UNIVERSITAS
GADJAH MADA

PROOF OF CONCEPT SERANGAN PADDING ORACLE PADA PENYANDIAN AES DENGAN MODE PCBC
RAFIE MUHAMMAD, Anny Kartika Sari, S.Si., M.Sc., Ph.D.
Universitas Gadjah Mada, 2020 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR PUSTAKA

Al Fardan, N.J. dan Paterson, K.G., 2013, Lucky Thirteen: Breaking the TLS and DTLS Record Protocols, *2013 IEEE Symposium on Security and Privacy*, Berkeley, CA.

Avoine, G. dan Ferreira, L., 2018, Attacking GlobalPlatform SCP02-compliant Smart Cards Using a Padding Oracle Attack, IACR Transactions on Cryptographic Hardware and Embedded Systems, *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2, 149–170.

Bellare, M., Kohno, T. dan Namprempre, C., 2004, Breaking and Provably Repairing the SSH Authenticated Encryption Scheme: A Case Study of the Encode-then-Encrypt-and-MAC Paradigm, *ACM Transactions on Information and System Security (TISSEC)*, 7, 2, 206-241.

Bellare, M. dan Namprempre, C., 2007, Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm, *Journal of Cryptology*, 21, 4, 469-491.

Boyd, C., Hale, B., Mjølsnes, S.F. dan Stebila, D., 2016, From Stateless to Stateful: Generic Authentication and Authenticated Encryption Constructions with Application to TLS, *Proceedings of the RSA Conference on Topics in Cryptology - CT-RSA 2016*, Springer-Verlag, New York, USA.

Breier, J., Jap, D., Hou, X. dan Bhasin, S., 2020, On Side Channel Vulnerabilities of Bit Permutations in Cryptographic Algorithms, *IEEE Transactions on Information Forensics and Security*, 15, pp. 1072–1085.

Chhotaray, A., Nahiyan, A., Shrimpton, T., Forte, D. dan Tehranipoor, M., 2017, Standardizing Bad Cryptographic Practice: A Teardown of the IEEE Standard for Protecting Electronic-design Intellectual Property, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS '17*, ACM Press, Dallas, Texas, USA.

Di, B., 2015, Analysis of One-pass Block Cipher Based Authenticated Encryption Schemes, *Tesis*, Science and Engineering Faculty, Queensland University of Technology, Brisbane.

UNIVERSITAS
GADJAH MADA
PROOF OF CONCEPT SERANGAN PADDING ORACLE PADA PENYANDIAN AES DENGAN MODE PCBC
RAFIE MUHAMMAD, Anny Kartika Sari, S.Si., M.Sc., Ph.D.
Universitas Gadjah Mada, 2020 | Diunduh dari http://etd.repository.ugm.ac.id/

Gutmann, P., Using Message Authentication Code (MAC) Encryption in the Cryptographic Message Syntax (CMS). IETF Internet Request for Comments 2315, Januari 2012.

Kaliski, B., PKCS #7: Cryptographic Message Syntax Version 1.5, RFC 2315. IETF Internet Request for Comments 2315, Maret 1998.

Kupser, D., Mainka, C., Schwenk, J. dan Somorovsky, J., 2015, How to Break XML Encryption - Automatically, *WOOT'15 Proceedings of the 9th USENIX Conference on Offensive Technologies*, Washington, D.C, USA.

Maqableh, M. dan Mohammad, 2012, Analysis and Design Security Primitives Based on Chaotic Systems for eCommerce, *Thesis*, School of Engineering and Computing Sciences, Durham University, United Kingdom.

McGehee, J., 1996, SPOCK - Security Proof Of Concept Keystone, *Proceedings of the 19th National Information Systems Security Conference*, COACT, Inc., Baltimore, Maryland, USA.

Mitchell, C.J., 2005, Cryptanalysis of Two Variants of PCBC Mode When Used for Message Integrity, C. Boyd and J. M. González Nieto, eds. Information Security and Privacy, Springer, Berlin, Heidelberg.

Möller, B., Duong, T. dan Kotowicz, K., 2014, This POODLE Bites: Exploiting The SSL 3.0 Fallback, Google security advisory, https://www.openssl.org/ bodo/ssl-poodle.pdf, diakses 8 Oktober 2019.

Rizzo, J. dan Duong, T., 2011, Here Come The $\oplus$ Ninjas, (unpublished manuscript).

Sierra, J.M., Hernandez, J.C., Jayaram, N. dan Ribagorda, A., 2004, Low Computational Cost Integrity for Block Ciphers, Future Generation Computer Systems 20, 857–863.

Stallings, W., 2006, *Cryptography and network security: principles and practice*, 4th ed, Pearson/Prentice Hall, Upper Saddle River, N.J.

Vaudenay, S., 2002, Security Flaws Induced by CBC Padding — Applications to SSL, IPSEC, WTLS..., *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EU-ROCRYPT '02)*, Springer-Verlag, London, UK.

UNIVERSITAS
GADJAH MADA
PROOF OF CONCEPT SERANGAN PADDING ORACLE PADA PENYANDIAN AES DENGAN MODE PCBC
RAFIE MUHAMMAD, Anny Kartika Sari, S.Si., M.Sc., Ph.D.
Universitas Gadjah Mada, 2020 | Diunduh dari http://etd.repository.ugm.ac.id/

Yu, T., Hartman, S. dan Raeburn, K., 2004, The Perils of Unauthenticated Encryption: Kerberos Version 4, *Proceedings of the Network and Distributed Systems Security Symposium*, The Internet Society.