the public receivers: hence the name of a subliminal channel. Clearly subliminal receivers must have private information not known to public receivers—and as we will see, the nature of this private information provides a natural classification for subliminal channels.

Before discussing subliminal channels in detail, though, it may be useful to consider the simplest possible example of such a channel, i.e., one that can only communicate a single subliminal bit for each cipher text transmitted. To realize such a channel, assume that there exists a cryptoalgorithm with the unusual property that for each plaintext there are two possible ciphertexts—both of which decrypt unambiguously to the same plaintext. Also assume that all of these pairs of cipher texts can be separated easily into two classes—say "odd" and "even"—and that it is feasible for the transmitter to choose and for the subliminal receiver to recognize the cipher class used to communicate a particular plaintext. Given a crypto channel satisfying these conditions, an unconditionally secure one-bit (per cipher) subliminal channel is possible using Vernam encryption to conceal the subliminal bit. To set up such a channel, prior to using it the transmitter and receiver secretly share a one-time key consisting of a sequence of randomly chosen bits: 1's and 0's. They also agree on both an encoding and on an encryption/decryption rule. For example, an odd cipher is to be decoded as a 1 and an even cipher as a 0. To hide a bit, b_i, in the subliminal channel using this rule, the transmitter forms the exclusive or of the i-th bit of the key with the subliminal bit and sends the odd or even cipher depending on whether $b_i \oplus k_i$ is a 1 or a 0, respectively. The subliminal receiver reverses this procedure to recover b_i. Both public receivers and the subliminal receiver decrypt the cipher—irrespective of whether it is odd or even—to recover the plaintext, however, the subliminal receiver has received one additional bit of information. Even if someone suspects that the subliminal channel is being used and even if he knows the subliminal bit, b_i, that the transmitter wishes to communicate, it is impossible for him to detect whether the channel is in use or not. This follows from the unconditional security of Vernam encryption when using a one-time key having the same symbol equivocation as the symbols in the message (the subliminal bit in this case). This one-bit subliminal channel generalizes in an obvious—but far from trivial—way, if for each plaintext there are k possible ciphers which can be easily partitioned into k classes, etc. In a series of papers [5,6,7], Simmons showed how to construct crypto channels with these properties.