5.1 The History of Encryption

Encrypting communications is a very old concept. People have found the need to send private communications throughout the majority of human civilization. The need for privacy originally started from military and political needs, but has expanded beyond that. Businesses need to keep data private to maintain a competitive edge. People want to keep certain information, such as their medical records and financial records private.

Throughout human history, private communications meant encrypting written communications. Over the past century, this has expanded to radio transmission, telephone communications, and computer/Internet communications. In the past several decades, the encryption of computerized transmissions has actually become ordinary. In fact you can find computer/Internet communications encrypted more often than phone or radio. The digital environment makes implementing a particular type of encryption much easier.

Whatever the nature of the data you are encrypting, or the mode of transmitting data, the basic concept is actually quite simple. Messages must be changed in such a way that they cannot be read easily by any party that intercepts them but can be decoded easily by the intended recipient. In this section, a few historical methods of encryption will be examined. Note that these are very old methods, and they cannot be used for secure communication today. An amateur could easily crack the methods discussed in this section. However, they are wonderful examples for conveying the concept of encryption without having to incorporate a great deal of math, which is required for the more complex encryption methods.

5.1.1 The Caesar Cipher

One of the oldest recorded encryption methods is the Caesar cipher. This name is based on a claim that ancient Roman emperors used this method. This method is simple to implement, requiring no technological assistance.

You choose certain numbers by which you shift each letter of a text. For example, if the text is “**A cat”** and you choose to shift by two letters, then the message becomes “**C ecv”**. Or, if you choose to shift by three letters, it becomes “**D fdw”**.

In this example, you can choose any shifting pattern you want. You can either shift to the right or to the left by any number of spaces you like. As this is a simple method to understand, it makes a good starting point to your study of encryption. It is, however, extremely easy to crack. You see, any language has a certain letter and word frequency, meaning that some letters are used more frequently than others. In the English language, the most common single-letter word is "**a**". The most common three-letter word is "**the**".

Knowing these two characteristics alone could help you decrypt a Caesar cipher. For example, if you saw a string of seemingly nonsense letters and noticed that a three-letter word was frequently repeated in the message, you might easily guess that this word was "**the**"—and the odds are highly in favour of this being correct.

Furthermore, if you frequently noticed a single-letter word in the text, it is most likely the letter "**a**". You now have found the substitution scheme for **a, t, h,** and **e**. You can now either translate all of those letters in the message and attempt to surmise the rest or simply analyse the substitute letters used for **a, t, h,** and **e** and derive the substitution cipher that was used for this message. Decrypting a message of this type does not even require a computer. Someone with no background in cryptography could do it in less than ten minutes using pen and paper.

Caesar ciphers belong to a class of encryption algorithms known as substitution ciphers. The name derives from the fact that each character in the unencrypted message is substituted by one character in the encrypted text.

The particular substitution scheme used (for example, 12 or 11) in a Caesar cipher is called a substitution alphabet (that is, b substitutes for a, u substitutes for t, etc.). As one letter always substitutes for one other letter, the Caesar cipher is sometimes called a mono-alphabet substitution method, meaning that it uses a single substitution for the encryption.

The Caesar cipher, like all historical ciphers, is simply too weak for modern use. This example is to help you understand the concepts of cryptography.

5.1.2 ROT 13

ROT 13 is another single alphabet substitution cipher. All characters are rotated 13 characters through the alphabet. For example the phrase “**A CAT”** will become “**N PNG”**.

5.1.3 Multi-Alphabet Substitution

Eventually, a slight improvement on the Caesar cipher was developed, called multi-alphabet substitution (also called polyalphabetic substitution). In this scheme, you select multiple numbers by which to shift letters (that is, multiple substitution alphabets). For example, if you select three substitution alphabets (12, 22, 13), then “**A CAT”** becomes “**C ADV”.**

Notice that the fourth letter starts over with another 12, and you can see that the first A was transformed to C and the second A was transformed to D. This makes deciphering the underlying text more difficult. Although this is harder to decrypt than a Caesar cipher, it is not overly difficult to decode. It can be done with simple pen and paper and a bit of effort. It can be cracked quickly with a computer. In fact, no one would use such a method today to send any secure message. This type of encryption is considered very weak.

Multi-alphabet ciphers are more secure than single-substitution ciphers. However, they are still not acceptable for modern cryptographic usage. Computer-based cryptanalysis systems can crack historical cryptographic methods (both single alphabet and multi-alphabet) easily. The single-substitution and multi-substitution alphabet ciphers are discussed to show you the history of cryptography, and to help you understand how cryptography works.

5.1.4 Rail Fence

All the preceding ciphers are substitution ciphers. Another approach to classic cryptography is the transposition cipher. The rail fence cipher may be the most widely known transposition cipher. You simply take the message you wish to encrypt and alter each letter on a different row. So “**attack at dawn”** is written as

A tc a dw

ta k ta n

Next, you write down the text reading from left to right as one normally would, thus producing

atcadwtaktan

In order to decrypt the message, the recipient must write it out on rows:

A tc a dw

ta k ta n

Then the recipient reconstructs the original message. Most texts use two rows as examples; however, this can be done with any number of rows you wish to use.

5.1.5 Vigenère

Vigenère is a polyalphabetic cipher and uses multiple substitutions in order to disrupt letter and word frequency. Let us consider a simple example. Remember a Caesar cipher has a shift, for example a shift of +2 (two to the right). A polyalphabetic substitution cipher would use multiple shifts. Perhaps a +2, –1, +1, +3. When you get to the fifth letter, you simply start over again. So, consider the word "**Attack"**, being encrypted

A (1) + 2 = 3 or C

T (20) –1 = 19 or S

T (20) +1 = 21 or U

A (1) +3 = 4 or D

C (3) +2 = 5 or E

K (11) –1 = 10 or J

Therefore, the ciphertext is "**CSUDEJ"**. Given that each letter has four possible substitutions, the letter and word frequency is significantly disrupted.

Perhaps the most widely known polyalphabetic cipher is the Vigenère cipher. This cipher was actually invented in 1553 by Giovan Battista Bellaso, though it is named after Blaise de Vigenère. It is a method of encrypting alphabetic text by using a series of different mono-alphabet ciphers selected, based on the letters of a keyword. Bellaso

added the concept of using any keyword one might wish, thereby making the choice of substitution alphabets difficult to calculate.

5.1.6 Enigma

It is physically impossible to discuss cryptography and not mention Enigma. Contrary to popular misconceptions, the Enigma is not a single machine but rather a family of machines. The first version was invented by German engineer Arthur Scherbius near the end of World War I. It was not used just by the Germans, but by several different militaries also.

Certain encrypted military texts using a version of Enigma were broken by Polish cryptanalysts Marian Rejewski, Jerzy Rozycki, and Henryk Zygalski. The three basically reverse engineered a working Enigma machine and used that information to develop tools for breaking Enigma ciphers, including one tool named the ‘cryptologic bomb’.

The core of the Enigma machine was the rotors, or disks, that were arranged in a circle with 26 letters on them. The rotors were lined up. Essentially, each rotor represented a different single substitution cipher. You can think of the Enigma as a sort of mechanical polyalphabetic cipher. The operator of the Enigma machine would be given a message in plaintext and then would type that message into Enigma. For each letter that was typed in, Enigma would provide a different ciphertext based on a different substitution alphabet. The recipient would type in the ciphertext, getting out the plaintext, provided both Enigma machines had the same rotor settings.

There were actually several variations of the Enigma machine. The Naval Enigma machine was eventually cracked by British cryptographers working at the now famous Bletchley Park. Alan Turing and a team of analysts were eventually able to break the Naval Enigma machine. Many historians claim this shortened World War II by as much as two years.