12 Security II (FMS)

The RSA cryptosystem can be tuned to make the workload asymmetric: with $d = 3$, encryption (cubing modulo n) becomes very cheap and almost all the computational expense shifts to decryption (extracting cubic roots modulo n).

The following public-key protocol uses the above property to allow two principals A and B to establish a common secret key N_b (invented by B) without incurring a high computational load, thanks to the help of a server S who computes all the cubic roots in the protocol. Attackers are assumed to be able to overhear, but not alter, the messages between A, B and S.

$$\begin{aligned} A \to S: &\quad B, N_a^3 \bmod n. \\ S \to B: &\quad A. \\ B \to S: &\quad A, N_b^3 \bmod n. \\ S \to A: &\quad B, N_a \oplus N_b. \end{aligned}$$

(a) What is the purpose of N_a? [3 marks]

(b) Describe in detail a protocol attack that will allow two colluding attackers C and D to recover N_b. Assume that S is stateless. [7 marks]

(c) Stop the attack you described in (b) by making S stateful. [3 marks]

(d) Describe in detail a more sophisticated protocol attack whereby the colluding attackers will recover N_b even if S adopts the precaution you described in (c). [4 marks]

(e) Fix the protocol to defeat the attack you described in (d). [3 marks]