Clarification of Encryption Terminologies and Math Notations

Hi, All:

It seems some students do not understand the encryption terms I introduced in class clearly. Here I want to clarify it.

**Notation Assumption Used in Lecture and Dr. Kurose's Networking Book:**

For a message $m$, $H(m)$ represents the hash value of the message by the hash function $H()$. $K(m)$ represents the encrypted message that is encrypted by the key $K$. $K_A^-$ represents node A's private key. $K_A^+$ represents node A's public key. If there is no "+" or "-" superscript, the key $K$ represents a symmetric encryption key. CA refers to "Certificate Authority".

**Terminologies:**

- **Message Digest** (or called **Fingerprint**) of a message $m$: $H(m)$
- **Digital Signature** of a message $m$ signed by node A: $K_A^-(H(m))$
- **Digital Certificate** (or simply called **Certificate**) of node B: $K_{CA}^-(K_B^+)$

The definition of digital certificate above is a conceptual and simplified notation. In the real world Public Key Infrastructure used by WWW, a Digital Certificate of a webserver B not only contains B's public key, but also contains many other text information (the server B's organization, the CA's official name/ID, the validation time, etc.). Therefore, in the real world, the actual Digital Certificate of a node B will be:

$$K_{CA}^-(H(\text{certificateContent}))$$

where the 'certificateContent' includes: $\text{certificateContent} = \{K_B^+, \text{text}\}$. And the 'text' includes all the text information of the certificate mentioned above.