Caesar's cipher is the oldest method of cryptography commonly accepted by history. It consists of a mono-alphabetic substitution: each letter is replaced ("substitution") by a single other letter ("mono-alphabetic"), according to a certain shift in the alphabet or in an arbitrary way. Caesar used to use an offset of 3 letters: A becomes D, B becomes E, C becomes F, etc. He therefore wrote his message normally, then replaced each letter with the one that corresponded to it.