Schneier B.: *Kryptografia dla praktyków: protokoły, algorytmy i programy źródłowe w języku C*. Warszawa: Wydawnictwa Naukowo-Techniczne, 2002 [ISBN 83-204-2678-2](https://pl.wikipedia.org/wiki/Specjalna:Ksi%C4%85%C5%BCki/8320426782).

Aumasson J. P.: *Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfrowania.*Warszawa: Wydawnictwo Naukowe PWN SA, 2018, s. 1-59. ISBN 978-83-01-19900-5.

Stinson D. R.: *Kryptografia. W teorii i praktyce.*Warszawa: Wydawnictwo Naukowo-Techniczne, 2005. ISBN 83-204-2982-X  
  
  
Kalaiselvi K., Kumar A.: *Enhanced AES cryptosystem by using genetic algorithm and neural network in S‑box*.  
Banglore: 2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC), 2006, s. 1-6. doi: 10.1109/ICCTAC.2016.7567340  
  
Floissac N., L'Hyver Y.: *From AES-128 to AES-192 and AES-256, How to Adapt Differential Fault Analysis Attacks on Key Expansion   
Nara:* 2011 Workshop on Fault Diagnosis and Tolerance in Cryptography, 2011, s. 43-53.  
doi: 10.1109/FDTC.2011.15

Liu N., et al.: *Cryptographic performance for Rijndael and RC6 block ciphers*.   
Xiamen: 2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID)*,* 2017, s. 36-39. doi: 10.1109/ICASID.2017.8285739  
  
Noura M. et al.: *S-DES: An efficient & secure DES variant.*   
Jounieh: 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)*,* 2018, s. 1-6. doi: 10.1109/MENACOMM.2018.8371019  
  
Sanchez-Avila C., Sanchez-Reillol R.: *The Rijndael block cipher (AES proposal): a comparison with DES.*  
Londyn: Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No.01CH37186), 2001, s. 229-234. doi: 10.1109/CCST.2001.962837  
  
Bhat B., Ali A. W., Gupta A.: *DES and AES performance evaluation.*  
Noida: International Conference on Computing, Communication & Automation, 2015, s. 887-890.  
doi: 10.1109/CCAA.2015.7148500

Cheng H., Ding Q.: *Overview of the Block Cipher*.   
Harbin: 2012 Second International Conference on Instrumentation, Measurement, Computer, Communication and Control, 2012, s. 1628-1631. *doi: 10.1109/IMCCC.2012.379*

Mohamed A. B., Zaibi G., Kachouri A.: *Implementation of RC5 and RC6 block ciphers on digital images.*Sousse: Eighth International Multi-Conference on Systems, Signals & Devices*,* 2011, s. 1-6.  
doi: 10.1109/SSD.2011.5767447

Vu A., et al., *A homogeneous parallel brute force cracking algorithm on the GPU*.   
Seoul: ICTC 2011*,* 2011, s. 561-564. doi: 10.1109/ICTC.2011.6082661

FIPS PUB 197. *The official AES standard.* NIST, 21.10.2001

Wang D., Sun S. *Replacement and Structure of S-Boxes in Rijndael*.   
Hubei: 2008 International Conference on Computer Science and Software Engineering*,* 2008, s. 782-784.  
doi: 10.1109/CSSE.2008.296

Trenholme S. *AES' Galois field*. W: <https://www.samiam.org/galois.html> [dostęp 01.04.19]

Hoang V. T., Rogaway P. *On Generalized Feistel Networks*, w: *Advances in Cryptology -- CRYPTO 2010.*  
Berlin: Springer Berlin Heidelberg, 2010, s 613-630. *ISBN: 978-3-642-14623-7*