Cryptography, winter 2015/16

MICHAEL NÜSKEN, SIMON SCHNEIDER

6. Exercise sheet
Hand in solutions until Saturday, 12 December 2015, 12:00

Exercise 6.1 (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 6.2 (Another cipher). (9 points)

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

(i) Can Π be OW-POA secure? (Attacker's task: Find m from $F_k(m)$. Further means: None.) [3]

(ii) Can Π be OW-CPA secure? (Attacker's task: Find m from $F_k(m)$. Further means: Calls to F_k.) [3]

(iii) Can Π be indistinguishable? (Attacker's task: Find h from $F_k(m_h)$ with attacker chosen m_0, m_1 where $h \in_R \{0,1\}$. Further means: None.) [3]

Of course, you have to prove your answers.