

The so-called “encryption race” is a complicated issue. Eavesdropping has been a staple among police forces for centuries and is now an anchor in the fight against government abuse of power, corporate espionage, and terrorism. Despite their own need for secure communication channels, many law enforcement agencies view cutting-edge encryption as the last refuge of the talented criminal elite — including many culprits hiding inside seemingly reputable governments and businesses. Who will win this ideological conflict remains to be seen, but the race that inspired it doesn’t look to be slowing down anytime soon.

BASIC CONCEPTS

Apocryphally, encryption began with Julius Caesar. Not trusting the messengers he used to send mail to his allies, Caesar wrote every message by hand, then copied it with each letter shifted one or more positions in the alphabet: “A” became “D,” “S” became “V,” and so forth. To the messengers, the letters looked like gibberish — they could only be read by someone who knew the “cipher” (Caesar’s method of shifting each letter by a set number of positions), as well as the “encryption key” (the number of positions to shift each letter). This was allegedly the first “cryptosystem,” or “cipher system,” a method of disguising an original message — called “clear text” or “plain text” — so that only those with the proper information could make sense of the disguised version, which is also known as “cipher text” or a “cryptogram.”

Several related disciplines come together in the study of ciphers and codes. “Cryptography” is the science of making them while “cryptanalysis” is the science of breaking them. These fields are jointly referred to as “cryptology.” The equipment used in the process is called “cryptomaterial” or “cryptosystems,” and the process itself is called “cryptosecurity.”

There is a contrast between ciphers and codes. A cipher manipulates a message by substituting letters of the alphabet, while a code manipulates a message by substituting words or phrases. Either must be read using cryptography or the proper key.

TRANSPOSITION

Rearranging the letters in a message is called “transposition.” This technique produces an anagram that is more secure as the message increases in length. One example is the “rail fence” system, in which a message is staggered between two or more lines, the letters spread alternately between them. For example, “Richard Poole is a bloody maniac” would look like this...

```
R C A D O L I A L O Y A I C
  I H R P O E S B O D M N A
```

Then the second and later lines are added to the end of the first. In this case...

```
RCADOLIALOYAICHRPOESBODMNA
```

The message could be read by reversing the process.

Another example is “scytale,” which dates back to the fifth century B.C. This system calls for a strip of parchment or leather to be wrapped around a round or polygon-cut dowel. A message is written horizontally across the strips, which are then removed from the dowel. Read from top to bottom, the strips mean nothing, but when they’re wrapped around another dowel of the same shape and diameter, they reform the secret missive. The strip could then be hidden along the inside of a belt or in the lining of a hat.

SUBSTITUTION CIPHERS

Replacing each letter in a message with another corresponding letter is called “substitution.” For example, the “Caesar shift cipher” replaces every character with the letter three places later in the alphabet (wrapping the alphabet around from Z to A). Thus, the message “Alex Kole owns the night” would read “DOHA NROH RZQV XKH QLJX.” This technique requires all cipher users to possess a key showing the translation of letters.

On its own, the Caesar cipher isn’t very secure, but if the alphabet is rearranged before it is applied, this simple cipher theoretically becomes far more difficult to crack. For example, if the substitution alphabet were reordered as follows...

```
MGZDARTBVWKXYFENHCOUQLJIPS
```

...then the same message, “Alex Kole owns the night,” would read “MXAI KEXA EJFO UBA XVTBU.” The words can be merged together into one unbroken stream for even greater security: “MXAIKEXAEJFOUBAXVTBU.”

Another variation of this involves choosing a key word or phrase, such as “Rear Window,” removing all the repeated letters (“REAWINDO”), and lining the rest of the alphabet behind the result...

```
REAWINDOBCFGHJKLMNPQSTUVXYZ
```

Thus, only the key word or phrase is required to read messages created with the cipher in question. This also allows for easy memorization.

Countless other options follow. Unfortunately, a technique called frequency analysis allows for relatively easy decryption by studying how often letters are used in substitute cipher text. In the English language, the letter “e” shows up approximately 12–13% of the time, whereas “q” and “z” are very rare, appearing far less than 1% of the time. An examination of substitution cipher text tends to reveal certain patterns based on these established percentages, reproducing the cipher key one letter at a time. This process applies best to lengthy samples where the average appearance of letters is less likely to deviate from the norm, and tends to produce complete keys in a landslide — all at once right after a few letters have been discovered.

Substitution ciphers developed after frequency analysis are more inventive. One example assigns a letter to each of 26 numbers ranging from 1–99, leaving all the other numbers as “nulls” to be ignored by an intended recipient. The nulls can be sprinkled throughout an encrypted message, leaving those studying it perplexed about its true length and composition. Another introduces a “dowbleth” symbol in place of the first of two side-by-side identical letters, reducing the chance that they’ll be spotted. The Great Cipher of Louis XIV uses a set of 587 numbers in place of French syllables.

A method that tries and in the end fails to elude frequency analysis is the homophonic substitution cipher, which replaces each letter in the alphabet with one or more symbols or numbers, depending on the letter’s frequency. The letter “e,” for instance, which shows up approximately 12–13% of the time, is replaced 12 different ways, while “r,” which shows up only 6% of the time, is replaced 6 different ways. Unfortunately, the study of extremely strict letter combinations, such as “q” followed by “u,” can yield lists of the replacements in each case, and the cipher begins to unravel.