Esecurity: secure internet & e-cash, summer 2015
MICHAEL NÜSKEN

10. Exercise sheet
Hand in solutions until Tuesday, 30 June 2015, 09:00

Exercise 10.1 (Compositions of hash functions). (7 points)
Consider to efficiently evaluable functions \( g : \{0, 1\}^n \to \{0, 1\}^m \) and \( f : \{0, 1\}^m \to \{0, 1\}^\ell \) with \( n > m > \ell \) and their composition \( f \circ g : \{0, 1\}^n \to \{0, 1\}^\ell \). Prove the following:

(i) If \( f \circ g \) is one-way then \( f \) is one-way or \( g \) is one-way. \( \Box \)

(ii) If \( f \) is one-way then \( f \circ g \) is one-way. \( \Box \)

(iii) If \( f \circ g \) is collision resistant then \( g \) is collision resistant. \( \Box \)

(iv) If \( f \circ g \) is collision resistant then \( f \) is collision resistant or \( g \) is one-way. \( \Box \)

(v) If \( f \) and \( g \) are both collision resistant then \( f \circ g \) is collision resistant. \( \Box \)

Exercise 10.2 (Breaking the Chaum-Fiat-Naor protocol?). (5+8 points)
From a hash function \( h : \{0, 1\}^\ell \to \mathbb{Z}_N \) we build a new hash function \( h^* : \{0, 1\}^{\ell k} \to \mathbb{Z}_N \) by sending a message \( m = m_1 \parallel \ldots \parallel m_k \in \{0, 1\}^{\ell k} \) with \( m_i \in \{0, 1\}^\ell \) to \( h^*(m) = \prod_{1 \leq i \leq k} h(m_i) \). Assume \( h \) is collision resistant.

(i) Show that \( h^* \) is not collision resistant. \( \Box \)

(ii) Let \( k = 2 \) and assume that for uniformly chosen \( m \) the hash values \( h(m) \) are uniformly distributed. We consider pairs \( (m_1 \parallel m_2, m_2 \parallel m_1) \) as trivial collisions. Describe an algorithm that computes a non-trivial collision of \( h^* \). Is it faster than the birthday-attack? Compute its expected runtime.

\textit{Hint:} Consider the zero divisors in \( \mathbb{Z}_N \). Maybe start with \( N \) being prime. \( \Box \)

(iii) Generalize your algorithm from (ii) to arbitrary \( k \) and compute the expected runtime. \( \Box \)

(iv) How can Alice use an algorithm from (iii) to cheat in the Chaum-Fiat-Naor protocol? \( \Box \)
Exercise 10.3 (Are blind signature schemes EUF-KMA insecure?).
(0+5 points)

Consider an signature scheme $S$. Denote by $\text{sign}_{sk}(m)$ a valid signature of $m$ under $S$. Assume one can build a blind signature scheme from $S$ such that there is a blinding function $b_r$ and an unblinding function $u_r$ depending on a blinding key $r$ such that $u_r(\text{sign}_{sk}(b_r(m))) = \text{sign}_{sk}(m)$ and it is hard or impossible to recover $m$ from $b_r(m)$ without the knowledge of $r$.

(i) Prove that if $b_r$ is not one-way, ie. for given $\tilde{m}$ it is easy to compute $m$ such that $\tilde{m} = b_r(m)$, then $S$ is not EUF-KMA secure, ie. existentially forgeable under know message attacks.

(ii) Build a blind signature scheme from RSA-FDH.

(iii) Is your scheme EUF-KSA secure? Why is this no contradiction to (i).