

# IB Extended Essay

Jacob Bruner

August 22, 2022

## Contents

<b>1</b>	<b>Introduction and Aim</b>	<b>2</b>
1.1	Motivating Problem . . . . .	2
1.2	The 'Public-Key' Paradox . . . . .	3
<b>2</b>	<b>What is 'Public-Key' Cryptography</b>	<b>3</b>
<b>3</b>	<b>How can we formalize this: An Introduction to Groups</b>	<b>4</b>
<b>4</b>	<b>Group Law on an Elliptic Curve</b>	<b>4</b>

# 1 Introduction and Aim

## 1.1 Motivating Problem

It's undeniable that our modern-day world is reliant on cryptography. Every time a phone sends a text, a browser connects to a server, an email gets sent off, a monetary transaction is made, and much much more, our devices are, unbeknownst to us, performing many hundreds of math operations to ensure our data are 'encrypted.' But what does 'encryption' mean? Let's introduce some definitions. 'Encryption' is the process of disguising a message to be, loosely speaking, hidden to all but the intended recipient. This is the process of converting a 'plaintext' message into a jumbled 'ciphertext', which can be readily shared without risk of the sensitive message leaking. Converting a plaintext message (typically a string/list of characters) into a ciphertext is known as an 'enciphering' or 'encrypting' transformation. Likewise the reverse operation of recovering the plaintext message from a ciphertext is known as the *deciphering transformation*.<sup>1</sup> If we denote the plain and cyphertext  $\mathcal{P}$  and  $\mathcal{C}$  respectively and the enciphering map  $f$  and its inverse  $f^{-1}$  we obtain the following diagram:

$$\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}$$

The most common formulation for this kind of cryptosystem would be that the two transacting parties agree upon the parameters for the map  $f$  in secret beforehand. Common examples include the 'Caesar Cipher' (supposedly invented by *the* Julius Caesar), where  $f$  is a shift operation that maps each letter to a new one a number of places ahead. We start encoding each letter as a number from 0, which is A, to 25, which is Z. Of course this depends on what alphabet one uses, if one chooses to include spaces etc. We can represent the operation that takes a letter and maps it  $n$  places ahead with addition. Importantly, this operation must 'wrap around' back to zero if you try to exceed 'z' in the alphabet. This process, known as '*modular arithmetic*', is like circling a clock, where after reaching twelve, the hour hand wrap back around to 1, but we start from 0 instead of 1. So, in our case, shifting 'z' by 3 letters looks like so:  $25 + 1 \bmod 26 \equiv 0$ , which reads "25 plus 1 is congruent to 0 modulo (or *mod*) 26". With this in mind, we obtain for each letter  $p \in \mathcal{P}$ :

$$f(p) = p + n \bmod 26$$

Representing a shifting of each letter in the plaintext by  $n$  places in the alphabet. Now clearly this isn't a very sophisticated cryptographic scheme.

---

<sup>1</sup>Neal Koblitz. *A Course in Number Theory and Cryptography*. 2nd ed. Graduate Texts in Mathematics No. 114. Springer, 1994. ISBN: 9781461264422, p. 54.

For instance, performing a frequency analysis and comparing the most commonly occurring letters to that of the English alphabet can easily break these sorts of schemes, known as 'substitution ciphers.' Modern schemes typically employ more resistant techniques such that changing one letter of plaintext often yields a completely different ciphertext. For instance, AES encryption, part of the modern web standard, is an example of a block substitution cypher. At a high level, it combines techniques similar to our Caesar Cipher with certain affine transformations (which can be thought of as an additional scaling action in combination with our translation) performed on blocks of plaintext. It's certainly more complicated than that, but essentially boils down to our system plus some bells and whistles to make it resistant to cryptanalysis, like permutations, combinations, text look-up-tables and more. In general, this type of encryption where there's a predetermined shared secret is well-studied, often bearing the name 'symmetric-key encryption,' to emphasize that the private keys are known beforehand. For instance, Claude Shannon (often called the father of cryptography) mathematically proved that the 'one-time-pad' encryption technique was unbreakable. His findings showed that if a random-generated key is at least as long as the plaintext, performing modular addition (i.e., wrapping around so as to not exceed the alphabet) on each letter by the private key yields a ciphertext that is uncrackable.<sup>2</sup> Although modern systems seek smaller key sizes for performance reasons, this worst-case scenario should demonstrate the strength of symmetric-key algorithms in general. The 'one-time-pad' gets its name from its use in WWII when the KGB would distribute palm-sized pads with these one-time-keys and a table to ease in conversion. Such pads were often made of flammable materials to be burned with no trace.<sup>3</sup>

## 1.2 The 'Public-Key' Paradox

## 2 What is 'Public-Key' Cryptography

The first protocol developed to address this motivating problem was RSA encryption. Leveraging intuitive properties of numbers, RSA establishes our idea of 'one-way operations' using simple multiplication of large, highly prime (minimal divisors), numbers.

---

<sup>2</sup>Claude E. Shannon. *Communication Theory of Secrecy Systems*. Vol. 28. The Bell System Technical Journal, 1949, pp. 656–715. DOI: 10.1002/j.1538-7305.1949.tb00928.x.

<sup>3</sup>Robert Edward Lewand. "The Perfect Cipher". In: *The Mathematical Gazette* 94.531 (2010), pp. 401–411. ISSN: 00255572. URL: <http://www.jstor.org/stable/25759724> (visited on 05/21/2022).

	A	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	B	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	C	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	D	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	E	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	F	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	G	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	H	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	I	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	J	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	K	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	L	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	M	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	N	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	O	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	P	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	Q	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	R	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	S	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	T	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	U	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	V	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	W	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	X	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	Y	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z
	Z	AB	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	Z

Figure 1: Format of a one-time-pad used by the NSA<sup>4</sup>

### 3 How can we formalize this: An Introduction to Groups

Group theory provides us a way to generalize certain, often intuitive, properties of number systems, by using axiomatic structure to classify groups ‘up to isomorphism’ and to prove various properties about their structures. A ‘Group’ boils down to a set, infinite or finite, and an operation that takes two elements and maps it to another while maintaining some structure. It’s common to think that this structure is too vague, or broad, but, in fact, it’s enough to prove sweeping conjectures and determine non-trivial properties, thereby making itself a staple of modern mathematics.

### 4 Group Law on an Elliptic Curve

While the elliptic curve group admits an intuitive geometric description, it’s important that our algebraic description satisfies the group axioms.  $E(\mathbb{F}_q)$ <sup>5</sup>

<sup>4</sup>Koblitz, *A Course in Number Theory and Cryptography*, p. 10.

## References

- A History of U.S. Communication Security*. Vol. 1. The David G. Boak Lectures. National Security Agency, 1973. URL: [https://www.governmentattic.org/18docs/Hist\\_US\\_COMSEC\\_Boak\\_NSA\\_1973u.pdf](https://www.governmentattic.org/18docs/Hist_US_COMSEC_Boak_NSA_1973u.pdf).
- Koblitz, Neal. *A Course in Number Theory and Cryptography*. 2nd ed. Graduate Texts in Mathematics No. 114. Springer, 1994. ISBN: 9781461264422.
- Lewand, Robert Edward. “The Perfect Cipher”. In: *The Mathematical Gazette* 94.531 (2010), pp. 401–411. ISSN: 00255572. URL: <http://www.jstor.org/stable/25759724> (visited on 05/21/2022).
- Shannon, Claude E. *Communication Theory of Secrecy Systems*. Vol. 28. The Bell System Technical Journal, 1949, pp. 656–715. DOI: 10.1002/j.1538-7305.1949.tb00928.x.