Padding Schemes for RSA and their Security

Calvin Ryan D’Souza
Department of Computer Science
Golisano College of Computing and Information Sciences
Rochester Institute of Technology
Rochester, NY 14586
cd5184@cs.rit.edu

***Abstract*— What is RSA? Why padding schemes? Paddings schemes and prime number details**

I. Introduction

Digital signatures are widely used on the internet for verifying the identity of websites. The Rivest-Shamir-Adleman encryption scheme commonly known as RSA is one of the main algorithms used for implementing digital signatures. RSA is based on the factorization problem. The security of RSA is based on the fact that the product of 2 large prime numbers is extremely difficult to factor. RSA is computationally expensive since it is implemented with 2048/4096-bit numbers. The primitive versions of RSA as mentioned in [1] are usually referred to as textbook implementations.

Textbook RSA is a deterministic cryptosystem (i.e., has no random component) which makes it susceptible to chosen-plaintext attacks. This means it is not semantically secure. Thus, in real-world scenarios, RSA is almost always implemented with a padding scheme. Padding Schemes add a random component to RSA and makes it probabilistic in nature. Before actually encrypting the message, the message is padded with some random string. This forms an embedded string which is then sent for RSA encryption. Commonly used padding schemes with RSA are PKCS #1 v1.5 (RSAES-PKCS1-v1_5) and Optimal Asymmetric Encryption Padding (RSAES-OAEP) [1]. The paper implements these schemes in accordance with [2] for experimental purposes.

Prime numbers generated are categorized as basic primes and safe primes for each RSAES padding scheme. These are generated using random number/bit generators and primality tests as mentioned in [2]. Safe primes are generated since prime numbers can often be factorized using Pollard’s p-1 algorithm [4]. This does not usually occur in case of prime numbers generated for cryptographic purposes. But if it does occur, it will be detrimental to the RSAES implementations even though a padding scheme is employed. The paper provides insight into implementing RSA with safe primes versus basic primes and the computational complexities related to them.

RSAES-PKCS1-v1_5 has been broken as demonstrated in [5]. However, it is still recommended as usable by FIPS 186-4 [2] and FIPS 186-5 [3]. This paper tests the feasibility of this attack in practical scenarios and discusses the security of RSAES-PKCS1-v1_5. The paper also provides results on how RSAES-OAEP may reduce message length for RSA signatures, thus increasing computational costs since a higher bit RSA implementation is required. SHA-3 is recommended as a Mask generation function in [4]. The paper also shows experiments with SHA-3 used as a mask generation function instead of older version of SHA. The results show how SHA-3/SHAKE can be used a standalone mask generation function versus current implementations described in [1]. Moreover, the paper looks at OAEP+ [6] and other padding scheme modification literature and contrasts them with RSAES-OAEP and RSA-PKCS1-v1_5.

II. Prerequisites & Prior Work

A. *Textbook RSA*

Template text

B. *Safe Primes Vs Basic Primes*

Template text

C. *Prior Work*

Information on prior work. Need to include references.

III. Padding Schemes

Introductory text

A. *PKCS #1 v1.5*

Introductory text and information along with image

B. *Optimal Assymmetric Encryption Padding (OAEP)*

Introductory text and information along with image

C. *Experiments with message length*

Experiment information (maybe include a graph)

IV. Bliechenbacher attack

Information on the attack. These things were done:

A. *Attack implementation in experimental scenario*

Some text information along with table.

B. *Attack implementation in Practical Scenario*

Some text information along with table.

Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors*).

V. SHA-3/SHAKE IMPLEMNTATION WITH OAEP

Some introductory text.

A. *Advantages of SHA-3 over earlier versions*

Some text Information and images

B. *Implementation details and length-based scenarios*

Highlight some details of implementation and tests

VI. SOME MORE PADDING SCHEMES

A. *OAEP+*

Information and some test info.

B. *Padding Scheme XYZ*

Information and some test info.

VII. RESULTS

Results broken down as per experiments and tests. Not defined currently, thus no sections created.

VIII. CONCLUSION

Cumulative conclusion based on research and experiments.

REFERENCES

[1] PKCS #1: RSA Cryptography Specifications Version 2.2, November 2016.

[2] FIPS PUB 186-4, Digital Signature Standard, July 2013.

[3] FIPS PUB 186-5 (Draft), Digital Signature Standard, October 2019.

[4] https://www.cs.purdue.edu/homes/ssw/cs355/2009f.pdf.

[5] Bleichenbacher, D., "Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1", Lecture Notes in Computer Science, Volume 1462, pp. 1-12, 1998.

[6] Victor Shoup, OAEP Reconsidered, IBM Zurich Research Lab. September 18, 2001.