For more than a quarter century William Safire has been writing his weekly “On Language” column for the New York Times. In one of his earliest columns he looked askance at President Carter's use of the term “encrypt” in a speech because Safire thought it was just a highfalutin substitution for the more plainspoken “encode.” It isn’t. I knew Safire was wrong because I was using cryptosystems as a US Navy radioman before today’s cypherpunks were born. So I wrote Safire a letter correcting his English.

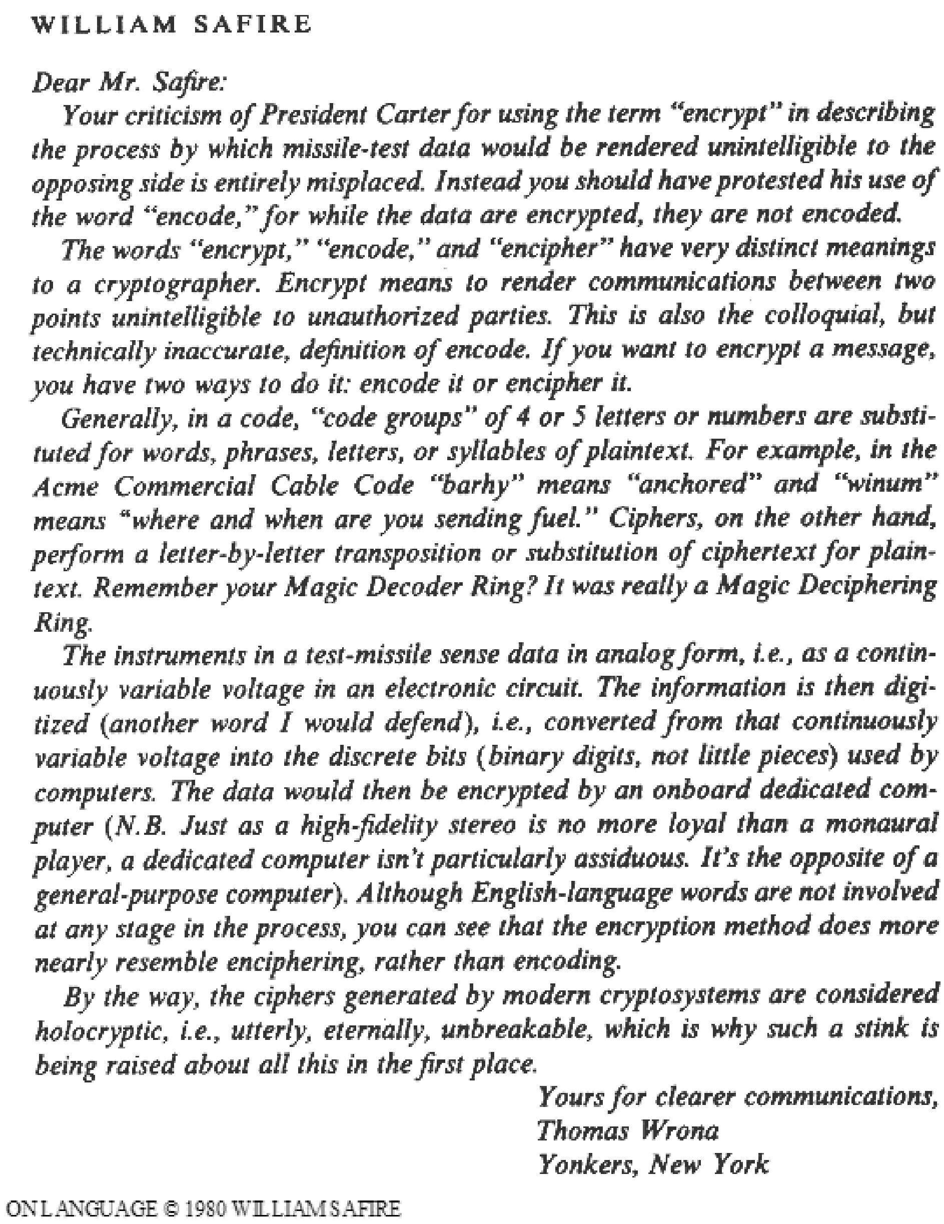
He never mentioned my letter in his column but some months later I got a letter from Times Books asking for my permission to use my letter in an upcoming book. The book would also be entitled *On Language* and it would consist of his columns and letters his readers wrote to him. I excitedly agreed.

A few months after that I was waiting for a date on 57th Street when I spied the book in the window of a Barnes and Noble store. I rushed into the store, grabbed a copy of the book, flicked to the index and saw my name. I let out a whoop and bought the book on the spot. It was a great date. And the first time my name was in a book more interesting than the white pages.

Tom Wrona

hire.tom.wrona@gmail.com

http://wrona.squarespace.com



WILLIAM SAFIRE

Dear Mr. Safire:

Your criticism of President Carter for using the term “encrypt” in describing the process by which missile-test data would be rendered unintelligible to the opposing side is entirely misplaced. Instead you should have protested his use of the word “encode,” for while the data are encrypted, they are not encoded.

The words “encrypt,” “encode,” and “encipher” have very distinct meanings to a cryptographer. Encrypt means to render communications between two points unintelligible to unauthorized parties. This is also the colloquial, but technically inaccurate, definition of encode. If you want to encrypt a message, you have two ways to do it: encode it or encipher it.

Generally, in a code, “code groups” of 4 or 5 letters or numbers are substituted for words, phrases, letters, or syllables of plaintext. For example, in the Acme Commercial Cable Code “barhy” means “anchored” and “winum” means “where and when are you sending fuel.” Ciphers, on the other hand, perform a letter-by-letter transposition or substitution of ciphertext for plaintext. Remember your Magic Decoder Ring? It was really a Magic Deciphering Ring.

The instruments in a test-missile sense data in analog form, i.e., as a continuously variable voltage in an electronic circuit. The information is then digitized (another word I would defend), i.e., converted from that continuously variable voltage into the discrete bits (binary digits, not little pieces) used by computers. The data would then be encrypted by an onboard dedicated computer (N.B. Just as a high-fidelity stereo is no more loyal than a monaural player, a dedicated computer isn’t particularly assiduous. It’s the opposite of a general-purpose computer). Although English-language words are not involved at any stage in the process, you can see that the encryption method does more nearly resemble enciphering, rather than encoding.

By the way, the ciphers generated by modern cryptosystems are considered holocryptic, i.e., utterly, eternally, unbreakable, which is why such a stink is being raised about all this in the first place.

Yours for clearer communications,
Thomas Wrona
Yonkers, New York