IV054 Coding, Cryptography and Cryptographic Protocols
2011 - Exercises IX.

1. Suppose Alice is using the Schnorr identification scheme with $q = 107$, $p = 7919$, $t = 6$ and $\alpha = 4586$.
   (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 $r = 61$. Compute Alice's response y.
   (e) Perform Bob's calculations to verify y.

2. A father wants to give family business to his 4 sons. The business is succesful because of a secret that is encoded into a natural number n. Sons who know the secret will get the business. The father wants the business to be taken either by his first-born son with at least one other son or by the three later-born sons together. Find a secret sharing scheme that will realize father's wish.

3. Consider an authentication mapping $auth_k$ where $k \in \{0,1\}^n$. Decide whether the following functions are message authentication codes. Justify your answers:
   (a) $e_k(m_1 \,||\, m_2) = auth_k(0 \,||\, m_1) \,||\, auth_k(1 \,||\, m_2)$ where $|m_1| = |m_2| = n - 1$;
   (b) $f_k(m_1 \,||\, m_2) = auth_k(m_1) \,||\, auth_k(auth_k(m_2))$ where $|m_1| = |m_2| = n$;
   (c) $g_k(m_1 \,||\, m_2 \,||\, \cdots \,||\, m_l) = auth_k(m_1) \,||\, auth_k(m_2) \,||\, \cdots \,||\, auth_k(m_l)$ where $|m_i| = n$ for $i \in \{1, 2, \dots, l\}$.

4. Consider the Shamir's threshold scheme. Let $n = 7$ and $k = 3$. Reconstruct the secret if $p = 67$ and participants P_1, P_3 and P_6 have their shares $(1, 28)$, $(3, 31)$ and $(7, 17)$, respectively.

5. Consider the following user identification protocol. A trusted third party Trent randomly chooses large primes p, q, computes $n = pq$ and randomly chooses a large e such that $gcd(e, \varphi(n)) = 1$. The numbers n, e are public.
   Each user U randomly chooses his or her private key $x_U \in \mathbb{Z}_n$ and computes his or her public key $X_U = x_U^e \pmod{n}$.
   If Alice decides to prove her identity to Bob, she initiates the following protocol:
   (i) Alice randomly chooses $r \in \mathbb{Z}_n$, computes $R = r^e \pmod{n}$ and sends R to Bob.
   (ii) Bob randomly chooses $f \in \{0, 1, \dots, e-1\}$ and sends it to Alice.
   (iii) Alice computes $y = r x_A^f \pmod{n}$ and sends it to Bob.
   (iv) Bob computes $Y = y^e \pmod{n}$ and accepts iff ....

   (a) Find the acceptance condition.
   (b) Show that if both Alice and Bob are honest, Bob always accepts.
   (c) Show that if bad Eve learns somehow the value of f before the beginning of the protocol, this enables her to impersonate Alice.

6. Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet, which can be opened only if six or more of them are present. An arbitrary number of locks could be used, where a single key can open just a single lock and a single lock could be opened by multiple keys. Cabinet is opened if for each lock there is a key to open it.
   (a) What is the smallest number of locks needed?
   (b) What is the smallest number of keys a scientist has to carry?