From Public-Key Cryptography to PKI: Reflections on Standardizing the RSA Algorithm

Jim Bidzos and Burt Kaliski, Verisign

2nd ZKProof Standards Workshop

April 12, 2019

RSA Public-Key Cryptosystem: Review

Key Pairs

- Public key: (n, e)
- Private key: (n, d)
  - where *modulus* n is product of two large primes p, q, and *exponents* e, d satisfy $e \cdot d \equiv 1 \bmod \text{lcm}(p-1, q-1)$

Public-Key Cryptosystem

- Encryption of message m with public key: $c = m^e \bmod n$
- Decryption of ciphertext c with private key: $m = c^d \bmod n$

Digital Signature Scheme

- Signature on message m with private key: $s = m^d \bmod n$
- Verification of signature s (and recovery of m) with public key: $m = s^e \bmod n$

About PKCS

"The *Public-Key Cryptography Standards* are specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of public-key cryptography."
(PKCS #1 v2.2, 2016 [RFC8017])

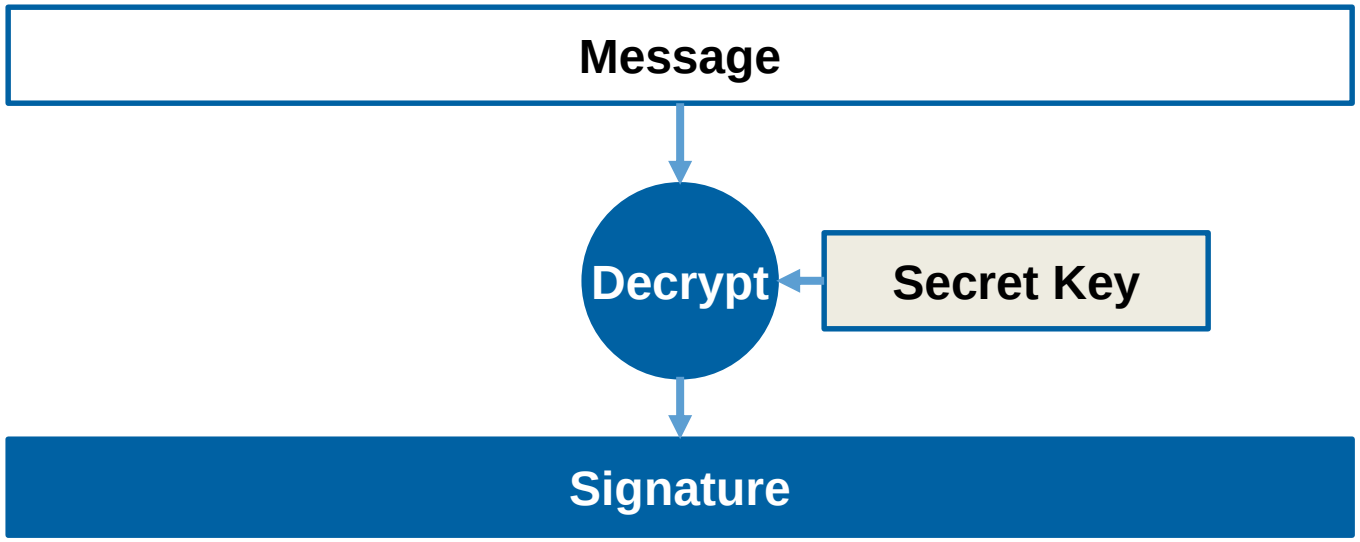
Outline

- Part I: RSA Signatures
- Part II: RSA Encryption
- Part III: Lessons Learned

Part I: RSA Signatures

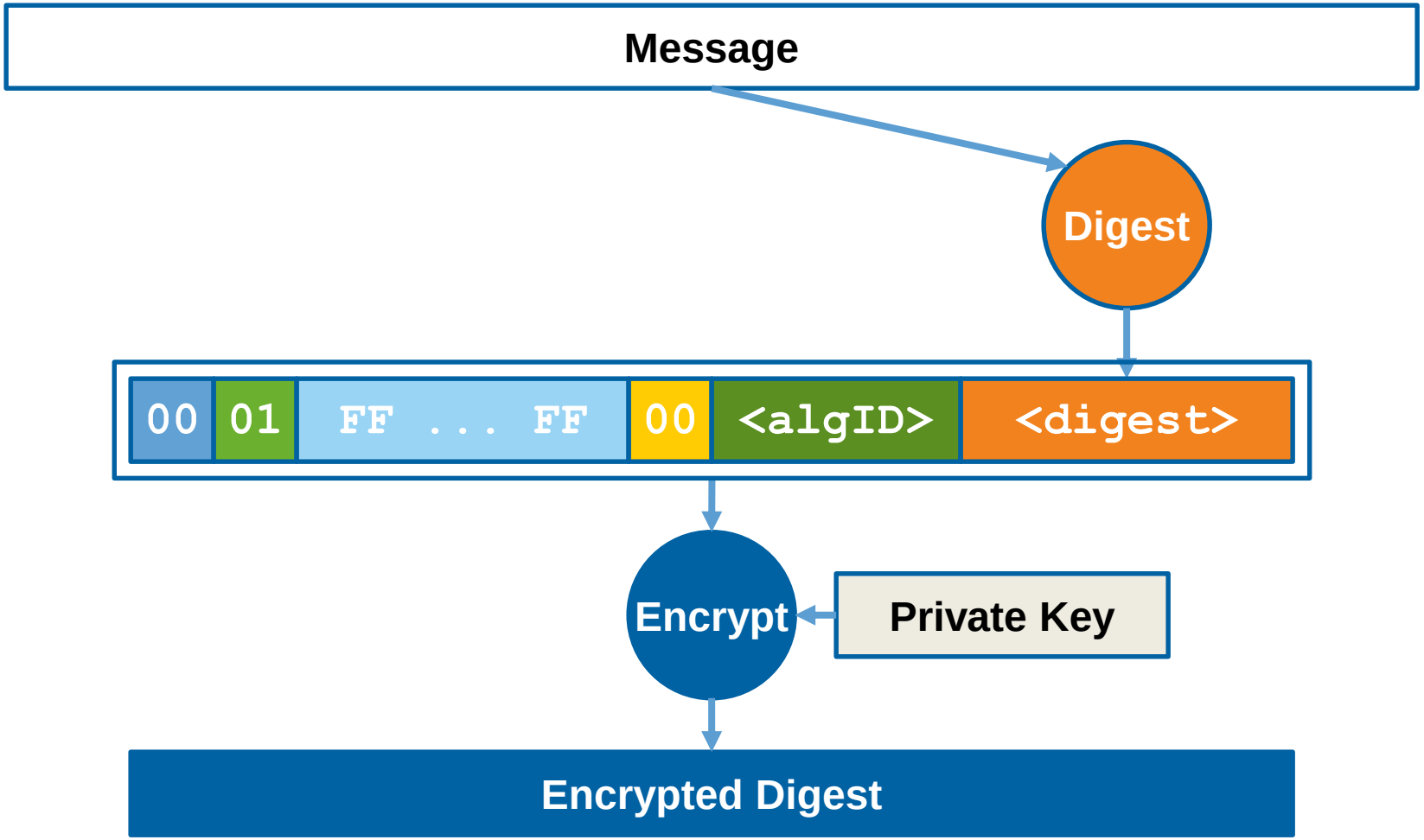
RSA Signatures: Original Model

Diffie-Hellman (1976) and RSA (1978)

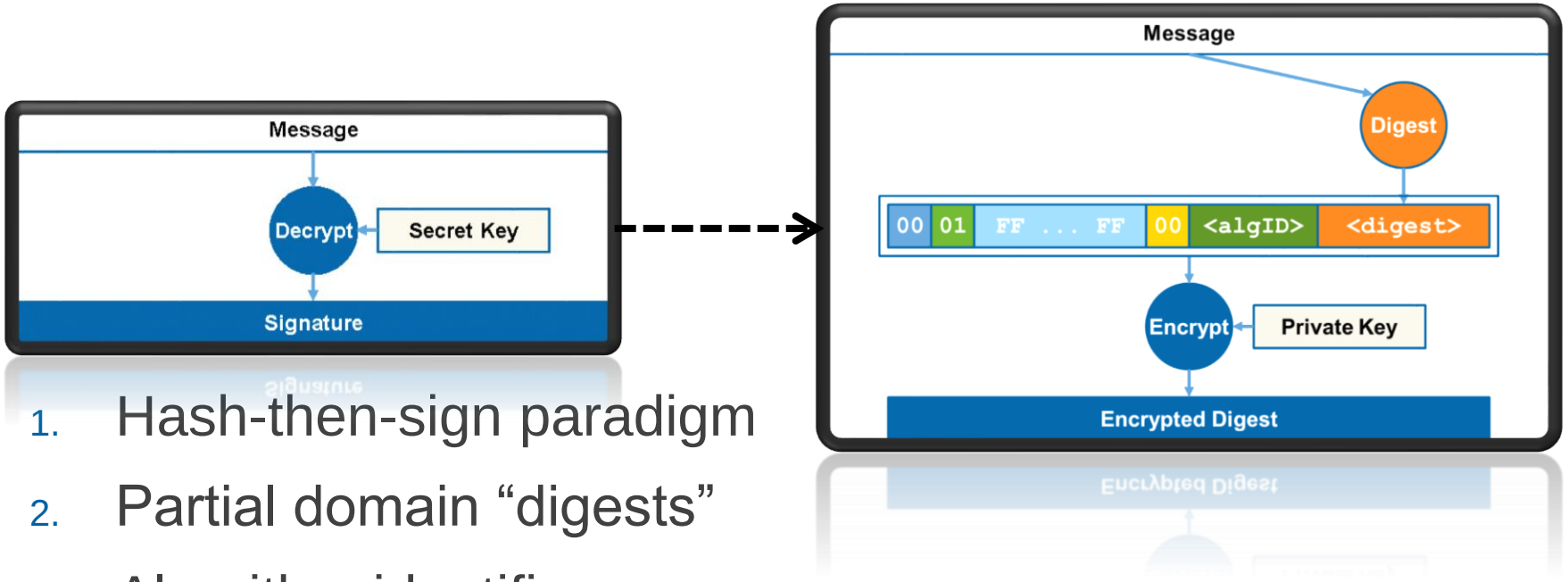


RSA Signatures: “Standard” Model

PKCS #1 (1991)

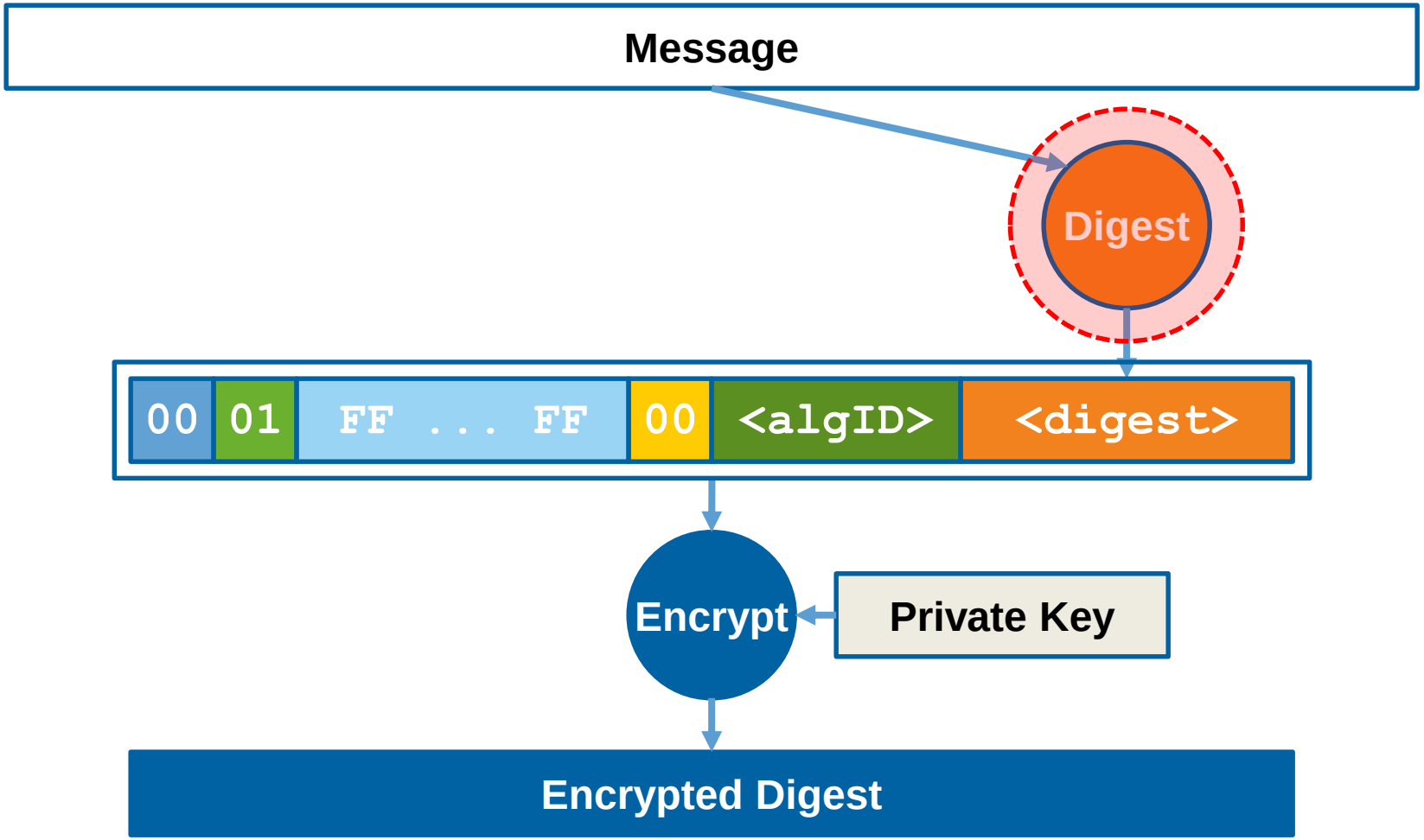


How Did Original Model Change to Standard?

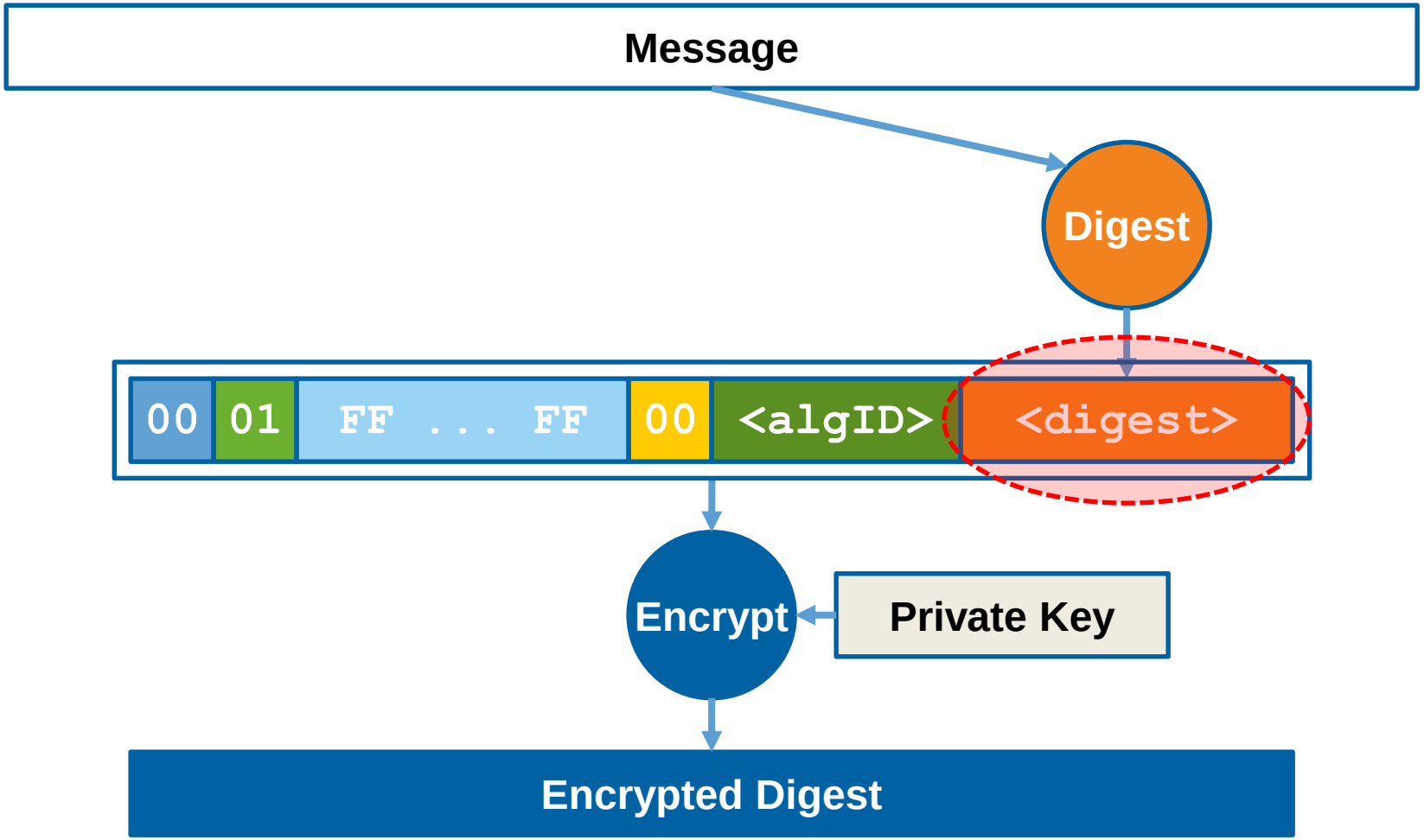


1. Hash-then-sign paradigm
2. Partial domain “digests”
3. Algorithm identifiers
4. Fixed padding
5. Block type
6. Encrypting with private key
7. Encrypted digest

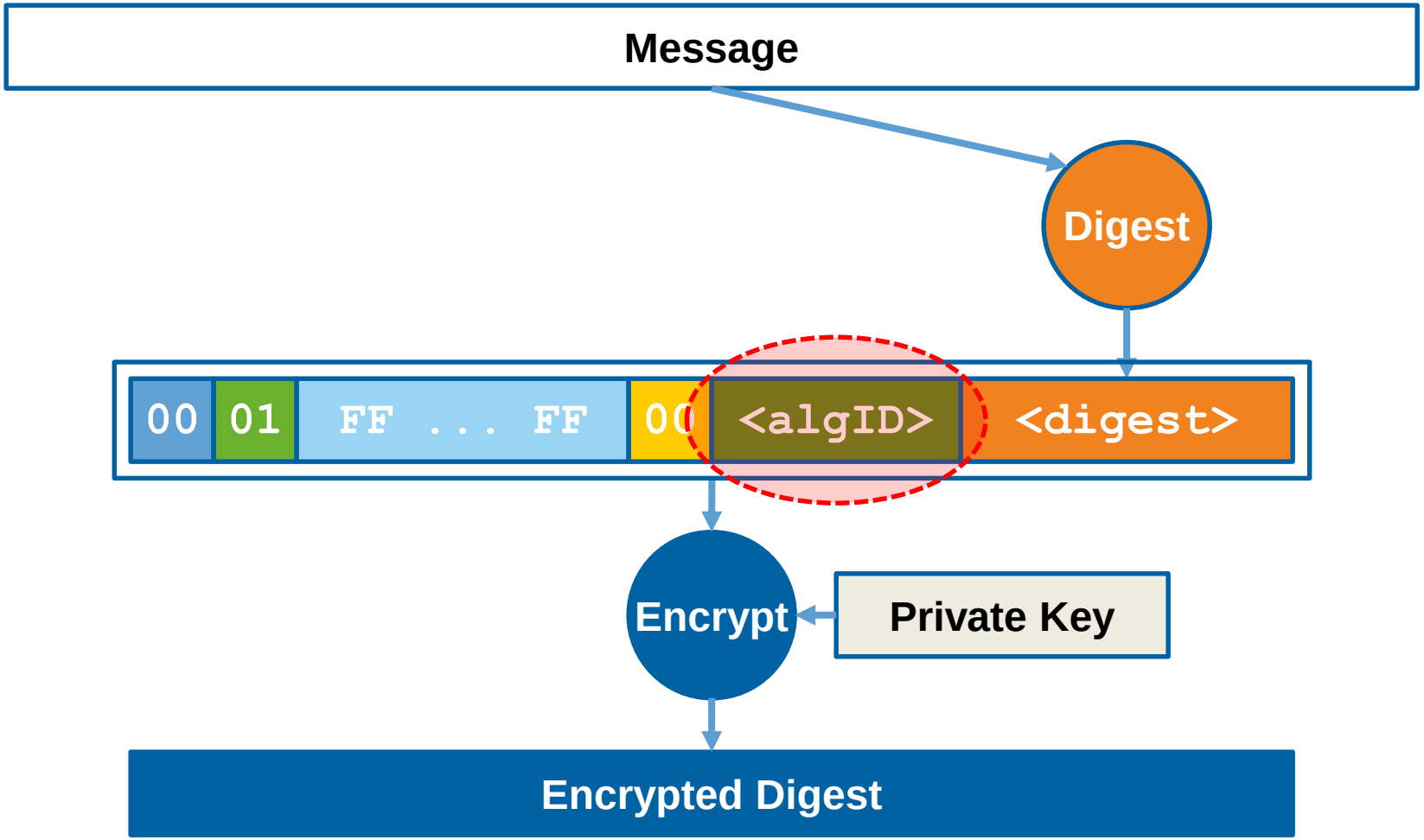
1. Hash-then-Sign Paradigm



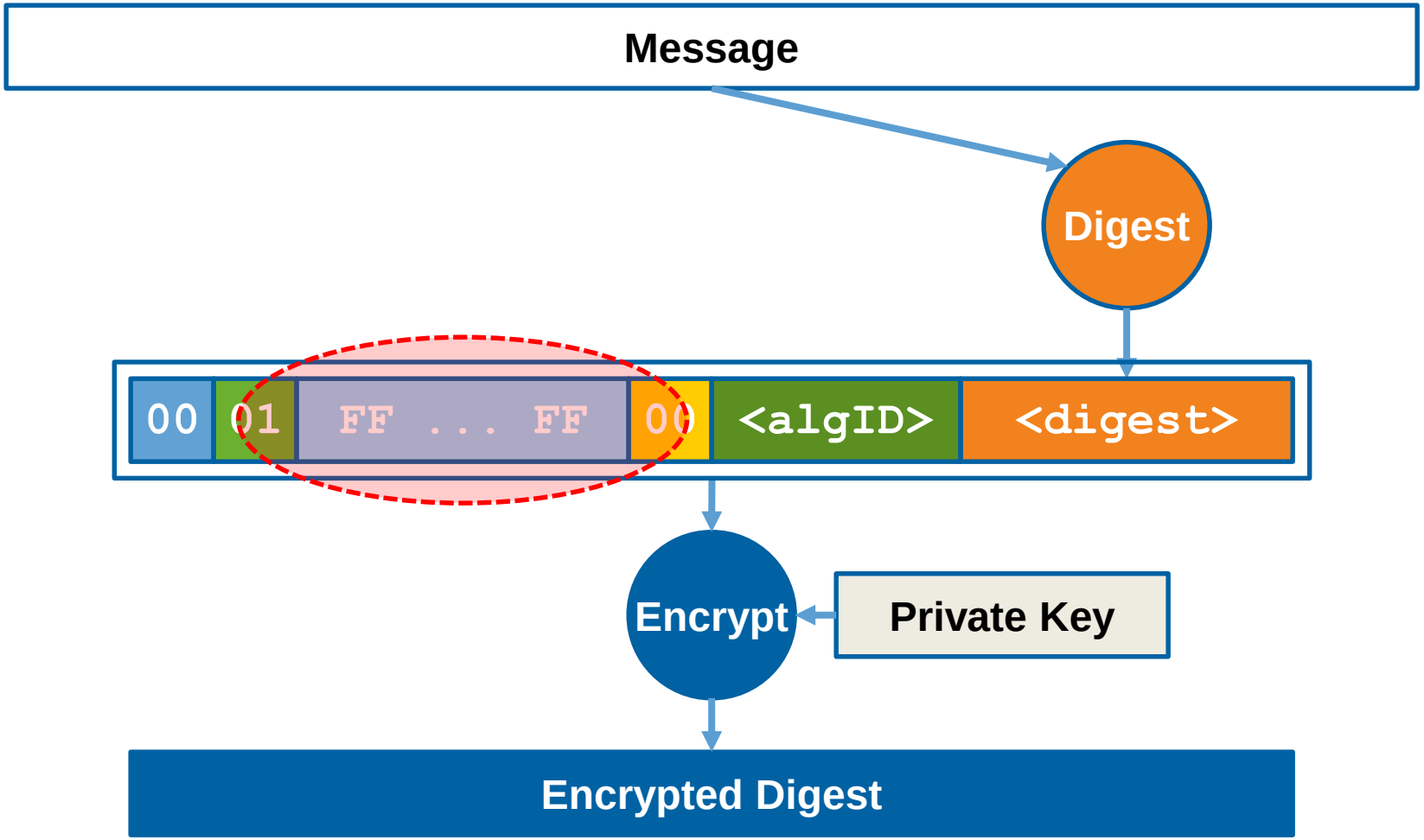
2. Partial Domain “Digests”



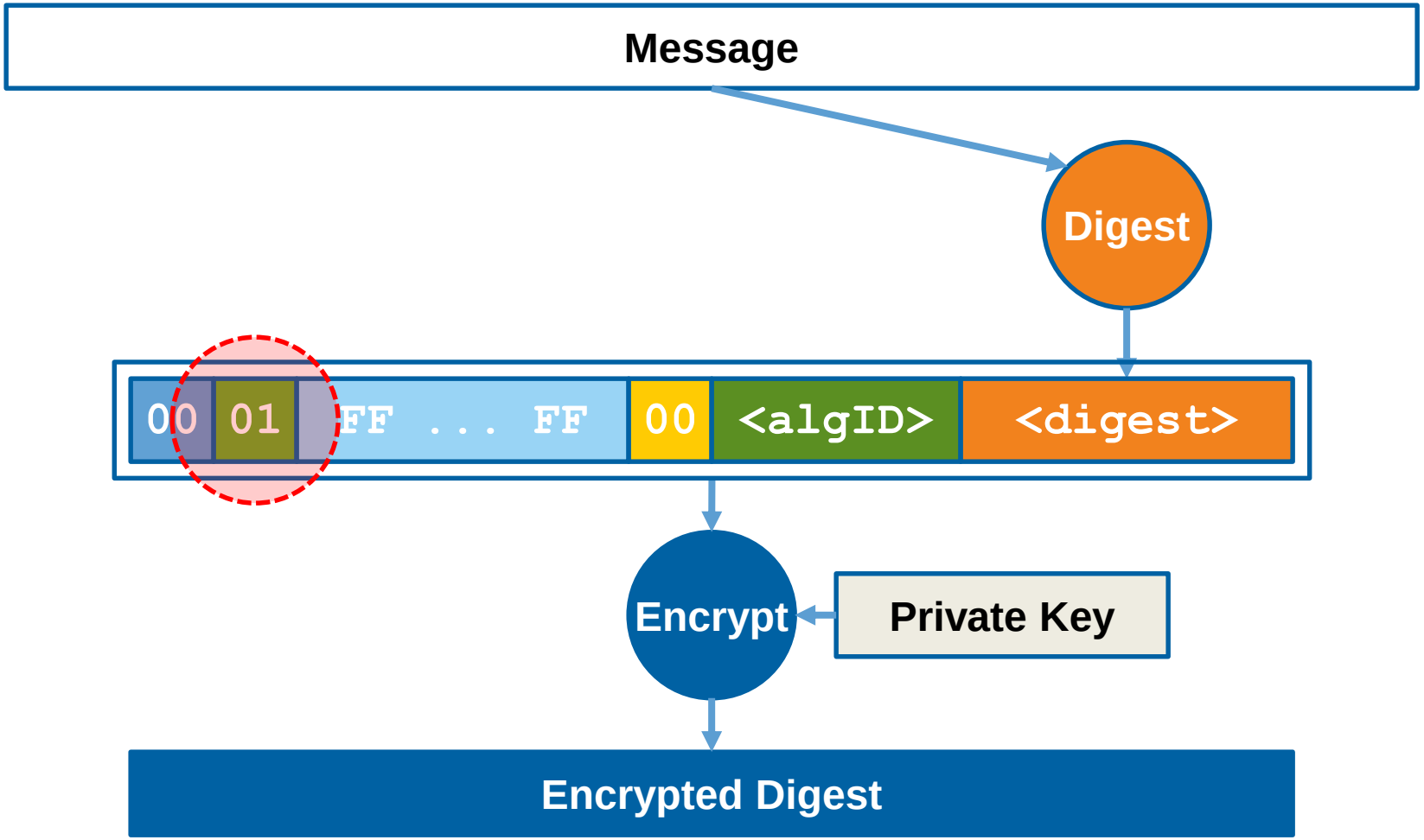
3. Algorithm Identifier



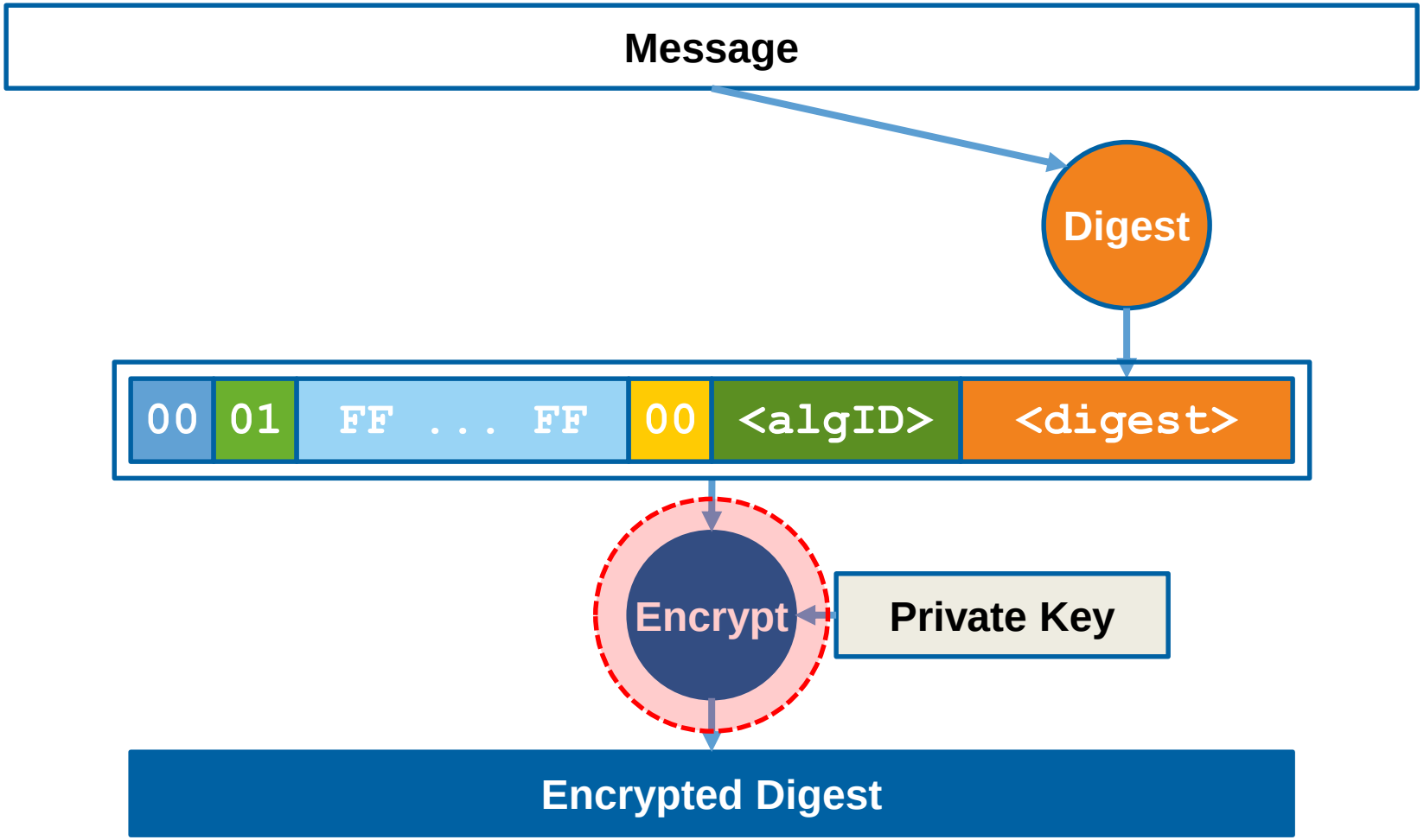
4. Fixed Padding



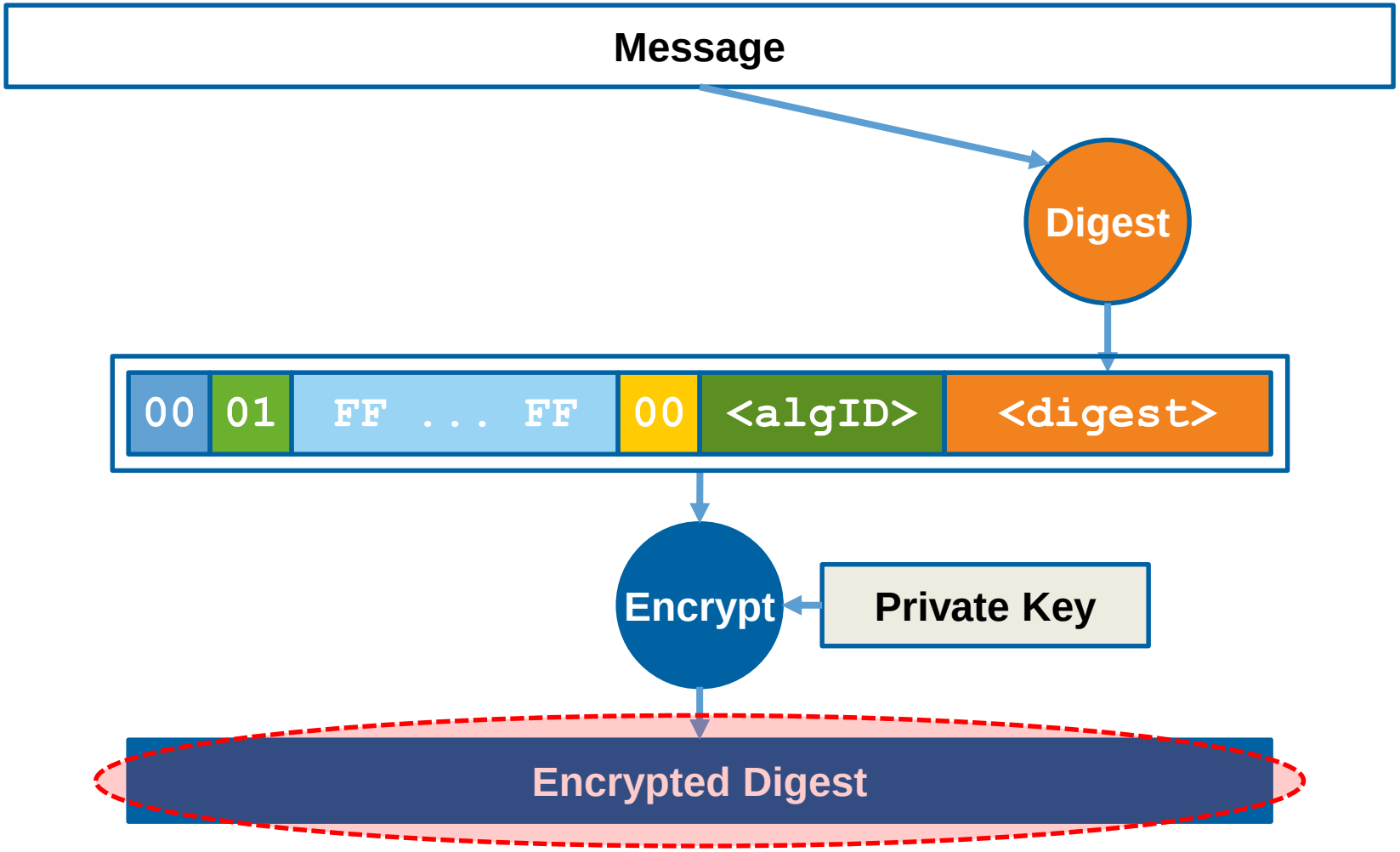
5. Block Type


Message
Digest
00
01
FF . . . FF
00
<algID>
<digest>
Encrypt
Private Key
Encrypted Digest

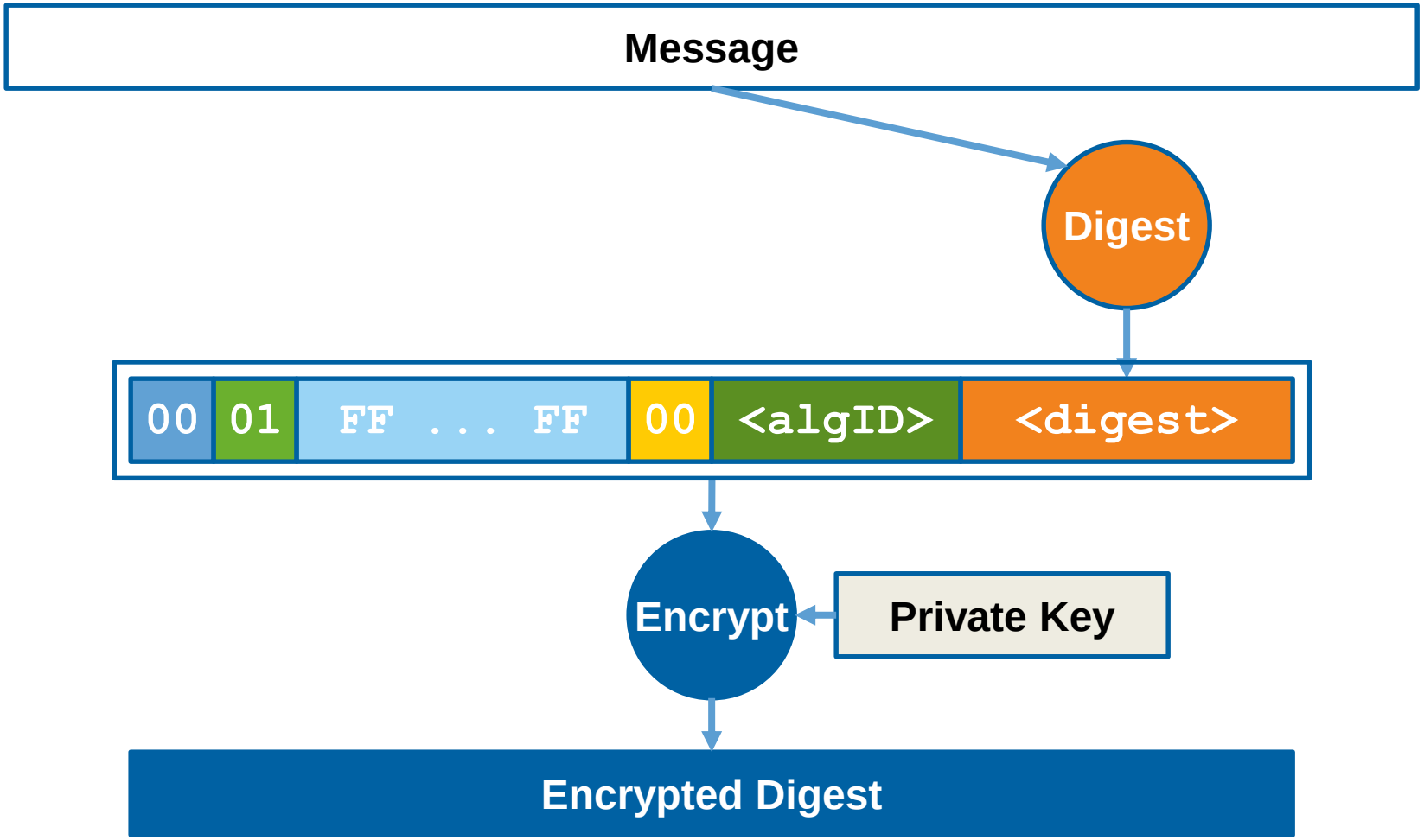
6. Encrypting with Private Key



7. Encrypted Digest



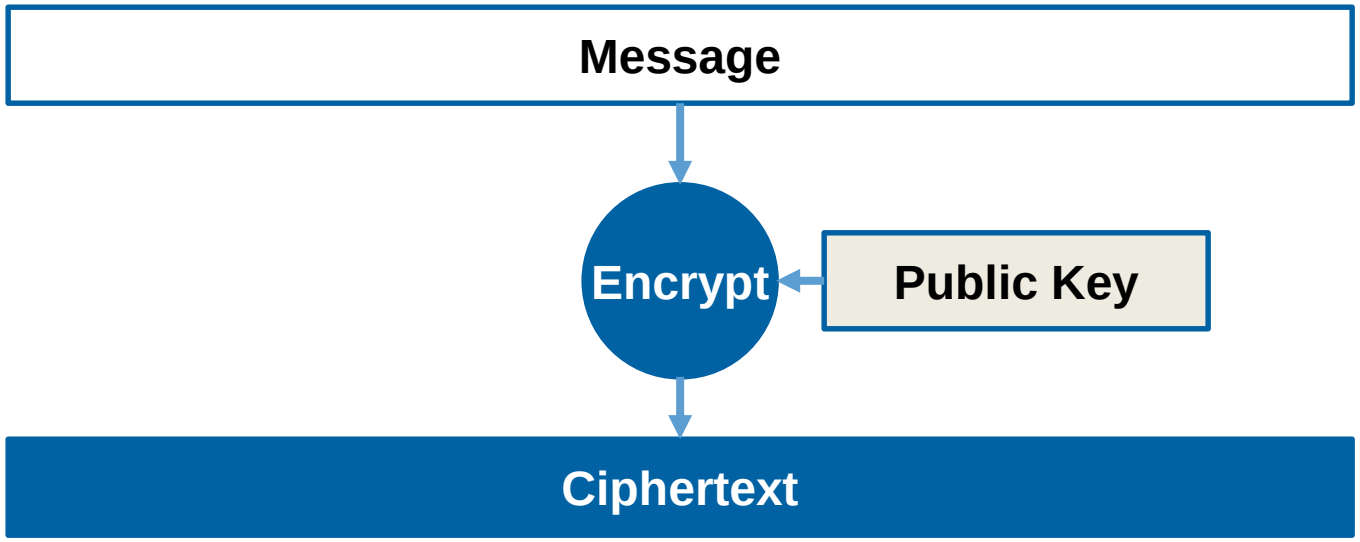
PKCS RSA Signatures: Summary



Part II: RSA Encryption

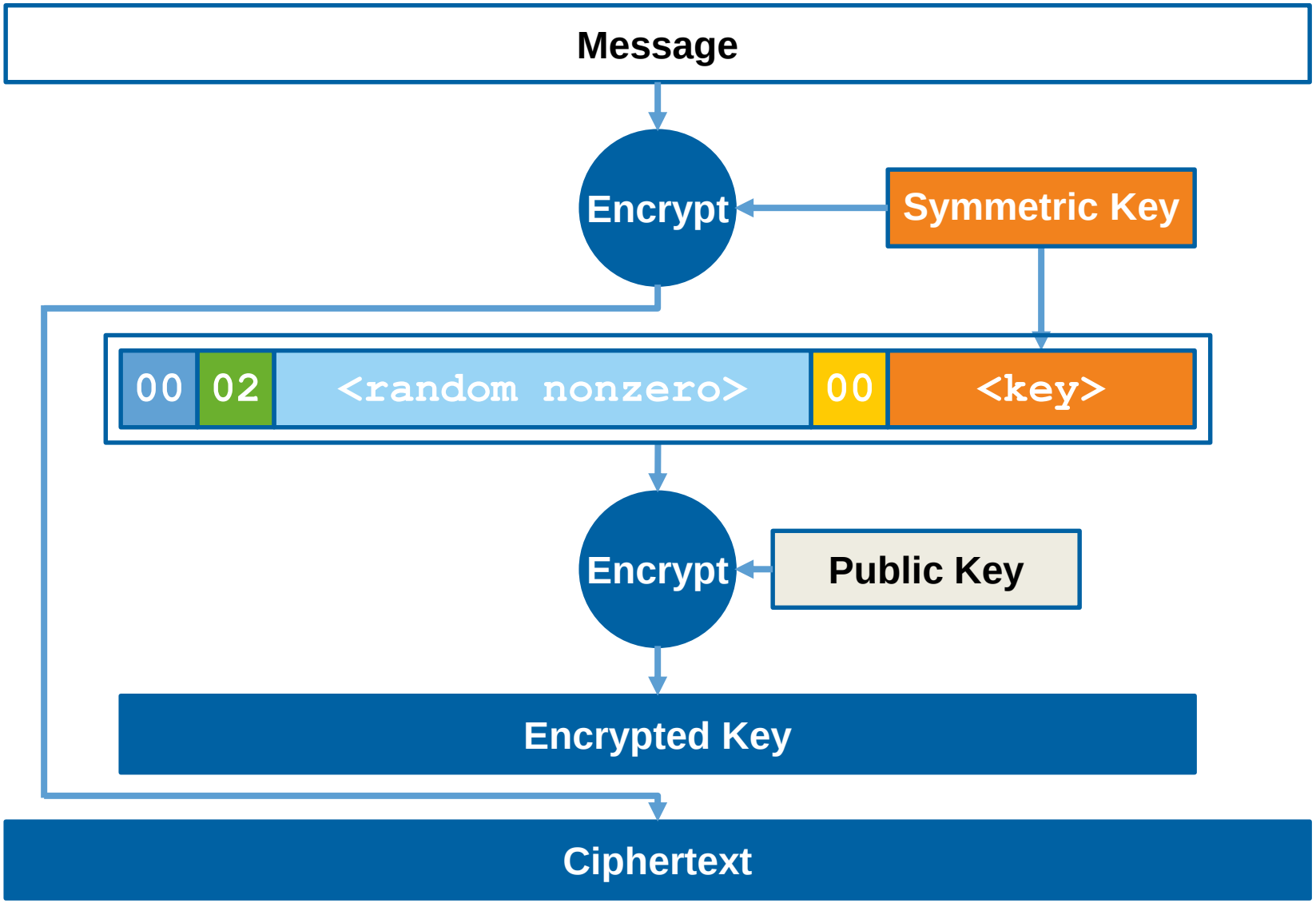
RSA Encryption: Original Model

Diffie-Hellman (1976) and RSA (1978)

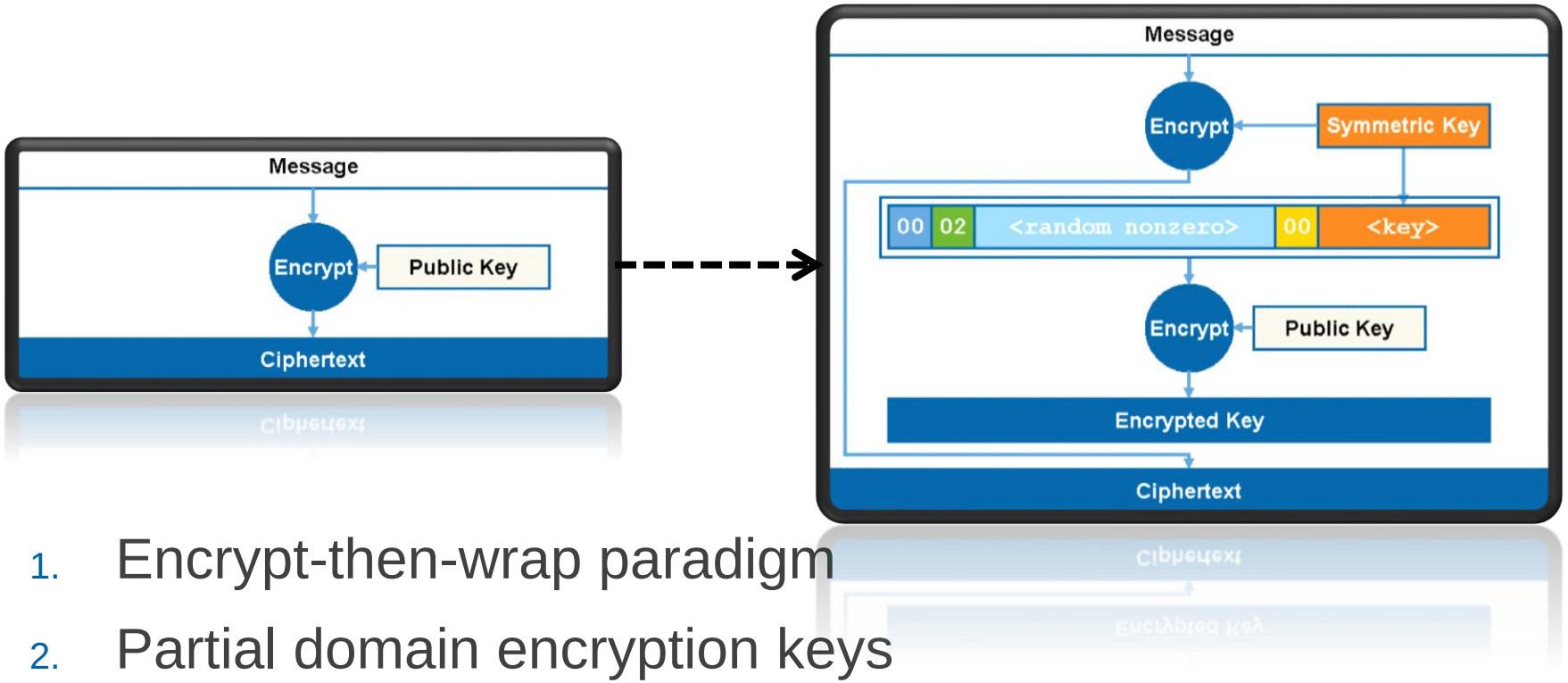


RSA Encryption: "Standard" Model

PKCS #1 and #7 (1991)

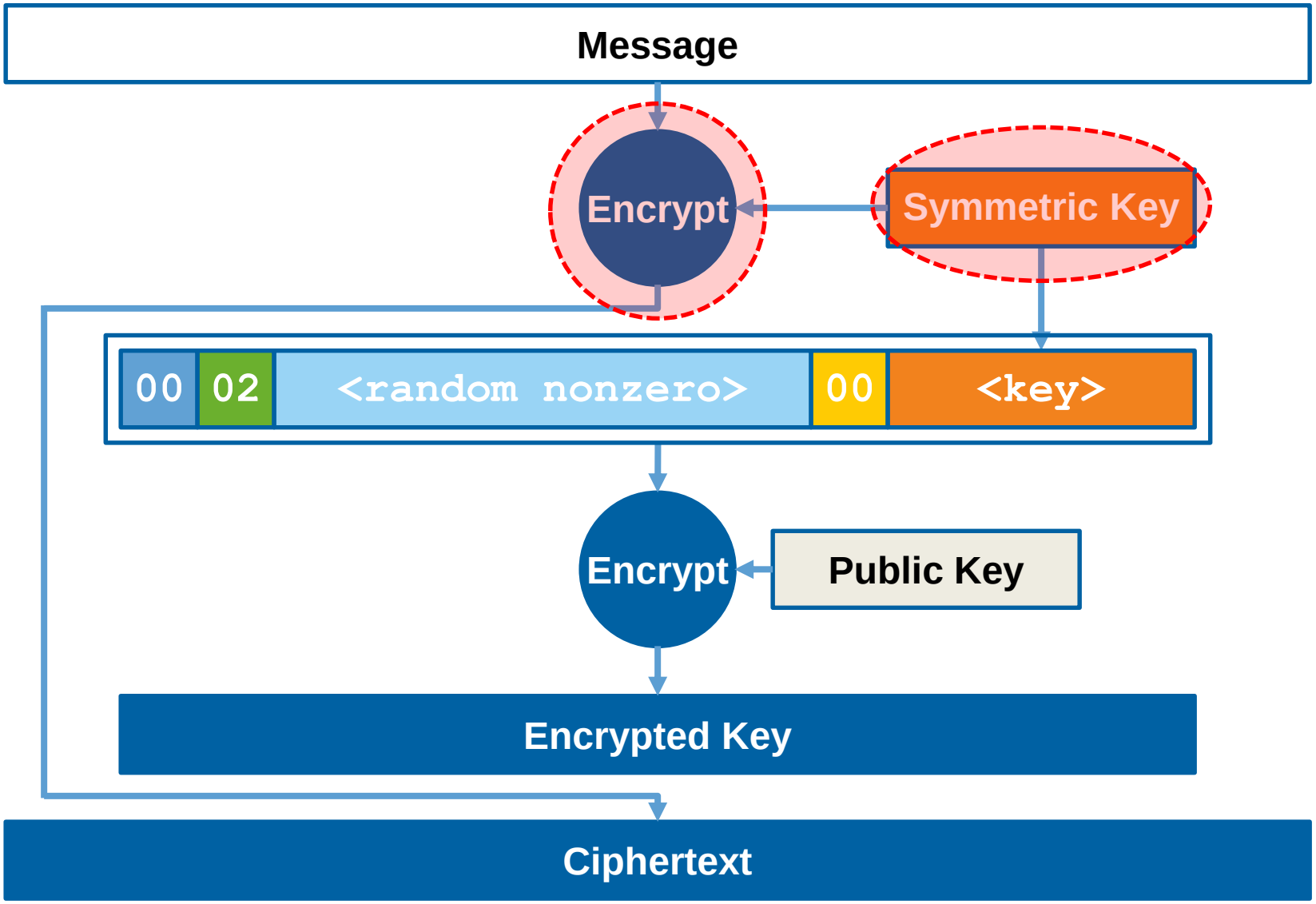


How Did Original Model Change to Standard?

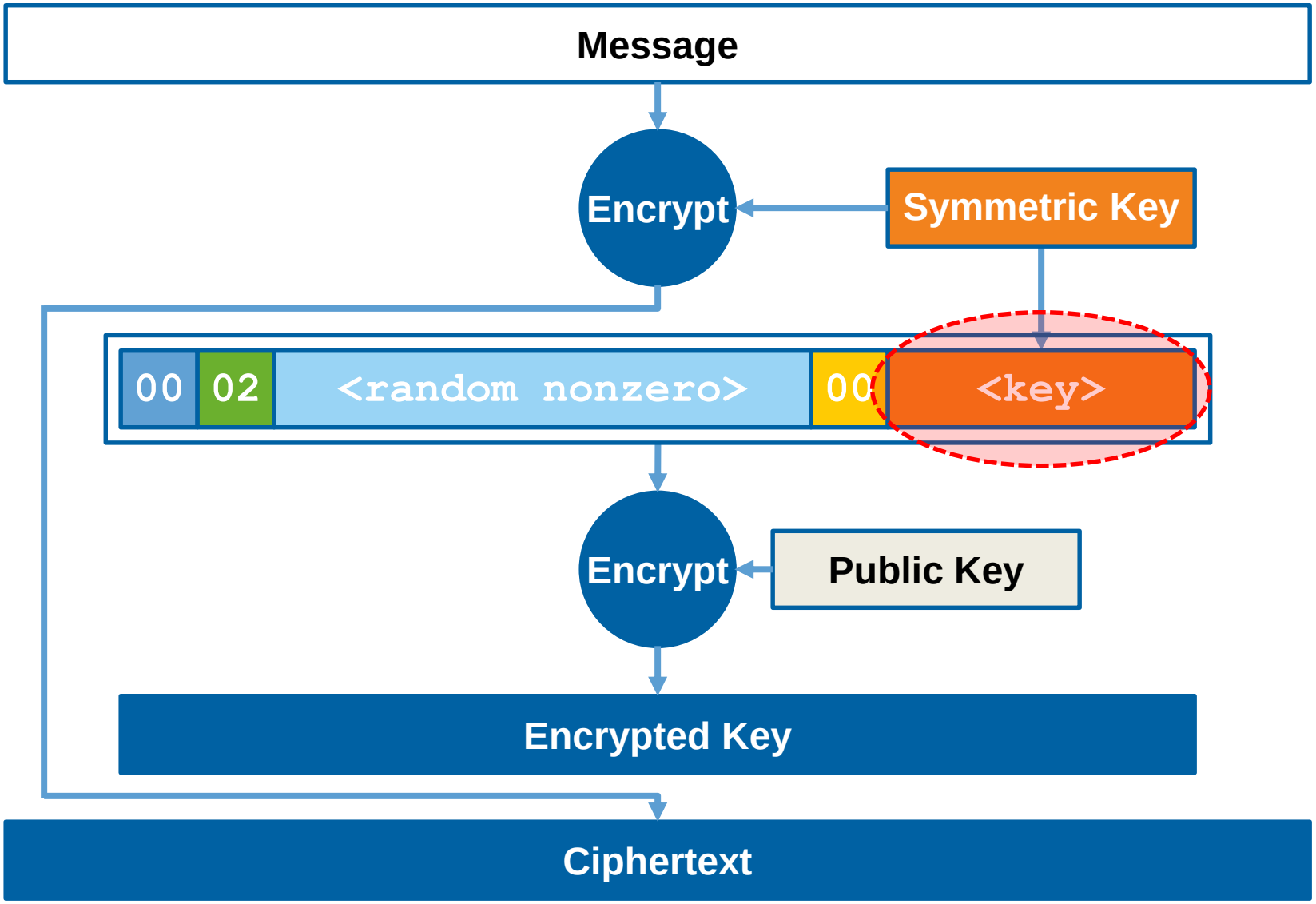


1. Encrypt-then-wrap paradigm
2. Partial domain encryption keys
3. Random padding
4. Block type

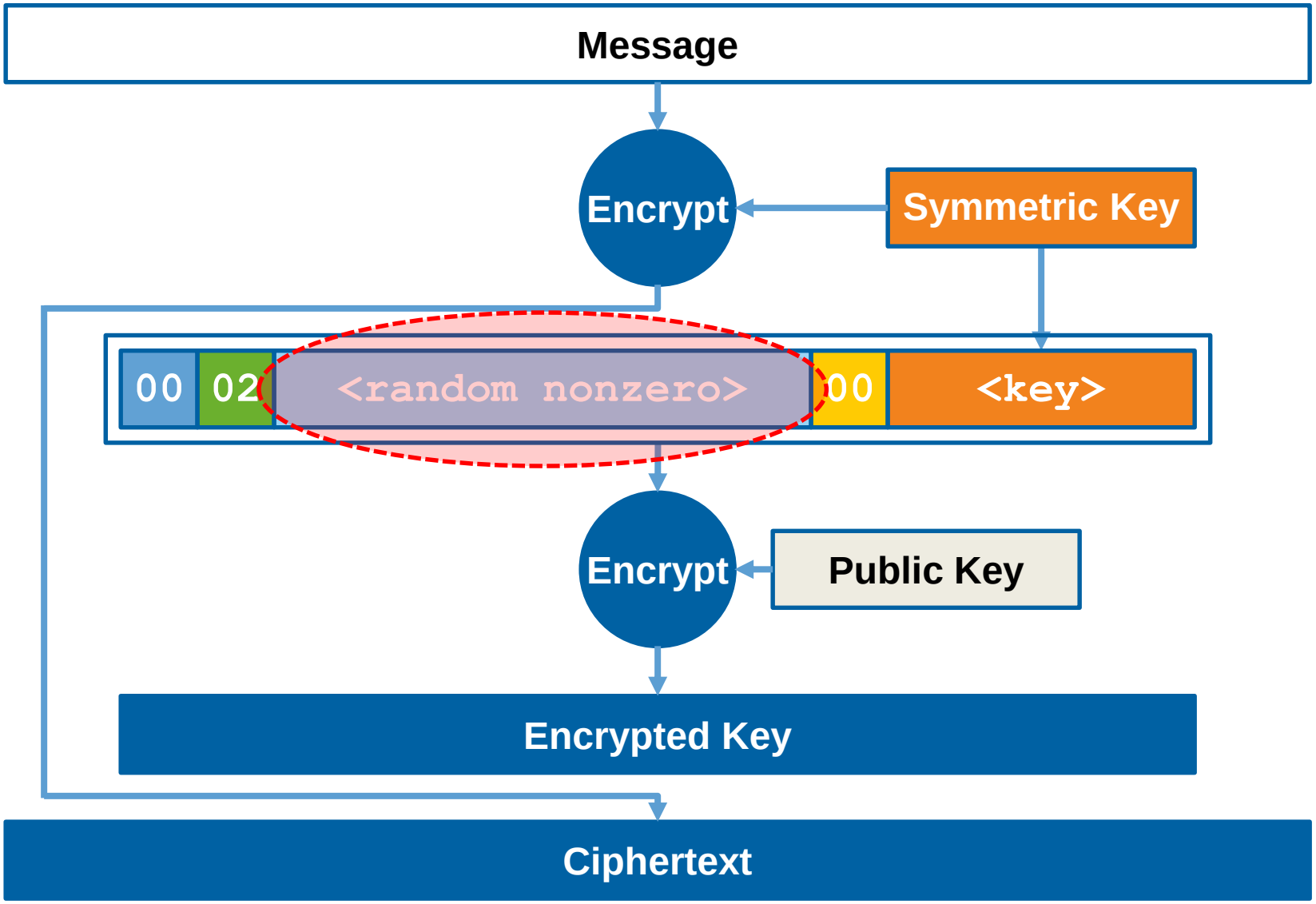
1. Encrypt-then-Wrap Paradigm



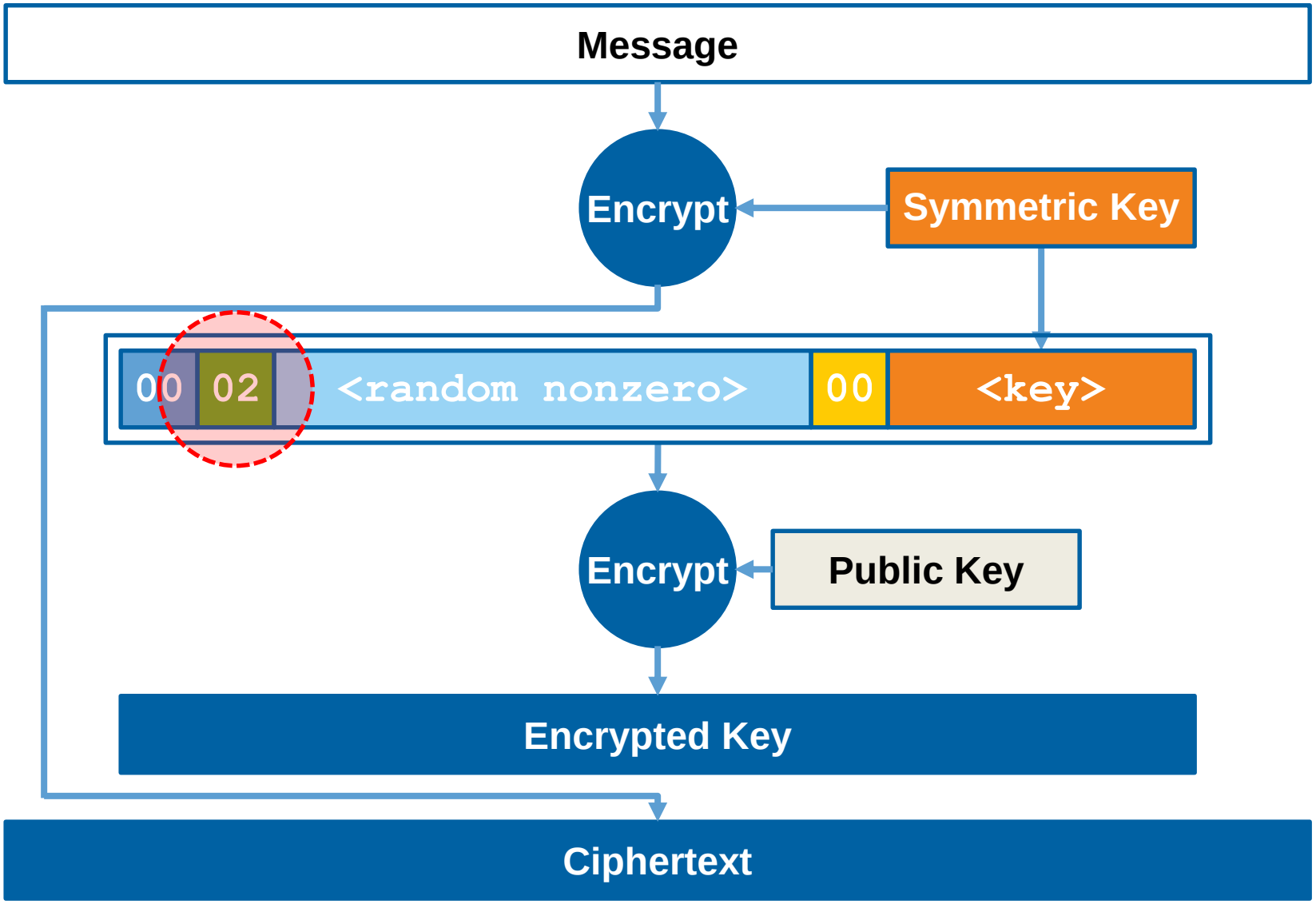
2. Partial Domain Encryption Keys



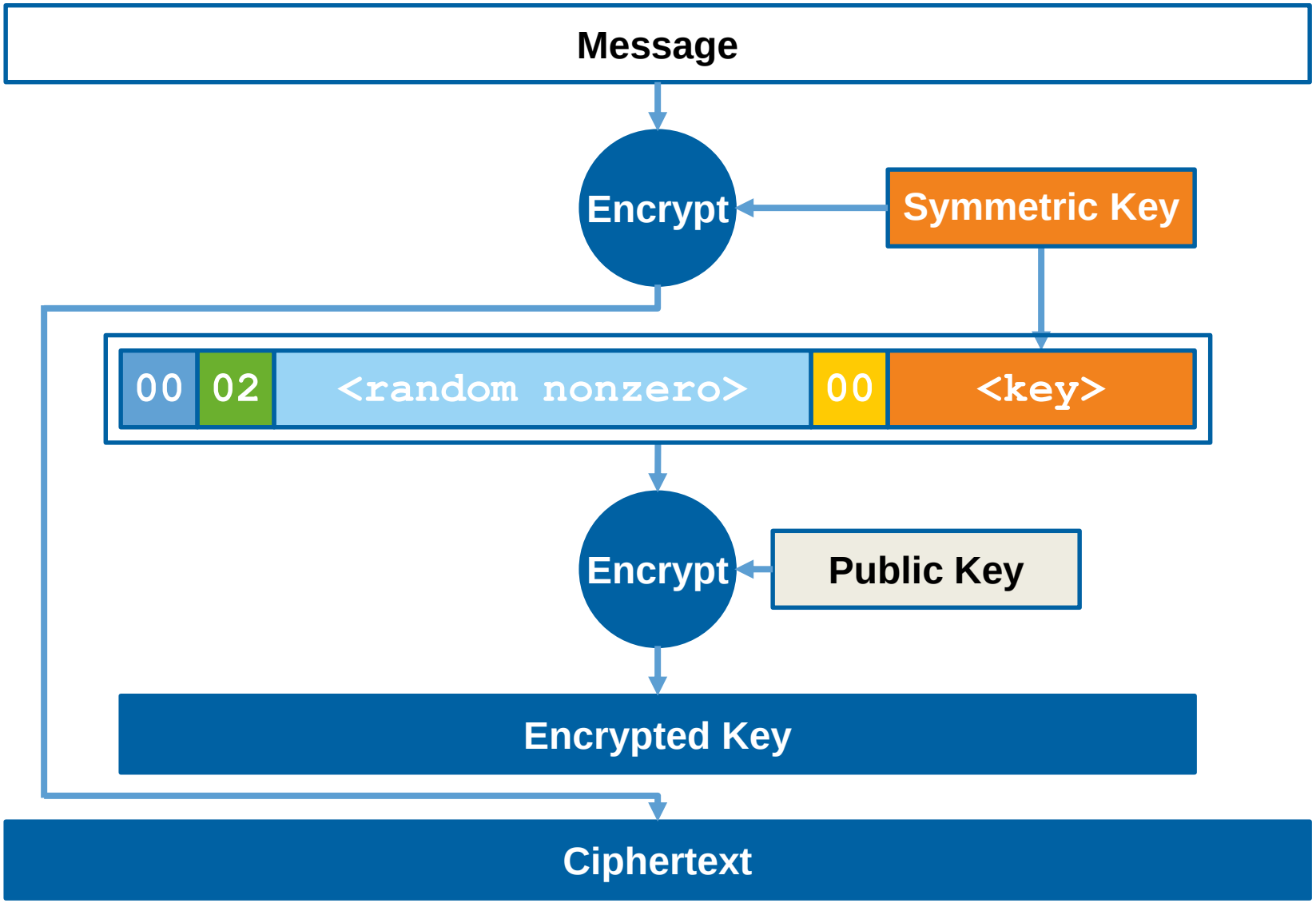
3. Random Padding



4. Block Type

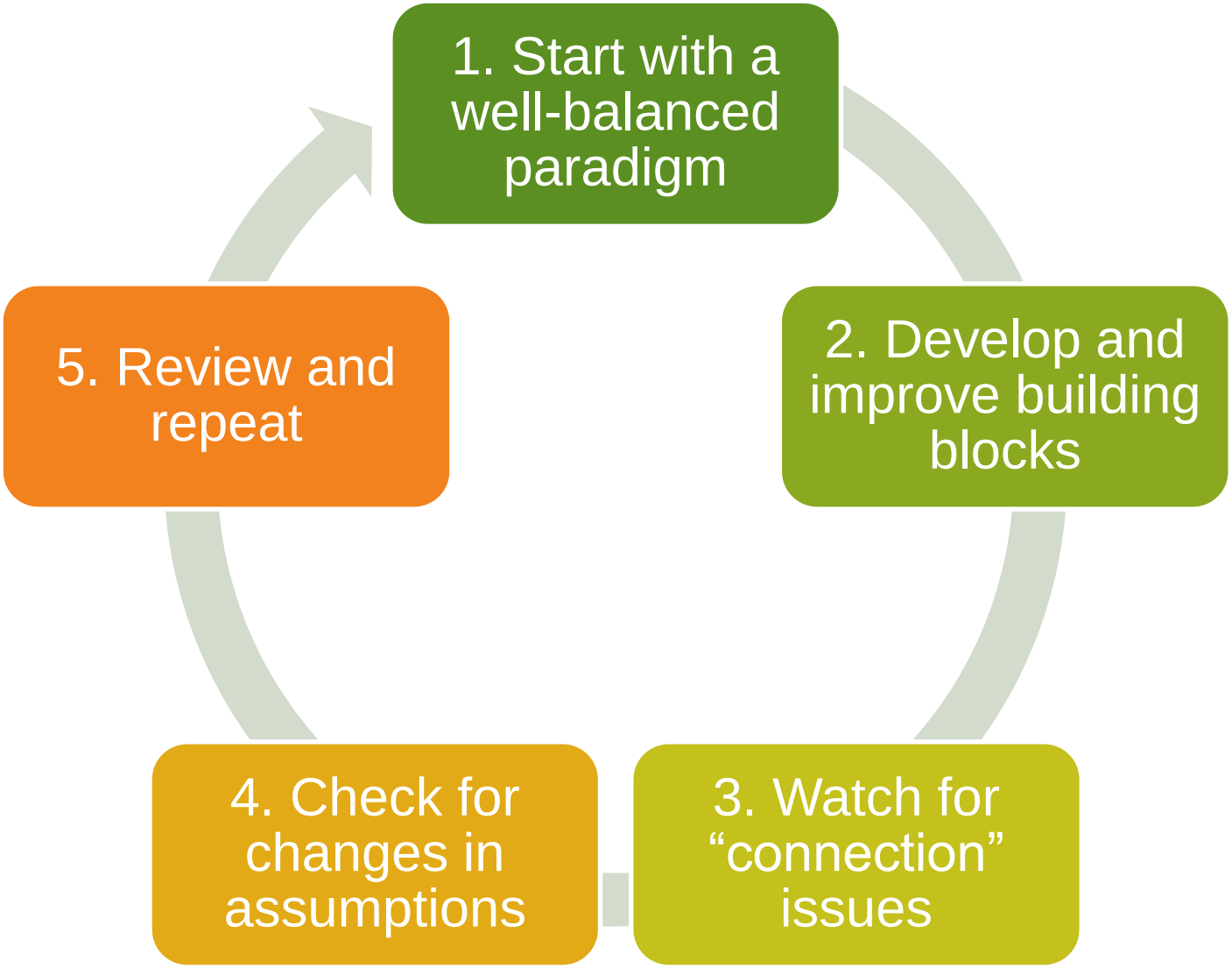

Message
Encrypt
Symmetric Key
00
02
<random nonzero>
00
<key>
Encrypt
Public Key
Encrypted Key
Ciphertext

PKCS RSA Encryption: Summary

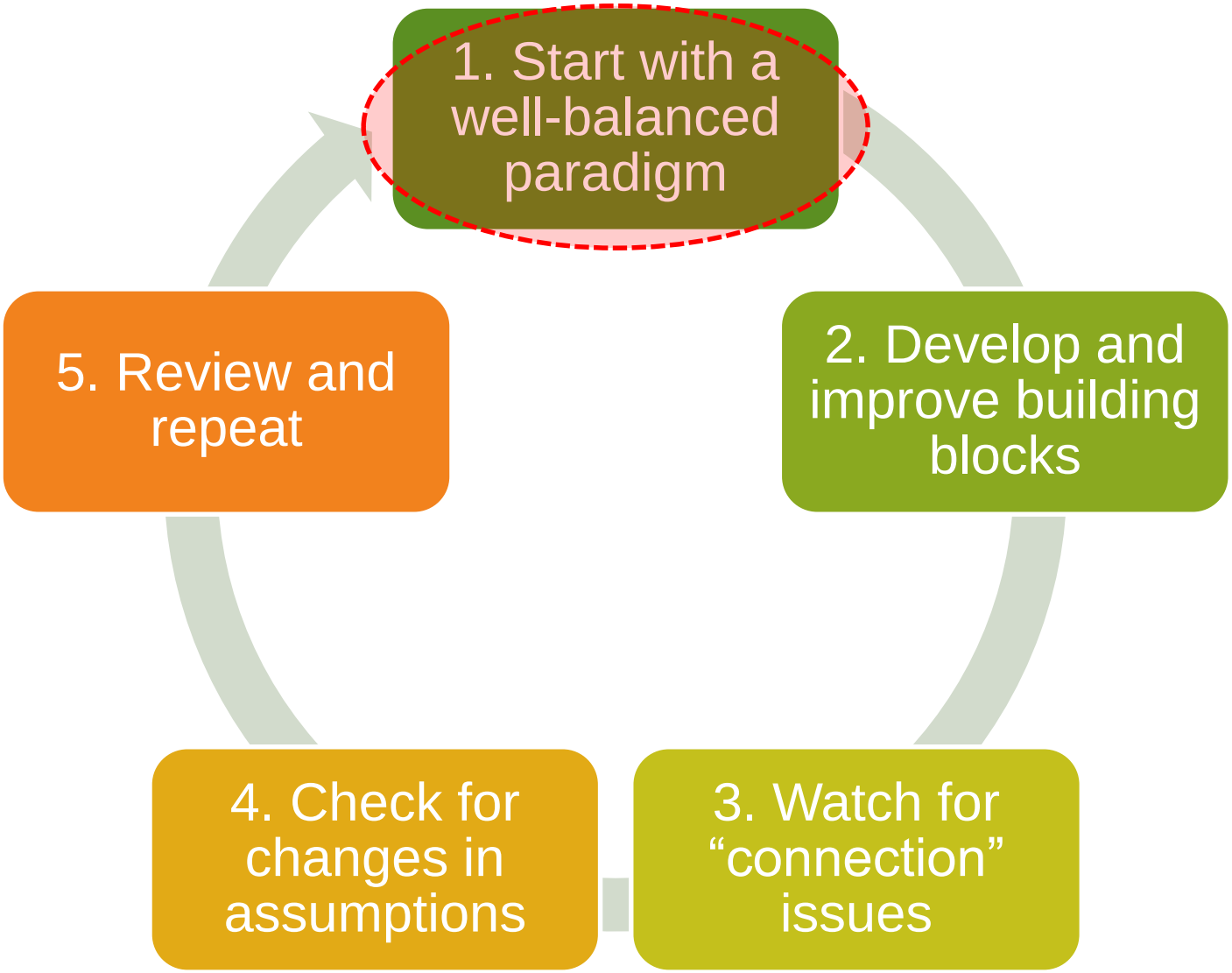


Conclusion: Five Lessons Learned about Standardizing Cryptography

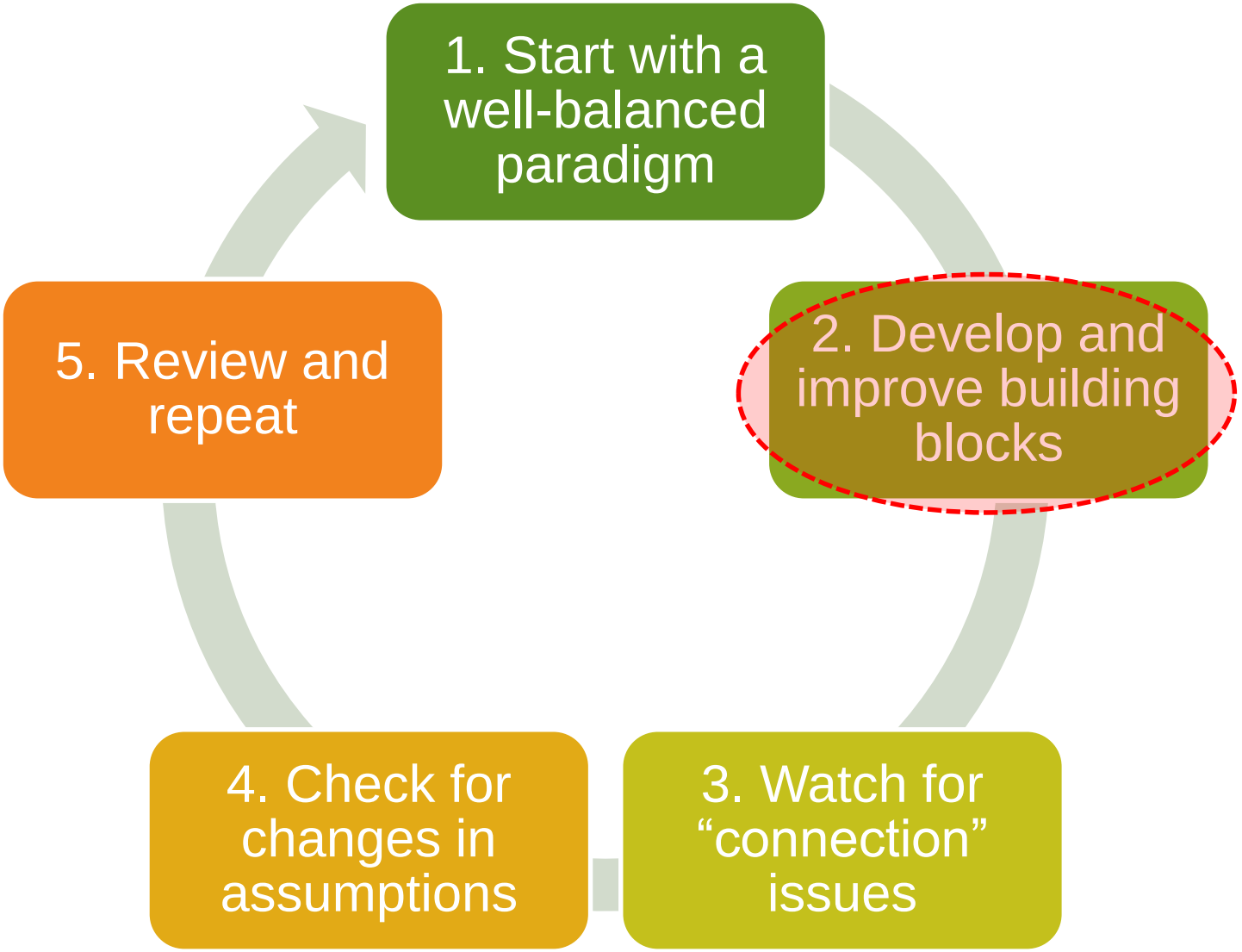
Five Lessons Learned about Standardizing Cryptography



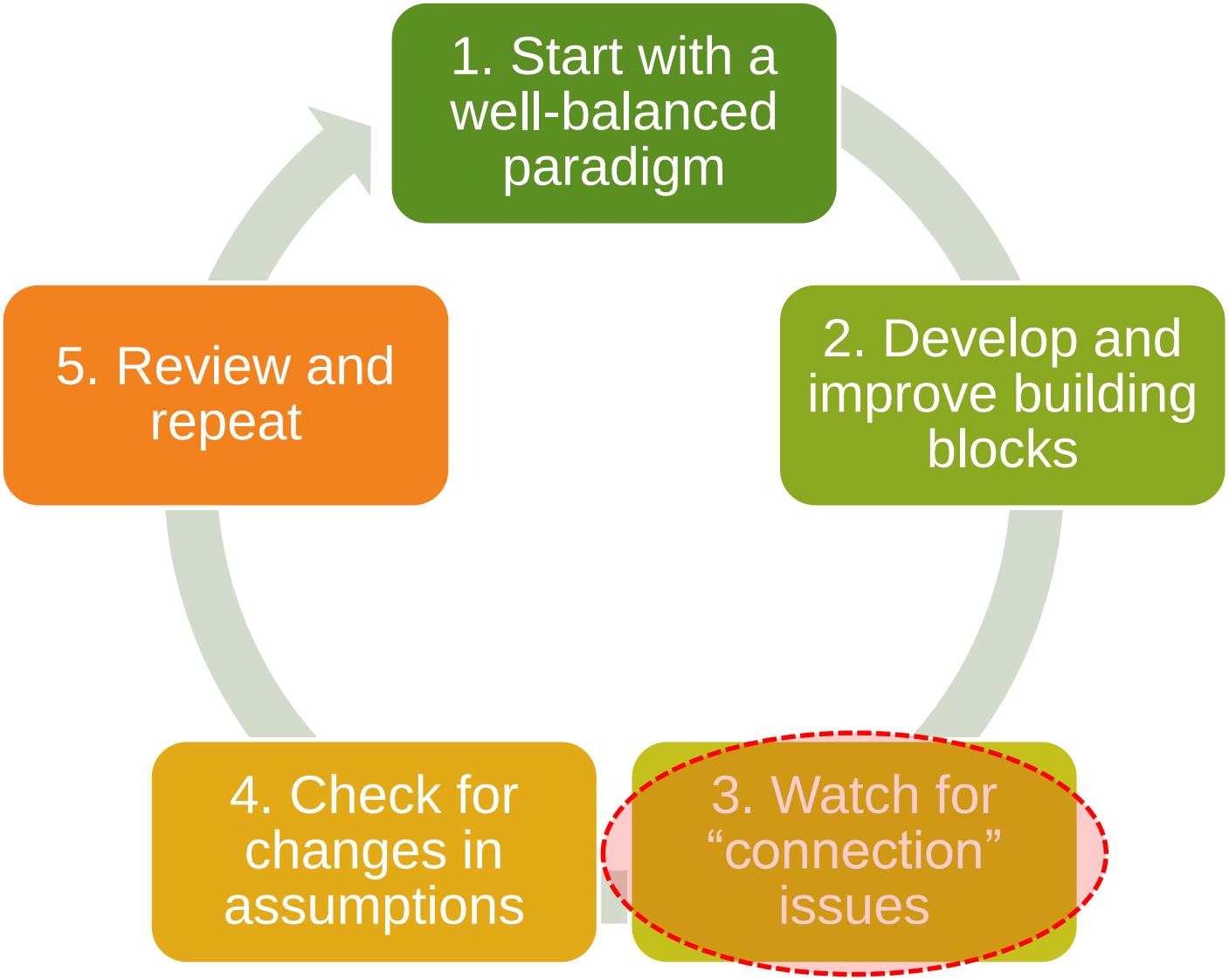
1. Start with a Well-Balanced Paradigm



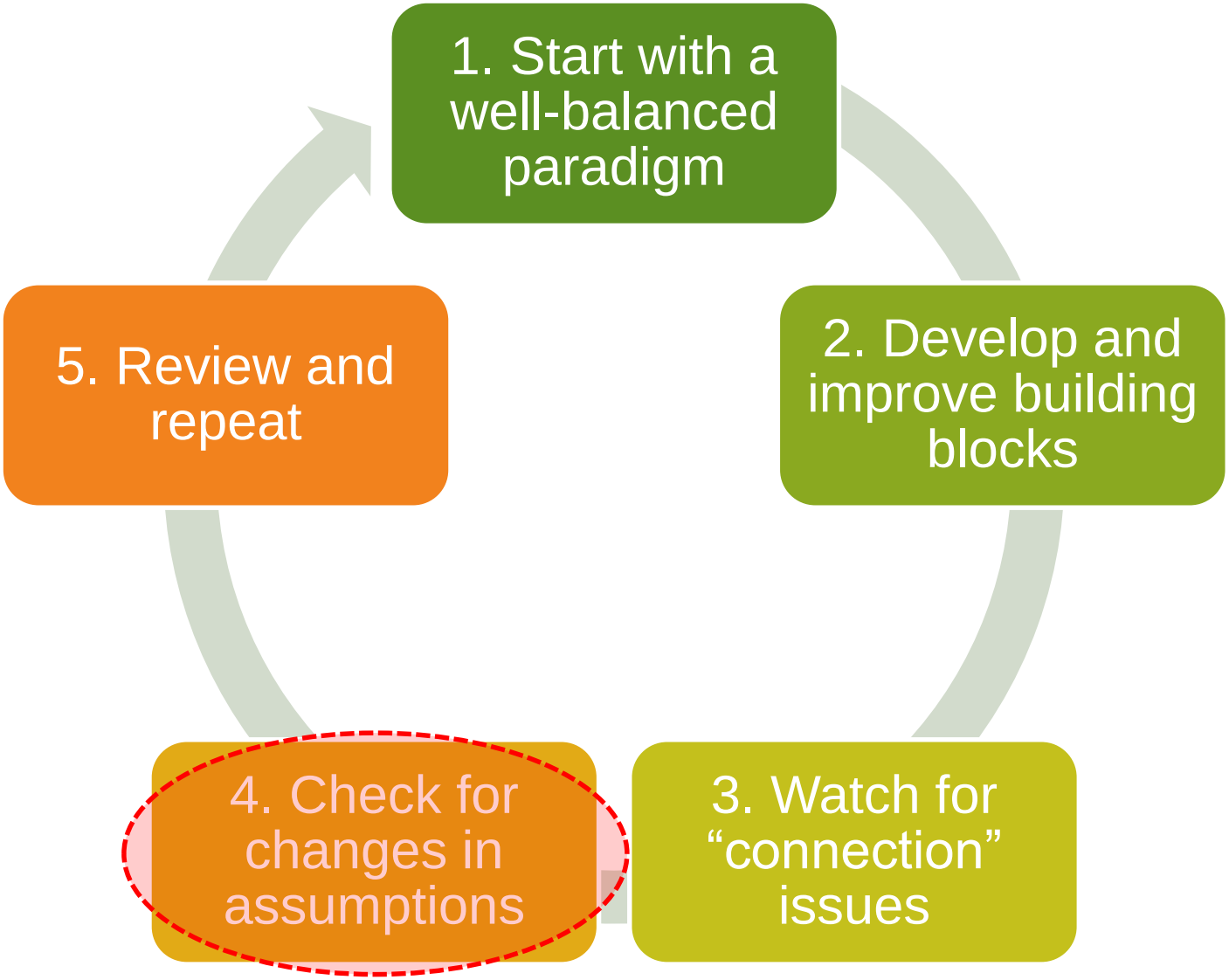
2. Develop and Improve Building Blocks



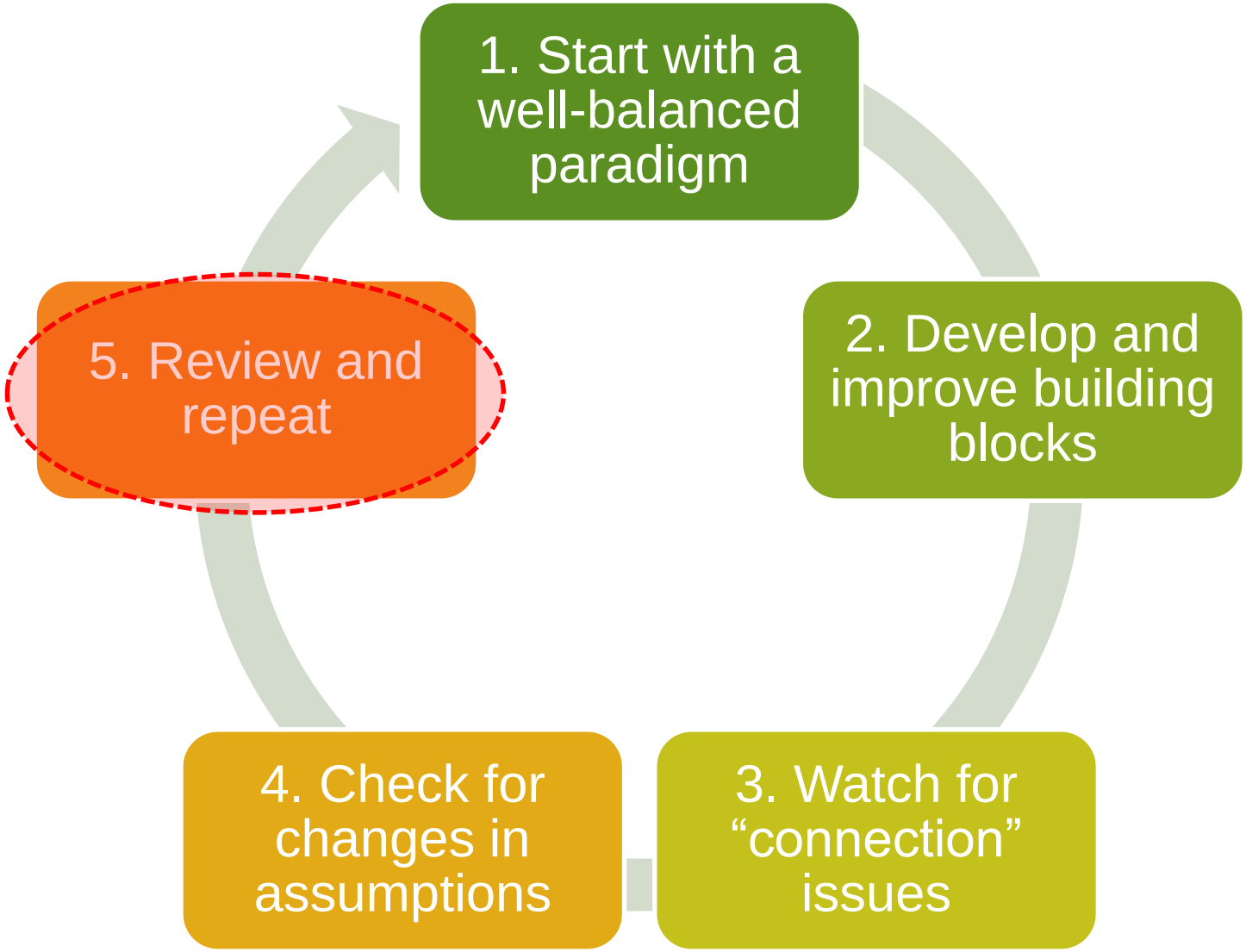
3. Watch for “Connection” Issues



4. Check for Changes in Assumptions



5. Review and Repeat



Questions?

Appendix:
Other RSA Standardization Issues

(overview)

Other RSA Standardization Issues

Public / private key pairs

- Modulus size
- Public exponent values
- Key pair (and prime) generation
- Public key validity
- Public key syntax
- Private key syntax

Message syntax

- Signed messages
- Enveloped (encrypted) messages

Key management

- Certificate syntax
- Certificate request syntax
- Certificate revocation list syntax
- Certificate lifecycle management
- Certificate status protocols
- Private key containers

Cryptographic APIs

and more …

Selected References for Further Reading

Research References (1)

[BR93] M. Bellare & P. Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. ACM CCS 1993.

[BR94] M. Bellare & P. Rogaway. Optimal Asymmetric Encryption — How to Encrypt with RSA. EUROCRYPT 1994.

[BR96] M. Bellare & P. Rogaway. The Exact Security of Digital Signatures-How to Sign with RSA and Rabin. EUROCRYPT 1996.

[Bl98] D. Bleichenbacher. Chosen Ciphertext Attacks against Protocols Based on the RSA Encryption Standard PKCS #1. CRYPTO 1998.

[Bl06] D. Bleichenbacher. Forging Some RSA Signatures with Pencil and Paper. CRYPTO 2006 Rump Session.

[Da82] C.I. Davida. Chosen Signature Cryptanalysis of the RSA (MIT) Public Key Cryptosystem. University of Wisconsin, 1982.

[DP80] D.W. Davies & W.L. Price. The Application of Digital Signatures Based on Public Key Cryptosystems. National Physical Laboratory, England, 1980.

[dJC85] W. deJonge and D. Chaum. Attacks on Some RSA Signatures. CRYPTO 1985.

[De84] D. Denning. Digital Signatures with RSA and Other Public-Key Cryptosystems. Communications of the ACM, 1984.

[DO85] Y. Desmedt & A.M. Odlyzko. A Chosen Text Attack on the RSA Cryptosystem and Some Discrete Logarithm Schemes. CRYPTO 1985.

Research References (2)

[DH76] W. Diffie and M.E. Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory, 1976.

[Hå88] J. Håstad. Solving Simultaneous Modular Equations of Low Degree. SIAM Journal of Computing, 1988.

[JKM18] T. Jager, S.A. Kavki & A. May. On the Security of the PKCS #1 v1.5 Signature Scheme. ACM CCS 2018

[JK02] J. Jonsson & B.S. Kaliski Jr. On the Security of RSA Encryption in TLS. CRYPTO 2002.

[Ju86] R.R. Jueneman. A High Speed Manipulation Detection Code. CRYPTO 1986.

[Me89] R.C Merkle. One Way Hash Functions and DES. CRYPTO 1989.

[MWR89] C. Mitchell, M. Walker & D. Rush. CCITT/ISO Standards for Secure Message Handling. IEEE Journal on Selected Areas in Communications, 1989.

[Mo88] J.H. Moore. Protocol Failures in Cryptosystems. Proceedings of the IEEE, 1988.

[RSA78] R.L. Rivest, A. Shamir & L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 1978.

[Sh01] V. Shoup. A Proposal for an ISO Standard for RSA Encryption. IACR ePrint 2001-112.

Standards References

[RFC1040] J. Linn. Privacy Enhancement for Internet Electronic Mail: Part I: Message Encipherment and Authentication Procedures. 1988.

[RFC1113] J. Linn. Privacy Enhancement for Internet Electronic Mail: Part I: Message Encipherment and Authentication Procedures. 1989.

[RFC2313] B. Kaliski. PKCS #1: RSA Encryption Version 1.5. 1998.

[RFC2315] B. Kaliski. PKCS #7: RSA Encryption Version 1.5. 1998.

[RFC6101] A. Freier, P. Karlton & P. Kocher. The Secure Sockets Layer (SSL) Protocol Version 3.0. 2011.

[RFC8017] K. Moriarty, Ed., B. Kaliski, J. Jonsson & A. Rusch. PKCS #1: RSA Cryptography Specifications Version 2.2. 2016.

[FIPS186] NIST. Digital Signature Standard. 1994.

[X.509-88] ITU-T. The Directory — Authentication Framework. 1988.

Special thanks to Chris Mitchell for helpful feedback on early history of public-key standards and access to additional publications, and to John Linn for perspective on the development of Privacy-Enhanced Mail.