

Cryptography Assignment 6

1. In class (and in the textbook) we discussed six properties that we would like for digital cash security. Give at least five properties one would want for a secure scheme for voting over an insecure network (like the Internet).
2. Show that “existential forgery attack” can be applied to the El Gamal Signature Scheme. That is given Alice’s public key (p, α, β) , Eve can find a message and signature (m, r, s) that passes the validity test, i.e., $\beta^s r^s = \alpha^m \pmod p$.

Does this attack still work if r and s are signatures of $h(m)$ where h is a cryptographic hash function?

3. Let $h(x) = x^2 \pmod n$ be a potential hash function where n is the product of two large primes. Discuss whether h is 1-way (given y hard to find m such that $f(m) = y$) and/or strongly collision free (hard to find m_1 and m_2 such that $h(m_1) = h(m_2)$).
4. Suppose spender Alice wishes to give her coin to another spender Bob. Alice gives Bob the coin (A, B, z, a, b, r) as well as u, s, x_1 and x_2 (but keeps α_1 and α_2 secret). Show that Bob can now spend the coin. But what can go wrong with this scheme? Give several answers.