

When to Hyphenate Phrases Such as “Public Key”

Kathleen Ward

Phillip Rogaway

University of California, Davis

CRYPTO '98 Rump-Session Rant

1. Background

In English, not only can adjectives modify nouns (as we all learned in school), but also nouns, in unchanged form, can modify other nouns. An example is *encryption function*, where *encryption* is the noun that modifies *function*. This “functional shift”—a change in the function of a word without a corresponding change in form—is a conspicuous (and sometimes detested) characteristic of contemporary English.

Things can get quite complex. In technical writing it is not uncommon for long strings of nouns and adjectives to, as unit, modify other nouns. Indeed papers on cryptography are full of expression like *non-interactive zero-knowledge proof of knowledge*, *universal one-way hash function* or *adaptive chosen-message attack*.

In such contexts, nonuse or misuse of hyphens can make for less clear writing. Is a *weak key membership test* supposed to be a weak test for key membership or a test for weak-key membership?

The first author once held the job title of

`international equalization compensation information officer.`

We defy the reader to figure out what that was supposed to mean without having some idea of what was the job! (The job was to figure out how much it costs to live like a stereotypical middle-class US-citizen in various cities of the world.)

2. The “Rule”

The relevant rules on what to hyphenate are actually quite simple:

(a) When a term like *public key* is used preminally (that is, before a noun), use a hyphen:

`a public-key encryption scheme`

This use of the hyphen shows that the words *public* and *key* belong together and jointly modify the N-N *encryption scheme*. The use of the hyphen avoids the (admittedly far-fetched) reading of *public* as modifier for a key-encryption scheme.

(b) If *public key* is used by itself as a noun, it is not hyphenated:

Extract the public key from the certificate.

(c) In the somewhat unusual cases in which a term like *public key* is used to modify a noun, but is not positioned before a noun, it is not hyphenated.

Our encryption scheme, public key in nature, does not require the sender and receiver to share a secret.

Here are a few more examples where a hyphen is appropriate:

chosen-ciphertext attack	block-cipher design
key-distribution protocol	secret-sharing scheme
related-key attack	zero-knowledge proof

and where one isn't:

a very long secret key
L is in zero knowledge
techniques for secret sharing

We comment that a few set phrases would seem to deserve a hyphen by the rule above, but invariably do not get one. These include *data origin authentication* and *message authentication code*. The failure to hyphenate such terms can be due to historical accident, widespread usage, or aesthetic sensibilities. We do not suggest to hyphenate such terms; the hyphenation rules above are most appropriately applied for terms which have been haphazardly treated in the literature, or terms which are new or obscure.

3. Avoiding Ugly Sequences of Modifiers

The problem of noun modifier “dis-ambiguation” has some natural remedies. One is that, over time, the words tend to get “spelled solid.” For example, we all write *plaintext* and *ciphertext*, not *plain-text* and *cipher-text*. And by now *pseudorandom* seems to be preferred by many people over *pseudo-random*.

Another way we deal with this problem is through acronyms. Within an established context, acronyms like CCA (chosen-ciphertext attack), KDC (Key Distribution Center), NIZK (non-interactive zero knowledge), and VSS (Verifiable Secret Sharing) seem to enhance readability and neatly eliminate those unsightly hyphens.