3. Exercise sheet
Hand in solutions until Friday, 19 May 2017, 11:59

Exercise 3.1 (RSA key exchange). (8+2 points)
Consider the RSA key exchange:

\[
\begin{align*}
\text{Alice} & \quad \text{Hello} \quad \rightarrow \quad (K, k) \leftarrow \text{RSAKeyGen}(1^n) \\
K & \leftarrow \{0,1\}^{2^n} \\
& \quad \text{pad}(s) \\
c & \leftarrow \text{RSAEnc}_K(s) \\
\rightarrow & \quad c \\
\to & \quad s \leftarrow \text{unpad}(\text{RSADec}_k(c))
\end{align*}
\]

(i) It is used in TLS. Under which name?

(ii) What is known about its security? Find related security proofs, cite the papers and briefly explain their results and assumptions.

In particular: Is it passively ROR-POA secure? Is it more?

(iii) In which respect is it worse than the Diffie-Hellman key exchange?

Exercise 3.2 (Hybrid crypto). (14+2 points)
Consider the situation in the exercises 1.2 and 1.3 from the last sheet. Eve has eavesdropped the conversation between Alice and Bob. She has recorded the RSA-cypher text \(c = \text{enc}_{N,e}(k)\) of the AES key \(k\). She tries the following attack to recover \(k\) from \(c\). We consider an attack as successful if it takes less than \(2^{100}\) bit operations.

(i) How could Eve recover \(k\) if she tries all possible values? Is this a successful attack?

(ii) Eve computes \(ex^{-e} \mod N\) and \(y^e\) for all \(1 \leq x, y \leq 2^{64}\) and stores these values in two lists. How can Eve recover \(k\) from these lists? Is this a successful attack?

(iii) The attack in (ii) may fail in some situations. In which does it fail? What is the probability of failing?

(iv) Eve finds that \(e = 3\). Can she successfully recover \(k\) even if the attack in (ii) fails?

(v) How can one fix the vulnerability in the way RSA and AES is employed by Alice and Bob?