5. Exercise sheet
Hand in solutions until Friday, 2 December 2016, 12:00 (noon)

Exercise 5.1 (AES amputated). (9 points)

As we have already seen during the lectures, AES is an extremely simple cipher, its description is rather short. But still, can we make it even simpler, by hacking out superfluous bits without impacting on its strength?

Considering the four steps (SubBytes, ShiftRows, MixColumns and AddRoundKey) performed in each round, we want to see whether those steps are essential or not to the security of the cipher.

(i) For instance, what would happen to AES should one remove the SubBytes step in each round? 2

(ii) What if one were to remove the ShiftRows step? 2

(iii) What about the MixColumns step? 2

(iv) And the AddRoundKey step? 2

(v) Conclude. 1

Exercise 5.2 (Another cipher). (9 points)

Let $G$ be a pseudorandom generator. Define $F_k(m) := G(s_0 \ldots s_{\kappa - 1}) \oplus m$ for $k, m \in \{0, 1\}^\kappa$. Here, $s_0 \ldots s_{\kappa - 1}$ means the string consisting of the bits $0 \ldots \kappa - 1$ of the bitstring $s$. We ask whether we can use $F_k$ as the encryption of some private-key encryption scheme $\Pi$. Assume that $\Pi$‘s key generator just picks a bit string in $\{0, 1\}^\kappa$ uniformly at random.

(i) Can $\Pi$ be OW-POA secure? (Attacker’s task: Find $m$ from $F_k(m)$.) Further means: None.) 3

(ii) Can $\Pi$ be OW-CPA secure? (Attacker’s task: Find $m$ from $F_k(m)$.) Further means: Calls to $F_k$.) 3

(iii) Can $\Pi$ be indistinguishable? (Attacker’s task: Find $h$ from $F_k(m_h)$ with attacker chosen $m_0, m_1$ where $h \in_{\text{rp}} \{0, 1\}$. Further means: None.) 3

Of course, you have to prove your answers.