

Presentation Topics:

1. In the future will biometric authentication methods be useful? Explain some of the attacks could be mounted?
2. Choose one physical tamper-resistant device application. Fully describe its security-related protocol. Discuss potential practical attacks on this protocol? Will the power analysis attack be feasible in your protocol?
3. Are identity-based cryptosystems likely to replace PKI? If Identity Based Cryptosystems are deployed will a password still be needed?