IV054 Coding, Cryptography and Cryptographic Protocols
2013 - Exercises IX.

1. Consider Shamir's $(10, 3)$-secret sharing scheme over $\mathbb{Z}_p$ where p is a large prime. Suppose an adversary corrupts one of the share holders and this share holder intends to give a bad share in the secret cumulation phase. The problem is that nobody knows which share holder is corrupted.

   (a) Describe a method to reconstruct s given all 10 shares and explain why it works.

   (b) Determine the smallest number x of shares that are sufficient to reconstruct s. Explain.

   (c) Is it true that any collection of fewer than x share holders can obtain no information about s? Explain.

2. Suppose Alice is using the Schnorr identification scheme where $q = 179$, $p = 3581$, $t = 7$ and $\alpha = 3443$.

   (a) Verify that α has order q in $\mathbb{Z}_p$.

   (b) Let Alice's secret exponent be $a = 42$. 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.

3. Consider a village consisting of 13 families (3-4 people) with 5 councilors and a mayor. They want to store a secret so that to recover the secret, the following people have to be present:

   - at least one person from each of at least 9 families;
   - at least 3 councilors;
   - the mayor.

   However, they only know Shamir's (n, t)-secret sharing scheme.
   Can they do it somehow without affecting the security of the protocol?
   (*ie.* so that a set of participants that does not qualify for recovering the secret will still get no information about the secret)

4. Consider the Schnorr identification scheme.

   (a) Why is it important that the steps 1, 2 and 4 in the scheme, as described in the lecture, are in this order? Would it affect security of the protocol if Bob chooses and sends the r first?

   (b) When following the protocol, after receiving γ from Alice, Bob realizes Alice is using the same γ that she previously used when identifying to him. He saved logfiles of that communication. Can he abuse this?

5. Let (m, t) be a message m authenticated by a tag t, computed according to some protocol. Perfectly secure authentication essentially means that the best strategy the adversary has to authenticate any message $m' \neq m$ is to guess it's valid tag t' uniformly at random, even after observing (m, t).

   Alice and Bob share a random key and they use it to authenticate their two bit messages with single bit tags. The protocol consists of picking one of the functions from the set H according to the secret key. Alice's message is then $(m, h_k(m))$, where h_k is the hash function chosen according to the secret key. Bob, after receiving (possibly modified) message (m', t') computes $h_k(m')$ and verifies if $t' = h_k(m')$.

More on next page >>>

(a) Consider H given by the following table. Is the protocol secure? Explain your reasoning.

$m \mapsto$	00	01	10	11
h_1	1	1	0	0
h_2	0	0	1	1
h_3	1	0	0	1
h_4	0	1	1	0

(b) Can you find a set H that provides a secure authentication?

6. Let f be a one-way permutation. Consider the following signature scheme for messages from $N = \{1, \ldots, n\}$:

- To generate keys, choose random $x \in \{0,1\}^n$ and set $y = f^n(x)$ (that is, f applied n times). The public key is y and the private key is x.
- To sign message $i \in \{1, \ldots, n\}$, output $f^{n-i}(x)$ (where $f^0(x) = x$ by definition).
- To verify signature σ on message i with respect to public key y, check whether $y = f^i(\sigma)$.

(a) Show that the above is not a secure (even one-time) signature scheme. Given a signature on a message i, for what messages $F_i \subseteq N$ can an adversary output a forgery?

(b) Prove that no polynomial time adversary, given a signature on i, can output a forgery on any message in $N \setminus F_i$ except with negligible probability.

(c) Suggest how to modify the scheme so as to obtain a secure one-time signature scheme.