Padding Schemes for RSA and their Security

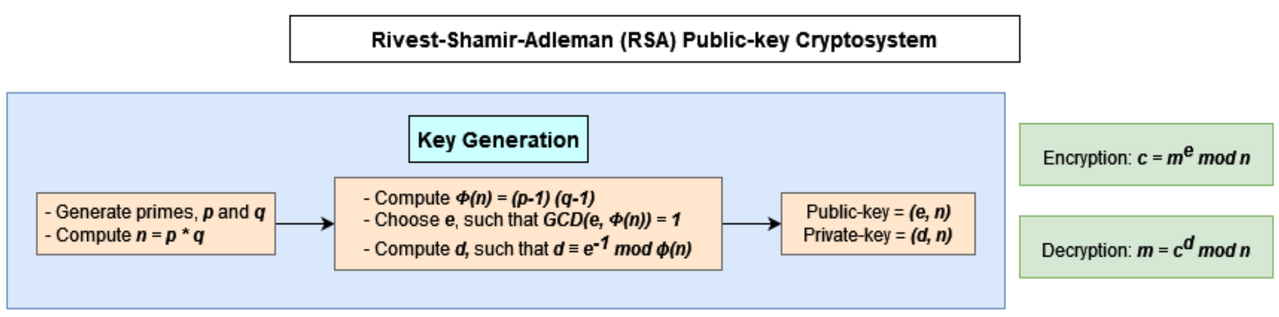
Calvin Ryan Dsouza (cd5184@rit.edu)

Advisor: Stanisław P. Radziszowski

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

INTRODUCTION

- Security is an important aspect of data transmission in today's digital world. Digital signatures are widely used on the internet for verifying websites along with encryption schemes for secure data transmission.
- 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.

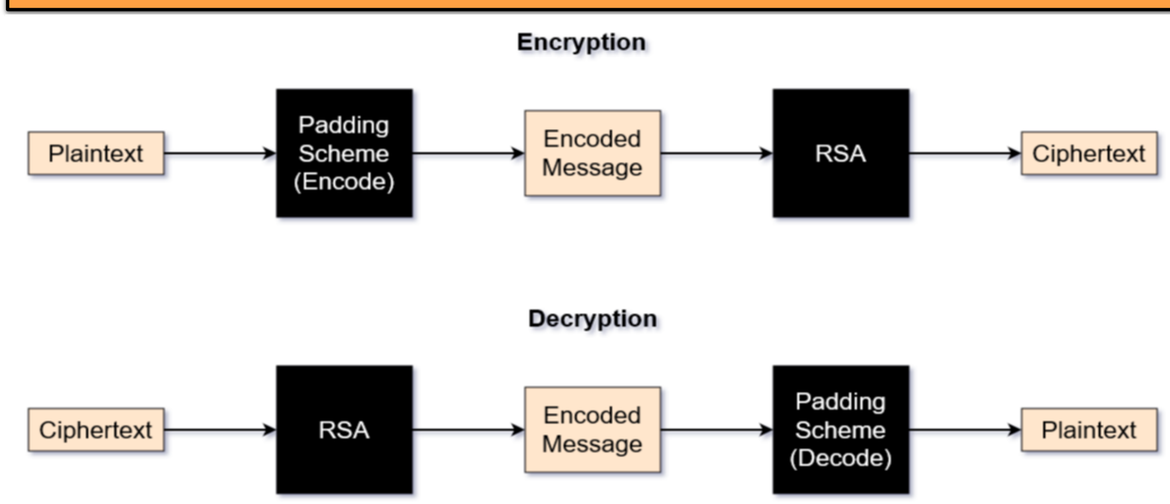


- In the real-world, RSA is implemented with 2048/4096-bit integers. Thus, RSA is computationally expensive and commonly only used for key transmission/ digital signatures.
- RSA is a deterministic cryptosystem, which makes it susceptible chosen-plaintext attacks. To mitigate this RSA is almost always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

GENERATING PRIMES FOR RSA

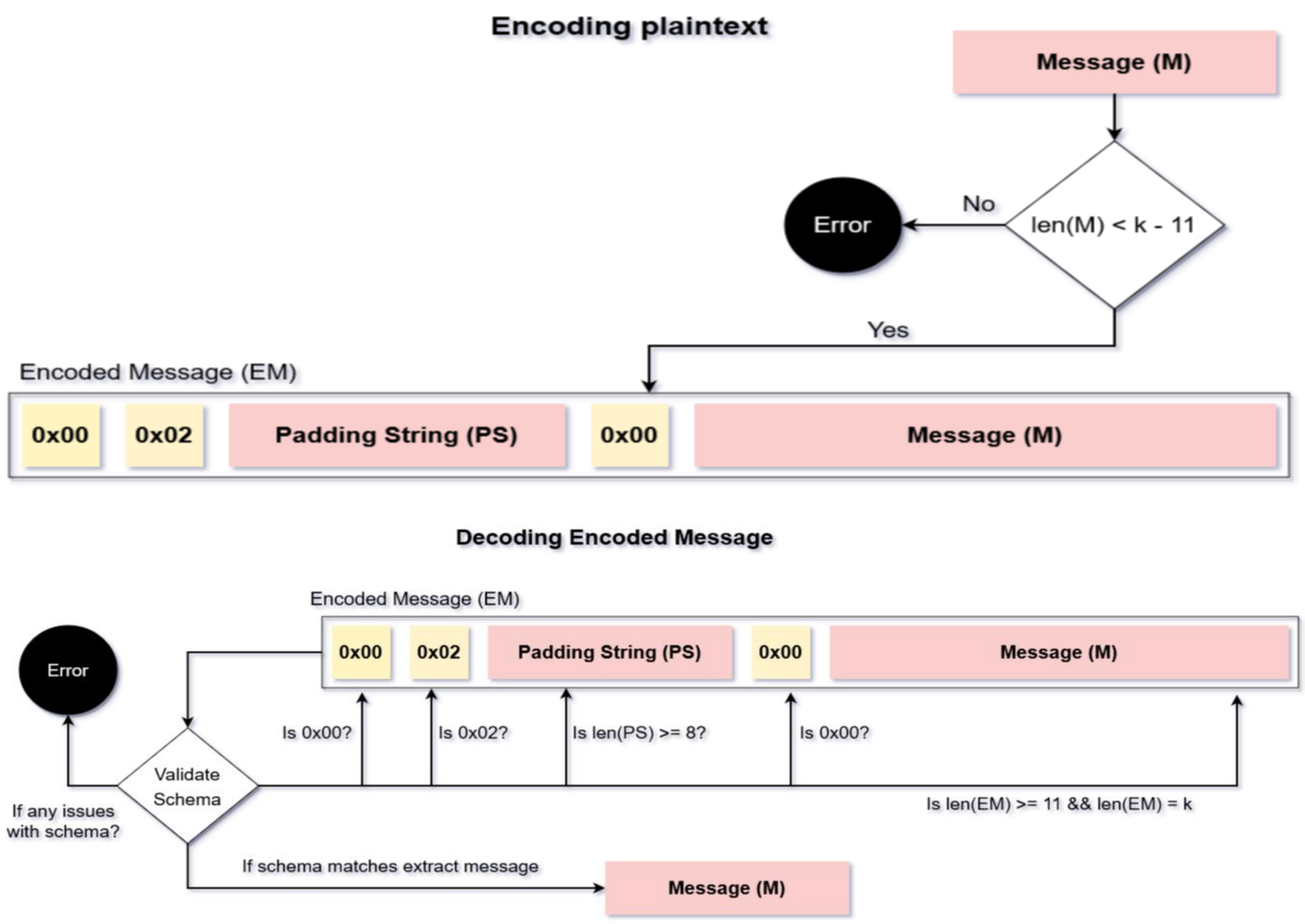
- For a prime number p if p-1 has many small factors, it is possible to find p given p-1 using **Pollard's *p-1* Algorithm**. This introduces the concept of Safe primes. For a prime p, if p-1 can be expressed as 2 * prime, then p is called a Safe prime.
- Prime numbers for RSA are generated using cryptographically 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



ANALYSIS AND RESULTS FOR PADDING SCHEMES

PUBLIC KEY CRYPTOGRAPHY STANDARDS #1 v1.5 (PKCS#1 v1.5)



ANALYSIS AND RESULTS

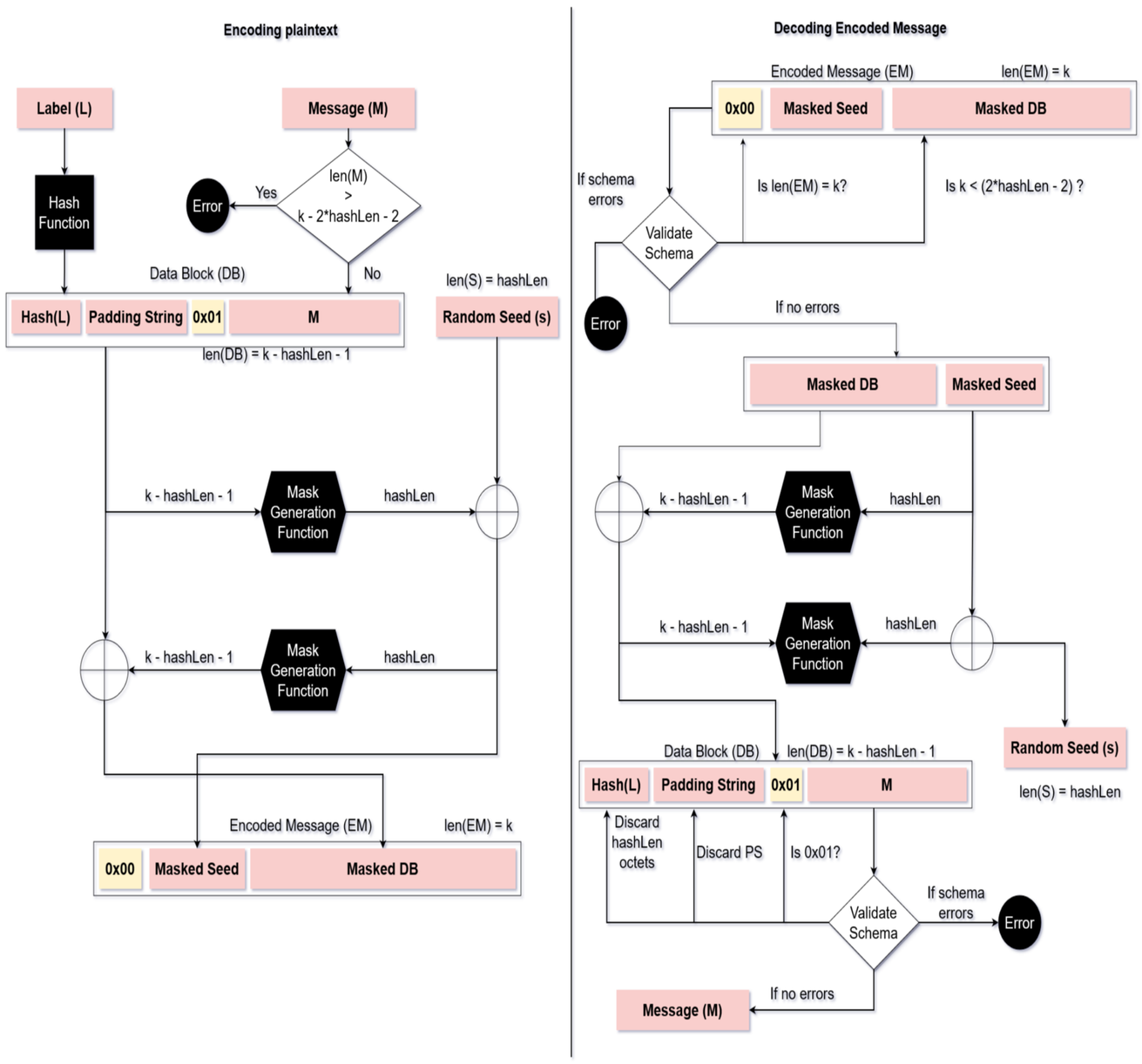
Security when used for Key transmission:-

Security when used for Digital signature:-

Security when used for data transmission:-

Comments on Bleichenbacher's attack

OPTIMAL ASYMMETRIC PADDING ENCRYPTION (OAEP)



ANALYSIS AND RESULTS

Security when used for Key transmission:-

Security when used for Digital signature:-

Security when used for data transmission:-

Integration of SHAKE128/256 with OAEP