Homework Assignment # 10

Due Date: Wednesday, November 29

0. Reading assignment: The article "Internet Security: Firewalls and Beyond" by Rolf Oppliger, Communications of the ACM, May 1997.

   Please note that all reading assignments are relevant for the final exam.

1. Given is an RSA signature scheme with the public key $(n = 9797, b = 131)$. Which of the following signatures are valid?

   (a) $(x = 123, \text{sig}(x) = 6292)$

   (b) $(x = 4333, \text{sig}(x) = 4768)$

   (c) $(x = 4333, \text{sig}(x) = 1424)$

2. One important aspect of digital signatures is the computational effort required to (i) sign a message, and (ii) to verify a signature. We will study the computational complexity of the RSA algorithm used as a digital signature in this problem.

   (a) How many multiplications do we need on average to perform (i) signing of a message with a general exponent and (ii) verification of a signature with the short exponent $b = 2^{16} + 1$? Assume that n as $l = \lceil \log_2 p \rceil$ bits. Assume the square-and-multiply algorithm is used for both, signing and verification. Derive general expressions with l as a variable.

   (b) What takes longer, signing or verification?

   (c) We will now derive estimations for the speed of actual software implementations. Use the following timing model for multiplication:

   The computer operates with 32 bit data structures. Hence, each full-length variable, that means in particular n and x, is represented by an array with $m = \lceil l/32 \rceil$ elements (with x being the basis of the exponentiation operation). We assume that one multiplication or squaring of two of these variables modulo n takes m^2 time units (a time unit is the clock period times some constant larger than one which depends on the implementation). Note that you never multiply with the exponents a and b. That means, the bit length of the exponent does not influence the time it takes to perform an individual modular squaring or multiplication.

   How long does it take to compute a signature/verify a signature if the time unit on a certain computer is 100 nsec, and p has 512 bits? How long does it take if p has 1024 bits?

(d) One important application for digital signatures are smart cards. Philips and Siemens have a smart card with a 8051 microprocessor kernel. The 8051 is an 8 bit processor. Which time unit is required in order to perform one signature generation in 0.5 sec if p has (i) 512 bits and (ii) 1024 bits? Since these processors can not be clocked at more than, say, 10 Mhz, is the required time unit realistic.

3. We consider three different hash functions which produce outputs of lengths 64, 128, and 160 bits. After how many random inputs do we have a probability of $\epsilon = 0.5$ for a collision? After how many random inputs do we have a probability of $\epsilon = 0.1$ for a collision?

4. Describe how exactly you would perform a search to find a pair x_1, x_2, such that $h(x_1) = h(x_2)$ for a given hash function h. What are the memory requirements for this type of search if the hash function has an output length of n bits?