Cracking the code

How do you keep a secret? One way is esczfrs ncjaezrclasj.* If you understood that, you already may know a little about codes and ciphers.

Codes and ciphers have been used throughout history whenever people wanted to keep messages private.

In American history, George Washington sent coded messages to his agents, and the Culper Spy ring used codes to communicate with each other. Members of the Continental Congress also used code in their documents.

During World War II, America and the allies used the Enigma cipher machine to read German secret messages, while the US Marine Corps used the Navajo language to create an unbreakable code.

What's the Difference Between Codes and Ciphers? Though often used interchangeably, the terms codes and ciphers are very different.

A code changes the meaning of a word or phrase by replacing it with a different word or phrase to make a message secret. A cipher, on the other hand, makes a word or phrase secret by changing or rearranging the individual letters in a message.

Together, codes and ciphers are called encryption. The art of writing and solving codes and ciphers is called cryptography: breaking them is cryptanalysis.

For more than 3,000 years people have encrypted messages to keep their communications secret. Encryption is still used today, although it's much more sophisticated from the simple encryption from our past.

Cracking the code

Simple Ciphers: First off, to make a successful cipher, you'll need two things: an algorithm (mathematical equation) and a key to encrypt and decrypt the information. The key must be kept secret, known only by the creator of the message and the person whom the message is for.
You may be familiar with one of the most basic ciphers, which is often used with the secret decoder rings found inside cereal boxes or in toy stores. That's called a substitution cipher: We used that type of cipher in the secret message at the top of this briefing!

There are various substitution ciphers, but one of the easiest is the Caesar cipher, also known as the shift cipher.

This cipher is named after the Roman Emperor, Julius Caesar, who is said to have used this simple cipher to communicate with his army. To secure his messages, Caesar shifted the letters of the alphabet and sent messages that looked like scrambled text to those who did not hold the key.

The recipients of his message knew the letter shift algorithm and could easily decipher the message – once they knew how many letters to shift for the key.

But these simple ciphers, though fun to use, are not secure.

In a modern world, every time we use an ATM card or type in a computer password, we encounter advanced encryptions. Complex encryption is needed to secure intelligence secrets too.

Complex Cryptography: A great example of a complex encryption using codes and ciphers together comes from way back in World War II. The Germans used a device called Enigma, a cipher machine, to develop nearly unbreakable codes for sending messages. Enigma's settings offered 158,000,000,000,000,000,000 possible solutions, yet the Allies were eventually able to crack its secrets.

The Enigma machine was created by the Dutch to communicate banking secrets. The Germans bought the machine in 1923 for intelligence purposes. Soon after, Polish intelligence found an Enigma machine

Cracking the code

at a market and they got a codebook for it from a French spy. They began to try and crack the German's encryption (technically they were enciphering codes, also known as double encryption). However, when Poland was overrun by Germany in 1939, Poland realized they wouldn't be able to solve the encryption in time, so they gave all the information they had to their British and American allies.

By end of the WWII, we were able to read 10 percent of all German Enigma secret messages! It might not sound like a lot, but being able to read just 10 percent of these messages helped us win the war.

Enigma was just the beginning. In today's world—where people keep and share secret data digitally—encryption has become incredibly complex.

There are still some pretty amazing codes outside of the digital and computer realm, however.

One of the most secret codes is in a piece of artwork at CIA's Headquarters! It's called Kryptos. It's been on display in our headquarters courtyard for nearly 30 years. In that time, no one has ever fully deciphered Kryptos' coded message.

Dare to try? KRYPTOS

If you want to start on some easier codes and ciphers before tackling Kryptos, visit the Spy Kids games section.

Note: *esczfrs ncjaezrclasj translates to "through cryptography" using the Caesar cipher. With this simple cipher, we shifted the alphabet by 11 places, so A equals L, B equals M, etc.