Role of Linear Diophantine Equations in RSA Encryption

Yi Zhou

Shanghai Starriver Bilingual School, Shanghai, China

joyee.zhou@outlook.com

Abstract. Diophantine equations are mathematical equations that include only integer solutions and two or more unknown variables. To illustrate, the most elementary form of Diophantine equations are linear Diophantine equations when two different one-degree monomials added up to a constant value. Such equations were given the name of the extraordinary Greek mathematician Diophantus who made great contribution to algebra and number theory. In addition, they help in defining concepts in algebraic geometry and contribute to the development of algorithms for cryptography. They work in the same way as public keys do in cryptocurrencies within blockchain technology to curb cyber threats and scams targeting public systems. They serve as a means of securing transactions on a computer network when using cryptocurrencies such as bitcoins. These encryption techniques also permit cryptographers and mathematicians to create new ideas in relation to these number systems, thus making it possible for further cryptographic techniques to be put into place.

Keywords: Cryptography, Diophantine Equations, RSA mechanisms.

1. Introduction

The Diophantine equation named after the Greek mathematician Diophantus considers polynomial equations that are ringed by integers. It is, in fact, about finding solutions of the n-variable polynomial f(x1,x2,…,xn)=0 where its coefficients are integers and it takes on values from the set of integers. Solvability of Diophantine equations is an important and difficult problem for which a solution can be elusive. Often leading to insurmountable difficulties is the task of determining if a given Diophantine equation has solutions or not. Yet some cases like linear Diophantine equation ax+by=c can be easily solved in short time using Euclidean's algorithm thereby revealing possible greatest common divisor solutions.[1] As though this were not enough, as n increases further and more variables are introduced into the system, it becomes extremely difficult to find any such solution.

There are some well-known examples that illustrate how cumbersome such equations can be like Pythagorean theorem which states that for any right triangle, the sum of areas of two smaller squares formed on both triangle's legs equals to the area of square built on hypotenuse; and Pell equation (x^2-dy^2=1). There are many different approaches to solving Diophantine equations: they include factorization, infinite descent, modular arithmetic among others depending upon kind of problem being dealt with. In cryptography for example integer solutions play a crucial role in constructing secure encoding schemes while in computer science such equations arise when developing algorithms for method verification or program debugging purposes.

2. Lagrange's Four-Square Theorem

Fermat's polygon number theorem: Every positive integer can be expressed at most as the sum of the n polygon numbers of n. Each number can be expressed as the sum of at most three triangular numbers, the sum of four-square numbers, the sum of five pentagonal numbers, and so on.

Waring's theorem: For every positive integer k that is not 1, there is a positive integer g(k), so that every positive integer can be expressed as the sum of g(k) non-negative integers raised to the k-th power.

Lagrange's four-square theorem: Every positive integer can be expressed as the sum of the squares of four integers, which is a special case of Fermat's polygon number theorem and Waring's theorem.

For any n∈N, there exists an (w,x,y,z) ∈Z, s.t. n = w^2+x^2+y^2+z^2

Quadratic Diophantine equations x^2+y^2=z^2 has infinite solution. [2]

3. Primitive Triples

Hence, (a0, b0, c0) is a Pythagorean number when set of three natural numbers (a,b,c) is a Pythagorean number. The primitive or essential Pythagorean triangle refers only to the set of three numbers themselves (a_0, b_0, c_0). That is why it can be said that if Pythagorean numbers are primitive (or coprime), then two out of these three natural numbers are relatively prime. In fact gcd(a,b,c) = gcd(a,b) = gcd(b,c) = gcd(a,c). [3]

Primitive triple refers to a set of positive integer (a,b,c) that satisfy the equation a^2+b^2=c^2. These are triples for the sides of right triangles with hypotenuse represented by c and right-angle sides represented by a and b. These triples display rich arithmetical properties. Euclidean method generates infinite Primitive triples given by m>n, m>1; n=1 consequently producing this formula: m^2-n^2 as side "a", 2mn as side "b" and m^2+n^2 as side "c". This formula gives all prime primitive triples where a, b and c are relatively prime but not all non-prime solutions directly come from it. Properties include area being a multiple of 6 in primitive triples and any k>2 with k∈Z having at least one such triple divisible by k through its values for a, b, and c. The study of primitive triple not only enriches our understanding of number theory, but also provides practical applications in cryptography, computer science, and any field involving the representation of geometric shapes with right triangles.

Theorem 1:

"A triple (a,b,c) ∈Z^3 is primitive if gcd(a,b,c)=1 & a^2+b^2+c^2=1

Proof: The complete list of primitive Pythagorean triple is {(2rs,s^2-r^2,s^2+r^2)|r,s∈Z ;(r,s) are not both odd}

First, we cannot have a,b,c≡0 because gcd(a,b,c)=1. If both a and b were odd, then a^2+b^2≡2 (mod 4), but c^2≡2 (mod 4) is impossible. Without loss of generality, we can assume that a is even and b is odd. Therefore, c is also odd because a^2+b^2=c^2" [4].

Theorem 2:

a) Prerequisites
   i. $\alpha|\beta, \beta^2 and\ a\ are\ irreducible$ => $\alpha|\beta$ is called a unique factorization
   ii. a domain is a commutative ring R with the property a, b $\in R\{0\} => a, b \in R\{0\}$
b) Two elements $a, b \in R$ are associate ⇔ a|b when b= ac for some c∈R
c) Definitions:
   i. A nonzero r∈ $R\backslash R^*\ is\ irredcucible\ if\ the\ following\ property\ r = ab\ (a, b \in R) => a \in R^*$or b ∈ R*
   ii. A nonzero r∈ $R\backslash R^*\ is\ irredcucible\ if\ the\ following\ property\ r = ab\ (a, b \in R) => a \in R^*$ or b ∈ R*
d) In a domain R, x<- R prime => x is irreducible
e) A domain R is called a unique factorization domain if every r ∈ $R\{0\}$ factors into a product of irreducible elements and the factorization is unique up to reordering and associates
f) X ∈ R irreducible => X is prime (R is a unique factorization domain)

Note:

1. An ideal I in a commutative ring R is a subgroup of (R, t, 0) which is closed under multiplication be elements of R. Th principal ideal generated by α ∈ R is $\alpha = \{r\alpha | r\alpha \in R\}$
   g) The ideal generated by $\alpha 1, \dots \alpha \in R$
2. Unique factorization domain: irreducible numbers are prime, ideals are all principled, the group = ideals/principal ideal
   a) The group itself is an abelian group
3. A number x ∈ R^* which is algebraic is over Q is called an algebraic number Q
   a) Q is a field
   b) Proof: Given alpha and beta ∈ Q, alpha times beta, alpha + beta, alpha ∈ Q
   c) Say$a^n + r1a^n - 2 + \cdots = 0\ and\ same\ for\ beta$ where r and s both in the group b

4. RSA Encryption Process

The RSA encryption algorithm, put forward by Rivest, Shamir and Adleman in 1977, is a milestone of public-key cryptography that depends on hard computational problems in solving the product of two large prime numbers for confidentiality and digital signatures. [5] In the RSA scheme, the receiver generates a public-private key pair, starting by selecting two dissimilar prime numbers p and q; these are kept confidential and are used to determine their product n = pq which is known as modulo publicly. Consequently find Euler function φ(n) = (p-1)(q-1) which shows how many positive integers less than n are relatively prime to it (n). Then pick an index for public key e such that it should be between 1 < e < φ(n), gcd(e, φ(n)) = 1.

The common RSA encryption relies on the difficulty of factoring large composite numbers into their prime factors. This security rests on the assumption that it is computationally infeasible to factor the product of two large prime numbers. However, there exist scenarios where RSA encryption can be vulnerable to attacks based on Diophantine equations.

The private key exponent d is the modular inverse of e modulo φ(n). This is calculated using the extended Euclidean algorithm ed ≡ 1 (mod φ(n)). Publication of the public key (n, e) and keeping secret private key d does happen. Encryption is the process of computing ciphertext c ≡ m^e (mod n) with message m being expressed as an integer less than n. Decryption of the key recovers the original messages from c with m ≡ c^d (mod n). Because n is a random product of two prime coefficients, it is very hard to obtain the number n. This makes the algorithms secure by ensuring the low likelihood of someone guessing the combination of prime coefficient since it is a computationally infeasible attack even for the most advanced classical computers. Therefore, only someone with the private key can decrypt the ciphertext.

However, such systems are not infallible. One possible way to attack this kind of system is the Coppersmith’s method. It exploits the relatively smaller roots of modular polynomial equations when attacks occur. Such methods are particularly effective when applied to RSA encryption schemes. When a small portion of the plaintext is known, attackers can easily guess the combinations of the private keys. This method allows an attacker to recover the RSA private key with only partial information about the plaintext.

Diophantine equations come into play when there are such attacks that target specific properties of RSA keys. For example, attacks based on a small portion of known private exponents or public exponents satisfying Diophantine equations can easily tear down the entire RSA system. Understanding the role of Diophantine equations in RSA systems is both important to code encryptions and code attackers.

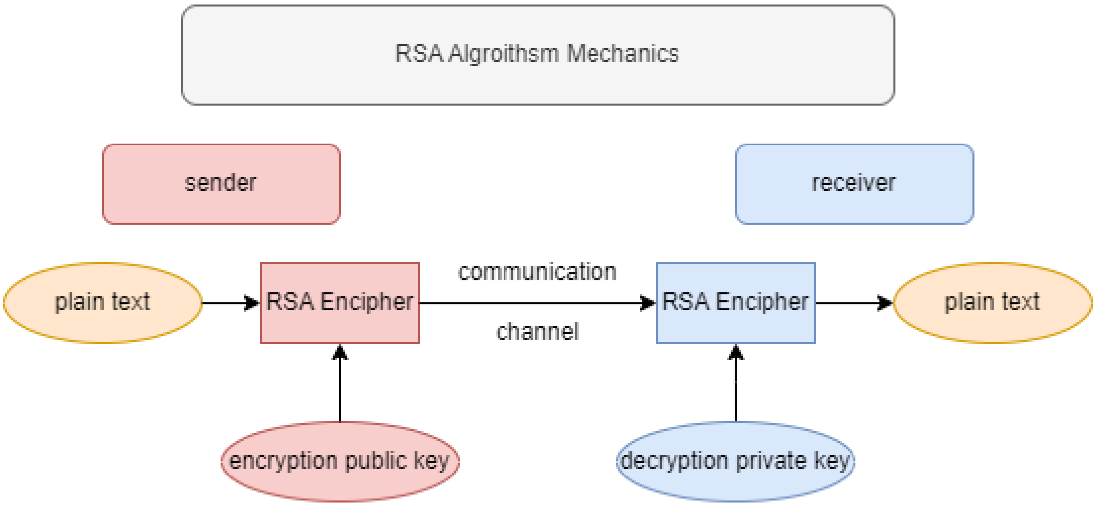

Figure 1. RSA Algorism Mechanics

5. Conclusion

We examined the role of Diophantine equations in the RSA cryptosystem and discussed the core elements of RSA in detail by explaining how keys generate, encrypt, and decrypt. Furthermore, we provided a thorough rundown of the mathematical instruments that are essential to comprehending the main RSA cryptanalytic assaults. These included ideas like Lagrange four squares theory, primitive triples and Diophantine approximations. We also clarified methods for finding tiny solutions to modular polynomial equations, after which explaining potential attacks that the system might be exposed to. These attacks use Coppersmith's methods for solving modular polynomials and lattice reduction. Diophantine equations are indeed limited when they come to the face of such attacks.

References

[1] K. Bogart, et.al., Cryptography and Number Theory, 2003.
[2] Burton, Elementary Number Theory, The McGraw-Hill Companies, Inc., New York, 2007.
[3] B. Kaliski, The Mathematics of the RSA Public-Key Cryptosystem, 2005.
[4] Kerr, M. (n.d.). Number Theory and Cryptography. Wustl Education, https://www.math.wustl.edu/~matkerr/NTCbook.pdf
[5] Rivest, R.; Shamir, A.; Adleman, L. (February 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"