Order	Date	Student ID	Name	Paper selection on SCA
7	Oct. 19	20093022	구동영	Strength of Two Data Encryption Standard Implementation under Timing Attacks
6	Oct. 19	20093605	황두호	Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems
5	Oct. 19	20103442	이동욱	An Implementation of DES and AES, Secure against Some Attacks
3	Oct. 14	20103576	정도영	A Timing Attack against RSA with the Chinese Remainder Theorem
2	Oct. 14	20104193	박이재	Power Analysis, What is now Possible …
1	Oct. 14	20105316	나해영	Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems
8	Oct. 19	20107114	김동욱	Cache-timing attacks on AES
4	Oct. 14		김기성	Examining smart-card security under the threat of power analysis attacks