

# Cryptography

## Introduction

The study of obscuring the content of messages is very old. Evidence suggests that it was used at least as early as the ancient Egyptians. Diplomacy throughout the ages has relied upon the secrecy granted by cryptology, with some of history's great events being decided in major part by cryptography. Throughout the sixteenth and seventeenth centuries, the study of cryptology played a crucial role in the struggles of the era, of Catholic against Protestant, of one nation vs. another. However, cryptology was very much a 'black art', obscure and esoteric, until the Second World War. The advent of radio, and the enormous distances involved, made cryptology necessary, and also promoted the study of cryptanalysis. By far the most famous cryptological story is the story of the cracking of the German's Enigma code by the Allies, and the corresponding advantages for them. In this paper I will be looking briefly at the history of cryptology, and as this proceeds introducing various methods of obscuring message content, and also looking at the ways in which these methods can be undone. By this I hope to give the reader some idea of the methods of cryptology so I can discuss intelligibly the interesting properties of cryptology as a discipline.

## Definitions

**Cryptology** is the study of codes and ciphers. It is composed of the complementary sciences of **cryptography**, or the science of encoding messages and **cryptanalysis**, or the science of breaking codes and ciphers. **Code** and **Cipher** are taken to mean two different things: a **code** is a system of substituting symbols or words for words or phrases in a message. Thus a **code** is primarily linguistic in nature. A **cipher**, however, is a transformation of the message, usually on a letter-by-letter basis. A **cipher** is independent of the content of the message and is usually based on mathematics. **Plaintext** is the message before any encipherment has taken place. **Ciphertext** is, similarly, the message after encipherment. The process of changing the message from plaintext to ciphertext can be called a number of different things: **encipherment**, **encoding**, **encryption**, and so on. I will be using these and other terms to describe the process, as certain terms carry associations with particular methods of encoding. **Encoding**, following from the definition of **code**, implies the translation into a code, while **encipherment** implies the translation into a cipher. **Encryption**, however, tends to be used more for modern methods of processing the

---

plaintext, such as public-key algorithms and other algorithms impossible without computers.<sup>1</sup>

Some other terms that will be useful in the modern era section are the standard names used when discussing cryptographic protocols. Alice and Bob are used as the main sender and receiver, with Eve being an eavesdropper, Trent being a trusted third party, and Malcolm being a malicious user of the protocol.

More terms will crop up during the history of cryptology, and I will define these as we encounter them. One term that is quite important in the early history of cryptology is **steganography**.<sup>2</sup> This is the science of hiding secret messages within other messages, so that the intended message's very existence is obscured. Various ingenious devices have been employed throughout history to accomplish this, as we shall see in the next section.

## A history of cryptology

### *The infancy of cryptology*

As one might think of a science whose purpose is obscurement, the origins of cryptology are murky. At the earliest stages, nothing about cryptanalysis was known, and so it makes sense to only consider cryptography until much later. Kahn<sup>3</sup> has the early origins of cryptography in ancient Egypt. What originally began as simple ornamentation designed to 'impart a dignity and authority'<sup>4</sup> to the text, slowly changed and became more a puzzle designed to induce visitors to tombs to decipher the puzzle and thus read a blessing for the luminary buried therein. As Kahn says, this is an inauspicious start to the deadly serious games of today. But 'great things have small beginnings'<sup>5</sup>, and thus began the study of cryptography.

---

<sup>1</sup> These definitions are much the same across cryptology references. However, the primary source for this material is Schneier, B. *Applied Cryptography Second Edition*, John Wiley & Sons, Toronto, 1996, Chapter 1 in particular for definitions.

<sup>2</sup> Throughout the paper, I will highlight important term definitions by printing the term itself in bold. This definition is also from Schneier, Ch. 1.

<sup>3</sup> Kahn, D. *The Codebreakers: The story of secret writing*. Abridged version, Signet, New York, 1973

<sup>4</sup> *ibid.*, pp. 69

<sup>5</sup> *ibid.*, pp. 71

Cryptography remained obscure for thousands of years, with whatever science had been discovered by a civilisation tending to be lost when that civilisation fell.<sup>6</sup> China apparently possessed rudimentary cryptography, but apparently ideographic writing was complicated enough for most purposes. Elements of cryptography have been found in the Old Testament, but it is, of course, with ancient Greece that cryptography gets its first boost.

### ***Antiquity***

Historians have uncovered many reports of the use of cryptography in ancient Greece. Homer, in the *Iliad*, was the first to document an account of the use of cryptography, in the story of Bellerophon and Proteus.<sup>7</sup> Other advances made by the Greeks were mainly advances in steganography. Many of the accounts come from Herodotus, such as the account of a method used to bypass the security of Xerxes the Persian, that of scraping the wax from wax tablets, scratching a message on the wood underneath, and then reapplying a wax coating.<sup>8</sup>

Another account from Herodotus tells of a similar, yet more permanent method: When Hystieus was in Persia, he wished to communicate with Aristogoras in Greece about revolting against the Persians. In *Padover*<sup>9</sup>, the story goes: 'Pretending to cure one of his servants who had sore eyes, he shaved the man's head and imprinted the message on the skull. When the servant's hair was grown, Hystieus told him that for a perfect recovery he should go to Aristogoras who, by again shaving his head, would cure his eyes.'<sup>10</sup> One must wonder what would happen to the servant with the secret message (presumably) tattooed onto his head after he had delivered the message and outlived his usefulness...

The Greeks (more specifically, the Spartans) were also among the first to create a device for encoding messages for use by the military. Called a scytale, it was a pair of hexagonal staves of the same diameter, which had a tape wrapped around them. The message was written on the tape, which was then unwrapped and sent to its recipient, who used the identical staff to read the message.<sup>11</sup> Obviously, unless the staves were the same size, the system would not work, so it provided some measure of security for military operations.

---

<sup>6</sup> paraphrased from *ibid.*, pp. 71

<sup>7</sup> from *ibid.* p 73-74

<sup>8</sup> *ibid.* p 75

<sup>9</sup> Padover, S. & Thompson, J.W. *Secret Diplomacy: Espionage and Cryptography 1500-1815*, Frederick Ungar, New York, 1963

<sup>10</sup> *ibid.* p 14

<sup>11</sup> *op. cit.* 3, p 75

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	
4	q	r	s	t	u
5	v	w	x	y	z

Diagram 1. The Polybius Square

An important invention in the field of cryptology, as opposed to steganography, was the system of signaling invented by Polybius. He devised a square containing the letters of the alphabet, and then used the numbers of the columns and rows to refer to a letter.

Thus each letter may be represented by two numbers, or other symbols. This is where this

device's use in later cryptography comes from, as it enables the same amount of information to be conveyed using fewer symbols.<sup>12</sup>

By far the most famous of the cryptological systems of antiquity is the Caesar cipher. To encipher a message in this simple yet successful cipher required the shifting of each letter three letters down the alphabet, like so:

plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Thus, Veni, vidi, vici becomes YHQL, YLGL, YLFL. Although this is simple, it was certainly sufficient for its day.<sup>13</sup>

This type of cipher is called a **direct standard alphabet**<sup>14</sup> or, more simply, a **monoalphabet**. That is, all twenty-six of the letters of the alphabet are rearranged in some way. Other, similar ciphers involve rearranging the alphabet on other ways than the simple method Caesar used, but this will be further discussed later. For now, it is enough to realise that a Caesar cipher is equivalent to any cipher involving a single alphabet rearranged.

### ***The Arabs and Cryptanalysis***

All of the methods of cryptography in the previous section only involve cryptography, not cryptanalysis. Cryptanalysis as a systematic body of knowledge did not exist until the time of the

<sup>12</sup> from *ibid.* p 76

<sup>13</sup> from *ibid.* p 77

<sup>14</sup> from Sinkov A. *Elementary Cryptanalysis: A mathematical approach*, Random House, New York, 1968

Arab empires, in the late centuries of the first millenium CE. The technique of frequency analysis was invented, to all appearances, by an Arab scholar named Ibn ad-Durahim, who published an encyclopedia in 1412.<sup>15</sup>

The technique of frequency analysis allows for the decipherment of any direct standard alphabet. The basic procedure is as follows: take a sample of text, 1000 letters will do, and count the relative frequencies of each letter. Then take the table of frequencies thus obtained as a reference. Next, take the text to be deciphered, and count the number of each type of letter in it. If it is a simple Caesar cipher, then all you have to do is match the letters with the highest frequencies in the message with those in your reference table. This will give you a probable translation. With only slightly more advanced techniques, it is possible to completely understand the system, and thus to read any message sent in it.<sup>16</sup>

### ***Post-Renaissance Europe to the end of the 18<sup>th</sup> Century – Black Chambers and Amateur savants***

Europe in the post-Renaissance was such a roiling mess of nations, all scheming for power, that it provided a fertile ground for cryptology to grow. In this era, all of the major nations had Black Chambers; organisations devoted to breaking the codes of other countries' diplomatic codes. Also in this era, public knowledge of cryptology began to rise, and, with the increasing education levels among gentlemen and so on, some major talents emerged in both cryptography and cryptanalysis.

In this time, the primary means of encipherment was the use of codes. Detailed code systems, called nomenclators, were used by all of the major powers. These systems consisted of cipher alphabets, and a code table for common terms. For example a nomenclator used by Phillip of Spain in 1589 consisted of a cipher alphabet, with code groups of letters for phrases and names such as 'Navarre', 'King of Spain', 'Your majesty' and so on.<sup>17</sup>

Codes were, however, not the only ciphers being considered. The Italian polymath Leon Battista Alberti designed the first device that could be used for what is now known as **polyalphabetic ciphering**. This is a technique of the same family as a monoalphabetic cipher, but as the name implies, more than one alphabet is used to encipher the plaintext. In the case of Alberti's system,

---

<sup>15</sup> op. cit. 9 p 80

<sup>16</sup> based on op. cit. 34, p 16-20

<sup>17</sup> from op. cit. 3, p 86

the alphabet was changed every few words, with a key letter marking the new alphabet. Also remarkable was Alberti's invention of a concentric-disc system for encipherment and decipherment. Alberti's other major addition to the growing field was the concept of an **enciphered code**. In this system, a code is used for some or all parts of a message, and the symbols that make up the code are then enciphered.<sup>18</sup> By 'layering' the techniques this way, the technique of frequency analysis was frustrated.

The polyalphabet continued to be developed, by a number of people, the last and most famous being Blaise de Vignère, who was also responsible for inventing the first **autokey** system, or encipherment system where the message itself is the key to the encryption. Thus, the sender and receiver would only have to agree on a single letter in advance, which would be used by the sender to encipher the first letter of the plaintext. The first letter of the plaintext would then be used to encipher the second letter, and so on. The problem with this was that a single error would garble the rest of the message. However, it is not this cipher for which Vignère is famous.

Perhaps unfairly, the cipher that today bears his name is much simpler. It consists of taking a keyword and using the repeated keyword as the key stream to encipher the text. However, the periodicity of the repeating keyword provides a means of attack for cryptanalysis. Again, though the nature of the system requires that a large amount of time and many calculations are involved in enciphering a message, and so this, in large part, explains why the major powers used nomenclators until much later.

Apart from these amateur yet surely gifted innovators, there were at this time people whose job it was to encipher and decipher messages for their respective governments. These were the Black Chambers.

Perhaps the exemplar of these was the Viennese Black Chamber, the Geheime Kabinets-Kanzlei. Kahn described the process involved:

The bags of mail for delivery that morning to the embassies in Vienna were brought to the black chamber each day at 7 a.m. There the letters were opened by melting their seals with a candle. The order of the letters in an envelope was noted and the letters given to a subdirector. He read them and ordered the important parts copied. All the employees could write rapidly, and some knew shorthand. Long letters were dictated to save

---

<sup>18</sup> all the Alberti information from *ibid.* p 90-94

time, sometimes using four stenographers to a single letter. If a letter was in a language that he did not know, the subdirector gave it to a cabinet employee familiar with it. Two translators were always on hand. All European languages could be read, and when a new one was needed, an official learned it... ..After copying, the letters were replaced in their envelopes and the envelopes resealed, using forged seals to impress the original wax. The letters were returned to the post office by 9:30 a.m.<sup>19</sup>

If only public services today could be so efficient! Apparently this process was repeated again in the evening with the letters being sent by the embassies that day. Also, the cryptanalytic team was also quite talented. The French ambassador is held to have commented that 'our ciphers of 1200 held out for only a short time against the cleverness of the Austrian decipherers.'<sup>20</sup>

### ***The Nineteenth century and the telegraph***

The invention of the telegraph changed cryptology forever. For the first time it was possible for other parties than the sender and or receiver to intercept a message with no possibility of discovery. This, combined with the fact that human clerks were doing the relaying, meant that it was necessary to have some sort of code. Thus, 'the great and widely felt need for secrecy awakened the latent interest in ciphers...'<sup>21</sup> The primary cipher used was the Vignère cipher, which unfortunately was broken in a general fashion (that is, independent of the key word) in 1863.

One solution to this was devised by Charles Wheatstone, and popularised by his friend Lyon Playfair, whose name it now uses. This cipher is similar in form to Polybius' checkerboard cipher in that the letters of the alphabet are arranged in a square arrangement, but this arrangement uses a key word, like so:

T	A	X	O	N	
M	Y	B	C	D	
E	F	G	H	I	J
K	L	P	Q	R	
S	U	V	Y	Z	

---

<sup>19</sup> *ibid.* p 104

<sup>20</sup> *op. cit.* 9, p 118

<sup>21</sup> *op. cit.* 3, p 111

This example uses TAXONOMY as the keyword. Next, to encode a short message such as THE HUNS ARE ATTACKING, we apply a number of simple rules. First, the plaintext is divided into pairs, TH EH UN SA RE AT TA CK IN GX. Then we look up each letter in the pair (called a **digraph**), and take the opposite corners of the rectangle so formed as the ciphertext. For example, TH becomes OE. If the two plaintext letters are on the same line, they are replaced with the letters one place to the right, thus EH becomes FI. If the letters are in the same column, they are replaced with the letters immediately below. Thus, GX becomes BP. So, the encoded message is OEFIAZTUIKXAAXMQDRBP. This has the advantage that the use of digraphs obscures single-letter frequencies.<sup>22</sup>

Also during this period lived Jean-Guillaume-Hubert-Victor-Francois-Alexandre-Auguste Kerckhoffs von Nieuwenhof. Known as Kerckhoffs, he published a book called *La Cryptographie Militaire*. This was an incisive summary of cryptography at that time, and Kerckhoffs also included six specific requirements of any cipher system:

1. The system should be, if not theoretically unbreakable, unbreakable in practice
2. compromise of the system should not inconvenience the correspondents
3. The key should be rememberable without notes and should be easily changeable.
4. The cryptograms should be transmissible by telegraph.
5. The apparatus or documents should be portable and operable by a single person.
6. The system should be easy, neither requiring knowledge of a long list of rules nor involving mental strain.<sup>23</sup>

These rules, somewhat reformulated, are still respected today. In particular a very important rule in modern cryptology is based on the second requirement. Secrecy should rest in the secrecy of the key, not of the system. This was shown decisively in the twentieth century, over both world wars.

## ***Pre-World War II***

The history of cryptology in the twentieth century is inevitably split in three by the Second World War. There is what happened before then, what happened during the war, and what has come after.

The First World War was the first war to be fought with the aid of radio. The problem with radio, from a military point of view, is that any message sent out over radio is very easy for an enemy to obtain. At least with telegraph lines there had to be a physical intrusion to listen to the signal. Also, this ease of interception can provide cryptanalysts with enough messages to be able to

---

<sup>22</sup> *ibid.* p 118-120

<sup>23</sup> *ibid.* p 126

extract useful frequency data, even for complex codes. Because of this, during the First World War it was seen that an army needed good cryptology to be competitive in the field. Some lucky strokes for the British early in the war allowed them to get hold of some German code-books, cracking the system wide open.

After the war, countries scrambled to update their cryptography, and to crack everyone else's, especially in the buildup to war in the late '30s. Before then, however came the work of William Friedman. Head of the Riverbank Laboratories' Department of Ciphers, he made two contributions that are absolutely invaluable to the study of cryptology. The first was a method of reconstructing a cipher alphabet without guessing any plaintext, by treating the frequency distribution of letters as just that, a distribution, amenable to the rapidly growing field of statistics. The importance of this cannot be overstated. As Kahn says, 'Friedman led cryptology out of the lonely wilderness and into the broad rich domain of statistics. He connected cryptology to mathematics.'<sup>24</sup> The other was a measure called the **index of coincidence**. This is the chance that two letters in a distribution are alike, or more simple, a measure of how like the normal distribution of frequencies a message's set of frequencies is. A high value indicates a monoalphabet, a low value an equal distribution.<sup>25</sup>

Another important development of the period between the wars was the rotor encryption device. This consists of a number of rotors, made of an insulating material, with a certain set or wiring connecting a number of points on each side. When the rotors are set up in series, the wiring dictates the encipherment of each plaintext letter. The rotors are also advanced some amount of steps each time, changing the wiring, and thus the enciphering alphabet for each letter of the plaintext. This solves some of the problems of earlier polyalphabeticity in that the key is very long and so repetitions are avoided.

This period also brought the invention of the only perfect encryption system, the one-time pad. This was invented by Joseph Mauborgne, a major in the US Army. Essentially, it is a sequence of randomly generated letters that are added to the plaintext, with each sequence being used only once. This creates perfect secrecy, because each key is used only once, avoiding attacks based on repetition of keys, and there are no systematic regularities in the enciphering alphabet for a cryptanalyst to exploit, and because each plaintext is thus equally likely to be the case. That is, if the enciphering letters were truly randomly generated, the only way to crack the message would

---

<sup>24</sup> *ibid.* p 189

<sup>25</sup> definition from *op. cit.* 34, p 68

be to try all possible alphabets. But this will also produce all possible messages of the same length as the original, so there is no way to tell which is the real one.

Why then is this system not in everyday use? Because of the difficulties inherent in it. It may sound easy to generate randomness, but generating numbers that are truly unpredictable is not easy. It must be accomplished by measuring a natural source of randomness, such as radioactive decay, which is expensive and time-consuming. Also, the pad sheets or letter sequences must be generated in advance, and both the sender and receiver must have a copy. It can be seen that in wartime, or in any time with a massive volume of messages being sent each day, this is simply not practical. However, one-time pads are still used when security is paramount.

### ***The Second World War***

The Second World War was a time of exponential growth in cryptology. As Kahn put it: 'The war worked no changes as basic as those of telegraphy... or of radio... Rather it enlarged, accelerated, intensified what was already there.'<sup>26</sup> Military forces discovered the importance of signal intelligence in an age of radio, of being able to know what your enemy's orders were, sometimes even before he did.

There is a great literature on cryptology and its use during the war, but the most famous story is most assuredly the story of the cracking of the Enigma code by the English.

The Enigma was a machine used by the Germans for encryption of military messages. Based on the rotor system, it was considered unbreakable by the Germans, and thus used for all levels of communication, with more complicated machines being used for higher-level communications. It consisted of a set of rotors, a keyboard and a plugboard. The plugboard was used to perform elementary scrambling of the ciphertext before the message went through the enciphering process. The rotors were originally set to a position given at the start of the message, which made cryptanalysis much easier. However, once this was realised, Enigma machines were issued with a codebook of daily keys, which told the receivers the initial settings of the rotors and the settings of the plugboard.

The success of the cracking efforts actually began with the Poles. Intelligence services in Poland were able to provide enough information for Polish cryptanalysts to construct a working model of the Enigma, and to invent a machine, which they called a bombe, which, given enough messages

---

<sup>26</sup> op. cit. 3, p 338

input, could arrive at a solution to the daily keys. This was when the Germans were still specifying the key at the start of each message. However, once the Germans switched to daily keys, the Poles had a very difficult time.<sup>27</sup> Once it seemed that war would certainly break out, the Poles gave the reconstructed Enigma and all their research to the English.

The nexus of the British efforts was the manor house at Bletchley Park. Over the war, this estate became the most successful cryptanalytic unit ever, even surpassing the Viennese Black chamber for efficiency.

At Bletchley Park were a large number of very talented men and women, but there are a few who stand out, and of them the one who stands out the most is Alan Turing. Partially, of course, this is because of his fame for other things, but, as may be seen from what he did, his fame for other ideas was interrelated with the work he did on cryptanalysis.

What Turing did that was so important was use regularities in the way Enigma enciphered messages, along with regularities in the messages sent, or cribs, to create a machine that would run through all of the possible solutions, and would cease searching when it found the correct solution. Thus, all that was required to determine the day keys was a message with a reasonably certain crib. The machines could be put to work on it, and within hours the machine would be able to deduce the day-key.<sup>28</sup> Later, this machine was refined into the Colossus Mark I, one of the first digital computers, which used a statistical method to crack much more complicated Enigma machine.

The Second World War was important for cryptology because the sheer volume of material to be analysed demanded that systematic methods be found for cryptanalysis. These advances also drove advances in cryptography. Some of these advances are reflected in new disciplines created around this time: information theory and complexity theory.

### ***Post World – War II Cryptology: Mathematical theories and computers***

In 1948, Claude Elwood Shannon published a paper in the *Bell Systems Technical Journal* named 'A mathematical theory of Communication', along with another paper, 'Communication theory in

---

<sup>27</sup> This info condensed from Garlinski J. *Intercept: The Enigma War*, J.M. Dent & Sons Ltd, London, 1979.

<sup>28</sup> from Singh, S. *The Code Book*, Doubleday, New York, 1999, p. 170-181

secrecy systems'. These papers outlined information theory and its application to cryptology respectively.<sup>29</sup>

The basic idea of information theory is that of measuring the amount of information conveyed in a message. This is defined as the **entropy** of the message. To use Schneier's example, the days of the week can be encoded with three bits: 001 for Monday, 010 for Tuesday, and so on up to 110 for Sunday, with 111 being unused. Therefore, a listing of the days of the week has slightly less than three bits of entropy, because the eighth combination is unused.

This sort of definition allows you to specify the amount of information conveyed by a language. English has a value somewhere between 1.0 and 1.5 bits per letter, depending on the text counted, for large numbers of letters. The amount of information it is possible to convey with language can also be defined, and is a function of the number of characters in the language. For English, this is around 4.7 bits/letter. This means that, in English, a large proportion of any message is redundant. Why this is okay will be explained shortly.<sup>30</sup>

However, in cryptology, it is desirable to have as little redundancy as possible, because the more redundancy you have in a text, the easier it is to find a decipherment for it. Shannon defined a measure, the **unicity distance**, as 'an approximation of the amount of ciphertext such that the sum of the real information (entropy) in the corresponding plaintext plus the entropy of the encryption key equals the number of ciphertext bits used.'<sup>31</sup> He also showed that ciphertexts longer than this distance are likely to have only one meaningful decryption, while those shorter than this are likely to have many equally valid decryptions, and therefore are more secure because there is no way to determine which is the correct one. The unicity distance is inversely proportional to the redundancy of the text.

The other mathematical theory that is of much use to modern cryptology is complexity theory. This gives a framework for considering how complex a problem and its solution are. Only the order of the complexity function is measured, because any other terms in the complexity function pale into insignificance with the size of the numbers generally being considered. Thus, problems are divided up into classes, based on the complexity of their solutions. Thus, some classes of problems have linear-order solutions, some have quadratic, or cubic, etc. solutions, and some

---

<sup>29</sup> op. cit. 3 p 443

<sup>30</sup> This data from Schneier (op. cit. 1), p 233-234

<sup>31</sup> *ibid.* p 235

have **exponential** solutions. The solutions of the orders of quadratic, cubic, and so on are called **polynomial** problems.

The inherent complexity of problems is defined with reference to the minimum amount of time and space required to solve the hardest instance of a problem on a Turing machine. Problems that are solvable with polynomial algorithms are called **tractable**, in that they can be solve in a 'reasonable' amount of time. Problems that cannot be solved in polynomial time are called **intractable**, or simply **hard**. These classes can be considered as extensions of one another; polynomial time-problems are a subset of non-polynomial time problems. The problems that are usually of interest to cryptologists are those that are in the area that is called **NP-complete** in this space. This area contains problems which are as hard as any in Non-polynomial space. The prototypical example is the Satisfiability problem: Given a propositional Boolean formula, is there a way to assign truth values to the variables that makes the formula true? Over 300 problems have been shown to be equivalent to this problem, including the Travelling Salesman (given  $n$  cities, with array of distances  $D(n,n)$ , what is the maximum number of cities the salesman can visit).<sup>32</sup>

### ***Public – Key Cryptography***

The invention of computers forever changed cryptology. The speed at which computers were able to perform calculations of any type made them very, very good at solving problems that would previously have been considered intractable.

The advent of computers, and of basic networking, created a need for an efficient, secure encryption system, that also dealt with the very large problem of key distribution. The problem of key distribution is the problem of getting the key to the recipient so they can decrypt the message. Singh put it another way, 'before two people can exchange a secret (an encrypted message) they must already share a secret (the key).'<sup>33</sup> Before, this problem had been solved by issuing authorised key books to authorised people. However, with the possibility of meeting a stranger on a computer network, this problem is much bigger.

In the 1970's, however, the problem changed. Whitfield Diffie and Martin Hellman changed cryptology forever by introducing the idea of an **asymmetric** encryption system. In this system, a message is encrypted with one key, and decrypted with another. This is the idea that is so

---

<sup>32</sup> from op. cit. 1, p237-242

<sup>33</sup> op. cit. 28, p 256

different. Before, all cryptology had been what is now called symmetric, or required the same key to encrypt and decrypt. Not only did Diffie and Hellman come up with this idea, they came up with a way to implement it, using hard problems in modular arithmetic to guarantee security. Because of the nature of modular arithmetic, it is easy to create a function that, if you know a number, you can calculate a result, but if you do not know the key number, the problem is unsolvable in NP time.

Singh used the analogy of colour as the key. Alice has a tin of paint of a particular colour, as does Bob. Eve wishes to find out the secret colours. Alice and Bob both take a litre of yellow paint and mix a litre of their secret colour in with it. Alice and Bob then send the tins to each other. Even if Eve manages to capture the pots, she has no way of knowing what the secret colours are, because they have been mixed with yellow and thus cannot be reobtained. Once Alice and Bob get the paint from the other person, they both add their own colour to the pot with the other person's and presto! they have the same colour, without exchanging enough information for Eve to figure out what is going on.

Currently many popular algorithms use the hard problem of factoring very large prime numbers to provide security. Each person generates a key pair, keeping one key secret and openly publishing the second. The secret key is called the **private** key and the openly published on the **public** key. By encrypting a message with a person's public key, the nature of the mathematical function means that only the private key will be able to decrypt it. Other advantages of this system include digital signing. By encrypting a message with her public key, Alice guarantees that the message is from her. By then encrypting a message Bob's public key, she makes sure that only Bob can read it. This eliminates the possibility of tampering with the message, or Eve managing to fool Bob into thinking she is Alice in order to eavesdrop.<sup>34</sup>

The history of cryptology has been a long and interesting story, of which I have only been able to present a very small part here, especially with regard to the events of the Second World War, simply because there is so much to tell, and if I told any more than the very brief outline, this paper would become a novel. However, all that aside, I feel that we have some common ground for examining the anatomy of cryptology as a discipline...

---

<sup>34</sup> material on asymmetric and public-key encryption from op. cit. 28 and op. cit. 1

## Understanding Cryptology – Occult Art to Modern Science?

Now that we share a conception of the history of cryptology, I can begin to explicate what makes cryptology interesting in a History and Philosophy of Science sense.

### ***Cryptology as a science***

Cryptology as a discipline consists of the twin, or reciprocal sciences of cryptography and cryptanalysis. Kahn pointed out that cryptography, being based in modern times on mathematical abstractions, is very much an analytic field, while cryptanalysis is synthetic, dealing as it does with 'the coarse rubble of reality', as he puts it.<sup>35</sup>

Both sciences of cryptology are thus similar to many other sciences. Cryptography is similar to pure disciplines such as mathematics, etc. while cryptanalysis is similar to the physical sciences in that it, at some point, is about data taken from the real world. However, both of these sciences do have something in common; they are both, in some sense, sciences of the artificial. Simon<sup>36</sup> gave four criteria for 'artificial' things, to be used in defining artificial sciences:

1. Artificial things are synthesized (though not always or usually with full forethought) by man.
2. Artificial things may imitate appearances in natural things while lacking, in one or many respects, the reality of the latter.
3. Artificial things can be characterized in terms of functions, goals, and adaptation.
4. Artificial things are often discussed, particularly when they are being designed, in terms of imperatives as well as descriptives.<sup>37</sup>

Simon is using the word 'synthesized' here, not only in its American spelling, but also in the sense of 'designed' or 'composed'.<sup>38</sup> The point of this for cryptology is that it is a science that studies human creations. This means that they are designed for a purpose (thus the point about imperatives as well as descriptives). I tend to disagree with Simon about the third point, in that

---

<sup>35</sup> op. cit. 3, p 410

<sup>36</sup> Simon, H.A. *The Sciences of the Artificial, Second Edition*, MIT Press, Massachusetts, 1981

<sup>37</sup> *ibid.* p 8

<sup>38</sup> see *ibid.* p 7

everything can be characterised in terms of functions, goals, adaptation (a.k.a. the basis of functionalist philosophy of mind.)

However, a point I feel that Simon does not make is that cryptology is, really, a science concerned with communication, and the obstruction of communication. It is somewhat paradoxical that a science can be concerned with the obscurement of the truth, or more accurately with discovering the truth about obscuring the truth. (How marvelously self-referential...)

As Kahn said, 'Cryptology is protection. It is to that extension of modern man – communications – what the carapace is the turtle, ink to the squid, camouflage to the chameleon.'<sup>39</sup> To this extent, cryptology is an artificial science, born of the study of human communication. Because of this, cryptology shares intimate ties with the discipline of information theory, and complexity theory, as I indicated in the history.

One thing I did not explicate in the history was the intimate relationship of cryptology with computers, not only on an operational level, but also on a cultural level, but more on this later. For now, it is enough to keep in mind that computers are in a large part descended from machines designed explicitly to work on cryptanalysis.

Now I would like to briefly look at cryptology in a philosophy of science sense, by looking at how it fits or fails to fit with the models of Popper and Kuhn. Cryptology has some interesting resonances with some of what each of these two are saying, which I am not sure other sciences have.

### ***Popper and Cryptology***

Popper's primary idea is encapsulated in his criterion of demarcation: science should make risky predictions, predictions that are possibly falsifiable. An argument that has been put forward against Popper relates to the impossibility of a single test falsifying the theory. This is because of the theory-loading of perception, and because of problems relating to the collection of accurate data for the test.<sup>40</sup> However, if we regard the creation of a cryptosystem in cryptology as an analogue of the postulation of a theory, interesting things happen. Firstly, because cryptosystems are written mainly in the language of mathematics, they inherit some of its properties, such as a

---

<sup>39</sup> op. cit. 3, p 455

<sup>40</sup> See Schuster, J. *The Scientific Revolution*, Schuster, Sydney, 1995, ch. 10 for a deeper explication of these problems.

more deductive structure. This is especially the case for cryptography, which is, as Kahn said, an analytic discipline. Because of this, in this discipline, a single result can falsify (render insecure) a theory (cryptosystem).

Cryptanalysis is the arm that more interests us on our Popperian quest, however. Dealing as it does with data culled from the world, it seems more relevant to Popper's point. Now if the theories a cryptanalyst makes in search of the decipherment of a text are the case, it will be very obvious, as the code will be deciphered, or not. This is a definite departure from other sciences.

In cryptology, the test data *can* speak for themselves, because the systems that create the observed phenomena, if they exist at all, can only really be said to be existent in the sense that a computer program is, as an enmattered formulable essence, to borrow a term of Aristotle's.<sup>41</sup> Thus measuring data does not really involve a measurement at all. In a sense, this is a second-order science, about relations of relations of ideas, that is meaningless without the relations of ideas that form its substrate.

### ***Kuhn and Cryptology***

Thomas Kuhn had a lot to say about the method of science.<sup>42</sup> The history of cryptology does exhibit some similarities to Kuhn's story of scientific revolutions. The science could certainly be considered to be in the pre-science era up until just before the Second World War, when Friedman began publishing papers seriously connecting cryptology with statistics and mathematics. I don't think the earlier work done by Kerckhoffs can really be considered the beginnings of the science, as his work did not gain wide acceptance straight away. However, World War II would seem to be a good example of normal science, with all the scientists having a common perceptual framework, and solving problems in the defined area. I think, also, that the idea of asymmetric cryptosystems did cause a revolution in the Kuhnian sense, because it forced people to rethink what had since been a basic assumption, that there must only be one key for both encryption and decryption.

Since then I think cryptology has seen another period of normal science develop. The field of asymmetric-key cryptology is only beginning to be explored; there's a lot of problems that are possible candidates for cryptosystems.

---

<sup>41</sup> from Aristotle, 'De Anima', *The Basic Works of Aristotle*, R McKeon ed. Random House, 1941, p 561

<sup>42</sup> I used Kuhn, T.S *The Structure of Scientific Revolutions*, 2<sup>nd</sup> Ed., Uni of Chicago Press, Chicago, 1970 as a reference for this portion of the paper.

---

## ***Cryptology as Culture***

The discipline of cryptology has some interesting cultural properties. In great part, these are similar to the properties of the computer science community, probably in great part because of the intimate linkage between the two.

One thing that cryptology does have is a very dry sense of humour. When a problem is classified as merely 'hard' or 'non-trivial', and by that it is meant that all of the computers invented by humanity would not be able to solve it before the heat death of the universe, there is certainly a humorous side to the use of these words...

The choice of a certain set of names to explicate the systems of cryptography is similar in many ways to the jargon of MIT-style 'hackers' by that meaning people who like to experiment with the limitations of systems, not those who like to break into computers. The names are chosen on an alphabetical basis, with the first two names beginning with A and B, while the eavesdropper's name begins with E, the trusted third party with T, and so on. All aimed at making the names mnemonic and transparent. This is where the similarity with hacker culture comes in, as this is a primary goal of hackish usage, transparency.<sup>43</sup>

## ***Cryptology and Politics***

As you have no doubt seen from the history, cryptology has always played a big part in politics, whether it be in wartime, or in diplomacy, or in domestic communications. With the proliferation of computer networks, the conflict between those who wish for secure cryptography to maintain privacy and those who are against it on the grounds it will allow for ease of criminal activity is growing.

Unfortunately, in cryptology as in many, many other fields, the US is the country that does a large proportion of the development and implementation of cryptosystems. The unfortunate thing about this is that cryptography is considered a munition by the US government, and thus those selling cryptography overseas are arms trafficking. This is the reason why software products available for download from Internet sites in the US must have a version with a lower strength of encryption (=smaller key). However, the crazy thing about this is that, once the program code is published in

---

<sup>43</sup> for more info on hackish culture, consult The Jargon File 4.2.0,  
<<http://www.tuxedo.org/~esr/jargon/jargon.html>>

a book, that code is in the public domain and thus can be distributed as you wish, but a disk with that code on it is considered a program, and thus a munition!<sup>44</sup>

As Kahn said, cryptography, or more correctly cryptanalysis, is for government 'the cheapest, the latest, and the truest source of information.'<sup>45</sup> To me it seems that the US government, and indeed the Australian Government, are allowing themselves to be dictated to by law enforcement authorities who cannot stand the idea that they might have to resort to other methods than intercepted communications to catch criminals. The attempted introduction of key-escrow solutions, where 'non-governmental' bodies have control of copies of *everyone's* keys, seems like an attempt to pacify people while retaining the ability to read their mail at will.

Speaking of this, it appears that a system to perform exactly this type of operation may already be in place. The ECHELON system, long considered to be a paranoid fantasy, now appears to be within the realm of possibility. A number of patents have been found, registered to the American NSA, which would appear to allow computers to perform the necessary operation on not only text, but also on voice (i.e. telephone calls etc.)<sup>46</sup> (!).

This sort of information really does indicate why, if private communications are desired, it is necessary to have good crypto. Schneier gives a number of reasons why you may want to communicate privately: '[you] may be planning a political campaign discussing taxes, or having an illicit affair. [You] may be designing a new product, discussing a marketing strategy, or planning a hostile business takeover. Or they may be living in a country that does not respect the rights of its citizens. They may be doing something that they feel shouldn't be illegal, but is.'<sup>47</sup> I definitely agree. The rights of the individual to private communication are more important than the government's ability to monitor those communications for subversion.

---

<sup>44</sup> op. cit. 1 p xxi

<sup>45</sup> op. cit. 3 p 340

<sup>46</sup> see Oakes, C. 'ACLU to spy on ECHELON',

<<http://www.wired.com/news/print/0,1294,32586.00.html>> for a report on some evidence associated with this, and <<http://www.aclu.org/echelonwatch/index.html>> for a more in-depth explanation of exactly what ECHELON is. See Schneier, B. 'The Crypto-Gram'

<<http://www.counterpane.com/crypto-gram-9912.html#ECHELONTechnology>> for an explanation of the patents and links to the actual patents themselves.

<sup>47</sup> op. cit. 1, p xx

But what can be done about this? A number of options have been considered apart from getting *very* strong encryption. One of the more interesting is the creation of 'data havens' or extraterritorial areas that have little to no regulation of cryptography, and allow for the anonymisation of communication passing through their borders.

A method for doing this was put forward by Neal Stephenson in his book, 'Cryptonomicon'. This involved finding a sovereign island in the Pacific, gaining the cooperation of the royal family, and creating a data haven deep inside a mountain, to protect from nuclear strikes. The data haven was intended to be for a number of things, including storing information on guerilla warfare to enable people in countries with oppressive governments to effectively resist. Also, it creates the possibility of an anonymous, digital, gold-backed currency for use in on-line transactions.

This would only be of marginal interest except that some of it has already begun to be made true! As of June, 2000, the company of Havenco has declared itself open for business as a 'collocation' provider, situated on the extraterritorial province of Sealand, near the United Kingdom. The royal family of the island is cooperating, and have only placed two limitations on material stored in the data haven: no providers of spam or child pornography. Anything else goes, however.<sup>48</sup>

### **Conclusion**

The study of cryptology has a long and colourful history; with some of the most colourful material being from this century.<sup>49</sup> In the last decade cryptology has become a very hot topic indeed, because of the proliferation of worldwide computer networks. I think that cryptology, as a science, has some very interesting properties that make it amenable to study by HPS practitioners. The insights gained from looking at the history of cryptology are invaluable in considering where cryptology should go, and more importantly, in communicating the importance of cryptology to non-technical people who have a genuine need to know what the hell is going on, viz. politicians. Only knowing cryptology can those who are involved in policy decisions make the right decisions.

---

<sup>48</sup> see [www.havenco.com](http://www.havenco.com) for details.

<sup>49</sup> I am firmly in the '21<sup>st</sup> century begins on 1<sup>st</sup> Jan 2001 camp'.

---

## References / Works Consulted

1. Aristotle, 'De Anima', *The Basic Works of Aristotle*, R McKeon ed. Random House, 1941, p 561
2. ECHELON Watch <<http://www.aclu.org/echelonwatch/index.html>>
3. Garlinski J. *Intercept: The Enigma War*, J.M. Dent & Sons Ltd, London, 1979.
4. Havenco Website <http://www.havenco.com>
5. Kahn, D. *The Codebreakers: The story of secret writing*. Abridged version, Signet, New York, 1973
6. Kuhn, T.S *The Structure of Scientific Revolutions, 2<sup>nd</sup> Ed.*, Uni of Chicago Press, Chicago, 1970
7. Oakes, C. 'ACLU to spy on ECHELON',  
<http://www.wired.com/news/print/0,1294,32586,00.html>
8. Padover, S. & Thompson, J.W. *Secret Diplomacy: Espionage and Cryptography 1500-1815*, Frederick Ungar, New York, 1963
9. Schneier, B. *Applied Cryptography Second Edition*, John Wiley & Sons, Toronto, 1996, Chapter 1 in particular for definitions.
10. Schneier, B. 'The Crypto-Gram' <<http://www.counterpane.com/crypto-gram-9912.htm#ECHELONTechnology>>
11. Schuster, J. *The Scientific Revolution*, Schuster, Sydney, 1995, ch. 10
12. Simon, H.A. *The Sciences of the Artificial, Second Edition*, MIT Press, Massachusetts, 1981
13. Singh, S. *The Code Book*, Doubleday, New York, 1999, p. 170-181
14. Sinkov A. *Elementary Cryptanalysis: A mathematical approach*, Random House, New York, 1968
15. 'The Jargon File 4.2.0', <<http://www.tuxedo.org/~esr/jargon/jargon.html>>