- According to the textbook notation, how to represent a node A's digital signature? Digital certificate? Message digest?

Note Title 11/27/2013

digital signature: $K_A^-(H(m))$

digital certificate: $K_{CA}^-(K_A^+)$

message digest: $H(m)$ $H()$: { MD5, SHA-1

---

① ②

$p(1-p)\cdot p + (1-p)\cdot p\cdot p = 2p^2(1-p)$