The Caesar Cipher

The Caesar cipher is one of the earliest known and simplest ciphers. It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on. The method is named after Julius Caesar, who apparently used it to communicate with his generals.

In this example, let's try a shift of 5. We wrap around to "A" again when we reach "Z" as shown in the second row.

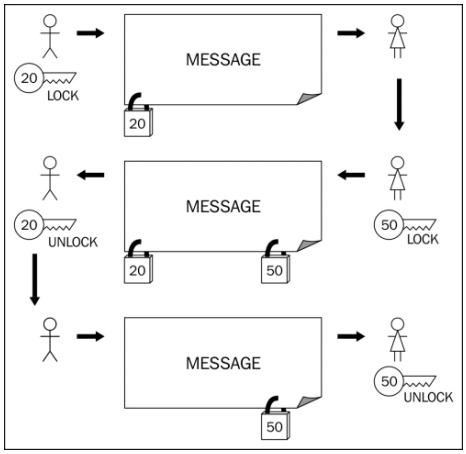
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

U	V	W	X	Y	Z
Z	A	B	C	D	E

In the table above, the original letters are in the top row, and the "scrambled" letters in the bottom row.
The word JULIUS becomes OZQNZX.

In Julius Caesar's time, those that could read were few, and so to figure out a message would be difficult, and the message itself would not make sense. Today, a typical reader could decipher the text with a bit of time. It would still take a few minutes of sorting out. For computers this is an easy task. For security of the message a different means must be used. This method relies on 25 different combinations. Today's computer communications use 128 bit (3.4×10^{38} combinations) which computers would take a very long time (100+ years) to decipher without the key.

A neat feature of using coded messages is that you don't need to send the shift number (called a KEY). As an example of Three Pass Protocol (developed by Adi Shamir in 1980), you send a message like this: Essentially, you send a message that is encoded with your key. The person receiving the message then encodes the message with their key and sends it back to you. You decode the message with your key, which leaves the message still scrambled because of the key that the receiver put on it. Now, your scrambling is gone, but their scrambling still keeps the message ciphered. When they get the message back, they only need to get rid of their scrambling and the message is readable again.



The problem with this is that if somebody can see all the communications, then they can see what changes have been made. Comparing changes can reveal the key. This process is called "Man in the Middle Attack"

Sender:
ATTACK THE CASTLE → CVVCEM VJG ECUVNG (KEY IS 2)
Send the locked encryption

Receiver:
CVVCEM VJG ECUVNG → HAAHJR AOL JHZASL (KEY IS 5)
Send back the double encryption

Sender:
HAAHJR AOL JHZASL → FYYFHP YMJ HFXYQJ
Send the unlocked encryption

Receiver: FYYFHP YMJ HFXYQJ → ATTACK THE CASTLE
Read the message