Proving The Existence Of A Second Private Key That Decrypts a Message Encrypted With The RSA Encryption Algorithm

Marina Ibrishimova

University of Victoria
http://www.uvic.ca

Abstract. *The RSA algorithm is a widely used asymmetric encryption algorithm. It consists of one public key used to encrypt messages and one private key used to decrypt messages. This paper proves the existence of a second private key for every public key that decrypts all messages just like the intended private key.*

Keywords: Cryptography [MSC2010 94A60]

1 Introduction

In this paper we construct a proof for the existence of a second private key for the RSA encryption algorithm based on results from Number Theory and we explore the relation of this second private key to the public key (n,e).

According to the RSA encryption algorithm [3], the intended private key d_1 is computed using the public key e and $\phi(n)$ where $\phi(n)$ is Euler's totient function

$$e * d_1 = 1(\text{mod } \phi(n)) \tag{1}$$

Recently, the Carmichael function was proposed to be used in order to ensure generating a small private key and empirical evidence revealed that the function sometimes uncovers a second private key that is different than the one generated using $\phi(n)$ function.[2] However, the Carmichael function reveals a different private key only sometimes and thus the existence of a second private key for all messages has not been proven and a formula for finding a second private key was not provided. In addition to proving the existence of a second private key in this paper we also provide a formula for obtaining it.

2 Formulating the claim

Claim 1. Given an RSA public key (n, e) where n is the product of two primes both greater than 2, e is an integer smaller than n such that GCD(e,$\phi(n)$) = 1 and e* d_1 = 1 mod $\phi(n)$, there exists a second private key d_2 such that e* d_2 = 1 mod $\phi(n)/2$.

There are several different definitions and theorems to keep in mind when proving the existence of a second private key.

2.1 Definitions

Definition 1: The order of an element a in Z_n is the smallest integer k such that a^k= 1 mod n. [1]

Definition 2: If r and n are relatively prime (co-prime) integers and the order of r mod n is equal to $\phi(n)$ where $\phi(n)$ is Euler's totient function, then r is called a primitive root modulo n. [1]

Definition 3: A universal exponent of the positive integer n is a positive integer U such that

$$a^U = 1 \mod \text{n} \tag{2}$$

for all integers a relatively prime to n. [1]

2.2 Theoretic Background

Theorem 1. *The product of two odd integers is an odd integer.*

Proof: By definition, an odd integer is of the form 2k + 1 for some k in Z Let a = 2m + 1 and b = 2n + 1 for some n,m in Z Then a*b = (2m + 1)*(2n + 1) = 4mn + 2m +2n + 1 = 2(2mn +m + n) + 1 . Let r = (2mn + m + n). Since n, m are in Z and Z is closedwith respect to multiplication and addition, then r is also in Z and therefore 2r + 1 is an odd integer.

Theorem 2.*Let $\phi(n)$ be Euler's totient function, then $\phi(n)$ is even when n = p*q where p and q are 2 distinct prime integers.*

Proof: All prime integers greater than 2 are odd since by definition of an even integer e, e is 2 times some other integer, namelye = 2k for some positive integer k in Z, therefore e is divisible by 2 and yet a prime integer is only divisible by itself and 1. Therefore, all primes greater than 2 are odd and by definition of odd integers, an odd integer is an even integer plus one, so if x is a prime integer greater than 2 then x = 2v + 1 for some v in Z. On the other hand, (x-1) = (2v+1)-1= 2v. So therefore (x-1) is an even integer by definition. If p and q are two odd prime integers then (p-1) = 2r for some r in Z and (q-1) = 2s for some s in Z. Therefore,

$$(p-1)(q-1) = 2r2s = 4rs = 2(2rs) \tag{3}$$

and since 2,r,s are all integers in Z, which is closed with respect to multiplication, then their product is also an integer in Z. Therefore,(p-1)(q-1) is an even integer. Therefore, $\phi(n)$ is even when n = p*q where p and q are both prime integers greater than 2.

Theorem 3. *A positive integer n has a primitive root if and only if it is of the form 2, 4, p^t, or $2p^t$ where p is prime and t is a positive integer in Z.*

Proof: See pages 351 to 353 from [1]. In particular, Theorem 9.15 from chapter 9.3: The Existence of Primitive Roots

Theorem 4. *If n is the product of two odd primes, then $\phi(n)/2$ is a universal exponent.*

Proof: Since n is the product of two odd integers then n is odd by Theorem 1 and by Theorem 3 it does not have a primitive root. By Theorem 2 $\phi(n)$ is an even integer and so it is divisible by at least 2. Since n does not have a primitive root then for all integers a smaller than and coprime with n,

$$a^{\phi(n)/2} = 1 \pmod{n} \tag{4}$$

2.3 The Proof

The public key in the RSA encryption algorithm consists of two integers (n, e) such that n is the product of two distinct odd primes. [3] Since n is the product of two distinct odd primes then it does not have a primitive root and $\phi(n)/2$ is a universal exponent mod n. Therefore, for every integer a coprime with n,

a^1 (mod n) = $a^{\phi(n)/2)+1}$ (mod n)
a^2 (mod n) = $a^{\phi(n)/2)+2}$ (mod n)
a^3 (mod n) = $a^{\phi(n)/2)+3}$ (mod n)
a^4 (mod n) = $a^{\phi(n)/2)+4}$ (mod n)
a^5 (mod n) = $a^{\phi(n)/2)+5}$ (mod n)
.
.
.
$a^{\phi(n)/2}$ (mod n) = $a^{\phi(n)}$ (mod n) = 1

In other words, the sets A = [a^1 (mod n) , a^2 (mod n) , a^3 (mod n), ..., $a^{\phi(n)/2}$ (mod n)] and B = [$a^{(\phi(n)/2)+1}$ (mod n) , $a^{(\phi(n)/2)+2}$ (mod n), $a^{(\phi(n)/2)+3}$ (mod n), $a^{\phi(n)}$ (mod n) = 1] are equivalent.

If (n, e) is the public key, then d_1 is the private key that decrypts all messages encrypted with the public key (n, e). From a number theoretic perspective, this first key is an integer such that GCD(n, d_1) = 1 so d_1 is coprime with n. Clearly,

d_1 is an exponent in either set A or set B.

If d_1 is in set A, then the next private key d_2 will be at a distance d_1 + $\phi(n)/2$ from the first key. If d_1 is in set B, then the next private key d_2 will be at a distance d_1 - $\phi(n)/2$ from the first key.

2.4 Conclusion

There exists a second key that decrypts all messages encrypted with the public key (n, e). If d_1 is the intended key then the second private key d_2 is

$$d_2 = d_1 + \phi(n)/2 \tag{5}$$

$$d_2 * e = 1 (\text{mod } \phi(n)/2) \tag{6}$$

References

1. Rosen, K.H., Elementary Number Theory and Its Applications, Pearson/Addison Wesley, San Francisco, 2005
2. Ramanjaneya Reddy N., Reddy P.C., Padmavathamma M. (2016) Study the Impact of Carmichael Function on RSA. In: Unal A., Nayak M., Mishra D., Singh D., Joshi A. (eds) Smart Trends in Information Technology and Computer Communications. SmartCom 2016. Communications in Computer and Information Science, vol 628. Springer, Singapore
3. Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21(2), 120126 (1978)