Padding Schemes for RSA and their Security

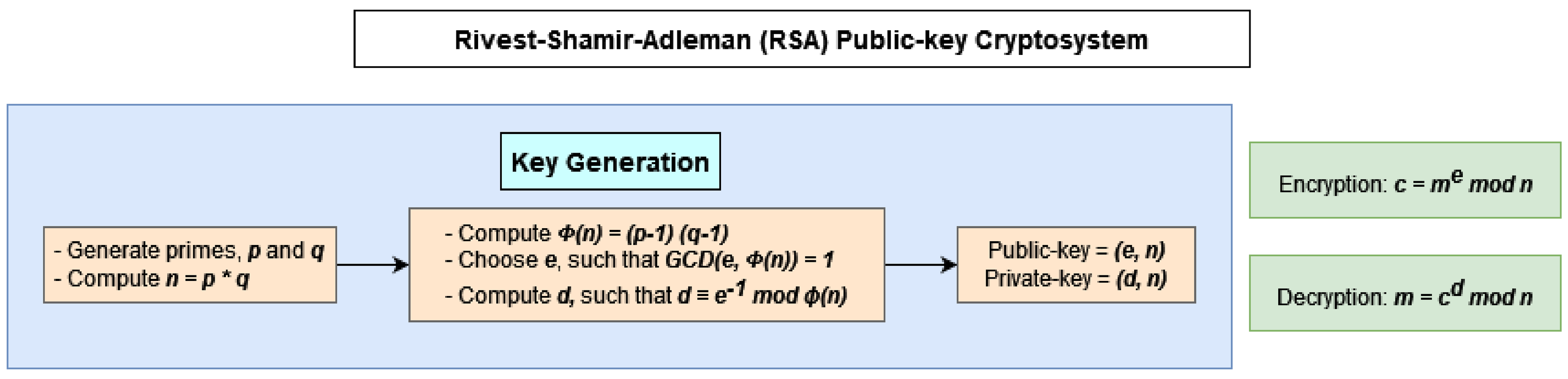
Calvin Ryan Dsouza (cd5184@rit.edu)

Advisor: Stanisław P. Radziszowski

Computer Science @ RIT
B.Thomas Golisano College of Computing & Information Sciences

INTRODUCTION

- One of the oldest algorithms used for data transmission and digital signatures is the Rivest-Shamir-Adleman (RSA) public-key cryptosystem. The security of RSA banks on difficulty of factoring the product of 2 large prime numbers i.e., the factorization problem.

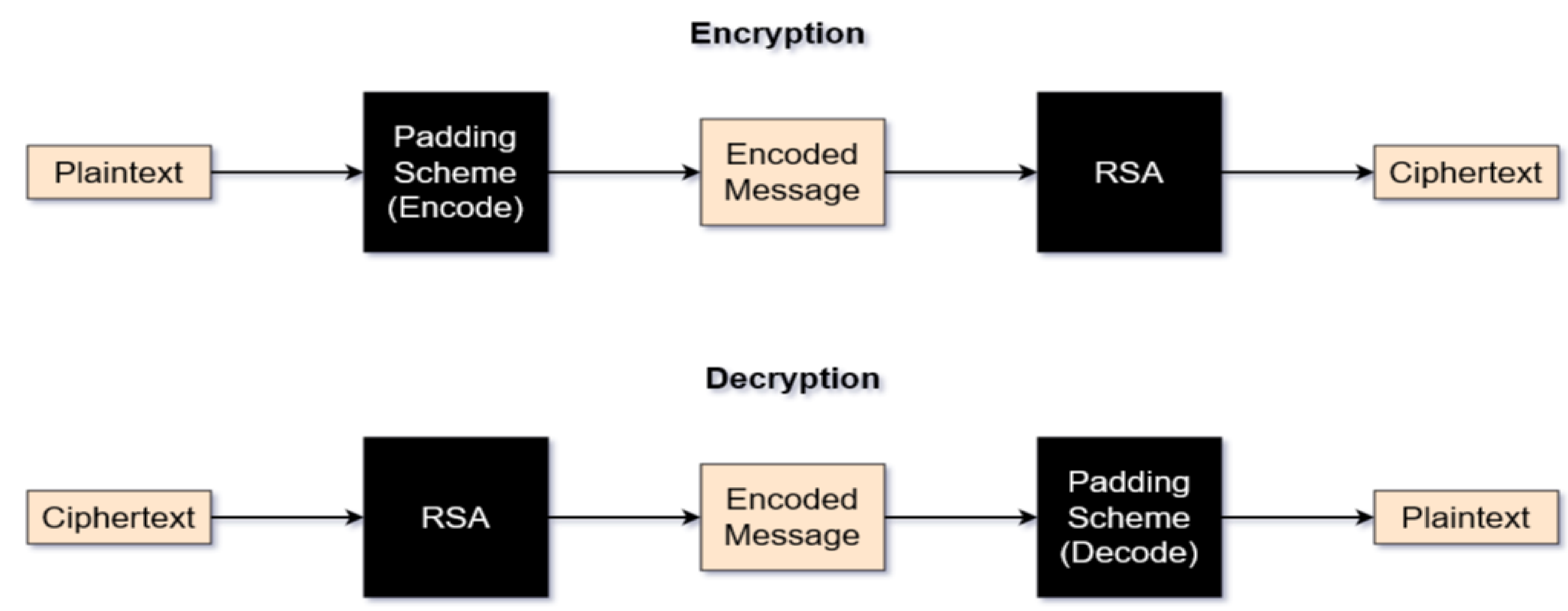


- In the real-world, RSA is implemented with modulus of 2048/4096-bit integers. Thus, RSA is computationally expensive and commonly only used for key transmission/digital signatures.
- RSA is a deterministic cryptosystem, which makes it susceptible chosen-plaintext attacks. To mitigate this RSA is almost always employed along with padding schemes.
- Padding schemes introduce a random component into RSA, thus making the algorithm probabilistic.

GENERATING PRIMES FOR RSA

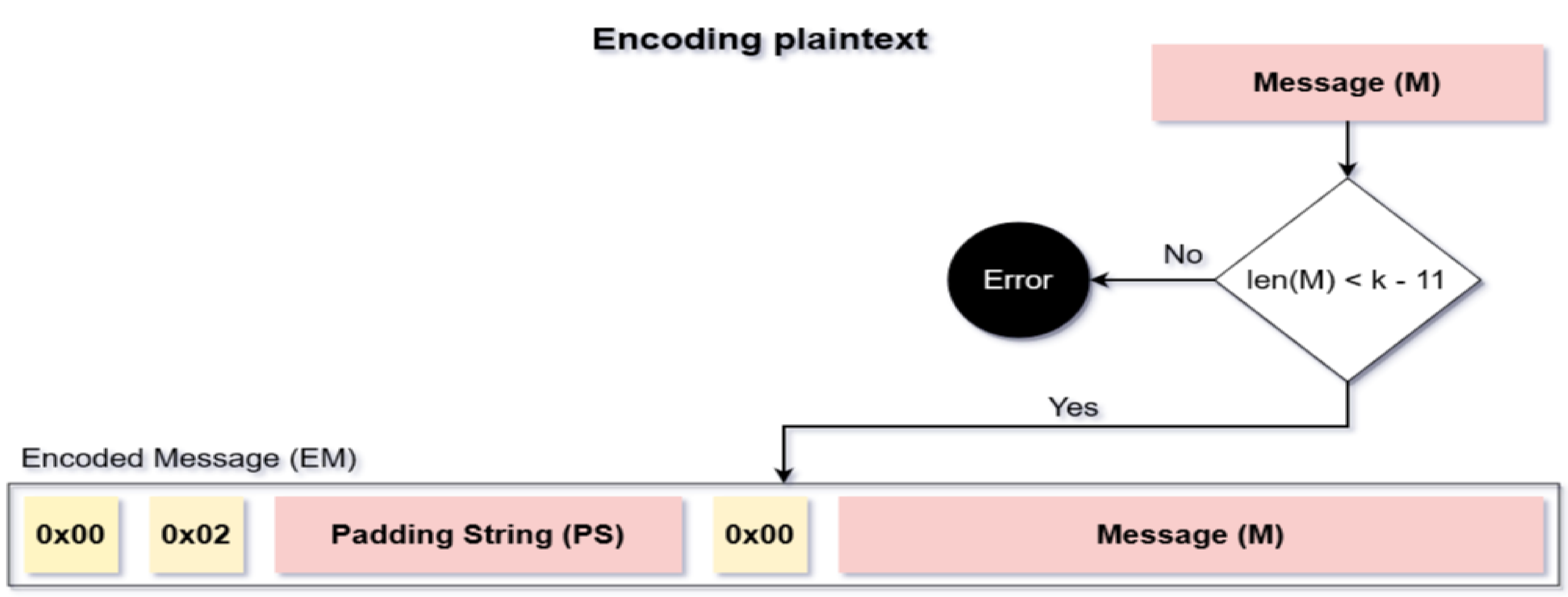
- For a prime number ***p***, if ***p-1*** has many small factors, it is possible to find p given ***p-1*** using **Pollard's *p-1* Algorithm**. This introduces the concept of Safe primes. For a prime ***p***, if ***p-1 = 2 * prime***, then ***p*** is called a **Safe prime**.
- Prime numbers for RSA are generated using cryptographically safe random number generators and often not susceptible to Pollards Algorithm. However, if the prime numbers aren't chosen with care, it could be detrimental to RSA.

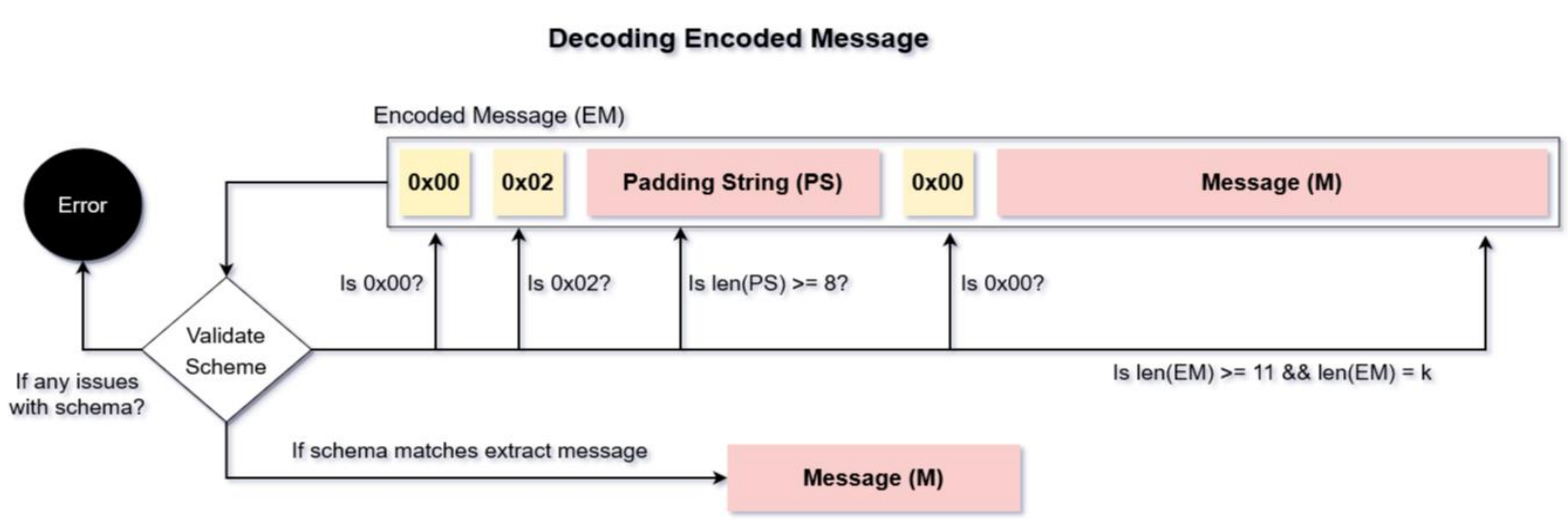
HOW PADDING SCHEME'S FUNCTION



PADDING SCHEMES

Public-Key Cryptography Standard (PKCS) #1 v1.5





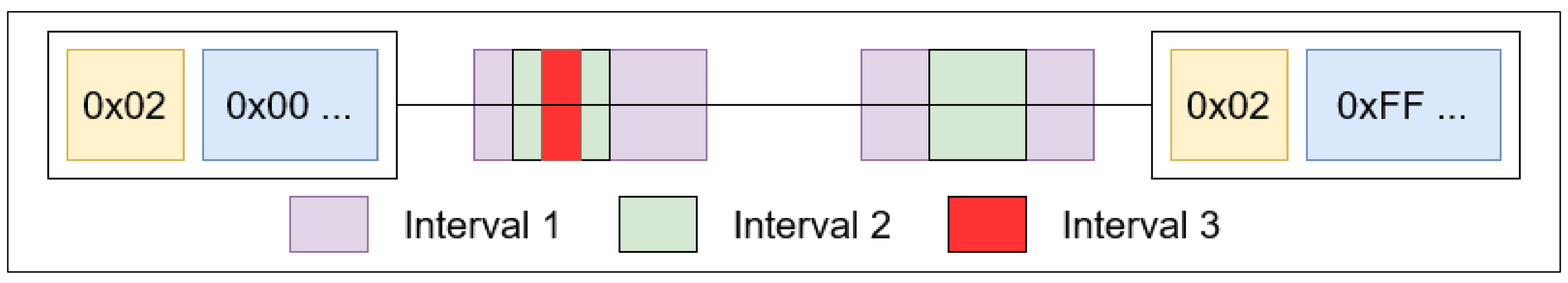
Data transmission with RSA-PKCS

RSA Modulus (bits)	RSA Modulus (bytes)	Max(Len(input message)) (bytes)
2048	256	**245**
4096	512	**501**

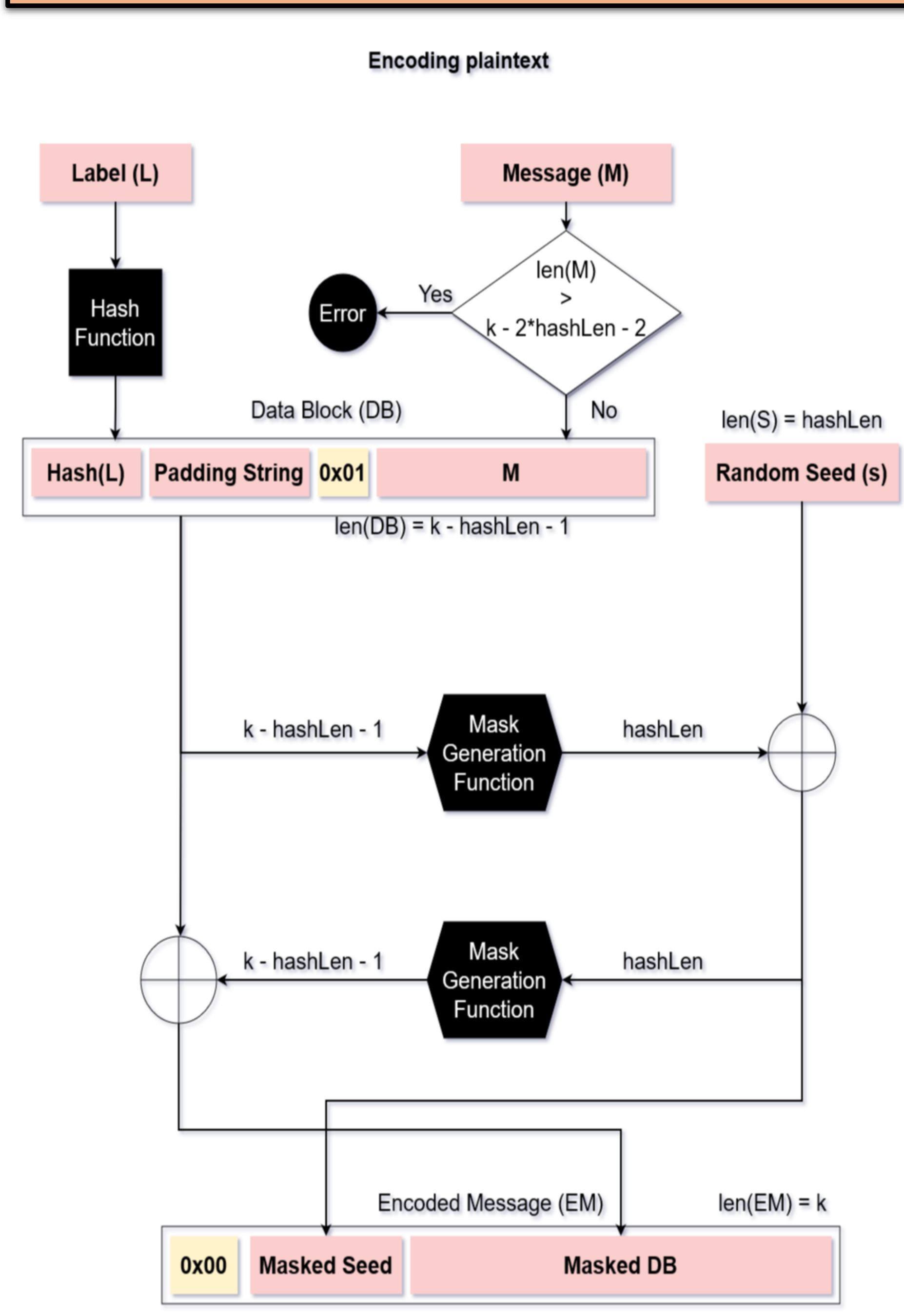
- At maximum message length, number of variable padding bytes = 8
- Each padding byte is non-zero. Hence there are 255 possible characters.
- Thus, number of ciphertext for one plaintext approximately 2^{64}.

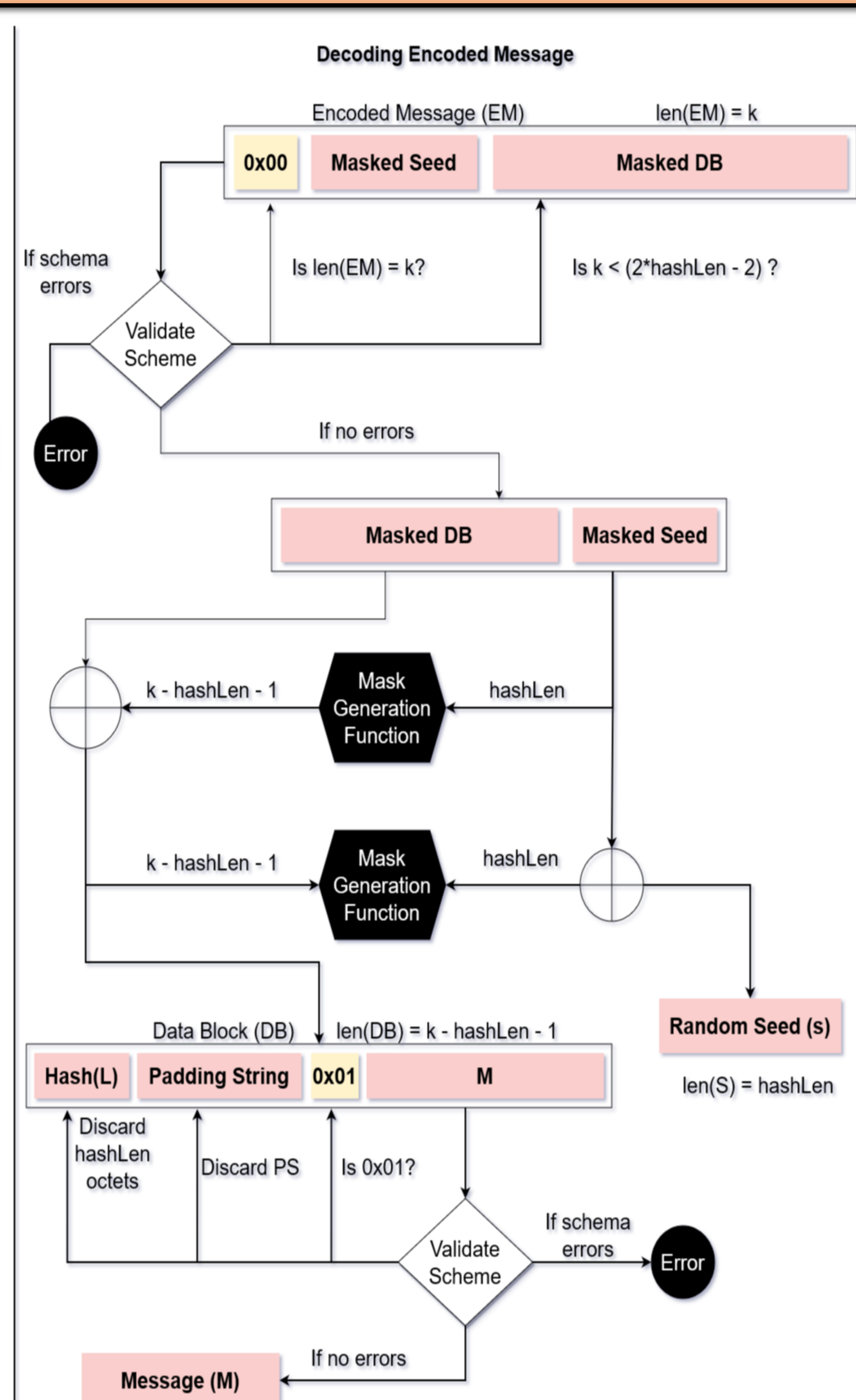
Bleichenbacher's Attack

- This attack exploits the fact that PKCS starts with 0x00 0x02. The attacker must have access to an oracle which confirms if ciphertext is PKCS compliant.
- In the real-world, these oracles could be RSA-PKCS decryption APIs with verbose error messages. Thus, PKCS should not be employed.



Optimal Asymmetric Encryption Padding (OAEP)





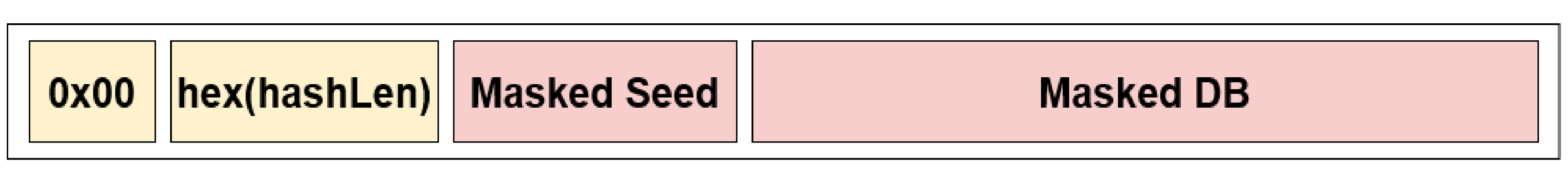
Data transmission with RSA-OAEP

RSA Modulus (bits)	RSA Modulus (bytes)	Max(Len(input message)) (bytes)			
		SHA3-224	SHA3-256	SHA3-384	SHA3-512
2048	256	**198**	**190**	**158**	**126**
4096	512	**454**	**446**	**414**	**382**

- At maximum message length, the only random component is the randomly generated seed value.
- The seed value (s) is randomly generated such that len(s) = hashLen.
- Thus, number of ciphertext for one plaintext = 2^n, where n = output len of hash function.

SHAKE128/256 with OAEP

- Replace Mask Generation Function with SHAKE128/256.
- Randomly generate hashLen for OAEP as:
  - For SHAKE128: $8 \le$ hashLen ≤ 32
  - For SHAKE256: $32 \le$ hashLen ≤ 64
- While encryption, generate encoded message as shown below. hex(hashLen) is encoded to help with decryption.



REFERENCES

- M. J. Dworkin et al., "SHA-3 standard: Permutation-based hash and extendable-output functions," 2015.
- C. F. Kerry and C. R. Director, "FIPS PUB 186-4 Federal Information Processing Standards publication Digital Signature Standard (DSS)," 2013.
- K. Moriarty, B. Kaliski, J. Jonsson, and A. Rusch, "PKCS# 1: RSA Cryptography Specifications Version 2.2," Internet Engineering Task Force, vol. 8017, p. 72, 2016.