Standard**. Gaithersburg, 2001. Disponível em: https://csrc.nist.gov. Acesso em: 10 mar. 2025.

SCHNEIER, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. 2. ed. Hoboken: Wiley, 2015. p. 243.

Características:

Padrão global com chaves de 128, 192 ou 256 bits, utilizado em VPNs e sistemas bancários. Resistente a ataques quânticos (até 2023).

b) ChaCha20

BERNSTEIN, D. **ChaCha, a variant of Salsa20**. Documento técnico, 2008. Disponível em: https://cr.yp.to/chacha.html. Acesso em: 10 mar. 2025.

GOOGLE SECURITY BLOG. **Speeding up and strengthening HTTPS connections for Chrome on Android**. 2014. Disponível em: https://security.googleblog.com. Acesso em: 10 mar. 2025.

Características:

Cifra de fluxo 20% mais rápida que AES em dispositivos móveis, adotada no TLS 1.3 (ex.: WhatsApp).

3. Algoritmos de Criptografia Assimétrica Atuais

a) RSA (Rivest-Shamir-Adleman)

RIVEST, R.; SHAMIR, A.; ADLEMAN, L. **A Method for Obtaining Digital Signatures and Public-Key Cryptosystems**. *Communications of the ACM*, v. 21, n. 2, p. 120-126, 1978.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **SP 800-57: Recommendation for Key Management**. Gaithersburg, 2020. Disponível em: https://csrc.nist.gov. Acesso em: 10 mar. 2025.

Características:

Baseado na fatoração de números primos, com chaves de 2048+ bits em certificados SSL/TLS.

b) ECDSA (Elliptic Curve Digital Signature Algorithm)

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI). **X9.62: Elliptic Curve Digital Signature Algorithm (ECDSA)**. Nova York, 2001.

NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 10 mar. 2025.

Características:

Usa curvas elípticas para assinaturas digitais, com chaves de 256 bits (equivalente a RSA 3072 bits). Adotado no Bitcoin.

Tabela Comparativa

Critério	AES (NIST, 2001)	RSA (MIT, 1978)
Tipo de Chave	Simétrica (256 bits)	Assimétrica (2048 bits)
Velocidade	~1 GB/s (hardware)	~100 KB/s (assinaturas)
Aplicação	Criptografia de dados	Troca de chaves SSL/TLS