PADDING SCHEMES FOR RSA AND THEIR SECURITY

CALVIN RYAN D'SOUZA

ADVISOR:- PROF. STANISŁAW RADZISZOWSKI

03/15/2022

REVIEW OF PROJECT GOALS

- Rivest-Shamir-Adleman (RSA) encryption scheme is deterministic i.e., It has no random component. This makes RSA susceptible to chosen plaintext attacks. Padding schemes help solve this problem by making RSA probabilistic in nature.

- Padding Schemes currently used with RSA:

Padding Scheme	Used since
Public-Key Cryptography Standards #1 v1.5 (PKCS #1 v1.5)	March 1998
Optimal Asymmetric Encryption Padding (OAEP)	October 1998

- Analyze computational costs and security of using padding schemes with RSA.

MILESTONE 1 PROGRESS

- Review literature on RSA and Padding Schemes.

- Generate parameters for RSA:
  - Generating primes/safe primes to calculate RSA modulus.
  - Bit lengths for primes generated are 512, 647, 813, 1024 and 2048.
  - RSA modulus length is twice the length of primes generated.
  - Public key exponent (e) was chosen as 65537.

- Implement RSA Cryptosystem.

MILESTONE 2 GOALS

- Review literature on Padding Schemes for RSA:
  - Federal Information Processing Standards (FIPS) 186-4, July 2013.
  - FIPS 186-5 (Draft), October 2019.
  - RSA Cryptography Specifications v2.2, November 2016.

- Implement following Padding Schemes for RSA:
  - Public-Key Cryptography Standard (PKCS) #1 v1.5
  - Optimal Asymmetric Encryption Padding (OAEP)
  - Optimal Asymmetric Encryption Padding (OAEP) with SHAKE128/256

PREREQUISITES

OCTET/BYTE STRINGS

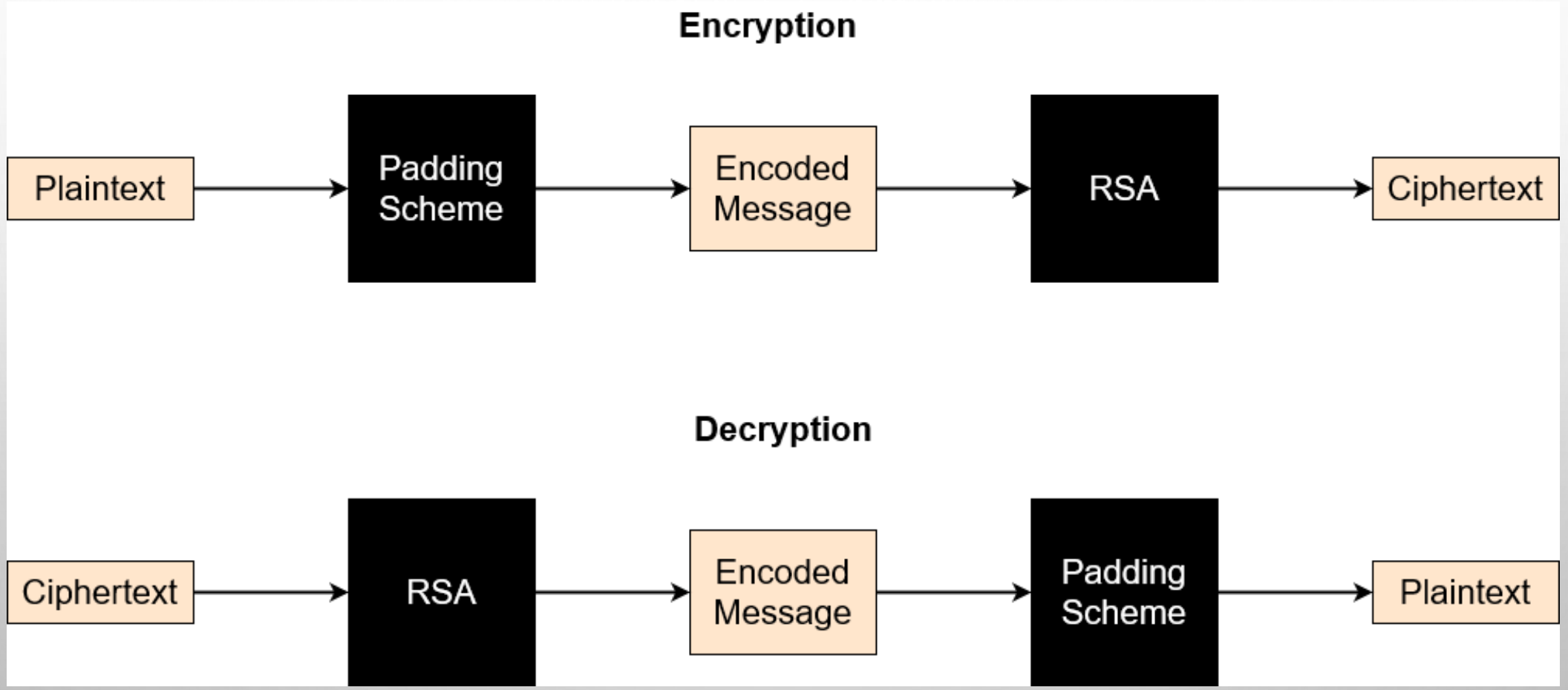
- An Octet string is the base 256 representation of a decimal integer in hexadecimal format.

- Messages supplied to encoding and decoding functions of padding schemes are always octet strings.

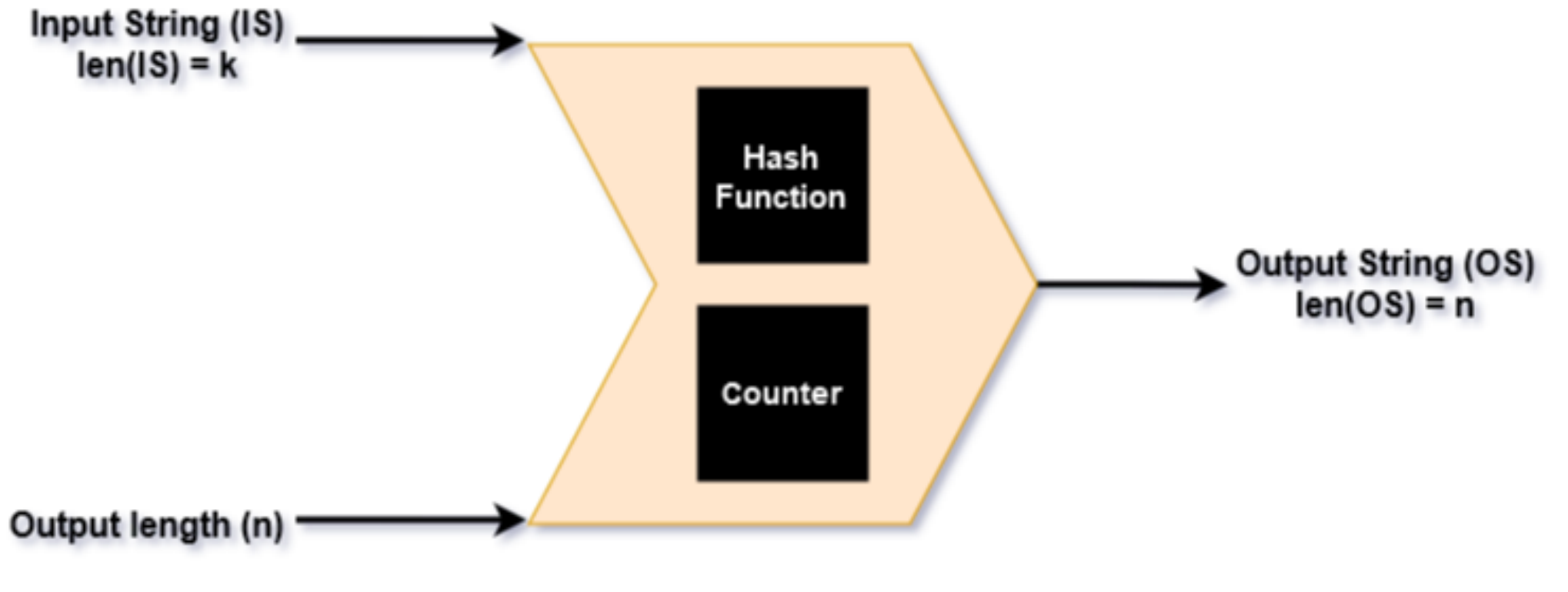
- Examples:

Decimal	Binary	Octet
255	11111111	FF
256	00000001 00000000	01:00
65535	11111111 11111111	FF:FF

ENCRYPTION AND DECRYPTION WITH RSA USING A PADDING SCHEME

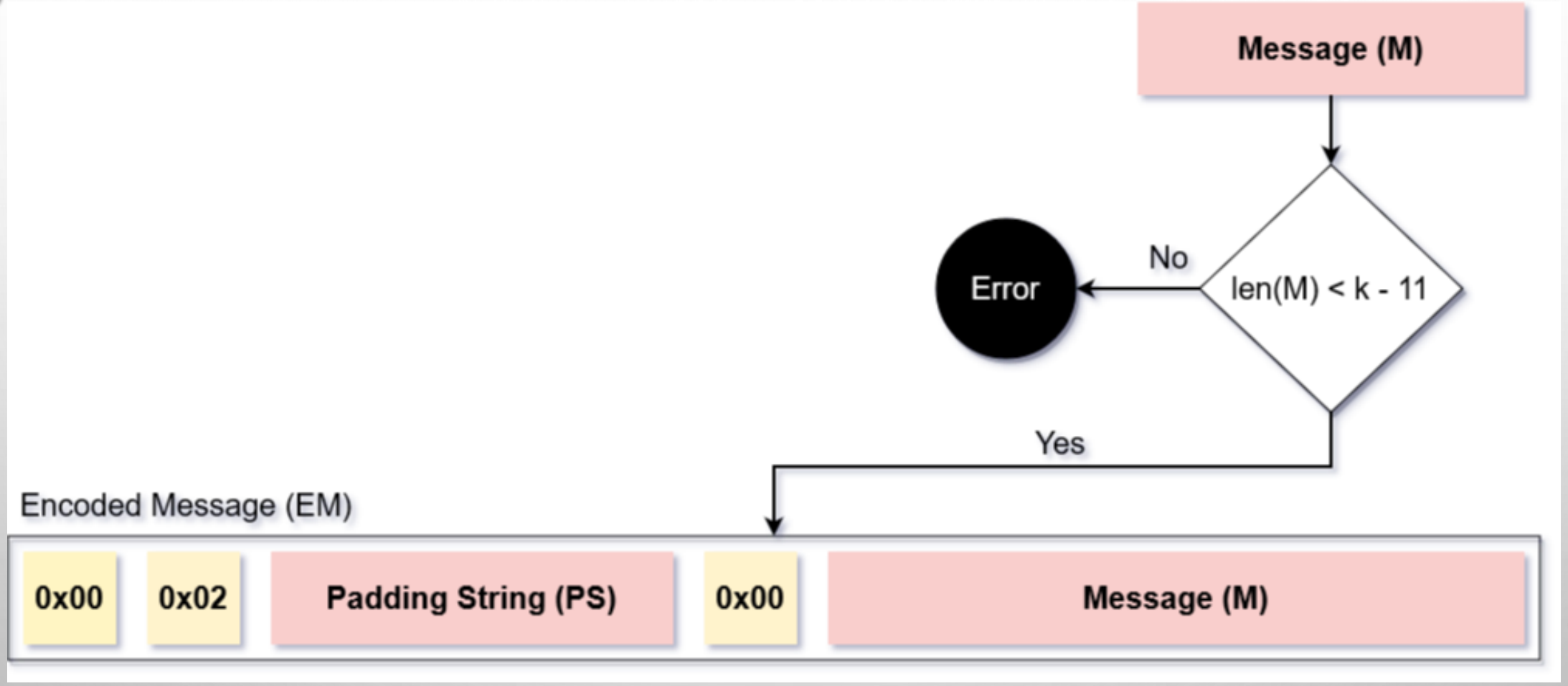


MASK GENERATION FUNCTION (MGF)

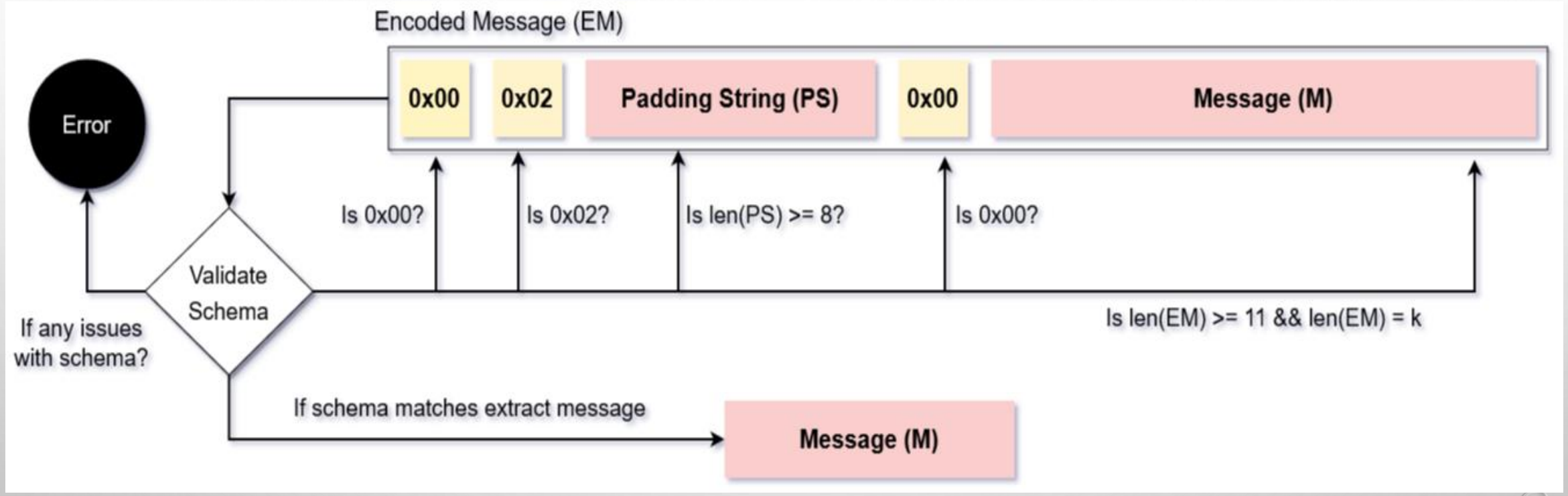


PUBLIC-KEY CRYPTOGRAPHY STANDARD #1 v1.5 (PKCS#1 v1.5)

ENCODING SCHEMATIC



DECODING SCHEMATIC



OPTIMAL ASYMMETRIC ENCRYPTION PADDING (OAEP)

ENCODING AND DECODING SCHEMATIC

QUESTIONS ?

THANK YOU