Forrest Timour

An Abridged History of Cryptography

In this modern day of information and technology, we sometimes take for granted the complex mathematics and tools that allow us to send sensitive data all over the world without worrying about breaches in confidentiality or integrity. The act of encoding and decoding information has a long and complex history dating all the way back to ancient Rome and Egypt. For thousands of years, humans have been inventing increasingly complex information-hiding schemes, and other humans have been breaking them. We've gone from very simple encodings that rely on a simple secret shared between parties to incredibly complex computer algorithms that are publicly known yet still secure, and rely only on the computational complexity bounds of the underlying mathematics as we understand them today.

Caesar Cipher

One of the first, most simple ciphers we know of is the Caesar cipher, dating back to sometime around the year 45 BC. The basic idea was to encode a plaintext (decoded message) by assigning each letter of the alphabet a number, and using a fixed offset to replace each letter of the ciphertext (encoded message). This is an example of a code that is extremely easy to break, because there are only 25 possible shifts that could have been used. However, because the method was not widely known, it would have appeared as gibberish to most people.

The following Caesar cipher has a fixed offset of 5, so each letter at some index i is replaced by the letter at $i + 5 \mod 26$. If we were to encode the plaintext word "coffee", with the input letters corresponding to the first row, the resulting ciphertext would be "htkkjj".

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
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e

The Caesar cipher is now regarded as the most widely recognized and simplest encryption techniques, and provides nothing in the way of security. It can easily be calculated by hand, and can easily be recognized in ciphertext form because the distribution of letters mimics that of the English language exactly.

Vigenère Cipher

The Caesar cipher was fairly easy to break, and in the mid-1500's the Italian cryptologist Giovan Battista Bellaso described a variation on it to make it more secure. It was later misattributed to the french cryptologist Blaise de Vigenère, hence the name. Two specific problems with the Caesar cipher as it was originally described were the small number of possible plaintexts and the statistical repetition of letters. The "small number of plaintexts" refers to the 25 possible decodings for a given ciphertext, from which it would be easy to guess the intended message. The statistical repetition of letters refers to the easy deduction that if "e" is the most-often used letter in the English language, and "k" is the most-repeated used letter in a ciphertext, the it is likely that each "k" is an encoded "e", and the shift is 6. The longer the ciphertext, the easier to decode using this method (law of large numbers). This practice of analyzing ciphertext to gain clues about the encrypted content (eventually decoding it) became an important part of cryptanalysis.

In order to overcome these problems, Bellaso used a series of multiple Caesar ciphers in repetition. In the following chart, the first row is the input row, the second row is the cipher for even-indexed letters (0, 2, ...), and the third row is the cipher for odd-indexed letters (1, 3, ...).

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
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j

If we encrypt the same plaintext we did before, "coffee", we get the ciphertext "hykpjo". This fixes both of the problems, to some degree. Instead of 25 possible decodings, there are $25 \times k$ encodings, where k is the number of ciphers used before they cycle back and are used again. The distributions of ciphertext letters still

appear if we partition by some index, but they are very much "flattened out" if we look at the ciphertext as a whole. Notice that "coffee" has two e's and two f's. In the original Caesar cipher, we had two k's and two j's, but now we have "kpjo", hiding the fact that letters have been repeated.

Cryptanalysis

Cryptanalysis is the practice of analyzing and attempting to breach cryptographically secured systems and messages. For as long as people have been inventing cryptographic schemes, others have been trying to break them. This sometimes takes the form of finding weaknesses in the algorithms and encryption schemes themselves, but sometimes it also focuses on human weaknesses in how the are implemented. Through the centuries, we have progressed from pen-and-paper, to analytic machines, to modern supercomputers in order to break the newest and most secure ciphers.

There are a few categories of attacks that can be carried out against a cryptographic scheme. A "ciphertext-only" attack is one where the attacker can read ciphertexts, but has no other information about the content of the messages or any way to gain any insight into the contents. A "known-plaintext" attack is one where the attacker is able to gain access to both the encrypted and unencrypted version(s) of one or more messages. A chosen-ciphertext or chosen-plaintext attack is the easiest to exploit, and the attacker is allowed to encrypt and decrypt arbitrary messages. This is realistic if, for example, the encryption mechanism is a physical machine, and one of them is obtained through espionage.

Attacks being carried out are typically very systematic, logical analyses of ciphertexts and distributions, and a touch of guesswork. This lends itself very nicely to automation, and computational tools have long helped in the analysis and decryption of ciphers. The metrics we typically use to measure the effectiveness of a decryption attempt are the time, amount of memory, and amount of plain/ciphertext data required for analysis. As technology improved, especially throughout the nineteenth and twentieth centuries, the speed of computation and amount of memory available for cryptanalysis increased greatly for automated methods.

The Enigma Code

One of the most famous cryptographic schemes ever used and broken was the german "Enigma Code", invented at the end of World War I and used for communication during World War II. The basic principle of the cipher was poly-alphabetic substitution, the same principle behind the Vigenère cipher, albeit much more complex. The enigma machines used internal rotors with electronic pathways in order to achieve an extremely long period before the keys were repeated. The period (number of substitutions before repetition begins) was 16,900, much longer than any messages that were sent. There were also two scramblers that could be set in 26^4 ways (on the order of 450,000), and a plugboard that allowed arbitrary pairs of letters to be interchanged. In the most complex machines, there were on the order of 151 trillion interchangings possible.

The enigma code was complex enough that no computational tool would be reasonably able to find a brute-force solution to cracking the cipher. However, there were a few shortcomings of the encryption. A letter could never be encrypted to itself, the exchanged letters were always reciprocal, and the design of the alphabet rings made it possible to work out the wheel order. However, none of these were turned into successful attacks against the cipher. The human component is often the weakest link in a secure system, and unsafe operating procedures eventually made it possible for enemies of the Nazis to decode some of the messages. The germans would choose a message key for each day, and transmit them with the same base indicator settings. The polish mathematician Marian Rejewski managed to decipher a few messages and was able to work out the logical structure of the machine.

After an exchange of information between the Polish and the British in preemption of the growing german threat, the British were able to improve on the earlier Polish efforts to break the code. In Letchworth, the mathematician and cryptologist Alan Turing, with the help of Harold Keen from the British Tabulating Machine Company, was able to invent an electromechanical computing device to help break the code called the *Bombe*. It worked to help identify the daily wheel order, reducing the number of possible combinations from about 17,500 to a more reasonable, small number. Eventually, with the combined efforts of the Americans and the British working to break the code, crucial intelligence was gathered and the tide of war was turned

and the germans were eventually defeated. This was one of the most important instances of cryptography having an effect on the course of history.

Symmetric- and Public/Private-Key Modern Cryptography

Even though the war was over, cryptography continued. As we moved into the modern digital age, secure encryption schemes became ever-increasingly important. With the popularization of the internet, we have started to use it to protect information in our everyday lives. As computers have grown exponentially in their processing power, we've gone from increasingly complex schemes that are hard to break, to simple (at least in concept) schemes that rely on the known computational hardness of certain mathematical problems. One such problem is the factoring of very large (thousands of bits) composite numbers into primes. Another is solving discrete logarithms, i.e. finding an x such that $g^x \equiv m$ for some known cyclic group generator g and some desired output m (often expressed with modular arithmetic and a generator co-prime to the modulus).

Modern algorithms usually rely on long, unique keys that are computationally infeasible to derive. These algorithms can be split into two groups; symmetric-key cryptography (where two parties share the same key), and asymmetric-key cryptography (where each party has a public key that is published and a private key that is kept secret).

One famous problem in cryptography is finding a secure way to exchange information over a public channel. In other words, in the modern internet, how can two parties exchange symmetric keys for use in private communication? Using the computational hardness of solving discrete logarithms, the Diffie-Hellman key exchange is a provably-secure way of generating a new symmetric key that is known by two parties. It was published in 1976 and is still widely used today. By abusing the fact that $(g^x)^y \equiv (g^y)^x \mod P$, and that neither x nor y can be recovered from sending g^x and g^y over a public channel (would involve solving discrete logarithms), it is possible for two parties to choose x and y, exchange two messages, and then calculate a unique number that can't be calculated efficiently. This is used as the symmetric key shared by two parties that creates the backbone of security for other cryptographic algorithms.

This is one well-known and commonly-used example of how simple but difficult computational problems are used to provide security today. One of the other most well-known algorithms today is the RSA cryptosystem, from 1978. RSA users create public keys based on two large prime numbers, and publishes the keys (keeping the primes secret). They also generate a private key used for decryption. The mathematics behind it use Euler's totient function and the large primes to find numbers e, d, and n such that $(m^d)^e \equiv m \mod n$. For encryption, a message is exponentiated modulo n, and the same encrypted message is exponentiated again to recover the original message. Both of these modern algorithms have stood the test of time so far, and have remained unbroken because of their strong mathematical roots. However, historically, many such schemes have been broken by user error, other secondary attack vectors, and bugs in the implementation of the algorithms. No breakthroughs are expected in the near future, but the struggle between crypto-designers and cryptanalysis is hardly over.