1. Blind Chaum Signatures
2. ECash – David Chaum Anonymous Electronic Cash
3. Existential forgery of RSA signatures
4. Show that the second preimage resistance implies one-wayness (pre–image resistance)
5. Show that $\pmod n$ and modular exponent $g^x \pmod n$ are not cryptographic hash functions.