The RSA Encryption Algorithm

John Paul S. Guzman

Mathematics Department, De La Salle University, 2401 Taft Ave., Manila 0922, Philippines

Abstract

Encryption is the process of scrambling information in such a way that it can only be read by select individuals. It is an essential tool as we rely on the internet in our activities such as online banking, transactions, and private messaging. In these activities, we are often required to communicate sensitive information like passwords, credit card information, social security number, and home addresses. Encryption prevents unwanted individuals from having access to these types of information.

Keywords: Cryptography, Internet security, Prime numbers.

1 Introduction

The RSA encryption algorithm is a widely used encryption algorithm that secures sensitive data from "man-in-the-middle" attacks wherein malicious third-party eavesdrops on the communication between two parties with the intent of stealing sensitive information [1]. It is one of the earliest implementations of public-key or asymmetric encryption which allows users to establish a private communication over a public channel [5].

// It does this by having separate keys to do: discuss one way? trap doors?? security of factoring algos???

Another key feature of RSA is the ability to create electronic signatures. Similar to a physical signature, an electronic signature provides a way to prove that a message originated from the sender [5]. It also provides the means to show that the message was not tampered with.

RSA uses Euler's theorem to: (a) scramble or encrypt a message into ciphertext, (b) unscramble or decrypt ciphertext back to the original message, (c) generate electronic signatures.

2 Cryptographic System

In order to create the public key and private key, we first need to choose two large distinct prime numbers p and q at random, and let n be the product of the two. Then, pick a large random integer d such that it is relatively prime to $\phi(n)$ where ϕ is the Euler totient function. Finally, we choose e to be the multiplicative inverse of d modulo $\phi(n)$.

$$ed \equiv 1 \mod \phi(n)$$

We know that such an e is exists since $gcd(d, \phi(n)) = 1$. The pair (e, n) will serve as the public key, while the pair (d, n) will serve as the private key. Although n is publicly shared, its factors p and q are kept private.

Let M be a plaintext message encoded as a number. We insist that $M < n$. In the case where $M \geq n$, then we split M into multiple chunks and send them separately. Furthermore, we insist that M is relatively prime to n. In practice, this is a safe assumption since it is unlikely that M is a multiple of p or q. Regardless, we could easily check for this case since we have access to p and q, then we can simply split M further or add some padding until it is relatively prime to n.

We can generate the ciphertext C by raising M to eth power then taking modulo n. Then, we can decipher C to the plaintext D by raising C to the dth power then taking modulo n. Lastly, we can create the electronic signature S by raising M to the dth power then taking modulo n.

$$C \equiv M^e \mod n$$
$$D \equiv C^d \mod n$$
$$S \equiv M^d \mod n$$

To illustrate the correctness of these of operations, we first need to discuss some results in number theory.

Theorem 2.1. If $a \equiv b \mod n$, then $ca \equiv cb \mod n$ and $a^k \equiv b^k \mod n$ for any positive integer k.

Theorem 2.2. If a and b are relatively prime with $a \mid c$ and $b \mid c$, then $ab \mid c$.

Corollary 2.3. If m and n are relatively prime with $a \equiv b \mod m$ and $a \equiv b \mod n$, then $a \equiv b \mod mn$.

Theorem 2.4. If p is prime, then $\phi(p) = p - 1$.

Theorem 2.5. If a and b are relatively prime, then $\phi(ab) = \phi(a)\phi(b)$.

Theorem 2.6 (Euler, 1763). If a is relatively prime to b, then $a^{\phi(b)} \equiv 1 \mod b$.

We can apply these to our scenario and make several observations.

By our choice of e and d, we have $ed = k\phi(n)+1$ for some integer k.

Since p and q are distinct primes, $\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$.

Since M and p are relatively prime, $M^{\phi(p)} \equiv M^{p-1} \equiv 1 \mod p$.

We have $M^{k\phi(n)} \equiv (M^{p-1})^{k(q-1)} \equiv 1^{k(q-1)} \equiv 1 \mod p$.

Thus, $M^{ed} \equiv M^{k\phi(n)+1} \equiv M(1) \equiv M \mod p$.

Similarly for q, $M^{ed} \equiv M^{k\phi(n)+1} \equiv M(1) \equiv M \mod q$.

Hence, $M^{ed} \equiv M \mod pq$ equivalently, $M^{ed} \equiv M \mod n$.

We have shown that the deciphered plaintext matches the original message. $D \equiv C^d \equiv (M^e)^d \equiv M^{ed} \equiv M \mod n$.

Now suppose that Alice wants to send a message M to Bob. Alice would take Bob's public key (e_B, n_B) and use it to create the ciphertext $C \equiv M^{e_B} \mod n_B$. When Bob receives C, he can then decrypt it to retrieve the original message $M \equiv D \equiv C^{d_B} \mod n_B$.

Now suppose Eve who is an eavesdropper. She obtains a copy to C

TODO: signatures

How to solve for d with public data?

3 2Introduction

222456 Papers for ICPRS-2021 need to be submitted for review by the **15 November 2020**. The submission should be the format described here and should be **anonymous**. If your paper is accepted, a final camera-ready non-anonymous version should be submitted, using the same electronic submission system, no later than the **29 January 2021**. Papers received after that date will not be included in the Proceedings. Your final version should be prepared taking into account the comments made by the reviewers and available to authors via the submission system. The Proceedings produced for ICPRS-2021 will contain **all** the papers accepted **and presented** in the conference.

4 2Manuscript preparation

Full papers must be typed in English. This instruction page is an example of the format and font sizes to be used. MS Word users can download from the conference site these instructions in Word format. LaTeX is preferred as it is easier to change paper style and formatting.

These are detailed instructions valid for any word processor. In the title of the paper the initial letters should be capitalised in all words except articles and prepositions (e.g.: in, a, an, and, the, there, their, do, on, of, from, with, at etc.). E.g. "ErDoped Si Nanocrystals as a Candidate for Optical Amplification" The type should be boldface 18pt and centred on the page. The authors' names (in the final non-anonymous version) are typed in capital and lower case bold letters and centred on the page. Directly under the authors' names in capital and lower case letters and also centred are the authors' affiliation(s), address(es), plus email address(es) of (at least) the corresponding author. Manuscripts must be typed single spaced using 10 point characters. Only Times, Times Roman, Times New Roman and Symbol fonts are accepted. The text must fall within a frame of 18 cm x 24 cm centred on an A4 page (21 cm x 29.7 cm).Paragraphs are separated by 6 points and with no indentation. The text of the full papers is written in two columns and justified. Each column has a width of 8.8 cm and the columns are separated by a margin of 0.4 cm. The maximum length of the full paper is 6 pages (min 4 pages). **Do not number the pages and avoid the use of footnotes**. The final format in which the papers will appear on the Proceedings will be a PDF file. Authors are required to upload a **PDF** file of their final paper to be included directly in the Proceedings. **All PDF files should NOT be locked and all fonts and graphics should be embedded**.

4.1 2Figures and tables

Figures and tables should be centred in the column, numbered consecutively throughout the text, and each should have a caption underneath it (see for example Table 1). Care should be taken that the lettering is not too small. All figures and tables should be included in the electronic versions of the full paper. We cannot guarantee that any printed version of the proceedings will use colour.

Figure 1. This is an example of a figure caption.

nn!1
2
31
6

Table 1. This is an example of a table caption.

4.2 2Equations

Equations should be typed within the text, centred, and should be numbered consecutively throughout the text. They should be referred to in the text as Equation (n). Their numbers should be typed in parentheses, flush right, as in the following example.

$$PA + A'P - PBR^{-1}B'P + Q = 0 \ . \qquad (1)$$

5 Generating a PDF file

The PDF format will be the final format under which the papers will appear in the Proceedings. Therefore you are required to submit your paper as a PDF document. If this is not possible, Postscript format is also accepted as long as no fonts other than the recommended fonts are used.

You can use any of the popular free LaTeX editors (e.g. Kile, TexMaker, etc).

6 2Electronic submission of the full paper

The submission process for ICPRS 2021 should be done on line at http://www.icprs.org

A PDF version of your final paper is required. It should be expected that after your submission, your paper is published directly from the file you send without any further proofreading.

Therefore, it is advisable for the authors to print a hard copy of their final version and read it carefully.

Note that the publisher reserves the right not to publish a paper that is deemed to be poorly formatted or with poor use of English.

7 2Your References

The list of references should be ordered in the same order as first cited in the text. All references should be cited in the text, and using square brackets such as [1] and [1, 2]. We recommend the use of IEEE Transactions style for references. *Avoid any references that could identify any of the authors, e.g. avoid "as we showed in ..."*

2Acknowledgements

The acknowledgement for funding organisations etc. should be placed in a separate section at the end of the text.

Thank you for your cooperation in complying with these instructions.

References

[1] A. B. Author and C. D. Author, "Title of the Article," *The Journal*, 2006.

[2] E. Author and F. Author, "Title of the Paper," in *International Conference on Something*, (Place (Country)), 2007.