IV054 Coding, Cryptography and Cryptographic Protocols
2008 – Exercises IX.

1. Consider the Shamir's threshold scheme.
   (a) Prove that $f(x_k) \equiv y_k \pmod{p}$ for $1 \leq k \leq t$.
   (b) Let $n = 5$ and $t = 3$. Reconstruct the secret if $p = 3361$ and participants P_2, P_3 and P_5 have the shares $(2, 596)$, $(3, 1407)$ and $(5, 334)$, respectively.
2. Prove correctness of the following identification protocol:
   (1) Peggy chooses distinct primes p and q, computes $n = pq$ and chooses e such that $\gcd(e, \varphi(n)) = 1$.
   She chooses $x \in \mathbb{Z}_n^*$ and computes $y = x^e \pmod{n}$. Peggy's public key is (n, e, y) and her private key is x.
   (2) Peggy randomly chooses $r \in \mathbb{Z}_n^*$ and sends $a = r^e \pmod{n}$ to Victor.
   (3) Victor randomly chooses $b \in \mathbb{Z}_e$ and sends it to Peggy.
   (4) Peggy computes $c = x^b r \pmod{n}$ and sends it to Victor.
   (5) Victor accepts if and only if $c^e \equiv y^b a \pmod{n}$.
3. Consider Feldman's (k, n)-protocol for secret sharing with verification. Prove that if the dealer is honest, the equality
   $$g^{y_i} = \prod_{j=0}^{k-1} (v_j)^{x_i{}^j} \pmod{p}$$
   is satisfied for each $i \in \{1, \ldots, n\}$.
4. Peggy and Victor share a bit string k. Peggy identifies herself to Victor using the following protocol:
   (1) Victor randomly chooses a bit string r and sends it to Peggy.
   (2) Peggy computes $r \oplus k$ and sends it to Victor.
   (3) Victor accepts if and only if $k = r \oplus c$ where c is the received bit string.

   Is this protocol secure? Explain your reasoning.
5. Suppose Alice is using the Schnorr identification scheme where $q = 617$, $p = 4937$, $t = 9$ and $\alpha = 1624$.
   (a) Verify that α has order q in $\mathbb{Z}_p^*$.
   (b) Let Alice's secret exponent be $a = 55$. Compute v.
   (c) Suppose that $k = 29$. Compute γ.
   (d) Suppose that Bob sends the challenge $r = 105$. Compute Alice's response y.
   (e) Perform Bob's calculations to verify y.

6. Let E be a block cipher which produces blocks of length k using keys of length k. Consider the following hash function. The message m which is to be hashed is divided into a sequence $m_1, m_2, \ldots, m_n$ of blocks, each of length k. For the sake of simplicity, the length of m is supposed to be a multiple of k. The hash h_n of m is computed in the following way:

   - $h_0 = IV$ (initialization vector)
   - $h_i = E_{m_i}(h_{i-1})$

   Let h and m be any hash value and any message, respectively. Propose an attack which extends m with two more blocks in such a way that h is a hash value of the resulting message. The number of decryptions and encryptions of a single block performed by your attack should be $O(2^k)$.