

# RSA ENCRYPTION AND DIFFIE HELLMAN KEY EXCHANGE

MIRA SCARVALONE

ABSTRACT. This paper is an introductory explanation of two algorithms from cryptography, RSA and the Diffie Hellman Key Exchange. The preliminary sections discuss necessary background in number theory to understand the algorithms, while later sections provide explanations of how the algorithms work mathematically.

## CONTENTS

1. Introduction	1
2. Preliminary Number Theory	2
3. RSA Algorithm	3
4. Digital Signatures	4
5. Diffie Hellman Key Exchange	4
Acknowledgments	5
References	5

## 1. INTRODUCTION

The science of cryptography seeks to find methods of encoding and decoding messages so that they can be securely transmitted between parties. Typically, encryption uses a key to read encrypted messages, and the more difficult it is to find and break this key, the more secure the encryption is. Early methods of cryptography involved an initial secure exchange of secret keys known only by the involved parties. However, several breakthroughs in the 1970's introduced public-key cryptography, whereby an initial secure exchange is not involved and users are able to communicate over a public channel without agreeing on a secret key beforehand. One of these prominent breakthroughs, RSA, is a widely used algorithm for public-key cryptography that utilizes basic principles of number theory. RSA was first publicly described in 1978 by Ron Rivest, Adi Shamir, and Leonard Adelman at MIT, all three of whom the algorithm is named after.

The theory behind RSA stems from the attempt to create a cryptography scheme that is easy to encrypt but difficult to decrypt or break by someone not intended to receive the message. The RSA algorithm is an example of a “trapdoor function,” an operation that is easy to do but hard to undo without additional information. RSA utilizes the fact that multiplying very large numbers is much easier than factoring them. There are few known ways to factor a  $2n$ -digit number other than trying to

---

*Date:* July 17, 2009.

divide it by all  $10^n$  numbers of  $\leq n$  digits, and even with a computer, these kinds of factorizations cannot be done quickly, especially as  $n$  gets larger. Thus, the security of RSA rests on the premise that factorization of large numbers is difficult.

The Diffie Hellman Key Exchange involves simple calculations between two parties to determine secret private keys based on publicly known parameters. The algorithm utilizes the fact that given two powers of a given number (mod  $n$ ), it is difficult to determine those exponents themselves without further information.

Section 2 of this paper will explore the components of number theory that led to the creation of RSA, Section 3 describes the algorithm itself, Section 4 discusses digital signatures, and Section 5 explains the Diffie Hellman Key Exchange.

## 2. PRELIMINARY NUMBER THEORY

The theory behind RSA utilizes many important principles of number theory. Primarily, RSA involves several characteristics of the ring  $\mathbb{Z}/n\mathbb{Z}$ , which we will prove in this section to provide a background of how RSA works. We begin by discussing the Euclidean Algorithm, which along with characteristics of prime numbers, prominently influences the theory behind RSA.

As a consequence of the Euclidean Algorithm, for any two integers  $a$  and  $b$  with  $\gcd(a, b) = d$ , there exist integers  $m$  and  $n$  such that  $d = ma + nb$

**Definition 2.1.**  $(\mathbb{Z}/n\mathbb{Z})^\times = \{r \in \mathbb{Z}/n\mathbb{Z} \mid \exists s \text{ such that } rs = 1\}$

**Definition 2.2.** The Euler Function,  $\varphi(n)$ , assigns to  $n$  the number of integers between 1 and  $n$  that are relatively prime to  $n$ .

**Proposition 2.3.** *The integers that are relatively prime to  $n$  are those that have inverses in the ring  $\mathbb{Z}/n\mathbb{Z}$ .*

*Proof.* Suppose  $r$  and  $n$  are relatively prime. Then by the Euclidean Algorithm,  $\gcd(r, n) = 1 = mr + kn$  for some integers  $k$  and  $m$ . Thus,  $mr = 1 \pmod{n}$ , so  $m$  is an inverse of  $r \pmod{n}$ . Now conversely, suppose  $r$  has an inverse  $m \pmod{n}$ , then  $mr = 1 \pmod{n}$ , so  $mr + kn = 1$  for some  $k$ . Suppose an integer  $p$  divides  $r$  and  $n$ , then it also must divide  $mr + kn = 1$ , so therefore  $p = 1$ , and  $r$  and  $n$  must be relatively prime.  $\square$

Therefore, it follows that  $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

**Theorem 2.4** (Fermat's Little Theorem). *If  $p$  is a prime integer, and  $p$  does not divide  $a$ , then  $a^{p-1} \equiv 1 \pmod{p}$ .*

*Proof.*  $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$  since all integers less than  $p$  are relatively prime to  $p$ . We know that  $a \in G$  because  $a$  and  $p$  are relatively prime, so  $a$  must have an inverse in  $\mathbb{Z}/p\mathbb{Z}$ . Let  $n$  be the smallest integer for which  $a^n \equiv 1 \pmod{p}$ . Therefore  $n$  is the order of  $a$ , so  $n = |H|$  where  $H$  is the subgroup generated by  $a$ . Therefore  $n$  divides  $p - 1$  by Lagrange's Theorem, since the order of a subgroup must divide the order of the group, so  $p - 1 = mn$  for some  $n$ . Therefore  $a^{p-1} \equiv a^{mn} \equiv (a^n)^m \equiv 1^m \equiv 1 \pmod{p}$ .  $\square$

**Theorem 2.5** (Euler's Theorem). *If  $a$  and  $n$  are relatively prime integers, then  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .*

*Proof.* Suppose  $a$  and  $n$  are relatively prime integers. Let  $G = (\mathbb{Z}/n\mathbb{Z})^\times$ . As shown above,  $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = |G|$ . We know that  $a \in G$  because  $a$  and  $n$  are relatively prime, so  $a$  must have an inverse in  $\mathbb{Z}/n\mathbb{Z}$ . Let  $H$  be the cyclic subgroup of  $G$  generated by  $a$ . The order of  $H$  equals  $|H| = h$  is also the order of  $a$ , and since  $h$  is finite, then  $h$  is the smallest positive integer such that  $a^h \equiv 1 \pmod{n}$ . By Lagrange's Theorem, since the order of a subgroup must divide the order of the group,  $h$  divides  $|G|$ , so  $h$  divides  $\varphi(n)$ , and  $\varphi(n) = hm$  for some integer  $m$ .

$$\text{Therefore } a^{\varphi(n)} = a^{hm} = (a^h)^m \equiv 1 \pmod{n}.$$

□

**Theorem 2.6** (Chinese Remainder Theorem). *If  $p$  and  $q$  are relatively prime, then for any integers  $a_1$  and  $a_2$  less than  $pq$ , there exists a unique integer  $x$  such that  $x \pmod{pq} \equiv a_1 \pmod{p} \equiv a_2 \pmod{q}$ .*

*Proof.* The value of  $a_1 \pmod{p}$  reflects the remainder when  $a_1$  is divided by  $p$ . The remainder as  $p$  divides any integer repeats itself every  $p$  steps. As we move through successive integer values of  $a_1$ , the value of  $a_1 \pmod{p}$  repeats every  $p$  values, and similarly the value of  $a_2 \pmod{q}$  repeats every  $q$  values. Therefore, no pair of remainders is repeated until after  $\text{lcm}(p, q)$  steps. Since  $p$  and  $q$  are relatively prime,  $\text{lcm}(p, q) = pq$ , and hence the first  $pq$  pairs of remainders are unique. Furthermore, all possible pairs of remainders have been included after  $pq$  steps because there are only  $pq$  possible pairs and they are unique. □

The Chinese Remainder Theorem also implies that  $x \equiv y \pmod{p} \equiv y \pmod{q}$  if and only if  $x \equiv y \pmod{pq}$ . This can be shown easily by demonstrating that if  $x \equiv y \pmod{p}$ , then  $p$  divides  $x - y$ , and if  $x \equiv y \pmod{q}$ , then  $q$  divides  $x - y$  as well. Since  $p$  and  $q$  are relatively prime, then  $pq$  divides  $x - y$ , so  $x \equiv y \pmod{pq}$ .

### 3. RSA ALGORITHM

Suppose Alice and Bob want to send private messages to each other that they can easily understand but others cannot. Alice creates a key based on two large prime numbers,  $p_1$  and  $p_2$ , as follows. First, she computes  $n = p_1 p_2$ , which can be safely revealed to the public without disclosing  $p_1$  and  $p_2$  themselves. Alice then computes  $\varphi(n) = \varphi(p_1 p_2)$

**Proposition 3.1.** *If  $p_1$  and  $p_2$  are prime,  $\varphi(p_1 p_2) = (p_1 - 1)(p_2 - 1)$*

*Proof.*  $\varphi(p_1 p_2)$  represents the number of integers less than  $p_1 p_2$  that are relatively prime to  $p_1 p_2$ . The only integers less than  $p_1 p_2$  that are not relatively prime to  $p_1 p_2$  are the  $(p_2 - 1)$  multiples of  $p_1$  and the  $(p_1 - 1)$  multiples of  $p_2$ . These  $p_1 + p_2 - 2$  numbers are distinct because  $p_1 p_2$  is the smallest integer that is a multiple of both  $p_1$  and  $p_2$  since they are each prime. Since  $\varphi(p_1 p_2)$  is equivalent to the number of integers that are not relatively prime to  $p_1 p_2$  subtracted from the total number of integers less than  $p_1 p_2$ ,  $\varphi(p_1 p_2) = p_1 p_2 - 1 - (p_1 + p_2 - 2) = p_1 p_2 - p_1 - p_2 + 1 = (p_1 - 1)(p_2 - 1)$  □

Next, Alice chooses an encryption exponent  $e$  such that  $e < \varphi(n)$  and  $e$  and  $\varphi(n)$  are relatively prime. She then determines the decryption exponent  $d$  which is the inverse of  $e \pmod{\varphi(n)}$ . The inverse can be easily computed by the Euclidean

Algorithm using  $e$  and  $\varphi(n)$ . It is important to note that the values  $e$  and  $n$  are made public so that anyone can send encrypted messages to Alice. The values of  $p_1$ ,  $p_2$ ,  $\varphi(n)$ , and  $d$  are kept private.

Suppose Bob wants to send a message to Alice. He must first convert his message to an integer  $m < n$  using a simple translation of letters into numerals. Bob then sends the message by raising  $m$  to the encryption exponent  $e$  and thus sending  $m^e \pmod n$  to Alice.

Alice then receives the encrypted message and raises it to the power of the decryption exponent  $d$ . She obtains  $(m^e)^d \equiv m^{ed} \pmod n$ .

Since  $e$  and  $d$  are inverses,  $ed = 1 \pmod{\varphi(n)} = 1 + k\varphi(n)$  so

$$m^{ed} = (m^{1+k\varphi(n)}) = m(m^{k\varphi(n)}) = m(m^{\varphi(n)})^k.$$

**Proposition 3.2.**  $m(m^{\varphi(n)})^k \equiv m \pmod n$

*Proof.* Suppose  $m$  and  $n$  are relatively prime. Then  $m^{\varphi(n)} \equiv 1 \pmod n$  by Euler's Theorem, and  $m(m^{\varphi(n)})^k \equiv m(1)^k \equiv m \pmod n$ .

Now suppose  $m$  and  $n$  are not relatively prime. If  $m$  is a multiple of  $n$ , then  $m \pmod n = 0 = m(m^{\varphi(n)})^k$ . If  $m$  is not a multiple of  $n$ , then either  $p_1$  or  $p_2$  must divide  $m$ , but not both. We know that  $\varphi(p_1p_2) = (p_1 - 1)(p_2 - 1)$  by Proposition 3.1, so  $m(m^{\varphi(n)})^k$  can be rewritten as  $m(m^{\varphi(n)})^k = m((m^{p_1-1})^{p_2-1})^k$ . Suppose  $p_2$  divides  $m$ , then  $p_1$  must not divide  $m$ . By Fermat's Little Theorem,  $m^{p_1-1} \equiv 1 \pmod{p_1}$ , so  $m(m^{\varphi(n)})^k \equiv m((1)^{p_2-1})^k \equiv m \pmod{p_1}$ . Since  $p_2$  divides  $m$ , then  $m \pmod{p_2} \equiv 0 \equiv m(m^{\varphi(n)})^k$ , and  $m(m^{\varphi(n)})^k \equiv m \pmod{p_1} \equiv m \pmod{p_2}$ . By the Chinese Remainder Theorem,  $m(m^{\varphi(n)})^k \equiv m \pmod{p_1p_2} \equiv m \pmod n$ . The same argument holds if  $p_1$  divides  $m$  and  $p_2$  does not.  $\square$

Therefore, the message that Alice has decrypted,  $m^{ed} \pmod n$ , is equivalent to  $m(m^{\varphi(n)})^k \equiv m \pmod n$ , so the original message that Bob sent is obtained through this process.

#### 4. DIGITAL SIGNATURES

If a user wants to demonstrate authenticity, he or she can use RSA to sign a message proving that the user is who he or she claims. This can be done by selecting a well known message  $m$  and sending  $m^d \pmod n$ , which a public user can decipher by raising it to the power  $e$ . The public user will obtain  $(m^d)^e \pmod n = m^{de} \pmod n = m \pmod n$  as before, and thus be able to verify the status of the sender. Since  $d$  is not publicly known, and only  $m^d \pmod n$  would produce the original  $m$  when raised to the  $e$ -th power, the user is authentic.

#### 5. DIFFIE HELLMAN KEY EXCHANGE

The Diffie Hellman key exchange is another breakthrough in public-key cryptography of the 1970's. Invented by Whitfield Diffie and Martin Hellman in their groundbreaking 1976 paper "New Directions in Cryptography," this key exchange utilizes two integer parameters,  $p$  and  $g$ , which are available to the public. Parameter  $p$  is prime and  $g$  is any integer less than  $p$  (although this method will work for

any finite cyclic group with generator  $g$ ).

Suppose Alice and Bob want to exchange messages using these parameters. First, Alice chooses a random private integer value  $a$ , and Bob chooses a random private integer  $b$ . Neither  $a$  nor  $b$  is revealed to the public. Alice sends  $g^a \pmod{p}$  to Bob, and Bob sends  $g^b \pmod{p}$  to Alice, and these values are revealed publicly. Privately, Alice then computes  $(g^b)^a \pmod{p}$ , and Bob computes  $(g^a)^b \pmod{p}$ . Since  $(g^b)^a \equiv g^{ba} \equiv g^{ab} \equiv (g^a)^b \pmod{p}$ , Alice and Bob have a shared secret key,  $g^{ab}$ , which they can use to send messages.

The security of the Diffie Hellman key exchange rests on the assumption of the difficulty of computing  $g^{ab} \pmod{p}$  only knowing public values  $g$ ,  $g^a \pmod{p}$ , and  $g^b \pmod{p}$ , but not  $a$  and  $b$  themselves. However, both parties are able to derive a shared secret value from one party's public key and the other's private key.

**Acknowledgments.** I would like to thank my mentors Emily Riehl and Aaron Marcus for their careful guidance and editing.

#### REFERENCES

- [1] John Stillwell. Elements of Number Theory. Springer. 2003.
- [2] Whitfield Diffie and Martin Hellman New Directions in Cryptography. IEEE Communications Magazine. 1978.