Cryptology 1 – five supplemental exercises

1. Construct a preimage resistant (*one-way*) function $f : \{0,1\}^n \to \{0,1\}^n$ such that function $f \circ f$ is not preimage resistant. So for a random $y \in f(\{0,1\}^n)$ it is hard to find x such that $f(x) = y$, but for a random $y \in f(f(\{0,1\}^n))$ it is easy to find x such that $f(f(x)) = y$.
   Hint: When constructing the function f use $h : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$, that is preimage resistant and split the input of f into two halves.

2. Let's assume the EdDSA scheme (simplified variant presented in the lecture)

   a) We use H that returns $H(R, A, m)$ as a single constant value in 50% of cases. Describe how to forge signature in this scenario (for a chosen message).
   b) A collision in H happened while signing two messages, i.e. $H(h[b \dots 2b-1], m) = H(h[b \dots 2b-1], m')$. Describe the implication for the scheme.

3. Propose (i.e. describe a construction) a perfect secret sharing scheme for the following access structure:

   $$\mathcal{A} = \{B \mid \{P_1, P_2, P_5\} \subseteq B \ \vee \ \{P_2, P_3, P_4\} \subseteq B \ \vee \ \{P_3, P_5\} \subseteq B\}$$

   Justify why your construction has this access structure and why it is perfect. You can use the fact that Shamir secret sharing scheme is perfect.

4. (Fast verification of RSA signatures) Let $\langle m_i, s_i \rangle_{i=1}^k$ be a sequence of pairs: message and the corresponding RSA signature. We perform a fast verification of all signature at once in the following way:

   $$\left(\prod_{i=1}^{k} s_i^i \right)^e \equiv \prod_{i=1}^{k} H(m_i)^i \pmod{n}.$$

   Show:

   1. If all signatures are correct, then the verification is successful.
   2. An attacker can construct pairs (with incorrect signatures) $\langle m_i, s_i \rangle_{i=1}^k$, such that the verification equation is satisfied.

5. (Protocol) The goals of the following protocol are distribution of the session key K, and after its use the mutual authentication of participants A and B. Protocol uses a trusted third party (server) S.

   1. $A \to B$: A, N_A
   2. $B \to S$: $A, B, \{N_A, N_B\}_{K_B}$
   3. $S \to A$: $\{B, K, N_A\}_{K_A}$
   4. $S \to B$: $\{A, K, N_B\}_{K_B}$

   Descibe at least two (distinct) attacks that abuse improper implementation of different parts/components of the protocol.