PADDING SCHEMES FOR RSA AND THEIR SECURITY

CALVIN RYAN D'SOUZA

ADVISOR:- PROF. STANISŁAW RADZISZOWSKI

03/31/2022

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.

PROGRESS SO FAR…

- Review literature on RSA and Padding Schemes.
- Implement parameter selection algorithm for RSA.
- Implement RSA Cryptosystem.
- Implement following Padding Schemes for RSA:
  - Public-Key Cryptography Standard (PKCS) #1 v1.5
  - Optimal Asymmetric Encryption Padding (OAEP)

MILESTONE 3

MESSAGE LENGTH-BASED ANALYSIS - PKCS

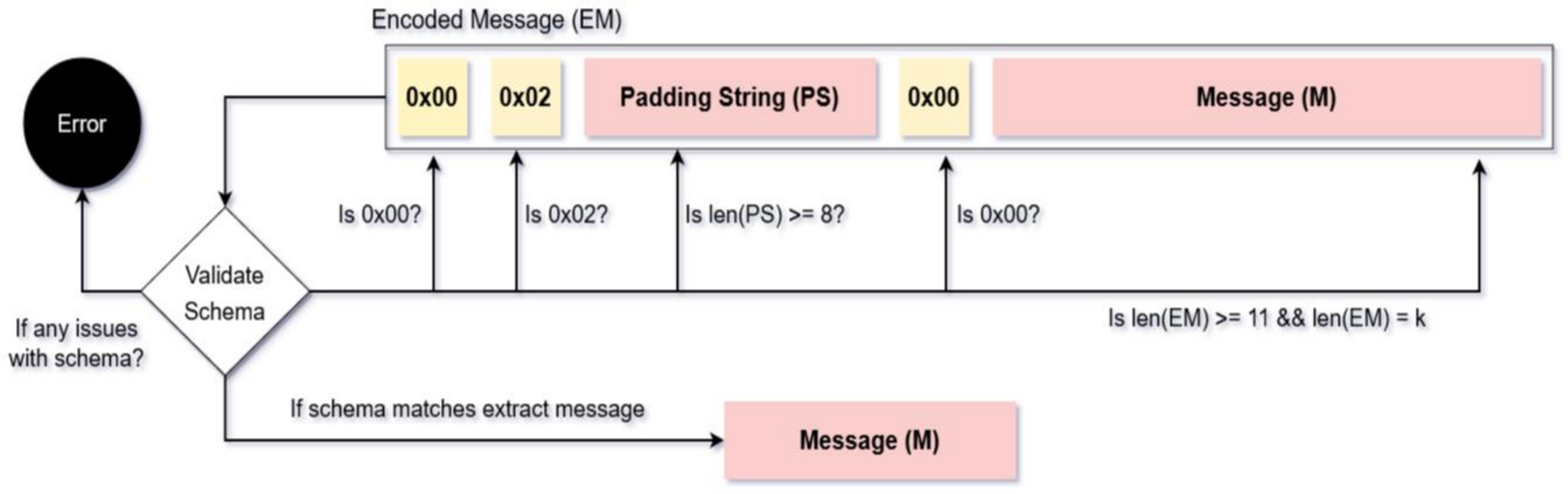
RSA Modulus (bits)	RSA Modulus (bytes)	Max(Len(input message)) in bytes	Permutations
1024	128	117	2^{56}
1294	161	150	
1536	192	181	
1626	203	192	
2048	256	245	
4096	512	501	

MESSAGE LENGTH-BASED ANALYSIS - OAEP

RSA Modulus (bits)	RSA Modulus (bytes)	Max(Len(input message)) in bytes				Permutations
		SHA3-224	SHA3-256	SHA3-384	SHA3-512	SHA3-n
1024	128	70	62	30	NA	2^n
1294	161	103	95	63	31	
1536	192	134	126	94	62	
1626	203	145	137	105	73	
2048	256	198	190	158	126	
4096	512	454	446	414	382	

SECURITY OF PKCS#1 V1.5 AGAINST BLEICHENBACHER'S ATTACK

DECODING SCHEMATIC



OAEP WITH SHAKE128/256

QUESTIONS ?

THANK YOU