Levi Seibert

00086809

lseiber1@my.athens.edu

ITE 523 – Dr. Yahia Fadlalla

Number Theory and Cryptography

The Importance of Number Theory in Cryptography

Cryptography is foundationally a mathematical concept. The encryption process relies primarily upon math and arithmetic operations. This should not be surprising, since computers are truly mathematical tools (in fact, the original computers only performed mathematical operations, much like modern day calculators). It is worth mentioning; however, that cryptography is not solely a computer concept. The origins of encryption can be dated back to Julius Caesar and his Caesar Cipher. But even this cipher was mathematical, as it solely consisted of shifting the alphabet by a given number, modulus the number of letters in the alphabet in use (the modulus operation means to divide by the given number and return the remainder; for example, 27 mod 26 = 1).

An encryption algorithm is only as strong as its weakest link, which often times happens to be its mathematical methods. If the math is not complex enough, then the encryption will ultimately fail and be weak enough for the average hacker to decipher. As mentioned above, the Caesar Cipher encryption process only consisted of shifting the alphabet. This blatant weakness is why the cipher is only mentioned as an example of antique ciphers, rather than an example of modern cryptography. So, how does math actually come into play in the encryption process? Other then the fact that all computer work is mathematical (everything is 1s and 0s), encryption relies on the field of number theory to ensure algorithms are sufficiently strong and invulnerable.

Number theory is a branch of mathematics that deals with the properties of numbers, specifically integers. Operations such as modulus are introduced, concepts such as the Greatest Common Factor and the Lowest Common Multiple are defined, and theorems like the Fundamental Theorem of Arithmetic, the Prime Number Theorem, and the Chinese Remainder Theorem are considered. All of these concepts (some of which are described below in the section entitled “Reading Review”) play an instrumental role in cryptographical-mathematical calculations. While many of the concepts may seem confusing to an outsider, this complexity is what makes cryptography secure. Number theory gives rules to a computer for how to work with numbers and how to make the supporting math correct yet complex.

Ultimately, encryption can be thought of as a function itself. As in algebra, where there are functions of x that operate on x and return a value (sometimes considered the y value), encryption accepts a plaintext as its input, performs operations based on a key, and then produces an output called the ciphertext. The question becomes what operation is performed on the input and the answer to that depends on the algorithm and the key. Some encryption methodologies make this connection between encryption functions and mathematical functions inseparable, like

Elliptic Curve Cryptography (described below), which literally uses a algebraic function to create a key.

In public key cryptographic systems (encryption algorithms that have both a public and a private key) in particular, the concept of a trapdoor function is of the upmost importance. A trapdoor function is a mathematical function that given a certain value input, an output value is easily produced; however, it is very difficult to reverse this operation and produce the input when given the output [1]. A proper trapdoor function is a must for proper key productions. Without a strong trapdoor function, a key can be easily discovered, which makes encryption useless and open to the public, or at least all those who want to know and take the effort to do so. Therefore, properties from number theory need to be properly applied to the encryption algorithm in order to produce a robust trapdoor function.

Elliptic Curves

Elliptic curves are a specific branch of number theory that have growing significance in the cryptographic realm. Elliptic curves are used to make secure private keys with very strong trapdoor functions, as they are quite difficult to reverse. This is one application of number theory that makes cryptography explicitly mathematical; the source of encryption relies on algebraic concepts. Elliptic Curve Cryptography is based upon a mathematical equation of the form $y^2 = x^3 + ax + b$. The graph of this looks something like Figure 1; however, the exact shape will depend on the values of a and b.

Two noteworthy properties of elliptic curve graphs is that they are symmetric about the x-axis (meaning that the shape is a mirror image around the horizontal axis) and any non-vertical line will intersect the curve at a maximum of 3 points. If a non-vertical line is drawn through two points on the graph, it will intersect the curve at exactly one other point.

As a consequence of these two properties, there is an operation called the “dot” operation. When two points are “dotted” together, you draw a line connecting the two points, and then wherever the line meets the curve, the point is mirrored onto the other side of the graph (horizontally). This process can be repeated over and over to get new points (for example, a dot b = c, a dot c = d, etc.). To see an example of this dotting process, see Figure 2 (this animation shows a series of dottings taking place; if the animation does not get preserved through the saving and uploading process, visit the reference link to the view the animation).

In Elliptic Curve Cryptography, there is a known starting point and a known ending point. Even if someone knows the first point and the final point, it is very difficult to deduce how many “dotting” operations took place to reach the final destination. This is the basis of the trapdoor function for the Elliptic Curve Cryptography.

There is also a set max size for the curve (a vertical line which points are not allowed to cross) which corresponds to the keysize for the encryption. As expected, the larger the keysize, the stronger the encryption. The curve definition, starting point, and end point can all be publicly known, as long as the number of times the function is dotted remains secret. This is the private

key and can be used in other cryptographic algorithms. This key can then be used for encryption and is often paired with other methods like the Diffie-Helman Key Exchange.

Elliptic Curve Cryptography allows encryption to take place with significantly smaller keys than alternative methodologies (like RSA which is based on prime number factorization), without sacrificing security. As a result, encryption can take place faster. Because of these benefits, elliptic curve cryptography is used by a vast array of entities, including the U.S. Government, Bitcoin, Apple, CloudFlare, and so many others. That being said, there are some groups who are not in favor of Elliptic Curve Cryptography, for reasons such as the potential for a backdoor, miscalculations of random numbers, and issues with patents [1, 2].

Reading Review

The assigned reading from "Lecture Notes: Number Theory and Cryptography" by Matt Kerr had the following main points:

- Chapter 1 introduces the Euclidean Algorithm. It begins by discussing the division algorithm and then defines divisibility and the Greatest Common Denominator (GCD). The Euclidean algorithm is the theory that the GCD of two integers can be discovered by using repetitions of the division algorithm. In addition, the GCD of two integers can be found to be the linear combination of the two numbers. The Least Common Multiple (LCM) is defined and several related Theorems, Corollaries, and Lemmas are presented.
- Chapter 2 discusses the concept of natural number primes (natural numbers that are irreducible; that is, they can only be divided by themselves or 1). This definition leads to the Fundamental Theorem of Arithmetic, which states that any natural number greater than 1 can factored into prime numbers. From the Fundamental Theorem of Arithmetic, Euclid's argues that there are infinitely many primes.
- Chapter 4 introduces the Prime Number Theorem, which states that the function $\pi(x)$, which counts the number of primes less than or equal to x, is approximately equal to x divided by the log of x. An alternative way of considering this is that the limit (as x approaches infinity) of $\pi(x)/(x/\log(x))$ is equal to 1.
- Chapter 5 begins a discussion on modular arithmetic, and the concepts of congruence/residue classes modulo an integer is considered. The modulo operator is an equivalence relation on the set of integers (it is reflexive, symmetric, and transitive), thus can partition the set of integers into equivalence classes. The set of these equivalence classes are called the ring of integers modulo *m*, where *m* is an integer. The definition of the inverse of a modulo operation is also presented, as is Euler's phi-function and Fermat's "Little" Theorem.
- Chapter 7 introduces the Chinese Remainder Theorem, which states that given *m* and *n* are both greater than 1 and coprime (they have no positive integer factors in common) and that *a* and *b* are integers, there is some integer *x* that modulo *m* produces *a* and modulo *n* produces *b*, and *x* is unique as long as it falls between 0 and the product and *m* and *n*. The Chinese Remainder Theorem can be further generalized, for example, given the same preconditions as the original, there exists an integer *x* that fulfills the earlier definition, if and only if *a* modulus the GCF of *m* and *n* is equal to *b*.

- Chapter 11 describes some more complex theorems and formulas but focuses on prime power moduli and power residues. For example, it describes a technique of how to reduce "mod $p_i^{r_i}$ to just p_i.

Each of the chapters go into much more detail, but these bullet points provide a brief summary of some of the larger topics that were discussed.

Figures

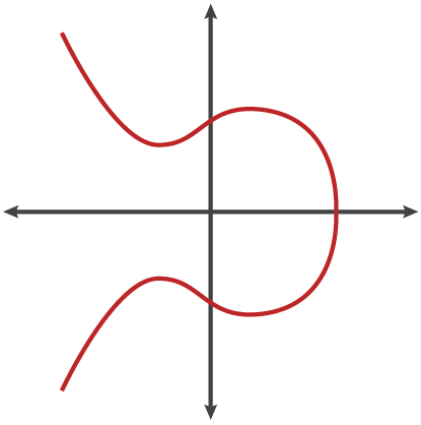

Figure 1: An Example Elliptic Curve Graph [2]

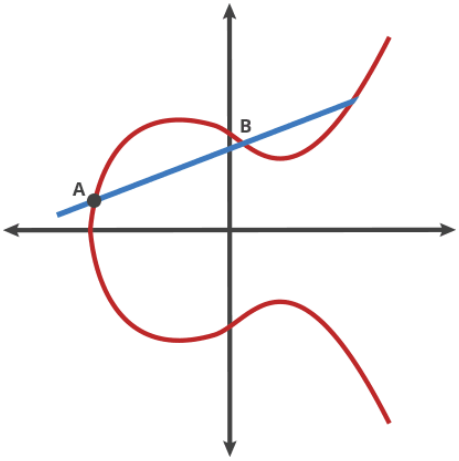

Figure 2: An Example of "Dotting" on an Elliptic Curve [2]

References

[1] F5 Dev Central. Elliptic Curve Cryptography Overview. (Oct. 14, 2015). Accessed: Feb. 15, 2023. [Online Video]. Available: https://www.youtube.com/watch?v=dCvB-mhkT0w

[2] N. Sullivan. *A (Relatively Easy To Understand) Primer on Elliptic Curve Cryptography*. CloudFlare. (Oct. 23, 2013). Accessed: Feb. 20, 2023. [Online Article]. Available: https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/